Lezione prof. Sbarra sui Gruppi Risolubili

2 febbraio 2011

1 Serie normali, Serie di composizione

Ricordiamo la definizione di gruppo semplice:

Definizione 1. (Gruppo Semplice) Un gruppo G si dice semplice se $N \lhd G \implies N = \{ e \} \vee N = G$.

Definizione 2. (Serie Normale) Sia G un gruppo. Una serie normale di G e' una sequenza di sottogruppi $G_0, G_1, \ldots, G_n$ di G tali che

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{ e \} \qquad G_i \supsetneq G_{i+1}$$

I gruppi quoziente $G_i/G_(i+1)$ vengono detti fattori della serie.

Definizione 3. (Serie di composizione) Sia G un gruppo. Una serie di composizione di G e' una serie normale che non puo' essere allungata. Cioe' e' una sequenza normale

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{ e \}$$

tale che per ogni i, se $G_i \rhd H \rhd G_{i+1}$, allora $H = G_i$ o $H = G_{i+1}$.

Ricordiamo il teorema di corrispondenza:

Teorema 1. *(Teorema di Corrispondenza) Sia G un gruppo e sia $N \rhd G$. Allora, consideriamo la proiezione standard $\pi : G \to G/N$ data da $\pi(g) = gN$. Vale che:*

1. $\pi^{-1} : \{ H < G/N \} \to \{ K < G \mid K \supseteq N \}$ *e' biunivoca.*
2. $H_1 \subseteq H_2 \implies \pi^{-1}(H_1) \subseteq \pi^{-1}(H_2)$.
3. $H \rhd G/N \implies \pi^{-1}(H) \rhd G$.
4. $[G/N : H] = [G : \pi^{-1}(H)]$.

Osservazione 1. Una serie normale di un gruppo G e' di composizione se e solo se i fattori della serie sono semplici.

Osservazione 2. Se G ha ordine finito, ogni serie normale puo'essere estesa ad una serie di composizione.

Osservazione 3. Se G e' un gruppo di ordine finito, allora G ammette una serie di composizione.

Esempio 1. Proviamo a vedere le serie di composizione di $G = \mathbb{Z}_2 \times S_3$.

1. Una serie di composizione di G e' $G \rhd \{ [0]_2 \} \times S_3 \rhd \{ [0]_2 \} \times A_3 \rhd \{ [0]_2 \} \times \{ id_{S_3} \}$ e i fattori di questa serie sono,nell'ordine e a meno di isomorfismo, $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

2. Un'altra serie di composizione per G e' $G \rhd \mathbb{Z}_2 \times A_5 \rhd \{ [0]_2 \} \times A_3 \rhd set[0]_2 \times \{ id_{S_3} \}$ e i fattori di questa serie sono, nell'órdine e a meno di isomorfismo, $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

Vediamo quindi che G ammette due serie di composizione differenti, ma vediamo anche che entrambe hanno la stessa lunghezza e hanno gli stessi fattori, a meno di isomorfismo. Questo risultato e'generalizzato dal seguente teorema, che enunciamo senza dimostrare:

Teorema 2. *(Teorema di Jordan-Holder) Due serie di composizione di uno stesso gruppo G hanno lo stesso numero di elementi ed i fattori sono a due a due isomorfi.*

2 Gruppi Risolubili

Definizione 4. (Gruppo Risolubile) Un gruppo G si dice risolubile se ammette una serie normale con fattori abeliani.

Osservazione 4. G gruppo abeliano e'semplice $\iff$ G e' gruppo ciclico di ordine primo.

Dimostrazione. ($\Longrightarrow$) Supponiamo G semplice. Allora, se $G = \{ e \}$, abbiamo finito, altrimenti, sia $a \in G,\ a \neq e$: poiche' G e'abeliano, ogni sottogruppo di G e'anche normale, e in particolare, $\langle a \rangle \lhd G$; ma G e'semplice e $\langle a \rangle \neq \{ e \}$, quindi $\langle a \rangle = G$. Percio' G e'ciclico; ora, supponiamo che $m | o(a)$, allora $o(a^m) = \frac{o(a)}{m}$ e quindi $| \langle a^m \rangle | = \frac{o(a)}{m}$, ma allora, per lo stesso ragionamento precedente, dev'essere $\langle a^m \rangle = G$, e quindi $m = 1$, oppure $\langle a^m \rangle = \{ e \}$ e allora $m = p$. Quindi $o(a)$ e'primo, e abbiamo finito.
($\Longleftarrow$) Si vede facilmente. □

Lemma 1. *Sia G un gruppo finito. Allora le seguenti proposizioni sono equivalenti:*

1. *G e' risolubile.*

2. *G ammette una serie di composizione con fattori ciclici di ordine primo.*

3. *Ogni serie di composizione di G ha fattori ciclici di ordine primo.*

Dimostrazione. (1) $\Longrightarrow$ (2): se G e'risolubile, allora ammette una serie normale con fattori abeliani, sia essa

