PRODOTTI SEMIDIRETTI (& S_N ...)

Note Title 10/17/2018

Generatori di S_n

$$A = \{ (i,j) \mid i \neq j,\ 1 \leq i,j \leq n \}$$

$\langle A \rangle$ = il sottogp di S_n generato da tutti gli elementi dell'insieme $A = S_n$

$$B = \{ (1,i) \mid i = 2, \dots, n \}$$

$$C = \{ (1,2), (2,3), (3,4), \dots, (n-1,n) \}$$

$$D = \{ (1,2), (1,2,3,\dots,n) \}$$

$$\langle B \rangle = \langle C \rangle = \langle D \rangle = S_n$$

⚠ In S_6 la trasp. $(1,4)$ e il ciclo $(1,2,3,4,5,6)$ non generano

B: il sottogp generato da B contiene, $\forall i,j$,

la permutaz $(1,i)(1,j)(1,i)^{-1} = (i,j)$.

$$\Rightarrow \quad A \subseteq \langle B \rangle \quad \Rightarrow \quad \langle A \rangle \subseteq \langle B \rangle$$

$\langle A \rangle = S_n$

C: per induzione mostriamo che $\langle C \rangle$ contiene

B. Passo base: $(1,2) \in C$

Passo induttivo: $(1,i) \in \langle C \rangle$
$(i,i+1) \in C$

$$\Rightarrow (i,i+1)(1,i)(i,i+1)^{-1} \in \langle C \rangle$$
$$\| $$
$$(1,i+1) .$$

D: $\langle D \rangle$ contiene $(1,\dots,n)^{i}(1\,2)(1,\dots,n)^{-i}$
$$\| $$
$$(1+i, 2+i) .$$

$\Rightarrow$ $\langle D \rangle$ contiene l'insieme C, che è un insieme di generatori.

Classi di coniugio in A_5

$\sigma_1 = (1,2,3,4,5)$

$\sigma_2 = (2,1,3,4,5)$

Le classi di coniugio di σ_1, σ_2 in A_5 sono disgiunte

Ovvero: $\nexists\, \tau \in A_5$ t.c. $\sigma_1 = \tau \sigma_2 \tau^{-1}$ (*)

In S_5 si fa: basta prendere $\tau = (1,2)$

Studiamo tutti i τ per cui vale $(*)$

$$\sigma_1 = \tau_1 \sigma_2 \tau_1^{-1} = \tau_2 \sigma_2 \tau_2^{-1}$$

$$\iff \underbrace{(\tau_2^{-1}\tau_1)}_{h}\sigma_2 = \sigma_2 \underbrace{(\tau_2^{-1}\tau_1)}_{h}$$

$$\iff h \in Z_{S_5}(\sigma_2) = \langle \sigma_2 \rangle$$

$h = \tau_2^{-1}\tau_1$

In particolare, scegliendo $\tau_2 = (1,2)$, ottengo che ogni soluzione di $(*)$ è della forma

$$(1,2)(2,1,3,4,5)^j$$

Ogni tale permutazione è dispari, quindi $(*)$ non si risolve in A_5.

Riprendiamo $Z_{S_9}\big((1,2,3)(4,5,6)(7,8,9)\big) = K$

Ieri: • $K > H \simeq \langle (1,2,3); (4,5,6); (7,8,9) \rangle$

$$\simeq (\mathbb{Z}/3\mathbb{Z})^3$$

• $H \triangleleft K$ $\qquad K/H \simeq S_3$

- $|K| = 3^3 \cdot 6$

Oggi: $K \simeq H \rtimes S_3$

Non è vero in generale che $N \trianglelefteq G$ e

$$G/N = L \implies G \simeq N \rtimes L$$

In K c'è una copia di S_3 (K contiene un sottogp. isomorfo a S_3)

$$\underbrace{(1,2,3)}_{A}\ \underbrace{(4,5,6)}_{B}\ \underbrace{(7,8,9)}_{C}$$

Considero $\sigma = (1,4,7)(2,5,8)(3,6,9)$

$$\tau = (1,4)(2,5)(3,6)$$

Vediamo che σ, τ generano un sottogp di S_9 isomorfo a $S_3 = \langle r, s \mid r^3 = 1,\ s^2 = 1,\ rs = sr^{-1} \rangle$

$\sigma^3 = id \qquad \tau^2 = id$

$$\tau\sigma\tau^{-1} = (4,1,7)(5,2,8)(6,3,9)$$

$$= (7,4,1)(8,5,2)(9,6,3)$$

$= \sigma^{-1}$

Quindi: $L = \langle \sigma, \tau \rangle \simeq S_3$ è contenuto in K

Ci manca: (i) $H \cap L = \{e\}$

(ii) $HL = K$

(ii) segue da (i) + $|H| \cdot |L| = |K|$

$\{hl \mid h \in H, l \in L\} \overset{?}{=} K$

Basta verificare che i prodotti siano tutti distinti: $h_1 l_1 = h_2 l_2$

$\iff h_2^{-1} h_1 = l_2 l_1^{-1} \in H \cap L = \{e\}$

$h_2^{-1} h_1 \in H$, $l_2 l_1^{-1} \in L$

$\iff h_1 = h_2, \ l_1 = l_2$

Per dimostrare (i) osservo che (da ieri)

