LEZIONE 19 - 10 - 2020

EQUAZIONI IN S_n

① Dato p primo, $\sigma^p = (1, 2, \dots, p)(p+1, \dots, 2p)$. $\sigma \in S_{2p}$

SOL Gli el. nella destra hanno ordine p e i due p-cicli sono disgiunti.
$\Rightarrow$ il membro dx ha ordine p.

Segue che $(\sigma^p)^p = id \Rightarrow \sigma^{p^2} = id \Rightarrow ord\, \sigma \mid p^2$.

Dunque $ord\, \sigma \in \{1, p, p^2\}$ ma non può essere né 1 né p altrimenti $\sigma^p = id$. Segue che σ ha ordine p^2, dunque contiene almeno un p^2 ciclo.

Ma $p^2 > 2p$ per ogni $p \in \mathbb{Z}, p > 2$:
dunque l'eq. non ha soluzione $\forall p > 2$.

$$p^2 \geq 2p \iff p^2 - 2p \geq 0 \iff p(p-2) \geq 0$$

0 2
+ − +

Per $p = 2$ abbiamo che $p^2 = 2p$, dunque vogliamo trovare un 4-ciclo $\sigma \in S_4$ t.c. $\sigma^2 = (1\ 2)(3\ 4)$

$\iff \sigma = (1\ 3\ 2\ 4)$ oppure
$\sigma = (1\ 4\ 2\ 3)$

② $\sigma^4 = (1\ 2\ 3)$ in S_6

$ord(\sigma) \mid 12$ poiché $\sigma^{12} = (\sigma^4)^3 = id$.

Quindi $ord(\sigma) \in \{\cancel{1}, \cancel{2}, 3, \cancel{4}, 6, \cancel{12}\}$

- Non può essere 1, 2, 4 poiché altrimenti $\sigma^4 = id$.
- Se $ord(\sigma) = 12$ allora σ è un 12-ciclo oppure contiene almeno un 4-ciclo e un 3-ciclo $\Rightarrow$ assurdo poiché siamo in S_6!
- Se $ord(\sigma) = 3$ allora $\sigma^4 = \sigma = (1\ 2\ 3)$ ✓

- Se $\operatorname{ord}(\sigma) = 6$ allora σ è un 6-ciclo oppure è un 3+2.

⊙ $\sigma = (a_1\ a_2\ a_3\ a_4\ a_5\ a_6)$

$\Rightarrow \sigma^2 = (a_1\ a_3\ a_5)(a_2\ a_4\ a_6)$

$\Rightarrow \sigma^4 = (a_1\ a_5\ a_3)(a_2\ a_6\ a_4)$ ASSURDO

⊙ $\sigma = (a_1\ a_2\ a_3)(b_1\ b_2)$

$\Rightarrow \sigma^4 = (a_1\ a_2\ a_3)^4 (b_1\ b_2)^4 = (a_1\ a_2\ a_3)$

Dunque $(a_1\ a_2\ a_3) = (1\ 2\ 3)$

Posso scegliere $(b_1\ b_2)$ in $\binom{3}{2} \cdot \frac{3!}{3} = \cancel{3} \cdot \frac{3!}{\cancel{3}} = 3! = 6$ modi.

GENERATORI DI S_n

(1) $S_n = \langle (i,j) \mid i,j = 1, \dots, n \rangle$ ~ visto a lezione

(2) $\quad = \langle (1,i) \mid i = 2, \dots, n \rangle$

(3) $\quad = \langle (i,i+1) \mid i = 1, \dots, n-1 \rangle =: H$

(4) $\quad = \langle (1,2), (1\ 2\ \dots\ n) \rangle$

DIM (2) $(i,j) = (1,j)(1,i)(1,j)^{-1} \Rightarrow$ ottengo tutte le trasp. a partire da $\langle (1,i) \mid i = 2, \dots, n \rangle$

(3) Per induzione mostriamo che $H \ni (1,i)$.

Certamente $(1,2) \in H$. Per hp. induttiva $(1,i) \in H$, dunque

$$(1, i+1) = (i, i+1)(1,i)(i,i+1)^{-1} \in H.$$

Dunque $H = S_n$ perché ci siamo ricondotti a (2).

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

$(1\ 2\ \dots\ n)^k (1\ 2)(1\ 2\ \dots\ n)^{-k} = (k+1,\ k+2)$

$\rightsquigarrow$ Ottengo tutte le trasp. tra el. adiacenti, dunque ottengo tutto S_n. $\square$

CENTRALIZZATORI

$\sigma = (1 \dots 4)(5\ 6\ 7)(8\ 9) \in S_9$. Descrivere $Z_{S_9}(\sigma) =: Z$.

