ALGEBRA 1 – 10 OTT 2018

Note Title 10/10/2018

(Avanzi di ieri).

G p-gruppo. $H < G$ $H \neq G \Rightarrow N(H) \supsetneq H$.

① Se $H \not\subseteq Z(G)$ allora basta prendere $H \cdot Z(G) \supsetneq H$

② Se Se $H \supseteq Z(G)$, considero la proiezione canonica

$$\pi : G \to G/Z(G).$$

(Ricordiamo che esiste una corrispondenza biunivoca fra: i sottogruppi di G che contengono $Z(G)$ e i sottogruppi di $G/Z(G)$. (Vale anche normale $\Leftrightarrow$ normale).

$$\pi(H) = HZ(G)/Z(G) = H'$$

Tramite la proiezione canonica

$N(H) \longleftrightarrow N(H')$

$g \in N(H) \iff gHg^{-1} = H$

$\iff \pi(g)\pi(H)\pi(g)^{-1} = \pi(H)$

$\iff \pi(g) H' \pi(g)^{-1} = H'$

$\iff \pi(g) \in N(H')$.

Siccome, per ipotesi induttiva $N(H') \supsetneq H'$

(cardinalità di $G/Z(G)$ < cardinalità di G)

allora $N(H) \supsetneq H$

Oss Se G è un p-gruppo, $|G| = p^n$ e $0 \le k \le n$, in G esiste un sottogruppo NORMALE di ordine p^k

$$\{e\} \lhd Z(G) \lhd G$$

$$|Z(G)| = p^a \qquad a \ge 1.$$

- Se $k \le a$ basta prendere un sottogruppo di $Z(G)$.
- Se $k > a$,

$$\pi : G \to G/Z(G)$$

$$p^n \qquad p^{n-a}$$

$$p^k \longleftrightarrow p^{k-a} \ge 1$$

a lui corrisponde un sgr normale di ordine p^k. $\leftarrow$ Un sgr normale qui esiste per ipotesi induttiva

---

PRODOTTI SEMIDIRETTI

Siano H, K due gruppi.
Considero l'insieme $G = H \times K$ (prodotto cartesiano).

Considero inoltre un omomorfismo $\varphi : K \to \mathrm{Aut}(H)$. $\quad k \mapsto \varphi_k$

Definisco in G questa operazione:

$$(h,k)\cdot(h',k') = (h\,\varphi_k(h'),\ kk')$$

- associatività (esercizio)
- elemento neutro: (e,e)

$(e,e)(h',k') = (e\,\varphi_e(h'),\ ek') = (eh', ek') = (h',k')$

$(h',k')(e,e) = (h'\,\varphi_{k'}(e),\ k'e) = (h'e, k'e) = (h',k')$.

- inverso:

$(h,k)(x,y) = (e,e)$

$(h\,\varphi_k(x),\ ky) = (e,e)$

2ª coordinata: $ky = e \quad y = k^{-1}$

1ª coordinata: $h\,\varphi_k(x) = e$

$\varphi_k(x) = h^{-1}$

$x = \varphi_k^{-1}(h^{-1}) = (\varphi_{k^{-1}})(h^{-1})$

Inverso di (h,e) $=$ (h^{-1},e)

(in ordine inverso, si verifica la stessa cosa)

Il gruppo G ha due sottogruppi ovvi:

$H\times\{e\}$, $\{e\}\times K$.

che "identifichiamo" con H e K.

Oss $H \trianglelefteq G$, in generale $K \not\trianglelefteq G$.

$\pi : G \to K$

$\pi_K(x,y) = y$

$\pi_k[(x_1,y_1)(x_2,y_2)] = \pi(\dots, y_1y_2) = y_1y_2$

$= \pi_k(x_1,y_1)\,\pi_k(x_2,y_2)$.

$\ker \pi_k = \{(x,e) \mid x\in H\} = H$.

Se φ è l'omomorfismo banale ($\varphi_k = id \ \forall k \in K$) il prodotto semidiretto si riconduce al prodotto diretto.

Se no esiste $k \in K$ tale che $\varphi_k \neq id$, cioè esiste $h \in H$ t.c. $\varphi_k(h) \neq h$.

Prendo questi h, k e calcolo

$$(h,e)(e,k)(h,e)^{-1} =$$
$$= (h,e)(e,k)(h^{-1},e)$$
$$= (h\,\varphi_e(e), ek)(h^{-1},e)$$
$$= (h,k)(h^{-1},e)$$
$$= (h\,\varphi_k(h^{-1}), ke)$$
$$= (\neq e, k)$$

$\varphi_k(h) \neq h$
$\varphi_k(h^{-1}) \neq h^{-1}$

K NON È UN SGR NORMALE.

