LEZIONE 28 - 10 - 2020

CRITERIO PER L'ISOMORFISMO DI DUE PROD. SEMIDIRETTI

Siano N, H gruppi, $\varphi : H \to \mathrm{Aut}(N)$, $f \in \mathrm{Aut}(H)$.

Allora $N \rtimes_\varphi H \simeq N \rtimes_{\varphi \circ f} H$.

DIM Sia $(G_1, \cdot) := N \rtimes_\varphi H$, $(G_2, *) := N \rtimes_{\varphi \circ f} H$.

Considero
$$\Phi : G_1 \longrightarrow G_2$$
$$(n, h) \longmapsto (n, f^{-1}(h))$$

[In G_2 : $(n_1, h_1) * (n_2, h_2) = (n_1 \cdot (\varphi f)(h_1)(n_2), h_1 h_2)$]

↳ voglio cancellare f!

Φ è biig: $\Phi^{-1} = (n, h) \longmapsto (n, f(h))$

Φ è omom:

$$\Phi((n_1, h_1) \cdot (n_2, h_2)) \overset{?}{=} \Phi((n_1, h_1)) * \Phi((n_2, h_2))$$

$$\Phi((n_1, h_1) \cdot (n_2, h_2)) = \Phi(n_1 \cdot \varphi(h_1)(n_2), h_1 h_2) = (n_1 \varphi(h_1)(n_2), f^{-1}(h_1 h_2))$$

$$\Phi((n_1, h_1)) * \Phi((n_2, h_2)) = (n_1, f^{-1}(h_1)) * (n_2, f^{-1}(h_2)) = (n_1 \cdot (\varphi f)(f^{-1}(h_1))(n_1), f^{-1}(h_1 h_2)) = (n_1 \cdot \varphi(h_1)(n_1), f^{-1}(h_1 h_2))$$

APPLICAZIONE: esiste un unico prod. semidiretto $\mathbb{Z}/p\mathbb{Z} \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$ con p, q primi e $q \mid p-1$.

$$\varphi : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}^\times \simeq \mathbb{Z}/{p-1}\mathbb{Z}$$

$\varphi_0 = 1 \longmapsto 0$

$\varphi_\alpha = 1 \longmapsto \alpha$ di ordine q

$\varphi_\beta = 1 \longmapsto \beta$ di ordine q

Vogliamo mostrare che $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_\alpha} \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_\beta} \mathbb{Z}/q\mathbb{Z}$

Siccome α e β hanno ord q, generano entrambi il sottogr. di $\mathbb{Z}/_{p-1}\mathbb{Z}$ con q elementi $\Rightarrow \alpha = k\beta$ con $(k,q)=1$.

Allora basta dire che $\varphi_\beta = \varphi_\alpha \psi$ con $\psi \in Aut(\mathbb{Z}/q\mathbb{Z})$

$\psi = x \mapsto kx$ è una scelta ovvia: $\varphi_\beta = 1 \mapsto \beta$

$\varphi_\alpha \psi = 1 \xmapsto{\psi} k \cdot 1 \xmapsto{\varphi_\alpha} k\alpha = \beta$

GRUPPI SEMPLICI DI ORDINE ≤ 100

- Se $|G| = p$ primo, allora $G \simeq \mathbb{Z}/p\mathbb{Z}$ che è semplice
- Se $|G| = 2d$, d dispari, $d > 1$, allora G ha un sottogr. norm. di ordine d.
- Se $|G| = p^n$, $n \geq 2$, allora G ha sottogr. normali di ogni ordine

IDEA 1: p-Sylow normale

ES: $|G| = 20 = 5 \cdot 2^2$; allora $n_5 \mid 20$ e $n_5 \equiv 1 \ (5)$

$\Rightarrow n_5 \mid 4$ e $n_5 \equiv 1 \ (5)$

$\Rightarrow n_5 = 1$

$\Rightarrow P_5$ è normale!

FATTO $|G| = n$, $p \mid |G|$. Allora esiste un p-Sylow normale se tale p-Sylow è unico.

DIM [$\Leftarrow$] Sia P il p-Sylow unico. Allora $\forall g \in G$: gPg^{-1} è un altro p-Sylow di G, ma P è l'unico $\Rightarrow gPg^{-1} = P$ $\forall g$ $\Rightarrow$ è normale.

