ALGEBRA 1 - 26 OTT 2018

Note Title 10/26/2018

p-gruppi abeliani finiti.

Quanti sono? $|G| = p^a$

$a_1 \geq a_2 \geq \dots \geq a_k > 0 \qquad a_1 + a_2 + \dots + a_k = a.$

$a = 5$:

$\mathbb{Z}/p^5\mathbb{Z}$	$(abcde)$
$\mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	$(abcd)$
$\mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$	$(abc)(de)$
$\mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	(abc)
$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	$(ab)(cd)$
$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	(ab)
$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$	e

n° di elementi di dato ordine e n° di sottogruppi ciclici di dato ordine

$$G = \mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$$

ordine	n° di elementi	n° di sgr ciclici
1	1	1
p	$p^3 - 1$	$(p^3-1)/(p-1)$
p^2	$p^6 - p^3$	$(p^6-p^3)/p(p-1)$
p^3	$p^8 - p^6$	$(p^8-p^6)/p^2(p-1)$
p^4	$p^9 - p^8$	$(p^9-p^8)/p^3(p-1)$

Sottogruppi di ordine p^2.

ciclici → già contati.

$\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. $= \langle x, y \rangle$

$\# (x,y) \quad = (p^3-1)(p^3-p)$

$\#$ basi $\quad = (p^2-1)(p^2-p)$

Risposta $\quad = \dfrac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)}$.

Sottogruppi di Sylow.

Esempio: $G = S_n$.

$p=2$ $\quad n=1 \quad \{e\}$

$n=2 \quad n=3 \quad$ 2-Sylow $\cong \mathbb{Z}/2\mathbb{Z}$.

($n=3$ tre sottogruppi di Sylow)

$n=4 \quad 4! = 24 = 2^3 \cdot 3$

Ogni 2-Sylow è isomorfo a D_4.

$\sigma = (12), \ \tau = (34)$

$H = \langle \sigma, \tau \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\lambda \in N(H)$

Posso prendere $\lambda = (1324)$

$(\lambda = (13)(24))$

Un 2-Sylow è $\langle \sigma, \tau, \lambda \rangle$.

$\cong \underbrace{(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})}_{H} \rtimes_\varphi \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\langle \lambda \rangle}$

$p=3 \quad n=1,2 \quad \{e\}$

$n=3,4,5 \quad \mathbb{Z}/3\mathbb{Z} \quad \langle (123) \rangle$

$n = 6, 7, 8$ $\quad \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$ $\quad <(123), (456)>$

$n = 9$

$H = <(123), (456), (789)>$ $\qquad |H| = 3^3 = 27.$

Un 3-Sylow ha invece $3^4 = 81$.

Cerco λ nel normalizzatore di H

$\lambda = (147)(258)(369)$

Un 3-Sylow è $<H, \lambda>$.

$G = GL_n(\mathbb{Z}/p\mathbb{Z})$.

$n = 2$ $\qquad |G| = (p^2 - 1)(p^2 - p)$

Un p-Sylow ha ordine p.

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \; a \in \mathbb{Z}/_{p\mathbb{Z}} \right\} = \underline{P}$$

Verifico che, se $M \in P$, allora $M^p = \underline{Id}$

$n = 3$ $\qquad |G| = (p^3 - 1)(p^3 - p)(p^3 - p^2)$

$p^3 \,\|\, \text{ord}(G)$

$$\left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \middle| \; x, y, z \in \mathbb{Z}/_{p\mathbb{Z}} \right\} = \underline{P}$$

Questo insieme ha p^3 elementi ed è un sottogruppo.

$\boxed{p > 2}$ Tutti gli elementi di P hanno ordine $| p$.

$M \in P \qquad M = I + N \qquad N = \begin{pmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{pmatrix}$

$N^2 = \begin{pmatrix} 0 & 0 & t \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad N^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$$M^p = (I+N)^p = I + pN + \underbrace{\binom{p}{2}}_{\text{coeff è divisibile per } p} N^2 + 0$$

$$= I .$$

Si verifica facilmente che il gruppo non è commutativo.

Allora $Z(P)$ ha ordine p.