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{ e \}$$

Allora questa serie puo' essere estesa ad una serie di composizione: mostriamo che quest' estensione mantiene l'abelianita' dei fattori: in generale, sia H un gruppo e sia $N \lhd H$ tale che H/N e' abeliano, e supponiamo che esista K tale che $N \lhd K \lhd H$, allora,$K/N \subseteq H/N$ e quindi K/N e'abeliano. Dobbiamo dimostrare che H/K e'abeliano: cioe'che $\forall\, x, y \in H \;\; xKyK = yKxK$; ma

$$xKyK = yKxK \iff xyK = yxK \iff (yx)^{-1}xyK = K \iff (yx)^{-1}xy \in K$$

. Tuttavia, H/N e'abeliano per ipotesi, e questo significa che $\forall\, x, y \in H \;\; (yx)^{-1}xy \in N$, e allora, dato che $N \subseteq K$,$(yx)^{-1}xy \in K$ e abbiamo finito. Quindi G ammette una serie di composizione con fattori abeliani, e per l'Osservazione 1, questi fattori devono essere anche semplici. Allora concludiamo per l'Osservazione 4.
(2) $\implies$ (1): questo segue facilmente dalle Osservazioni 1 e 4.
(2) $\iff$ (3): questo segue dal Teorema di Jordan-Holder. □

Esempio 2. Ogni gruppo abeliano finito é risolubile.
Infatti ogni gruppo finito ammette una serie di composizione e, se e'abeliano, tutti i fattori della serie sono abeliani.

Esempio 3. Ogni p-gruppo e'abeliano.
Infatti, se G e'un gruppo tale che $|G| = p^m$, per Sylow esiste un sottogruppo G_1 di G tale che $|G_1| = p^{m-1}$, ma allora questo sottogruppo e'normale, perche'$[G : G_1] = p$, che e'il piu'piccolo primo che divide $|G|$, ed inoltre $|G/G_1| = p$, quindi G/G_1 e'ciclico di ordine primo. In questo modo, si conclude facilmente per induzione su m.

3 Un criterio di risolubilita'

Vogliamo trovare un criterio per decidere se un gruppo e' risolubile. Iniziamo con una definizione:

Definizione 5. (Commutatore) Sia G un gruppo e siano $x, y \in G$. Allora definiamo commutatore di x e y l'elemento $[x, y] := xyx^{-1}y^{-1}$.

Lemma 2. *(Proprieta' del commutatore) Siano G un gruppo e $x, y, g \in G$. Allora:*

1. $[x, y]^{-1} = [y, x]$.
2. $g[x, y] = [gxg^{-1}, gyg^{-1}]g$

Dimostrazione. Si tratta di una facile verifica:

1. $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$.
2. $[gxg^{-1}, gyg^{-1}]g = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1}g = gxyx^{-1}y^{-1} = g[x, y]$.

□

Definizione 6. (Derivato) Sia G un gruppo, allora definiamo il derivato di G come il sottogruppo $G' := \langle [x, y] | x, y \in G \rangle$.

Lemma 3. *(Proprieta' del derivato) Sia G un gruppo e sia G' il suo derivato. Allora valgono le seguenti proprietá:*

1. *Ogni elemento di G' é prodotto di un numero finito di commutatori.*
2. *G é abeliano se e solo se $G' = \{ e \}$.*

3. G' é caratteristico in G, e quindi anche normale.

4. G/G' e'abeliano.

5. $N \lhd G$ e G/N abeliano $\implies N \supseteq G'$.

6. $H < G$ e $H \supseteq G' \implies H \lhd G$.

Dimostrazione. Tutte le proprietá si dimostrano facilmente:

1. Dalla definizione, ogni elemento di G' é prodotto di un numero finito di commutatori e di inversi di commutatori. Ma, dalle proprietá del commutatore, sappiamo che l'inverso di un commutatore é ancora un commmutatore.

2. Se G é abeliano, allora per ogni $x, y \in G$ vale che $[x, y] = xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = ee = e$, e quindi $G' = \{ e \}$. Se invece $G' = \{ e \}$, allora per ogni $x, y \in G$ vale che $[x, y] = xyx^{-1}y^{-1} = e$ e quindi $xy = yx$, cioé G é abeliano.

3. Sia $\phi \in \mathrm{Aut}(G)$, allora, $\forall x, y \in G$, vale che $\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x^{-1})\phi(y^{-1}) = \phi(x)\phi(y)(\phi(x))^{-1}(\phi(y))^{-1} = [\phi(x), \phi(y)]$. Allora, poiché l' immagine secondo $]phi$ di un commutatore é ancora un commutatore, e poiché il derivato é generato dai commutatori, il derivato é invariante rispetto a ϕ.

4. G/G' é abeliano se e solo se $\forall x, y \in G \;\; G'xG'y = G'yG'x$(consideriamo gli altri laterali perche'tanto G' é normale), ma, come prima, vediamo che

   $$G'xG'y = G'yG'x \iff G'xy = G'yx \iff xy(yx)^{-1}G' = G' \iff xyx^{-1}y^{-1} \in G'.$$

   E questo é sicuramente vero.

5. Come sopra, vediamo che, se $N \lhd G$, G/N é abeliano se e solo se $\forall x, y \in G$ $[x, y] \in G$ il che é equivalente a dire che $N \supseteq G'$.

