[Altro criterio per decidere risolubilità]

Def. G gruppo, $x, y \in G$

l'elemento $x^{-1}y^{-1}xy$ si indica con $[x,y]$ e si chiama il **commutatore** di x e y

Osservazione $[x,y] = 1_G \iff xy = yx$ [x, y commutano]

Def G gruppo, definiamo $G' \overset{\text{def}}{=} \langle [x,y] \mid x,y \in G \rangle$

il **derivato** di G [$G' \leq G$]

Osservazione $f \in \mathrm{Aut}(G) \Rightarrow f(G') = G'$

Dim: $G' = \{ \underbrace{[x_1,y_1][x_2,y_2]\cdots[x_m,y_m]}_{\text{prodotto finito di commutatori}} \mid x_i, y_i \in G \}$

Osserviamo che:

$$f(G') = \{ [f(x_1)f(y_1)] \cdots [f(x_m)f(y_m)] \mid x_i, y_i \in G \}$$

$$\Rightarrow f(G') \leq G' \quad (*)$$

Analogamente otteniamo $f^{-1}(G') \leq G'$

da cui $G' \leq f(G') \quad (**)$

Concludiamo $(*) + (**) \Rightarrow f(G') = G'$

Def. Sia $H \leq G$ tale che $f(H) = H$ per ogni $f \in Aut(G)$, allora H si dice caratteristico in G

[G' è caratteristico in G]

Oss. : $H \leq G$, H caratteristico in $G \Rightarrow H \trianglelefteq G$]

[da cui $G' \trianglelefteq G$]

Proposizione 1) G/G' è abeliano

2) se $H \trianglelefteq G$ t.c G/H è abeliano allora $G' \subseteq H$

Problema: dimostrare la proposizione

[G' è il più piccolo sottogruppo normale che dà un quoziente abeliano]

Esempi 1) G abeliano $\Rightarrow G' = \{1_G\}$

2) G semplice non abeliano $\Rightarrow G' = G$

[i gruppi per cui $G' = G$ si dicono *perfetti*]

3) Se $G = S_n$ allora $G' = A_n$

Def. definiamo per induzione:

- $G'' \overset{def}{=} (G')'$ derivato secondo di G
- $G^{(k)} \overset{def}{=} \left(G^{(k-1)}\right)'$ derivato k-esimo di G

- la serie di sottogruppi

$$G \rhd G' \rhd G'' \rhd \dots \rhd G^{(k)} \rhd G^{(k+1)} \rhd \dots$$

si dice serie dei derivati

Esempi: 1) se G è semplice non abeliano

allora $G^{(k)} = G$ per ogni k

2) Consideriamo S_4

definiamo $H = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

allora

$S_4' = A_4$ $\quad A_4' = S_4'' = H$ $\quad H' = S_4''' = \{Id\}$

$\left[S_4^{(k)} = \{Id\} \text{ per } k \geq 3\right]$

serie derivata: $S_4 \rhd A_4 \rhd H = \{Id\}$

(dettagli per esercizio)

Teorema

G è risolubile $\iff$ $G^{(k)} = \{1_G\}$ per qualche $k \geq 1$

Dim "$\Longleftarrow$"

Se $G^{(k)} = \{1_G\}$ otteniamo

$$G \rhd G' \rhd G'' \rhd \dots \rhd G^{(k-1)} \rhd G^{(k)} = \{1_G\}$$

una serie subnormale con quozienti abeliani

$$\left(\frac{G^{(i)}}{G^{(i+1)}} \text{ è abeliano} \right) \Longrightarrow G \text{ è risolubile}$$

"$\Longrightarrow$"

G risolubile allora esiste una serie subnormale con quozienti abeliani:

$$G = G_1 \rhd \dots \rhd G_s \rhd G_{s+1} = \{1\}$$

Osserviamo che

- $G_{i+1} \supseteq G_i'$ perchè G_i / G_{i+1} abeliano e G_i' è il più piccolo sottogruppo normale che dà un quoziente abeliano
- per induzione otteniamo $G_i \supseteq G^{(i)}$ infatti
  - $G_1 \supseteq G'$
  - se $G_i \supseteq G^{(i)}$ allora $G_{i+1} \supseteq G_i' \supseteq (G^{(i)})' \supseteq G^{(i+1)}$

concludendo $\{1\} = G_{s+1} \supseteq G^{(s+1)} \Longrightarrow G^{(s+1)} = \{1_G\}$

∎

[caso importante delle serie subnormali]

Def - Una serie subnormale $G = G_1 \triangleright G_2 \triangleright \dots \triangleright G_{s+1} = \{1_G\}$ si dice serie di composizione se G_{i+1} è massimale fra i sottogruppi normali propri di G_i per ogni $i = 1, \dots, s$

(i.e. $G_i \leq H \triangleleft G_{i+1} \Rightarrow H = G_i$ o $H = G_{i+1}$)

Osservazione: G_{i+1} massimale fra i sottogruppi normali propri $\iff$ I teorema di isomorfismo $\frac{G_i}{G_{i+1}}$ semplice

Def. se $\{G_i\}$ è una serie di composizione allora $\left\{\frac{G_i}{G_{i+1}}\right\}$ si dicono fattori di composizione

Osservazione: Se G è un gruppo finito allora G ha una serie di composizione

(si prende G_2 sottogruppo normale massimale di G
poi G_3 sottogruppo norm. mass. di G_2 ecc.
Siccome G è finito ad un certo punto compare $\{1_G\}$)