$\psi : K \longrightarrow S_3$

$K \twoheadrightarrow K/H \hookrightarrow S_3$

Vorrei dire che $\psi(L) = S_3$.

$$L/_{\ker \psi|_L} \overset{??}{=} L/_{H \cap L}$$

(Se so questo, $|L| = |S_3| = |L|/|H \cap L|$

$\Rightarrow |H \cap L| = 1$)

Infatti: $\psi(\sigma) = (A, B, C)$

$\psi(\tau) = (A, B)(C)$

$\Rightarrow Im(L) \ni (A,B)$ e $Im(L) \ni (A,B,C)$

$\Rightarrow Im(L) \supseteq S_3 \Rightarrow Im(L) = S_3$

Abbiamo tutte le ipotesi per dire che K è il prodotto semidiretto $H \rtimes_{\varphi} L \simeq (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_{\varphi} S_3$

$\varphi: S_3 \longrightarrow Aut\left((\mathbb{Z}/3\mathbb{Z})^3\right)$ è l'omomorf.

"ovvio" di permutazione delle coordinate

Prodotto semidiretto di $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$

(gruppo delle sostituzioni lineari)

- $G_1 = \left\{ f : \mathbb{F}_p \longrightarrow \mathbb{F}_p \;\middle|\; f(x) = ax+b, \; \begin{matrix} a \in \mathbb{F}_p^* \\ b \in \mathbb{F}_p \end{matrix} \right\}$

con la composizione

- $G_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{matrix} a \in \mathbb{F}_p^* \\ b \in \mathbb{F}_p \end{matrix} \right\}$ con il prodotto di matrici

Affermazione: $G_1 \simeq G_2 \simeq \mathbb{F}_p \rtimes \mathbb{F}_p^*$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & b+ad \\ 0 & 1 \end{pmatrix}$$

$$(a,b) \cdot (c,d) = (ac,\; b+ad)$$

$a \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p^*$, $ac \in \mathbb{F}_p^*$

Cos'è $b+ad$? È $b+$ interpreto "a" come un automorfismo di $\mathbb{Z}/p\mathbb{Z}$ e lo applico a "d"

Formalmente: G_2 contiene

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_p \right\}$$

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p^* \right\}$$

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix}$$

- $H \lhd G_2$: $\quad H = \ker\left(\det : G_2 \longrightarrow \mathbb{F}_p^*\right)$

$$\det : GL_2(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^*$$

- $H \cap K = \{Id\}$
- $HK = G_2$ (oppure $|H| \cdot |K| = |G_2|$ ok
  $p \quad p-1 \quad p(p-1)$)

$$\Longrightarrow G_2 \simeq H \rtimes K$$

E per G_1? I due sottogruppi sono

$$\{x \longmapsto x + b\} \quad \text{e} \quad \{x \longmapsto ax\}$$

$$\begin{array}{ccc} G_1 & \longrightarrow & G_2 \\ ax+b & \longmapsto & \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \end{array}$$

Come $\rtimes$ esterno: mi serve un

$$\varphi : \mathbb{F}_p^* \longrightarrow \mathrm{Aut}(\mathbb{F}_p) \simeq \mathbb{F}_p^*$$

È l'identità!

Diedrale

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

$$\{1, r, \dots, r^{n-1}\} \qquad \{1, s\}$$

Elementi di D_n: r^i, sr^j

$$(sr^j)\cdot(sr^k) = (srs)^j \cdot r^k$$

$$= r^{-j} \cdot r^k$$

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$$

$$1 \longmapsto (-1)$$

$$(sr^j)\cdot r^k = s\, r^{j+k}$$

$$r^k \cdot (sr^j) = s\, r^{-k+j}$$

Normalizzatore di $\langle (1,2,\dots,7) \rangle$ in S_7

$$H = N_{S_7}\left(\underbrace{\langle (1,\dots,7) \rangle}_{G}\right)$$

$|H| = 42$

$G \triangleleft H$ (perché H normalizzatore)

$$\rightsquigarrow |H/G| = \frac{|H|}{|G|} = \frac{42}{7} = 6$$

Domanda: H/G è S_3 o è $\mathbb{Z}/6\mathbb{Z}$?