<u>SOL</u>: Considero l'azione di coniugio di S_9 su S_9

$$\tau \cdot \rho := \tau \rho \tau^{-1}.$$

$$Z = \mathrm{Stab}_{S_9}(\sigma) \overset{\text{orb. stab.}}{\Longrightarrow} \# Z = \frac{\# S_9}{\# \mathrm{orb}(\sigma)}$$

el. con la stessa decomp. in cicli

Ma gli elementi di tipo $4+3+2$ in S_9 sono

$$\binom{9}{4}\frac{4!}{4} \cdot \binom{5}{3}\frac{3!}{3} \cdot \binom{2}{2}\frac{2!}{2}$$

$$= \frac{9 \cdot 8 \cdot 7 \cdot 6}{\cancel{4!}} \frac{\cancel{4!}}{\cancel{4}} \cdot \frac{5 \cdot \cancel{4} \cdot \cancel{3}}{\cancel{3!}} \frac{\cancel{3!}}{\cancel{3}} \cdot 1 = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = \frac{9!}{4!}$$

Dunque $\# Z = \dfrac{\# S_9}{\# \mathrm{orb}(\sigma)} = \dfrac{9!}{9!/4!} = 4! = 24$

Come troviamo Z come gruppo astratto?

<u>Oss</u>: Z contiene $(1\,2\,3\,4)$ e $(5\,6\,7)$ e $(8\,9)$

$$\Rightarrow Z \supseteq \langle (1\,2\,3\,4), (5\,6\,7), (8\,9) \rangle \simeq$$

COMMUTANO!

$$\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Ma allora $Z \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ per cardinalità.

⌈ Se fossimo stati in S_n, $n > 9$:

$$\# \mathrm{orb}(\sigma) = \binom{n}{4,3,2,n-9} 3! \cdot 2$$

$$\rightsquigarrow \# Z = \frac{n!}{\frac{n!}{4 \cdot 3 \cdot 2! \, (n-9)!} \cdot 3! \, 2!} = 24 \cdot (n-9)!$$

$$\Rightarrow Z \supseteq \langle (1\,2\,3\,4), (5\,6\,7), (8\,9), \rho \mid \rho \in S(\{10, \dots, n\}) \rangle$$

$\simeq \mathbb{Z}/_{4}\mathbb{Z} \times \mathbb{Z}/_{3}\mathbb{Z} \times \mathbb{Z}/_{2}\mathbb{Z} \times S_{n-9}$

Se ci sono cicli di lunghezza uguale?

$Z_{S_4}((1\,2)(3\,4)) \ni (1\,3)(2\,4)$ ⇝ scambio i due 2-cicli

$\#orb((1\,2)(3\,4)) = \binom{4}{2}\cdot\frac{2!}{2}\cdot\binom{2}{2}\cdot\frac{2!}{2}\cdot\frac{1}{2!} = \frac{4!}{2!\,2!}\cdot\frac{\cancel{2!}}{\cancel{2!}}\cdot\frac{1}{2!}$

$= \frac{4\cdot 3\cdot 2}{8} = 3$

$\Rightarrow \#Z = \frac{24}{3} = 8$

$\Rightarrow Z \supsetneq \langle (1\,2), (3\,4)\rangle$ ordine 4

$\Rightarrow Z = \langle (1\,2), (3\,4), (1\,3)(2\,4)\rangle$

L'ho trovato perché se $\sigma := (1\,2)(3\,4)$, $\tau := (1\,3)(2\,4)$

$\Rightarrow \tau\sigma\tau^{-1} = (3\;4)(1\;2) = \sigma$ ✓

Minimo n per cui S_n contiene un gruppo dato

Minimo n per cui S_n contiene un sgrp. di ordine 21.

OSS $21 = 7\cdot 3$ e $3 \mid 7-1 = 6$. Ci sono 2 gruppi di ordine 21

$\mathbb{Z}/_{21}\mathbb{Z}$ e $\mathbb{Z}/_{7}\mathbb{Z} \rtimes \mathbb{Z}/_{3}\mathbb{Z}$

(1) Minimo n t.c. $S_n > \mathbb{Z}/_{21}\mathbb{Z}$?