[la parte interessante è l'unicità]

TEOREMA DI JORDAN-HOLDER

Sia G gruppo finito e siano $G = G_1 \rhd G_2 \rhd \dots \rhd G_{s+1} = \{1_G\}$ e $G = H_1 \rhd H_2 \rhd \dots \rhd H_{t+1} = \{1_G\}$ due serie di composizione allora: $s = t$ ed esiste $\varphi \in S_t$ tale che

$$\frac{G_i}{G_{i+1}} \cong \frac{H_{\varphi(i)}}{H_{\varphi(i)+1}} \quad \text{per ogni } i = 1, \dots, s$$

Dimostrazione omessa

[I fattori di composizione differiscono solo per un riordinamento (sono univocamente determinati)]

Teorema: G è risolubile se e solo se i fattori di composizione sono ciclici di ordine primo.

Dim Osserviamo che se S è un gruppo semplice e S è non abeliano (e non risolubile) oppure $S \cong \mathbb{Z}_p$ con p primo

"$\Leftarrow$" i fattori di composizioni sono ciclici di ordine primo (quindi abeliani), allora le serie di composizione hanno quozienti abeliani

"$\Rightarrow$" G risolubile e $G = G_1 \rhd G_2 \rhd \dots \rhd G_{s+1} = \{1_G\}$ serie di composizione

$\Rightarrow G_i$ risolubile $\Rightarrow G_i/G_{i+1}$ semplice e risolubile $\Rightarrow$

$\Rightarrow G_i/G_{i+1}$ è ciclico di ordine primo

∎

Qualche risultato (senza dimostrazione) sui gruppi risolubili e semplici

Teorema Sia G gruppo finito e risolubile e siano m, n tali che $|G| = mn$ con $MCD(m,n) = 1$ Vale che

(i) G ha almeno un sottogruppo di ordine m

(ii) due sottogruppi di ordine m di G sono coniugati

(iii) un sottogruppo di G il cui ordine divide m è contenuto in un sottogruppo di ordine m

(Dimostrazione sul Suzuki, di livello simile al corso)

[una generalizzazione del teorema di Sylow nella classe dei gruppi risolubili]

Teorema (Feit-Thompson, 1963)

Ogni gruppo di ordine dispari è risolubile

(dimostrazione: centinaia di pagine)

conseguenza: ogni gruppo semplice non abeliano ha ordine pari e quindi contiene un elemento di ordine 2

Il teorema di Feit-Thompson assieme al seguente teorema hanno indicato la (lunga) strada verso la classificazione dei gruppi semplici

Teorema (Brauer-Fowler, 1955)
Esistono solo un numero finito di gruppi semplici che hanno un elemento di ordine 2 con il centralizzante di un determinato tipo

[Torniamo alla teoria di Galois, perchè i gruppi risolubili sono così importanti in questa teoria?]

Def $K \supseteq F$ campi

$F = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{k+1} = K$ serie di sottocampi è detta una <u>torre di radici</u> di K su F se per ogni $i = 1, \dots, k$ esiste $d_i \in F_{i+1}$ tale che $F_{i+1} = F_i(\sqrt[m_i]{d_i})$ e $d_i^{m_i} \in F_i$ per qualche m_i intero positivo

[generalizzazione torre di radici quadrate]

Def Sia $q(x) \in F[x]$ polinomio monico non costante. L'equazione $q(x) = 0$ è detta <u>risolubile per radicali</u> se esiste un'estensione di campi K su F con una torre di radici di K su F tale che F contiene il campo di spezzamento di $q(x)$ su F

<u>Osservazione</u>: Se $q(x)$ è risolubile per radicali e a radice di $q(x)$ allora a può essere ottenuto da elementi di F tramite una sequenza finita di operazioni di campo e eseguendo delle radici

Def. Sia $q(x) \in F[x]$ separabile, se E è il campo di spezzamento di $q(x)$ su F definiamo $Gal(E/F)$ il gruppo di Galois di $q(x)$

Oss: Consideriamo $q(x) = \prod_{i=1}^{n} (x - r_i)$ in E

(E campo di spezzamento di $q(x)$)

Gli r_i sono elementi distinti ($q(x)$ separabile)

e $E = F(r_1, \dots, r_n)$

Sappiamo che $\eta \in Gal(E/F)$ agisce su $\{r_1, \dots, r_n\}$

Costruiamo $\varphi : Gal(E/F) \longrightarrow S_n$

$$\eta \longrightarrow \eta|_{\{r_1, \dots, r_n\}}$$

ottenendo φ monomorfismo di gruppi

Definiamo

$$G_q \overset{def}{=} \varphi(G) \leq S_n$$

con

$$G_q \cong Gal(E/F)$$

Anche G_q viene detto gruppo di Galois di q

Il gruppo di Galois di q $Gal(E/F)$ con E campo di spezzamento viene visto come gruppo di automorfismi di E mentre G_q viene interpretato come sottogruppo di permutazioni. Comunque i due gruppi sono isomorfi

Teorema (Criterio di Galois per la risolubilità per radicali)

Sia F un campo di caratteristica 0 e $q(x) \in F[x]$ allora

$q(x)$ è risolubile per radicali $\iff$ G_q è un gruppo risolubile

La dimostrazione di questo teorema molto importante occuperà le prossime due lezioni