Oss. $H \xrightarrow{\psi} \mathrm{Aut}(G)$ omomorfismo

$h \longmapsto$ "coniugio per h" $\quad \varphi_h : G \longrightarrow G$

$g \longmapsto hgh^{-1}$

$$\ker \psi = Z_H(G) = Z_H((1,2,\dots,7)) = G$$

$$\mathrm{Aut}(G) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$$

$$|\mathrm{Im}\ \psi| = |H|/|G| = 42/7 = 6$$

$\rightsquigarrow$ H/G "gruppo astratto" $= H/\ker\psi$.

$\simeq \mathrm{Im}\ \psi = \mathbb{Z}/6\mathbb{Z}$.

Convinciamoci allora che $H \simeq \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z}$

- $G \triangleleft H$, $\quad G \simeq \mathbb{Z}/7\mathbb{Z}$
- $H/G \simeq \mathbb{Z}/6\mathbb{Z} \ni \bar{1}$ $\qquad \pi : H \longrightarrow H/G = \mathbb{Z}/6\mathbb{Z}$

Prendo un $h \in H$ t.c. $\pi(h) = \bar{1}$

$\operatorname{ord}(h) \equiv 0 \ (\operatorname{ord} \pi(h))$

$\Leftrightarrow$ 6 divide $\operatorname{ord}(h)$

$\langle h \rangle$ è un gruppo ciclico di ordine divisibile per 6

struttura gp ciclici $\Longrightarrow$ c'è un sottogp $K < \langle h \rangle$ ciclico di ordine 6

- $G \cap K = \{e\}$ (cardinalità)
- $|G| \cdot |K| = 7 \cdot 6 = 42 \Rightarrow GK = H$

$\rightsquigarrow$ concludiamo che $H \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Gruppi di ordine pq (p, q primi distinti)

- ce n'è uno abeliano: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$

SOLO

→ sia G abeliano di ordine pq

$\exists\ g \in G$ di ord $= p$

$\exists\ h \in G$ di ord $= q$

$\langle g \rangle = H_1$, $\langle h \rangle = H_2$ $\quad \triangleleft G$

$H_1 \cap H_2 = \{e\}$ $\qquad H_1 H_2 = G$

$\Rightarrow G \simeq H_1 \times H_2 \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

- caso non abeliano: $p > q$

$|H_1| = p$ $\qquad |H_2| = q$ $\qquad H_1 \triangleleft G$

↑ guardare l'indice

$H_1 \cap H_2 = \{e\}$ $\qquad H_1 H_2 = G$

$\Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z} \underset{\varphi}{\rtimes} \mathbb{Z}/q\mathbb{Z}$

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

* se $q \nmid p-1$: φ è l'omomorfismo banale $\rightsquigarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

* se $q \mid p-1$

$$\varphi : \mathbb{Z}/q\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$
$$1 \longmapsto k \text{ di ordine } q$$

$$\varphi_1 : 1 \longmapsto k_1 \rightsquigarrow G_1 \simeq \mathbb{Z}/p\mathbb{Z} \underset{\varphi_1}{\rtimes} \mathbb{Z}/q\mathbb{Z}$$

$$\varphi_2 : 1 \longmapsto k_2 \rightsquigarrow G_2 \simeq \mathbb{Z}/p\mathbb{Z} \underset{\varphi_2}{\rtimes} \mathbb{Z}/q\mathbb{Z}$$

Oss. Esiste i t.c. $k_2 = k_1^i$ $\quad q \nmid i$

$$(a_1, b_1) \underset{\varphi_1}{\cdot} (a_2, b_2) = (a_1 + \varphi_1(b_1)(a_2),\ b_1+b_2)$$
$$= (a_1 + k_1^{b_1} \cdot a_2,\ b_1+b_2)$$

$$(a_1, b_1) \underset{\varphi_2}{\cdot} (a_2, b_2) = (a_1 + k_2^{b_1} a_2,\ b_1+b_2)$$
$$= (a_1 + k_1^{ib_1} a_2,\ b_1+b_2)$$

Definiamo $\Phi : G_2 \longrightarrow G_1$
$$(a,b) \longmapsto (a, ib)$$

È una biiezione? Sì: l'inversa è

$$(a', b') \longmapsto (a', i^{-1} b')$$

$$\Phi(a_1, b_1) \underset{\varphi_1}{\cdot} \Phi(a_2, b_2) \overset{?}{=} \Phi\left((a_1, b_1) \underset{\varphi_2}{\cdot} (a_2, b_2)\right)$$

$$(a_1, ib_1) \underset{\varphi_1}{\cdot} (a_2, ib_2) \overset{?}{=} \Phi\left(a_1 + k_1^{ib_1} a_2, b_1 + b_2\right)$$

$$\left(a_1 + k_1^{ib_1} a_2, ib_1 + ib_2\right) \overset{?}{=} \left(a_1 + k_1^{ib_1} a_2, i(b_1 + b_2)\right)$$