6. Siano $g \in G$ e $h \in H$, allora $ghg^{-1}h^{-1} = [g, h] \implies gh = [g, h]hg$, quindi $ghg^{-1} = [g, h]hgg^{-1} = [g, h]h \in H$.

□

Definizione 7. (Derivati successivi) Sia G un gruppo. Allora definiamo i derivati successivi di G cosí: $G^{(0)} = G$ e $G^{(i)} = (G^{(i-1)})'$ per ogni i intero positivo.

Teorema 3. *(Criterio di risolubilitá) Sia G un gruppo. Allora G é risolubile se e solo se $G^{(i)} = e$ per un certo $i \geq 0$.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che G sia risolubile e sia $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{ e \}$ una serie normale di G con fattori abeliani. Allora, dalle proprietá del derivato, vediamo che $G_1 \supseteq G' = G^{(1)}$ e che $G_2 \supseteq (G_1)'$, ma $(G_1)' \supseteq (G^{(1)})' = G^{(2)}$ e quindi $G_2 \supseteq G^{(2)}$. Procedendo cosí, si puó dimostrare che $G_i \supseteq G^{(i)}$ per $i = 0, 1, 2, \ldots, n$. Ma allora $G^{(n)} = \{ e \}$.
($\Longrightarrow$) Sia n il piú piccolo intero non negativo tale che $G^{(n)} = \{ e \}$. Allora $G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(n)} = \{ e \}$ é una serie normale con fattori abeliani, come si vede dalle proprietá del derivato. □

4 Esempi ed applicazioni

Esempio 4. Ogni gruppo abeliano é risolubile.
Infatti in un gruppo abeliano G, $G' = \{ e \}$.

Lemma 4. *1. Siano G un gruppo e $H < G$. Allora se G é risolubile anche H é risolubile.*

2. Siano G un gruppo e $H \lhd G$. Allora se G é risolubile anche G/H é risolubile.

3. Siano G un gruppo e $H \lhd G$. Allora se H e G/H sono risolubili, anche G é risolubile.

Dimostrazione. Esercizio. □

Esempio 5. Ogni gruppo G di ordine p^2q, con p, q primi distinti, é risolubile.
Infatti abbiamo visto in un esercizio precedente che, se $q < p$, allora un p-Sylow P é normale ed abeliano, e quindi si vede che, preso un $q-$Sylow Q, la serie normale $G \rhd P \rhd \{ e \}$ ha i fattori abeliani. Invece, se $q > p$, abbiamo due possibilitá: o il $p-$Sylow é unico, e allora possamoo ricondurci al caso precedente, o il $q - Sylow$ é unico, e allora la serie normale $G \rhd Q \rhd \{ e \}$ ha tutti i fattori abeliani.

Esempio 6. Ogni gruppo G di ordine $p^n q^m$ é risolubile.
Dimostrare per esercizio, ma solo nel caso in cui $p^n < q$.

Proposizione 1. *Se $1 \leq n \leq 4$ allora S_n e A_n sono risolubili. Invece se $n \geq 5$, S_n e A_n non sono risolubili.*

Dimostrazione. Per la prima parte, grazie al Lemma 4, basta dimostrare che S_n é risolubile: se $n = 1, 2$ non c'é problema. Se $n = 3$, $S_n \rhd A_n \rhd \{ id \}$ é una serie normale con fattori abeliani. Se $n = 4$, vediamo che A_4 é risolubile perché ha ordine 12 e quindi possiamo costruire una serie normale con fattori abeliani $S_4 \rhd A_4 \rhd \ldots$ (la serie che risolve A_4) $\cdots \rhd \{ e \}$. Invece, per la seconda parte, sempre grazie al Lemma 4,basta dimostrare che A_5 é irriducibile: ma sappiamo giá che A_5 é semplice, e quindi é anche irriducibile. Se non volessimo utilizzare il fatto che A_5 é semplice, potremmo ragionare cosí: sappiamo che A_5 é generato dai 3-cicli, allora, se facciamo vedere che ogni tre ciclo é un commutatore, ne seguirá che $A_5' = A_5$ e quindi che A_5 é irriducibile per il criterio di risucibilitá: allora, sia (ijk) un 3-ciclo e siano v, w gli ealtri due elementi in $\{ 1, 2, 3, 4, 5 \}$ diversi da i, j, k, vediamo che $(ijk) = (jvi)(kwi)(jvi)^{-1}(kwi)^{-1}$. □

Esercizio 1. Mostrare che, per ogni $n \geq 5$, $S_n' = A_n$.

Dimostrazione. $A_n \lhd S_n$ e S_n/A_n é abeliano, quindi $A_n \supseteq S_n'$. Ma, come prima, sappiamo che A_n é generato dai 3-cicli, ed ogni 3-ciclo é un commutatore, quindi $A_n \subseteq S_n'$ e abbiamo finito. □

Esercizio 2. Sia $H < S_n$ tale che $[S_n : H] = 2$. Mostrare che $H = A_n$.

Dimostrazione. Esercizio. □