$\Leftrightarrow$ Minimo n t.c. S_n ha un el. di ordine 21 $\Rightarrow$ ha un el. che contiene un ciclo di lung. multiplo di 7 e uno di lung. mult. di 3

$\Leftrightarrow$ $n = 10$.

(2) Minimo n t.c. $S_n > \mathbb{Z}/_{7}\mathbb{Z} \rtimes \mathbb{Z}/_{3}\mathbb{Z}$

Per Lagrange $21 \mid n! \Rightarrow n \geq 7$. Basta S_7?

Sia H un presunto sgrp. di S_7 con 21 elementi. Allora $H \ni \sigma$ di ordine 7 e a meno di coniugio posso assumere che contenga proprio $(1 \dots 7)$.

Se H contiene σ di ord 7 e τ è una permutazione t.c. $\tau \sigma \tau^{-1} = (1 \dots 7)$, allora $\tau H \tau^{-1}$ è un sgrp. di S_7 di ordine 7 contenente $(1 \dots 7)$.

$$\langle (1 \dots 7) \rangle \trianglelefteq H < S_7$$

$\langle (1 \dots 7) \rangle \cong \mathbb{Z}/7\mathbb{Z}$ → in un gruppo di ord 21 c'è un unico sgrp di ord 7 ⇒ è normale

Quindi $H \leq N_{S_7}((1 \dots 7)) = \mathrm{Stab}_{S_7}(\langle (1, \dots, 7) \rangle)$ rispetto al coniugio sui sottogruppi

$$\# \mathrm{orb}(\langle (1 \dots 7) \rangle) = \#\{\text{sgrp. di ordine } 7\}$$ ← i sgrp. di ord 7 sono coniugati

i sgrp. di ordine 7 sono ciclici →
$$= \frac{\#\{\text{el di } S_7 \text{ di ord } 7\}}{\phi(7)}$$

$$= \frac{6!}{6} = 5!$$

Per orb-stab: $$\# N = \frac{\# S_7}{\# \mathrm{orb}} = \frac{7!}{5!} = 42$$

È vero che c'è un sgrp. di ordine 21 in uno di ord 42?

Sì: $\# N = 42 = 2 \cdot 21 \Rightarrow 2 \cdot$ dispari $\Rightarrow$ contiene un sgrp. di ord 21 $\Rightarrow$ è il $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ cercato!

SEMIDIRETTI $\quad \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}, \quad \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$

$$1 \longmapsto (x \mapsto kx)$$

Quali k vanno bene? Voglio che $\varphi(1)^3 = id$.

$\Rightarrow (x \mapsto k^3 x) = id \iff k^3 x = x \quad \forall x$

$\iff k^3 \equiv 1 \ (7) \iff k \equiv 1, 2, 4 \ (7)$

1 mi dà il prod. diretto, 2 e 4 mi danno lo stesso semidiretto

(*) Ordine degli el di $\mathbb{Z}/_{7\mathbb{Z}} \rtimes \mathbb{Z}/_{3\mathbb{Z}} =: G$?

no! sarebbe ciclico $\Rightarrow$ abeliano

Sicuramente ogni el. ha ordine ~~1~~, 3, 7 o ~~21~~.

solo id

Quanti ord 7 ? Quanti ord 3 ?

almeno $(\mathbb{Z}/_{7\mathbb{Z}} \setminus \{0\}) \times \{0\}$ almeno $\{0\} \times (\mathbb{Z}/_{3\mathbb{Z}} \setminus \{0\})$

almeno 6 ! almeno 2 !

Sia $H_1 := \mathbb{Z}/_{7\mathbb{Z}} \rtimes \{0\} \trianglelefteq G$. Se ho $g \in G \setminus H_1$, allora $\langle g \rangle = K$ è $\simeq \mathbb{Z}/_{7\mathbb{Z}}$.

Per normalità di $H_1 \trianglelefteq G$, H_1K è un sogr. di G con

$$|H_1K| = \frac{|H_1| \cdot |K|}{|H_1 \cap K|} = \frac{7 \cdot 7}{1} = 49 \text{ elementi}$$

$\Rightarrow$ non ci possono essere due sogr. di ordine 7

$\Rightarrow$ ci sono esattamente 6 el. di ordine 7

$\Rightarrow$ ci sono // 14 el. di ordine 3

DIM $H_1 \times K \xrightarrow{\Phi} H_1K$

$(g_1, g_2) \longmapsto g_1g_2$

è certamente surgettiva;