[$\Rightarrow$] Il 2° teorema di Sylow dice che i p-Sylow sono tutti coniugati tra loro.
Sia P un p-Sylow normale, P' un altro p-Sylow. Allora $\exists g \in G$ t.c. $gPg^{-1} = P'$, ma $gPg^{-1} = P = P'$, dunque P è unico. $\square$

FATTO PIÙ FORTE p-Sylow è caratteristico se è unico

[$\Leftarrow$] Stesso rag. ma con $\varphi \in Aut(G)$ qualsiasi

[$\Rightarrow$] Se P è caratt. allora è anche normale, dunque segue da sopra. $\square$

Questa idea funziona per tante cardinalità.

IDEA 2: Teorema di Poincaré sui Sylow

Poincaré: se $H < G$ di ind. n, allora $\exists N \triangleleft G$ con $n \mid [G:N] \mid n!$

ES: $n = 96 = 2^5 \cdot 3$. Ci potrebbero essere 3 2-Syl e 4/16 3-Syl.

Sia $P_2 < G$ (indice 3): allora $\exists N \triangleleft G$ con $3 \mid [G:N] \mid 6 \Rightarrow$ non può essere banale!

Questo elimina 48, 36, ecc...

36: P_3 ha indice 4 $\Rightarrow \exists N \triangleleft G$ con $4 \mid [G:N] \mid 24 \Rightarrow$ non può essere banale

Rimangono 60, 56, 72, 80

IDEA 3: Non c'è spazio!

$$|G| = 56 = 7 \cdot 8 \Rightarrow n_2 \mid 7 \text{ e } n_2 \equiv 1 \ (2), \quad n_7 \mid 8 \text{ e } n_7 \equiv 1 \ (7)$$

$$\Downarrow \qquad\qquad\qquad \Downarrow$$

$$n_2 \in \{1, 7\} \qquad\qquad n_7 \in \{1, 8\}$$

Se per assurdo $n_2 = 7$, $n_7 = 8$, consideriamo $P_7 \neq P_7'$. Allora $P_7 \cap P_7' = \{1\}$.

$\Rightarrow$ L'unione di tutti i 7-Sylow ha $\underbrace{1}_{id} + \underbrace{6 \cdot 8}_{\text{el di ord } 7} = 49$ elementi

Dove sono tutti gli el. di ordine 2? Se g ha ord. 2, $g \in P_2$ per qualche P_2 2-Sylow.

Dunque $\underbrace{P_2 \setminus \{e\}}_{7 \text{ elementi}} \subseteq \underbrace{G \setminus \bigcup_{P \in Syl_7(G)} P}_{7 \text{ elementi}} \Rightarrow P_2 = G \setminus \bigcup_{P \in Syl_7(G)} P = \{g \in G : \text{ord } g \neq 7\}$

$\Rightarrow n_2 = 1$.

Stessa cosa per $n = 80 = 5 \cdot 2^4$. $n_2 \mid 5$ e $n_2 \equiv 1 \ (2)$, $n_5 \mid 16$ e $n_5 \equiv 1 \ (5)$

$$\Downarrow \qquad\qquad\qquad \Downarrow$$

$$n_2 \in \{1, 5\} \qquad\qquad n_5 \in \{1, 16\}$$

Ma se $n_5 = 16$ allora ci sono $16 \cdot (5-1) = 64$ el di ordine 5, dunque rimangono $|G| - 65 = 15$ el. di ordine multiplo di 2 $\Rightarrow n_2 = 1$.

IDEA 4: Azione di coniugio sui Sylow

$$|G| = 72 = 3^2 2^3. \quad n_3 \mid 8 \text{ e } n_3 \equiv 1 \ (3), \quad n_2 \mid 9 \text{ e } n_2 \equiv 1 \ (2)$$

$$\Downarrow$$

$$n_3 \in \{1, 4\} \qquad\qquad \Rightarrow n_2 \in \{1, 3, 9\}$$

Per il 2° Teorema di Sylow si ha un'azione transitiva di G su $Syl_3(G)$.

Se $n_3 = 4$, allora $|Syl_3(G)| = 4 \Rightarrow$ l'azione è un omomorfismo

$$\Phi : G \longrightarrow S_4$$

Tale omomorfismo non può essere banale (altrimenti l'az. fisserebbe tutti i 3-Syl, ma a quel punto non sarebbe transitiva) né può essere iniettivo ($|G| = 72 \geq 24 = |S_4|$).

Dunque $\operatorname{Ker}\Phi$ è un sggp. normale non banale di G. $\square$

$|G| = 112 \Rightarrow G$ non è semplice

$|G| = 112 = 2^4 \cdot 7$. Segue che $n_2 \in \{1, 7\}$, $n_7 \mid 16$ e $n_7 \equiv 1\ (7) \Rightarrow n_7 \in \{1, 8\}$.

