LEZIONE 21-10-2029

Permutazioni

- Sia σ un km-ciclo (tipo: $\sigma=(1,\dots,km)$)

Allora $\sigma^k = (1, 1+k, 1+2k, \dots, 1+(m-1)k)\cdot$
$(2, 2+k, 2+2k, \dots, 2+(m-1)k)\cdot$
$\vdots$
$(k, 2k, 3k, \dots, mk)$

k cicli lunghi $m = \frac{mk}{k}$

Se invece $(n, km)=1$ allora

$\sigma^n \in \langle\sigma\rangle$ e $ord(\sigma^n)=ord(\sigma)$

↳ è un generatore perché l'ho el. ad una potenza coprima con km

In generale se σ è un a-ciclo, dato $b\in\mathbb{Z}$, $d:=(a,b)$
$a=da'$, $b=db'$ con $(a',b')=1$.

Allora $\sigma^b = \sigma^{db'} = (\sigma^d)^{b'} = (\underbrace{\sigma_1 \cdots \sigma_d}_{d \text{ cicli elevati lunghi } \frac{a}{d}=a'})^{b'} = \sigma_1^{b'}\cdots\sigma_d^{b'}$

ancora a'-cicli

Es: $(1\ 2 \cdots 6)^4 = ((1\ 3\ 5)(2\ 4\ 6))^2 = (1\ 5\ 3)(2\ 6\ 4)$

(*) p primo, $\sigma\in S_p$ un p-ciclo, $\tau\in S_p$ una trasposizione.
Allora $\langle\sigma,\tau\rangle = S_p$.

OSS: posso scegliere almeno uno tra il p-ciclo e la trasp.
$\Rightarrow$ Scelgo $\sigma=(0 \dots p-1)$

[Infatti sia $H=\langle\sigma,\tau\rangle$, $\rho\in S_p$ una perm. t.c. $\rho\sigma\rho^{-1}=(0\dots p-1)$
Allora $\rho H\rho^{-1} = \langle\rho\sigma\rho^{-1}, \rho\tau\rho^{-1}\rangle = \langle(0\dots p-1), \underbrace{\rho\tau\rho^{-1}}_{=\tau'}\rangle$ trasposizione

$= S_p$ ← x ho la tesi

$\Rightarrow H = \rho^{-1}S_p\rho = S_p$. $\square$

Sia $\tau = (a, b)$. Osservo che $H = \langle (0, \dots, p-1), \tau \rangle$ contiene

$$\underset{\substack{\| \\ (a+1,\, b+1)}}{\sigma \tau \sigma^{-1}}, \quad \underset{\substack{\| \\ (a+2,\, b+2)}}{\sigma^2 \tau \sigma^{-2}}, \quad \dots, \quad \underset{\substack{\| \\ (0,\, b-a) \,=:\, \alpha \\ \| \\ (0,\, K)}}{\sigma^{-a} \tau (\sigma^{-a})^{-1}}$$

Dunque $\alpha \in H$. In H ci sono anche

$$\sigma^K \alpha\, \alpha^{-K} = (K, 2K)$$
$$\sigma^{2K} \alpha\, \alpha^{-2K} = (2K, 3K)$$

$\Rightarrow$ In H ci sono tutte le trasp. del tipo $(iK, (i+1)K)$ dove tutto è modulo p e $K = b - a \neq 0$ in $\mathbb{Z}/_p\mathbb{Z}$, dunque $K \in (\mathbb{Z}/_p\mathbb{Z})^\times$.

Ora per induzione in H ci sono le trasp. $(0, iK)$:

- $(0, K) \in H$
- $(0, (i+1)K) = (iK, (i+1)K)(0, iK)(iK, (i+1)K)^{-1}$

$\to$ K è invertibile!

Ora scegliamo i t.c. $iK \equiv 1\ (p)$. Allora $(0, iK) = (0, 1) \in H$.

$\Rightarrow (0,1), (0, \dots, p-1) \in H$

$\Rightarrow \langle (0,1), (0, \dots, p-1) \rangle < H$

$\Rightarrow H = S_p$. $\blacksquare$

TEOREMA A_n è semplice $\forall n \geq 5$.