$Z(P) = \langle x \rangle$

$y \notin Z(P) \qquad \langle x, y \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$x^p = e \quad y^p = e \quad xy = yx .$

$H = \langle x, y \rangle$

$z \notin H \qquad K = \langle z \rangle .$

$$\Rightarrow \quad G \cong H \rtimes_{\varphi} K$$

$\uparrow$?

$$\varphi : K \to \mathrm{Aut}(H) = \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$$

$$\cong GL_2(\mathbb{Z}/p\mathbb{Z}).$$

φ <u>non è</u> l'omomorfismo banale

$\varphi(z)$ è un automorfismo di ordine p.

Per esempio, posso scegliere $\varphi(z) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$$z\,(x,y)\,z^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}$$

$$(x+y,\, y)$$

(L'altro gruppo non abeliano di ordine p^3 è
$\mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ dove

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\,(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^*$$

$$\varphi(\bar{1}) = \overline{1+p} \quad)$$

Caso $p=2$ Si verifica che il 2-Sylow è isomorfo a D_4.

Q_8 = gruppo di 8 elementi (quaternioni)

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

$i^2 = j^2 = k^2 = -1$ $\qquad$ $\pm i, \pm j, \pm k$ hanno ordine $= 4$.

$$ij = k \quad jk = i \quad ki = j$$
$$ji = -k \quad kj = -i \quad ik = -j.$$

Q_8 non si può scrivere come prodotto semidiretto di due sottogruppi propri
(Se no, un fattore avrebbe ordine 4 e l'altro avrebbe ordine 2).

Ma sia nel fattore di ordine 4 che in quello di ordine 2 ci dovrebbe essere un elemento di ordine 2. Ma in Q_8 c'è UN SOLO ELEMENTO di ordine 2 $\to$ IMPOSSIBILE.

Siano p, q, r primi distinti $(p > q > r)$
e $|G| = pqr$.

Allora G <u>non è</u> un gruppo semplice
(Un gruppo si dice semplice se i suoi unici sottogruppi normali sono $\{e\}$ e G).

Se G fosse semplice, i suoi sottogruppi di Sylow P, Q, R <u>non</u> sarebbero normali.

Siano n_p, n_q, n_r il n° dei sottogruppi coniugati a P, Q, R $\quad (n_p, n_q, n_r > 1)$

$$n_p = \begin{cases} \text{divisore di } qr & \text{(Indice del normalizzatore)} \\ \equiv 1 \pmod p & \text{(3° teo. di Sylow)} \end{cases}$$

$1, q, r, qr \qquad q < p \quad r < p.$

L'unica possibilità è qr.

$$n_q = \begin{cases} \text{divisore di } pr \\ \equiv 1 \pmod q \end{cases}$$

$1, p, r, pr$ — 1: NO; r: NO (è troppo piccolo)

$\Rightarrow n_q$ deve essere un multiplo di p

In particolare, $n_q \geq p$.

$$n_r = \begin{cases} \text{divisore di } pq \\ \equiv 1 \pmod r \end{cases}$$

1, p, q, pq
è il più piccolo possibile

$\Rightarrow n_r \geq q$.

$G \supseteq \{e\} \cup \{\text{elementi di ordine } p\} \cup \{\text{elementi di ordine } q\} \cup \{\text{elementi di ordine } r\}$

$$|G| = pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1)$$

$$= 1 + pqr - \cancel{qr} + pq - p + \cancel{qr} - q$$

$$0 \geq 1 + pq - p - q = (p-1)(q-1) \quad \text{ASSURDO}.$$

Oss: Il ragionamento precedente dice anche che almeno uno fra P, Q, R è un sottogruppo normale

Ora trascuriamo la disuguaglianza $p > q > r$.
Supponiamo $P \trianglelefteq G$

$$|G/P| = qr$$

G/P ha un sgr normale, per esempio

$$\pi(Q) = QP/P \qquad \pi : G \to G/P.$$

Per la corrispondenza biunivoca fra sgr

$QP \trianglelefteq G$ di ordine pq.

$|R| = r$

$\Rightarrow G \cong QP \rtimes_\varphi R$.