DECOMPOSIZIONE DI UN GRUPPO COME PRODOTTO DIRETTO DI DUE SOTTOGRUPPI.

- $H, K \trianglelefteq G$
- $H \cap K = \{e\}$
- $HK = G$

$\Rightarrow G \cong H \times K$

TEOREMA

PRODOTTO SEMIDIRETTO

- $H \trianglelefteq G$, $K < G$
- $H \cap K = \{e\}$
- $H \cdot K = G$

$\Rightarrow G = H \rtimes_\varphi K$

(è sottointeso: $\varphi : K \to Aut(H)$)

dove φ_k è l'automorfismo interno associato a k ($\varphi_k(h) = khk^{-1}$)

Dim. Costruiamo un isomorfismo

$$\lambda : H \rtimes_\varphi K \longrightarrow G$$

$$\lambda(h,k) = hk$$

OMOMORFISMO:

$$\lambda((h,k),(h',k')) \overset{?}{=} \lambda(h,k)\cdot\lambda(h',k')$$

$$\lambda(h\varphi_k(h'), kk') \qquad hk\cdot h'k'$$

$$\lambda(hkh'k^{-1}, kk')$$

$$hkh'k^{-1}k'$$

INIETTIVO: $\ker\lambda = \{(h,k) \mid hk = e\}$

$hk = e \quad h = k^{-1}$

$H \cap K = \{e\}$

$\Rightarrow h = k = e.$

SURGETTIVO: per definizione

ESEMPI $G = D_n$.

H = rotazioni $= \langle r \rangle = R$ $\qquad K = \langle s \rangle = S$ simmetria.

$H \trianglelefteq D_n \qquad K < D_n.$

$H \cap K = \{e\} \qquad HK = G.$

$$D_n \cong \underset{H}{R} \rtimes_\varphi \underset{K}{S}$$

$$\varphi_s(r) = srs^{-1} = s^2 r^{-1} = r^{-1}.$$

Esempio gruppo di ordine pq, con p, q primi distinti.

Possiamo supporre $p < q$ (per simmetria).

$|G| = pq$

Cauchy $\Rightarrow$ esistono un sottogruppo di ordine p e un sottogruppo di ordine q.

$|H| = q \Rightarrow H \trianglelefteq G$.

Infatti, c'è un solo sgr di G di ordine q.

Se ce ne fossero due distinti, $H_1 \neq H_2$, avrei

$$|H_1 H_2| \cdot |H_1 \cap H_2| = |H_1| \cdot |H_2|$$

$$\qquad\qquad\qquad\quad \| \qquad\qquad q \quad q$$

$$\qquad\qquad\qquad\quad 1$$

$\Rightarrow |H_1 H_2| = q^2 > pq = |G|$ ASSURDO.

$|K| = p$.

$H \cap K = \{e\}$

$HK = G$

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}.$$

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \cong \left(\mathbb{Z}/q\mathbb{Z}\right)^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

Se $p \nmid q-1$, l'unico φ possibile è quello banale e quindi

$$G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$$

è ciclico (Es. $|G| = 15 = 3 \cdot 5$)

Se $p \mid q-1$ esiste un omomorfismo non banale $\langle \bar{1} \rangle \mapsto$ elemento di ordine p. (ecc)

Es $p = 3$, $q = 7$.

$$\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right) \cong \left(\mathbb{Z}/7\mathbb{Z}\right)^* \cong \mathbb{Z}/6\mathbb{Z}$$

$$\begin{aligned} \bar{0} &\mapsto \bar{1} \\ \bar{1} &\mapsto \bar{2} \\ \bar{2} &\mapsto \bar{4} \end{aligned}$$

$\mathbb{Z}/7\mathbb{Z} = \langle x \rangle$ $\qquad$ $\mathbb{Z}/3\mathbb{Z} = \langle y \rangle$

$x^7 = e$ $\qquad$ $y^3 = e$

$\varphi_{\bar{1}}(x) = x^2$ $\qquad$ $\varphi_1(x) = yxy^{-1} = x^2$

$yx = x^2 y$

$\varphi_{\bar{2}}(x) = x^4$ $\qquad$ $y^2 x y^{-2} = x^4$.

Esercizi per il futuro

Con prodotti semidiretti, si possono costruire due gruppi non abeliani di ordine p^3 (p primo $\neq 2$)

del tipo.

$$(\mathbb{Z}/p^2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z}$$

$$(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z}.$$

(ha tutti elementi di ordine 1 o p, ma NON È ABELIANO).