DIM Per induzione su n.

[BASE] $n = 5$, già fatto

[IND] Sia $H \triangleleft A_{n+1}$: vogliamo mostrare che $H \in \{ \{id\}, A_{n+1} \}$.

Siano $R_1, \dots, R_{n+1}$ i sottogruppi di A_n dati da

$$R_i = \{ \sigma \in A_{n+1} : \sigma(i) = i \}$$ $\to$ permutazioni di A_n che fissano i

Ognuno di questi $R_i \simeq A_n$.

[Per es. R_{n+1} contiene tutte e sole le perm. pari che fissano $n+1$, cioè che agiscono solo su $\{1, \dots, n\}$ $\to A_n$!
Stessa cosa se prendo R_i: è come se A_n agisse su $\{1, \dots, i-1, i+1, \dots, n\}$.]

Infatti l'omomorfismo $A_n \longrightarrow A_{n+1}$ è iniettivo e ha
$\sigma \longmapsto \sigma \cdot (n+1)$

come immagine esattamente R_{n+1}. D'altra canto l'azione di A_{n+1} su $\{1, \dots, n+1\}$ è transitiva;

[devo far vedere che $\forall a, b \in \{1, \dots, n+1\}$ $\exists \sigma \in A_{n+1}$ t.c. $b = \sigma(a)$. Ma allora basta prendere
$\sigma = (a\, b)(c\, d)$ con $c, d \in \{1, \dots, n+1\} \setminus \{a, b\}$.]

Allora $R_{n+1} = \mathrm{Stab}(n+1)$ per quest'azione;
$R_i = \mathrm{Stab}(i)$ " " "

Siccome l'azione è trans. gli stab. sono coniugati e quindi isomorfi.

Consideriamo $H \cap R_i \overset{(**)}{\trianglelefteq} R_i \simeq A_n$. Per hp induttiva A_n è semplice, dunque $H \cap R_i = R_i$ oppure $\{id\}$.

Inoltre $\forall i$ $\exists \sigma_i \in A_{n+1}$ t.c. $\sigma_i R_1 \sigma_i^{-1} = R_i$.

Allora $\sigma_i (H \cap R_1) \sigma_i^{-1} \overset{(*)}{=} \sigma_i H \sigma_i^{-1} \cap \sigma_i R_1 \sigma_i^{-1}$
$= H \cap R_i$

Allora $H \cap R_1 = \{id\} \Rightarrow H \cap R_i = \{id\}$; $\rightarrow$ le int. sono tutte banali

$H \cap R_1 = R_1 \Rightarrow H \cap R_i = R_i$; $\rightarrow$ oppure $H \geq R_i \;\; \forall i$

[(*) $\sigma(H \cap R)\sigma^{-1} = \sigma H \sigma^{-1} \cap \sigma R \sigma^{-1}$
Infatti:
[$\subseteq$] $g \in H \cap R$, $\sigma g \sigma^{-1} \in \sigma (H \cap R) \sigma^{-1}$
Allora $\sigma g \sigma^{-1} \in \sigma H \sigma^{-1}$
$\sigma g \sigma^{-1} \in \sigma R \sigma^{-1}$
dunque $\sigma g \sigma^{-1} \in \sigma H \sigma^{-1} \cap \sigma R \sigma^{-1}$
[$\supseteq$] Supponiamo $\sigma h \sigma^{-1} = \sigma r \sigma^{-1}$
ma allora $h = r \in H \cap R$
dunque $\underset{= \sigma r \sigma^{-1}}{\sigma h \sigma^{-1}} \in \sigma (H \cap R) \sigma^{-1}$
È vero per qualsiasi automorfismo!]

[(**) $H \trianglelefteq G$, $H \cap R \trianglelefteq R$
Vogliamo far vedere che $r(H \cap R) r^{-1} = H \cap R$.
Ma per conto fatto in (*) $r(H \cap R) r^{-1}$
$\underset{\text{è normale}}{H} \cap \underset{r \in R}{R} = rHr^{-1} \cap rRr^{-1}$]

Caso 2: in H ci sono tutte le permutazioni che fissano almeno 1 elemento.

