Lezione 5 - 29/03/19

lunedì 25 marzo 2019 01:14

Def: Siano H, K gruppi e sia $\varphi: K \longrightarrow Aut(H)$ un morfismo di gruppi. Definiamo il PRODOTTO SEMIDIRETTO (secondo φ) $\varphi_k: H \to H$

$$(H \rtimes_\varphi K, \cdot) \quad \text{dove} \quad (h,k)\cdot(\bar{h},\bar{k}) = (h\varphi_k(\bar{h}), k\bar{k})$$

Oss:

(1) è ben definita l'operazione in quanto $\varphi_k(\bar{h}) \in H$

(2) È effettivamente un gruppo:

- (e_H, e_K) è l'elemento neutro

$$(e_H, e_K)\cdot(h,k) = (e_H\varphi_{e_K}(h), k) = (h,k) = (h\varphi_k(e_H), k) = (h,k)\cdot(e_H, e_K)$$

- Il prodotto è associativo:

$$[(h_1,k_1)\cdot(h_2,k_2)](h_3,k_3) = (h_1\varphi_{k_1}(h_2), k_1k_2)\cdot(h_3,k_3) = (h_1\varphi_{k_1}(h_2)\varphi_{k_1k_2}(h_3), k_1k_2k_3)$$

$$(h_1,k_1)[(h_2,k_2)(h_3,k_3)] = (h_1,k_1)(h_2\varphi_{k_2}(h_3), k_2k_3) = (h_1\varphi_{k_1}(h_2\varphi_{k_2}(h_3)), k_1k_2k_3)$$

- Esiste l'inverso:

$$(h,k)(\varphi_{k^{-1}}(h^{-1})\,k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), e_K) = (e_H, e_K)$$

(3) $H' = \{(h,e) \in H \rtimes_\varphi K\} \lhd H \rtimes_\varphi K$

Ovvio in quanto la seconda componente fa da se

(4) $K' = \{(e,k) \in H \rtimes_\varphi K\} < K \quad e \quad K' \cong {}^{H\rtimes_\varphi K}/_{H'} \cong K$

È sufficiente definire

$$F: H \rtimes_\varphi K \longrightarrow K, \quad (h,k) \longmapsto k$$

$$\ker F = \{(h,k) \mid F(h,k) = e_K\} = H'$$

È ovviamente surgettiva

Teorema Utile: Sia $H, K < G$ con $H \lhd G$. $|HK| = G$ $|H \cap K| = e$. Allora

$$G \cong H \rtimes_\tau K$$

dove $\tau: K \longrightarrow Aut(H)$ è il coniugio dentro G di un elemento di h rispetto a uno di k cioè:

$$\tau: K \longrightarrow Aut(H)$$

$$\tau: K \longrightarrow Aut(H)$$
$$k \longmapsto \tau_k: H \longrightarrow H$$
$$h \longmapsto khk^{-1}$$

Dim: Definiamo la mappa

$$F: H \times_\tau K \longrightarrow G$$
$$(h,k) \longmapsto hk$$

- F è di gruppi

$$F((h_1,k_1)(h_2,k_2)) = F(h_1\tau_{k_1}(h_2), k_1k_2) = h_1\tau_{k_1}(h_2)\,k_1k_2 =$$
$$= h_1k_1h_2k_1^{-1}k_1k_2 = h_1k_1h_2k_2 = F(h_1,k_1)F(h_2,k_2)$$

- **Iniettività**: $F(h,k) = e \Rightarrow hk = e$ cioè $h \in K$ e $k \in H$ cioè $h,k \in H \cap K = e \Rightarrow F$ iniettiva.
- **Suriettività**: Cardinalità: Dato che $|HK| = |G|$ si ha la tesi.