$\Phi(g_1, g_2) = \Phi(g_1', g_2')$

$\Leftrightarrow g_1g_2 = g_1'g_2'$

$\Leftrightarrow \underbrace{(g_1')^{-1}g_1 = (g_2')(g_2^{-1})}_{\in H_1 \cap K}$

Fissato un el nell'imm. di Φ, $\Phi(g_1, g_2)$ gli el. $(g_1', g_2') \in H_1 \times K$ con la stessa immagine sono in bigezione con $H_1 \cap K$: dato $h \in H_1 \cap K$ pongo $(g_1', g_2') = (g_1h, h^{-1}g_2)$ e viceversa dato (g_1', g_2') pongo $h = g_1^{-1}g_1'$.

METODO CALCOLATORIO

Sia $(a, b) \in G = \mathbb{Z}/_{7\mathbb{Z}} \rtimes \mathbb{Z}/_{3\mathbb{Z}}$

$$(a, b)(a', b') = (a + \underbrace{\varphi(b)}_{\in \text{Aut}(\mathbb{Z}/_{7\mathbb{Z}})}(a'), b + b')$$

$$(1, 2)(3, 1) = (1 + \varphi(2)(3), 2+1)$$
$$= (1 + (x \mapsto 2x)^2(3), 0)$$
$$= (1 + (x \mapsto 4x)(3), 0)$$
$$= (1 + 12, 0) = (6, 0).$$

$$(a,b)\cdot(a,b) = (a + \varphi(b)(a),\ 2b)$$

$$(a,b)^3 = (a,b)\cdot(a+\varphi(b)(a),\ 2b)$$

$$= (a + \varphi(b)(a+\varphi(b)(a)),\ 3b)$$

OSS $\varphi(b)(a) = (x \longmapsto 2x)^b a = 2^b a$

$$= (a + 2^b(a + 2^b a),\ 0)$$

$$= (a(1 + 2^b + 2^{2b}),\ 0)$$

Dunque $(a,b)^3 = 0$ se
- $a = 0$ [el di $\{0\} \rtimes \mathbb{Z}/3\mathbb{Z}$]
- $1 + 2^b + 2^{2b} = 0$ in $\mathbb{Z}/7\mathbb{Z}$, $b \in \mathbb{Z}/3\mathbb{Z}$

Con $b = 0$ non ho sol
Con $b = 1$ $1 + 2 + 4 \equiv 0 \ (7)$
Con $b = 2$ $1 + 4 + 2 \equiv 0 \ (7)$

$\Rightarrow$ Hanno ord 3 anche gli el di $(\mathbb{Z}/7\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/3\mathbb{Z} \setminus \{0\})$
$(a,\ 1/2)$, $a \neq 0$

OSS $1 + 2^b + 2^{2b} \equiv \dfrac{(2^b)^3 - 1}{2^b - 1} \equiv \dfrac{(2^3)^b - 1}{2^b - 1} \equiv 0 \quad (7)$

(che corrisponde ad $(x \mapsto 2x)^3 = id$ ...)

Realizzazione di $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ in S_7

Voglio costruire $G \xrightarrow{\Phi} S_7$

$$(1,0) \longmapsto (1,\dots,7) = \sigma$$

$$(0,1) \longmapsto \rho \quad \text{di ord } 3$$

Condizione: $\rho\sigma\rho^{-1} = \sigma^2$

$$\Phi((0,1)(1,0)(0,1)^{-1}) = \rho\sigma\rho^{-1}$$

$$\|$$

$$\| $$

$$\Phi\big((0,1)(1,0)(0,2)\big) \overset{(*)}{=} \Phi\big((2,0)\big) = \sigma^2$$

$$\begin{aligned}(0,1)(1,0)(0,2) &= (0,1)\cdot\big(1+\varphi(0)(0),\ 2\big)\\ &= (0,1)\cdot(1,2)\\ &= \big(0+\varphi(1)(1),\ 2+1\big)\\ &= \big(\varphi(1)(1),\ 0\big)\\ &= (2,0) \quad (*)\end{aligned}$$

Ma $\rho\sigma\rho^{-1} = \sigma^2 = (1\ 3\ 5\ 7\ 2\ 4\ 6)$

$$\|$$

$$(\rho(1), \dots, \rho(7)) \implies \rho = (1)(2\ 3\ 5)(4\ 7\ 6)$$

Affermo che $\langle \rho, \sigma \rangle \simeq \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$

$$\sigma^a\rho^b \longleftarrow\!\shortmid (a, b)$$