Siccome $n+1 \geq 6$, ogni $(a, b)(c, d)$ con $a \neq b$, $c \neq d$ sta in H (fissa almeno 2 el)

Ma l'insieme di questi prodotti genera A_{n+1}:
una permutazione pari $\sigma \in A_{n+1}$ si scrive come prodotto di un n° pari di trasposizioni
$\Rightarrow \sigma = (\tau_1 \tau_2)(\tau_3 \tau_4) \cdots (\tau_{2k-1} \tau_{2k}) \in H$.
$\Rightarrow H = A_{n+1}$.

Caso 1: ogni permutazione in H (tranne id) non ha punti fissi.

Sia ora $\sigma \in H$, $\sigma = (c_1)(c_2) \cdots (c_k)$

$$l_1 \le l_2 \le \cdots \le l_k$$

Sia $l := \min\{l_1, \dots, l_k\} = l_1$. Considero

$$\sigma^l = \underbrace{(c_1)^{l_1}}_{l_1 \text{ punti fissi}} (c_2)^{l_1} \cdots (c_k)^{l_1}$$

Ma l'unico el. di H con p.ti fissi, $\sigma^l = id$. Ma allora anche $(c_i)^{l_1} = id \Rightarrow$ tutti i cicli sono lunghi uguali (l).

Vorrei mostrare che $l = 1$.

Supponiamo $l \ge 4$: $(c_1) = (a_1\ a_2\ a_3\ a_4 \dots)$

Costruiamo $\tau \in A_{n+1}$ t.c. $\tau\sigma\tau^{-1}\sigma^{-1} \ne id$ ma abbia un pto fisso.

Questo sarebbe assurdo perché dato che $H \triangleleft A_{n+1}$, $\tau\sigma\tau^{-1} \in H$

$\Rightarrow (\tau\sigma\tau^{-1})\sigma^{-1} \in H \Rightarrow$ ho trovato una perm. in $H \ne id$ ma con punti fissi.

Prendiamo $\tau = (a_1\ a_2)(a_3\ a_4)$, allora

ES con $l = 4$:

$\tau\sigma\tau^{-1}\sigma^{-1}$ lascia invariati tutti gli el di $(c_2)(\cdots)(c_k)$ e questi sono almeno 2

D'altro canto $\tau\sigma\tau^{-1}\sigma^{-1} \ne id$ poiché σ e τ non commutano:

ad es $\tau\sigma\tau^{-1}\sigma^{-1}(a_2) = \tau\sigma\tau^{-1}(a_1) = \tau\sigma(a_2) = \tau(a_3) = a_4$

Se $l > 4$: $\tau\sigma\tau^{-1}\sigma^{-1}$ lascia fissi tutti i pti di $c_1 \ne a_1 \dots a_4$

Restano da fare $l = 2$, $l = 3$ ma si fa allo stesso modo (diversa τ).

$l = 2$: $\sigma = (a_1\ a_2)(a_3\ a_4)(\dots\dots)$

$\tau = (a_1\ a_2\ a_3\ a_4)$ $\quad$ $\tau\sigma\tau^{-1}\sigma^{-1}$ lascia fissi tutti i pti dopo

$\tau\sigma\tau^{-1} = (a_2\ a_3)(a_4\ a_1)(\dots) \ne \sigma$

$l = 3$: $\sigma = (a_1\ a_2\ a_3)(\dots\dots)$ $\quad$???

$\tau = (a_1$

Ne deduciamo $H = \{id\}$.

COR (sgrp. normali di S_n, $n \geq 5$)

Se $H \trianglelefteq S_n$, $n \geq 5$, allora $H \in \{\{id\}, A_n, S_n\}$.