Se $n_2 = 1$ ho finito $\Rightarrow$ suppongo $n_2 = 7$. Consideriamo allora l'azione di G sui 2-Sylow:

$$\Phi : G \longrightarrow S_7$$

$\operatorname{Ker}\Phi \triangleleft G$. $\operatorname{Ker}\Phi \neq G$ poiché l'azione di G sui 2-Syl è transitiva. $\Rightarrow \Phi(G) \neq \{e\}$

Se $\operatorname{Ker}\Phi = \{e\}$ allora $G \hookrightarrow S_7$: se così fosse potrei considerare $\Phi(G) \cap A_7 \triangleleft \Phi(G)$.

Se $G \simeq \Phi(G)$ fosse semplice, allora $\Phi(G) \cap A_7 = \Phi(G) \Rightarrow \Phi(G) \subseteq A_7$.

Ma $|\Phi(G)| = 2^4 \cdot 7 \nmid 2^3 \cdot 3 \cdot 5 \cdot 7 = |A_7|$.

A_5 è l'unico gruppo semplice di ord. 60

Sia G di ord. $60 = 2^2 \cdot 3 \cdot 5$. $n_2 \in \{1, 3, 5, 15\}$. Quanti 2-Sylow ci sono in A_5?

(*) Se $n_2 = 1$ allora $P_2 \triangleleft G \Rightarrow$ assurdo.

(*) Se $n_2 = 3$ allora $G \xrightarrow{\Phi} S(\mathrm{Syl}_2(G)) \simeq S_3$ è non banale $\Rightarrow \operatorname{Ker}\Phi \triangleleft G$ ma $\operatorname{Ker}\Phi \neq G$ e $\operatorname{Ker}\Phi = \{e\}$

perché altrimenti $G \hookrightarrow S_3$, ma $|G| = 60 > 6 = |S_3|$.

(*) Se $n_2 = 5$ allora $G \simeq A_5$. Infatti in questo caso l'azione di G sui 2-Sylow

$$\Phi : G \longrightarrow S(\mathrm{Syl}_2(G)) \simeq S_5$$

è non banale. Allora $\operatorname{Ker}\Phi \triangleleft G \Rightarrow \operatorname{Ker}\Phi = \{e\}$ ⌜G è semplice⌟

$$\Rightarrow G \longrightarrow S_5$$

⌜1° MODO DI CONCLUDERE⌟ $\Phi(G) \cap A_5 \triangleleft \Phi(G) \Rightarrow \Phi(G) \cap A_5 = \Phi(G)$

$\Rightarrow A_5 \subseteq \Phi(G) \Rightarrow$ per cardinalità sono uguali

Inoltre Φ è l'isomorfismo $G \xrightarrow{\sim} A_5$.

⌜2° MODO DI CONCLUDERE⌟ $\Phi(G)$ è di indice 2 in $S_5 \Rightarrow \Phi(G) \triangleleft S_5$

ma l'unico sggp. normale di S_5 è $A_5 \rightarrow \Phi(G) = A_5$.

(*) Se $n_2 = 15$ vorremmo mostrare che sono troppi elementi.

⌜Sarebbe difficile farlo contando poiché i 2-Syl hanno ord 4 $\Rightarrow$ la loro int. può avere 2 elementi⌟

Per Sylow $n_5 \mid 12$ e $n_5 \equiv 1\ (5) \Rightarrow n_5 \in \{1, 6\}$. Ma $n_5 \neq 1$ poiché G

è semplice, dunque supponiamo $n_5 = 6$.

Se i 2-Sylow si intersecassero tutti banalmente a coppie, in G ci sarebbero almeno

$$1 + n_5(5-1) + n_2(4-1) = 1 + 24 + 45 > 60 \quad \text{TROPPI}$$

id + el di ord 5 + el dei 4-Sylow

Dunque i 2-Sylow si devono intersecare: $\exists P_2, P_2' \in Syl_2(G)$ t.c. $|P_2 \cap P_2'| = 2$.

Sia $H := P_2 \cap P_2'$. Consideriamo $K := N_G(H)$. ← il più grande gruppo in cui H è normale

Ma $H \trianglelefteq P_2$ e $H \trianglelefteq P_2'$ (poiché $[P_2 : H] = [P_2' : H] = 2$)

$$\Rightarrow P_2, P_2' \leq K \Rightarrow 4 \mid |K| \mid 60.$$

Potrebbe essere $|K| = 4$? No! $\underbrace{P_2 \cup P_2'}_{\text{almeno 5 el}} \subseteq K$

Dunque $|K| \in \{12; 20; 60\}$.