□

Ci potremmo chiedere se il centro di un prodotto semidiretto è sempre banale oppure no. Quello che stiamo per vedere è un utile trucco per trovare degli elementi nel centro di un prodotto semidiretto:

Fatto Comodo: Siano H, K gruppi e sia $\varphi: K \longrightarrow Aut(H)$ un morfismo con $\ker\varphi \neq 0$. Allora gli elementi della forma

$$(e_H, k) \text{ con } k \in Z(K) \cap \ker\varphi$$

stanno nel centro di $H \times_\varphi K$

Dim: Mostriamo che tali elementi ci stanno. Sia (e,k) della forma indicata, allora $\forall (\bar h, \bar k)$ si ha che

$$(e,k)(\bar h, \bar k) = (e\,\varphi_k(\bar h), k\bar k) = (\bar h, k\bar k)$$
$$(\bar h, \bar k)(e,k) = (\bar h\varphi_{\bar k}(e), \bar k k) = (\bar h, \bar k k) = (\bar h, k\bar k)$$

□

Oss: Oltre quelli trovati ce ne potrebbero essere altri quindi ATTENZIONE!

Oss: Se K è abeliano, mi basta guardare il ker del morfismo.

Esempi (Finalmente)

Esempi (Finalmente)

(1) Gruppo diedrale: Sia $H = \mathbb{Z}/n$ $\quad K = \mathbb{Z}/2$ e sia

$$\varphi: K \longrightarrow Aut(H)$$
$$\mathbb{Z}/2 \longrightarrow Aut(\mathbb{Z}/n)$$
$$s \longmapsto \varphi_s : \mathbb{Z}/n \longrightarrow \mathbb{Z}/n$$
$$r^i \longrightarrow r^{-i}$$

È dunque facile costruire un isomorfismo:

$$F: \mathbb{Z}/n \times_\varphi \mathbb{Z}/2 \longrightarrow D_n$$
$$(r^i, s) \longmapsto r^i s$$

(2) Gruppo simmetrico: Sia $G = S_n$, $H = A_n \trianglelefteq S_n$ e $K = \langle (i,j) \rangle$ Vale che

- $|HK| = |G|$
- $|H \cap K| = 2$!
- $H \trianglelefteq G$

$\Rightarrow S_n = A_n \rtimes \langle (i,j) \rangle$

(3) Il famigerato $\mathbb{Z}/4 \times_\varphi \mathbb{Z}/4 = ?$ Sia $H = \mathbb{Z}/4$ e $K = \mathbb{Z}/4$. Sia inoltre

$$\varphi: \mathbb{Z}/4 \longrightarrow Aut(\mathbb{Z}/4)$$
$$1 \longmapsto \varphi_1 : \mathbb{Z}/4 \longrightarrow \mathbb{Z}/4$$
$$x \longmapsto x^{-1}$$

Vale dunque che $\varphi_2 = \varphi_1 \circ \varphi_1 = id$ e $\varphi_3 = \varphi_1 \circ \varphi_1 \circ \varphi_1 = \varphi_1$. Facciamo dei conti:

Osserviamo prima di tutto che $Z(G) \neq \emptyset$ in quanto per il fatto utile visto si ha che l'elemento $(0,2) \in Z(G)$. [2 elem φ].

[Spazio vuoto perché avevo scritto una bella cavolata ...]

Cerchiamo altri elementi nel centro e ricordiamoci che per quanto visto qualche volta fa non ce ne possono stare 8. Proviamo i più sensati:

$$(2,2)(a,b) = (2+\varphi_2(a), b+2) = (2+a, 2+b)$$
(Un Aut manda 2 in 2) $\quad =$
$$(a,b)(2,2) = (a+\varphi_b(2), b+2) = (a+2, 2+b)$$

e anche

$$(2,0)(a,b) = (2+a, b) \qquad (a,b)(2,0) = (a+\varphi_b(2), b) = (a+2, b)$$

Abbiamo dunque scoperto che $Z(G) = \{(2,0), (2,2), (0,2), (0,0)\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$

Vediamo ora i quozienti. Sappiamo che $Z(G)$ è caratteristico dunque ogni suo

Vediamo ora i quozienti. Sappiamo che $Z(G)$ è caratteristico dunque ogni suo sottogruppo normale è normale in G. Vediamo dunque i veri conti:

(a) $\frac{G}{Z(G)}$: Sappiamo che è un 2-gruppo con 4 elementi. È dunque abeliano: Ci chiediamo se è $\mathbb{Z}/4$ o $\mathbb{Z}/2 \times \mathbb{Z}/2$. Vediamo un po'

$$\overline{(1,0)}\,\overline{(1,0)} = \overline{(1+\varphi_0(1), 0)} = \overline{(2,0)} = \overline{(0,0)}$$

$$\overline{(0,1)}\,\overline{(0,1)} = \overline{(0,2)} = \overline{(0,0)}$$

Dunque se fosse vero che $\overline{(1,0)} \neq \overline{(0,1)}$ ho trovato due elementi di ordine 2 cioè il mio gruppo è necessariamente $\mathbb{Z}/2 \times \mathbb{Z}/2$. Vediamo se sono distinti:

$$\overline{(1,0)} = \{(1,0), (1,0)\cdot(2,0), (1,0)(2,2), (1,0)(0,2)\} =$$

$$= \{(1,0), (3,0), (3,2), (1,2)\} \neq (0,1)$$ ☺

(b) $\frac{G}{\langle(0,2)\rangle}$ è un gruppo di 8 elementi. Vogliamo capire chi è. Osserviamo che

L'elemento $(1,0)$ ha ordine 4 : $\overline{(1,0)} \rightsquigarrow \overline{(2,0)} \rightsquigarrow \overline{(3,0)} \rightsquigarrow \overline{(0,0)}$.
e inoltre l'elemento $(0,1)$ ha ordine 2. $\overline{(0,1)} \rightsquigarrow \overline{(0,2)} = \overline{(0,0)}$.

Come sopra vale che $\overline{(1,0)} \neq \overline{(0,1)}$ e dunque ho un elemento di ordine 4 e uno di ordine 2. Il sottogruppo $\langle\overline{(1,0)}\rangle$ è normale. Vediamo qual è la relazione tra $\overline{(1,0)}$ e $\overline{(0,1)}$ e poi applichiamo il teorema del prodotto semidiretto:

$$\overline{(0,1)}\,\overline{(1,0)}\,\overline{(0,1)}^{-1} = \overline{(0+\varphi_1(1), 1)}\,\overline{(0,1)} = \overline{(3,1)}\,\overline{(0,1)} = \overline{(3+\varphi_1(0), 0)} = \overline{(3,0)} = \overline{(1,0)}^{-1}$$

$$\frac{G}{\langle(2,0)\rangle} \cong \langle\overline{(1,0)}\rangle \rtimes \langle\overline{(0,1)}\rangle \cong \mathbb{Z}/4 \rtimes \mathbb{Z}/2 \cong D_4$$

(c) $\frac{G}{\langle R,0\rangle}$: Ragioniamo esattamente come sopra:

$a = \overline{(1,0)}$ ha ordine 2 in quanto $\overline{(1,0)}\,\overline{(1,0)} = \overline{(2,0)} = \overline{(0,0)}$

$b = \overline{(0,1)}$ ha ordine 4 in quanto $\overline{(0,1)} \rightsquigarrow \overline{(0,2)} \rightsquigarrow \overline{(0,3)} \rightsquigarrow \overline{(0,0)}$

Vediamo le relazioni di coniugio

$$\overline{(1,0)}\,\overline{(0,1)}\,\overline{(1,0)}^{-1} = \overline{(1+\varphi_0(0), 1)}\,\overline{(1,0)} = \overline{(1,1)}\,\overline{(1,0)} = \overline{(1+\varphi_1(1), 1)} = \overline{(0,1)}$$

Dunque a e b commutano. Dunque possiamo concludere (Π = tot prodotto tutto)

$$\frac{G}{\langle(2,0)\rangle} \cong \mathbb{Z}/4 \times \mathbb{Z}/2$$

Cd) Esercizio da fare!

Vediamo ora un altro fatto molto comodo: Dati due prodotti semidiretti tra H e K con due morfismi diversi vorremmo un modo sensato per capire se sono uguali. Abbiamo il seguente criterio:

Teo Utile: Siano H e K gruppi e siano $\varphi, \theta : K \longrightarrow Aut(H)$ e consideriamo i corrispettivi prodotti semidiretti:

$$H \rtimes_\varphi K \qquad H \rtimes_\theta K$$

Supponiamo $\exists \alpha \in Aut(H)$ e $\beta \in Aut(K)$ tali che

$$\alpha \circ \varphi_k \circ \alpha^{-1} = \theta_{\beta(k)} \qquad \forall k \in K$$

allora $H \rtimes_\varphi K \cong H \rtimes_\theta K$.

Dim: Definisco la mappa

$$F: H \rtimes_\varphi K \longrightarrow H \rtimes_\theta K$$
$$(h,k) \longmapsto (\alpha(h), \beta(k))$$

Voglio ora dimostrare che una tale F è un isomorfismo.

- F è morfismo:

$$F((h_1,k_1)(h_2,k_2)) = F(h_1\varphi_{k_1}(h_2), k_1k_2) = (\alpha(h_1\varphi_{k_1}(h_2)), \beta(k_1k_2)) =$$
$$= (\alpha(h_1)\cdot\alpha\circ\varphi_{k_1}(h_2), \beta(k_1k_2)) = (\alpha(h_1)\,\alpha\circ\varphi_{k_1}\circ\alpha^{-1}\circ\alpha(h_2), \beta(k_1)\beta(k_2)) =$$
$$= (\alpha(h_1)\,\theta_{\beta(k_1)}(\alpha(h_2)), \beta(k_1)\beta(k_2)) = (\alpha(h_1), \beta(k_1))(\alpha(h_2), \beta(k_2)) =$$
$$= F(h_1,k)\cdot F(h_2,k_2)$$

- F iniettiva: $F(h,k) = (e_H, e_K) \iff (\alpha(h), \beta(k)) = (e,e) \iff (h,k) = (e,e)$ in quanto α e β sono automorfismi.

- F suriettiva: Se $(h,k) \in H \rtimes_\theta K \Rightarrow$ Prendo in partenza $(\alpha^{-1}(h), \beta^{-1}(k))$ che esistono perché α e β suriettive

□

TEOREMI DI SYLOW - Enunciati:

Primo teo di Sylow: Sia G un gruppo finito e sia p un primo tale che $p^b \mid |G|$ e $p^{b+1} \nmid |G|$ con $b \geq 1$. Allora $\forall\, 0 \leq a \leq b$ $\exists$ un sottogruppo di G di ordine p^a

Secondo teo di Sylow: Sia G come prima e sia H un p-Sylow ($|H| = p^b$). Sia $K \leq G$ con $|K| = p^a$. Allora:
1) Esiste $g \in G$ tale che $K \leq gHg^{-1}$
2) Se K è un p-Sylow, allora esiste $g \in G$ t.c. $K = gHg^{-1}$

Terzo teo di Sylow: Sia G come prima. Allora vale la seguente relazione per n_p numero di p-Sylow

$$n_p \equiv 1 \pmod{p}$$

Oss: Per il II teo di Sylow è ben definita una azione

$$\begin{aligned} G \times X_p &\longrightarrow X_p \\ (g, H) &\longrightarrow gHg^{-1} \end{aligned}$$

Dove X_p è l'insieme dei p-Sylow di G. Inoltre, dato che sono tutti coniugati sono tutti isomorfi Tra di loro.

Oss: Il III teo di Sylow ci dice che $n_p \equiv 1 \pmod{p}$, ma abbiamo anche un'altra informazione e cioè che $n_p = |orb(H)|$ con H p-Sylow dell'azione definita sopra (in quanto è transitiva per il II teo). Ma allora sappiamo anche che

$$n_p \mid |G|$$