DIM Sia $K = H \cap A_n \trianglelefteq A_n$. Allora K $\begin{cases} \{e\} & ① \\ A_n & ② \end{cases}$

Nel caso ②, $A_n \subseteq H$,

$$\underbrace{A_n \overset{d_1}{<} H \overset{d_2}{<} S_n}_{2}$$

$d_1 d_2 = 2$

$\Rightarrow d_1 = 1$ $(H = A_n)$

oppure $d_2 = 1$ $(H = S_n)$

[Alt. i sgrp. di S_n contenenti A_n sono in bij. con i sgrp. di $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z} \Rightarrow$ fine]

Nel caso ①, $H \cap A_n = \operatorname{Ker} \operatorname{sgn}|_H$. Per il primo teo di isom.

$$\operatorname{sgn}|_H : H \to \mathbb{Z}/2\mathbb{Z}$$

si ha che $\dfrac{|H|}{|\operatorname{Im} \operatorname{sgn}|_H|} = |H \cap A_n| \Rightarrow |H| = \begin{cases} |H \cap A_n| = 1 \Rightarrow H = \{id\} \\ 2|H \cap A_n| = 2 \end{cases}$

$\Downarrow$ vogliamo escluderlo

Se $|H| = 2$ so che $H \subseteq Z(S_n)$, ma il centro di S_n è id, assurdo.

$$\begin{aligned} S_n &\xrightarrow{\Phi} \operatorname{Aut}(H) \quad \text{con } \operatorname{Ker}\Phi = Z_{S_n}(H) \\ g &\longmapsto \varphi_g|_H \qquad \overset{\shortparallel}{\{e\}} \end{aligned}$$

$\Rightarrow \operatorname{Ker}\Phi \simeq S_n \Rightarrow H \subseteq Z(S_n)$

$\operatorname{Ker}\Phi = Z_{S_n}(H)$

E S_4? Prendiamo $V = \{ id, (12)(34), (13)(24), (14)(23) \}$

$$\simeq \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z} \triangleleft S_4$$

- $S_4 \overset{?}{\simeq} V \rtimes H$?

$$|S_4| = |V| \cdot |H| \Rightarrow |H| = 6 \Rightarrow H \simeq \mathbb{Z}/_6\mathbb{Z} \text{ o } H \simeq S_3$$

Se fosse $\mathbb{Z}/_6\mathbb{Z}$, allora ci dovrebbe essere un el. di ordine 6 $\Rightarrow$ 6-cicli oppure $3+2 \Rightarrow$ NO: non sono in S_4

Per avere il semidir., $H \cap V = \{id\}$

Potremmo prendere $H = \langle (1\,2\,3), (1\,2) \rangle \simeq S_3$

$$\| $$

$$\mathrm{Stab}(4) = \{ \sigma \in S_4 : \sigma(4) = 4 \}$$

È evidente che $H \cap V = \{id\}$ poiché ogni perm. in V muove 4

$\Rightarrow$ Teorema di decomposizione: $S_4 \simeq V \rtimes H \simeq (\mathbb{Z}/_2\mathbb{Z})^2 \rtimes_\varphi S_3$

$$\varphi : S_3 \longrightarrow \mathrm{Aut}((\mathbb{Z}/_2\mathbb{Z})^2) \simeq S_3 \ ?$$

Basta seguire le identificazioni:

$$V \overset{\sim}{\longleftrightarrow} \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z} \qquad S_3 \overset{\sim}{\longleftrightarrow} H$$

$$(12)(34) \longmapsto (1,0) \qquad \sigma \longmapsto \sigma \cdot (4)$$

$$(13)(24) \longmapsto (0,1)$$

$$(14)(23) \longmapsto (1,1)$$

Chi è $\varphi((1\,2)) \in \mathrm{Aut}((\mathbb{Z}/_2\mathbb{Z})^2)$?

$$(12)(12)(34)(12) = (12)(34) \quad \leftarrow \text{fissato} \qquad (1,0)$$

$$(12)(13)(24)(12) = (23)(14) \qquad (1,1)$$

$$(12)(14)(23)(12) = (24)(13) \qquad (0,1)$$

scambiati!