- Se $|K| = 60$ allora $K = G \Rightarrow H \trianglelefteq G \Rightarrow$ assurdo
- Se $|K| = 20$ allora $[G:K] = 3$, dunque per Poincaré esisterebbe $N \trianglelefteq G$ con $3 \mid [G:N] \mid 6 \Rightarrow N \trianglelefteq G$ e non banale $\Rightarrow$ assurdo
- Se $|K| = 12$ l'azione $G \curvearrowright G/K$ mi dà ancora un omomorfismo

$$\Phi : G \longrightarrow S(G/K) \simeq S_5$$

non banale $\overset{(\text{caso } n_2 = 5)}{\Rightarrow} G \hookrightarrow S_5 \Rightarrow G \simeq A_5$, ma A_5 ha 5 2-Sylow e non 15, dunque è assurdo.

Classificazione dei gruppi di ord $3 \cdot 5 \cdot 17$

$n_{17} \mid 3 \cdot 5$ e $n_{17} \equiv 1 \ (17) \Rightarrow n_{17} = 1 \Rightarrow$ il 17-Sylow è normale!

Sia $P \trianglelefteq G$, $|P| = 17$. Consideriamo

$$\pi : G \twoheadrightarrow G/P \simeq \mathbb{Z}/_{15}\mathbb{Z}$$

⌜ l'unico gruppo di ord 15 è $\mathbb{Z}/_{15}\mathbb{Z}$ ⌟

In G/P esiste un gP di ordine 15. Ma $\mathrm{ord}(gP) = \mathrm{ord}(\pi g)) \mid \mathrm{ord}(g)$, dunque g ha ordine 15 oppure $15 \cdot 17$. (punto nella preimmagine)

Nel secondo caso evidentemente $G = \langle g \rangle \simeq \mathbb{Z}/_{3\cdot5\cdot17}\mathbb{Z}$.

Nel primo caso sia allora g di ordine 15. Allora $G \simeq P \rtimes_\varphi H$

Infatti: P è normale, $H \cap P = \{e\}$ per card. e $PH = G$.

Ma $\varphi : \underset{\underset{\mathbb{Z}/_{15}\mathbb{Z}}{\shortparallel}}{H} \longrightarrow \underset{\underset{\mathbb{Z}/_{16}\mathbb{Z}}{\shortparallel}}{Aut(P)}$ deve essere banale, poiché

- $|\mathrm{Im}\,\varphi| = \dfrac{|H|}{|\ker \varphi|} \mid |H| = 15$
- $|\mathrm{Im}\,\varphi| \mid |Aut\,P| = 16$

$\Rightarrow |\mathrm{Im}\,\varphi| \mid (15, 16) = 1$

$$\Rightarrow G \simeq P \times H \simeq \mathbb{Z}/_{17}\mathbb{Z} \times \mathbb{Z}/_{15}\mathbb{Z} \simeq \mathbb{Z}/_{3\cdot5\cdot17}\mathbb{Z}.$$

□

ALTRA SOL: $P \trianglelefteq G$. Consideriamo $G \xrightarrow{\Psi} \mathrm{Aut}(P)$, $g \longmapsto \varphi_g|_P$. $\mathrm{Ker}\,\Psi = Z_G(P)$.

Ma $\mathrm{Aut}(P) \simeq \mathbb{Z}/_{16}\mathbb{Z} \implies |\mathrm{Im}\,\Psi| = 1 \implies \mathrm{Ker}\,\Psi = Z_G(P) = G$.

↳ stesso ragionamento di sopra

$\implies P \subseteq Z(G)$.

Consideriamo $G/P \twoheadrightarrow G/_{Z(G)}$: questa è surgettiva per il 1° Teo di Isom:

$$\begin{tikzcd} G \arrow[rr, two heads] \arrow[dr] & & G/_{Z(G)} \\ & G/_P \arrow[ur, "\nu"'] & \end{tikzcd}$$

dove $G/_P$ è ciclico perché di ord 15.

Dunque $G/_{Z(G)}$ è un quoziente di un gruppo ciclico $\left(\text{è} \simeq \frac{G/P}{\mathrm{Ker}\,\nu} \right)$

e quindi è ciclico $\implies G$ è abeliano!

Per il Teorema di Struttura, $G \simeq \mathbb{Z}/_{3\cdot 5\cdot 17}\mathbb{Z}$. $\square$