Nel prod. semidir. esterno

$$\varphi((12)) = \left\{ \begin{array}{l} (1,0) \longmapsto (1,0) \\ (0,1) \longmapsto (1,1) \end{array} \right\}$$

— o — o —

Altro semidiretto

$$G = \left(\{ ax+b \; : \; a \in \mathbb{F}_p^\times, \; b \in \mathbb{F}_p \}, \circ \right)$$

G è un gruppo : · tutti gli el. sono invertibili

· la composizione è interna

· $f = ax+b \qquad g = cx+d \quad \Rightarrow \quad g \circ f = g(ax+b)$

$$= c(ax+b)+d$$

$$= \underbrace{ac}_{\in \mathbb{F}_p^\times} x + bc + d$$

· $f = ax+b$, $f^{-1} = cx+d$

dove $\begin{cases} ac \equiv 1 \; (p) \\ bc+d \equiv 0 \; (p) \end{cases}$

$$\Rightarrow \begin{cases} c \equiv a^{-1} \; (p) \\ d \equiv -ba^{-1} \; (p) \end{cases}$$

Se rappresentiamo $ax+b \longleftrightarrow (a,b) \in \overbrace{\mathbb{F}_p^\times \times \mathbb{F}_p}^{\text{come insieme}}$

$$(a,b) \circ (c,d) = (\underbrace{ac}_{\text{op. normale}}, \underbrace{bc+d}_{\text{mah!}})$$

1° PUNTO DI VISTA : G contiene

$$M = \{ ax \; : \; a \in \mathbb{F}_p^\times \} \simeq \mathbb{F}_p^\times \qquad T = \{ x+b \; : \; b \in \mathbb{F}_p \} \simeq \mathbb{F}_p$$

$M \cap T = \{ id \}$. Inoltre $T \trianglelefteq G$:

$$(ax+b)(x+q)(ax+b)^{-1} = (ax+b)(x+q)(a^{-1}x - a^{-1}x)$$

$$= (ax+b)(a^{-1}x + q - a^{-1}b)$$

$$= a(a^{-1}x + q - a^{-1}b) + b = x + aq \in T$$

Inoltre $p \cdot (p-1) = |G| = |MT| = |M| \cdot |T| = p(p-1)$

Conclusione: $G \simeq T \rtimes M \simeq \mathbb{F}_p \rtimes \mathbb{F}_p^\times$

2° PUNTO DI VISTA: $(a, b) \circ (c, d) = (ac, bc + d)$

Osservo che c'è un omom. ovvio $\varphi: \mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$

$m \longmapsto (t \mapsto mt)$

Allora $\mathbb{F}_p \rtimes_\varphi \mathbb{F}_p^\times \ni (b, a)$ e (d, c)

$$(b, a) \star (d, c) = (d + \varphi(c)(b), ac)$$

PRIMA APPL DEI TEOREMI DI SYLOW

Classificare i gruppi di ordine $45 = 3^2 \cdot 5$.

SOL. Consideriamo i 3-Sylow di G: per i Teoremi di Sylow

$n_3 \mid 5$ e $n_3 \equiv 1 \ (3) \Rightarrow n_3 = 1$

Segue dunque che esiste un solo 3-Sylow ed è normale in G

Sia $P_3 \lhd G$ il 3-Sylow di G.

Consideriamo ora i 5-Sylow di G: $n_5 \mid 9$ e $n_5 \equiv 1 \ (5)$

$n_5 = 1, \cancel{3}, \cancel{9}$

$\Rightarrow P_5 \lhd G$.

Allora $P_3 \cap P_5 = \{id\}$ per questioni di ordine,

$|P_3 P_5| = |G|$

$\Rightarrow G \simeq P_3 \times P_5$

Dato che $|P_3| = 9$ segue che P_3 è abeliano $\Rightarrow P_3 \simeq (\mathbb{Z}/3\mathbb{Z})^2$ o $\mathbb{Z}/9\mathbb{Z}$

$\Rightarrow$ Gli unici gruppi di ord 45 sono $\mathbb{Z}/45\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ ■