Esercizi sulle permutazioni (tratti dalle tracce d'esame)

Traccia del 25 settembre 2020

(a) L'intersezione cercata, in quanto sottogruppo di gruppi ciclici, è un sottogruppo ciclico di S_{18}. Sia α un suo generatore. Poiché α appartiene ad ognuno dei tre sottogruppi assegnati, sarà una potenza di ognuno dei loro generatori, ossia esisteranno numeri interi s, t, r tali che $\alpha = \sigma^s = \tau^t = \rho^r$. Condizioni su questi esponenti emergono dal confronto tra le orbite delle permutazioni assegnate e delle loro potenze. Sia k un intero.
L'orbita di 1

- sotto l'azione di σ^k o ρ^k è
  - $\{1, 2, 3\}$, se 3 non divide k;
  - $\{1\}$ se 3 divide k.

- sotto l'azione di τ^k è
  - $\{1, 2, 3, 4, 5, 6, 7\}$ se 7 non divide k;
  - $\{1\}$ se 7 divide k.

Da questo primo confronto ricaviamo che l'orbita di 1 sotto l'azione di α, dovendo rientrare contemporaneamente in entrambe le classificazioni, è necessariamente $\{1\}$. Ne ricaviamo una prima condizione su s, t, r:

(1) $s = 3h$, $t = 7k$, $r = 3\ell$, per opportuni interi h, k, ℓ.

Ne consegue che l'intersezione cercata è $\langle\alpha\rangle = \langle\sigma^3\rangle \cap \langle\tau^7\rangle \cap \langle\rho^3\rangle$, ove

$$\sigma^3 = (4, 7, 6, 5)(8, 11, 9, 12, 10)(13, 14)(15, 16)(17, 18)$$
$$\tau^7 = (8, 10, 12, 9, 11)(13, 16, 15, 14)(17, 18)$$
$$\rho^3 = (4, 7, 5, 8, 6)(9, 12, 11, 10)(13, 16, 14, 15)(17, 18)$$

Ora: τ^7, insieme ad ogni sua potenza, lascia fisso l'elemento 4. Ciò vale dunque per $\alpha = \left(\sigma^3\right)^h = \left(\tau^7\right)^k = \left(\rho^3\right)^\ell$. Di conseguenza, tenendo conto delle lunghezze delle orbite di 4 sotto l'azione di σ^3 e di ρ^3, si ha

(2) $h = 4u, \ell = 5v$, per opportuni interi u, v.

Ne consegue che l'intersezione cercata è $\langle\alpha\rangle = \langle\sigma^{12}\rangle \cap \langle\tau^7\rangle \cap \langle\rho^{15}\rangle$. D'altra parte, essendo $o(\sigma) = \text{mcm}(5, 4, 3, 2) = 60$, si ha

$$o\left(\sigma^{12}\right) = \frac{o(\sigma)}{\text{MCD}(o(\sigma), 12)} = \frac{60}{\text{MCD}(60, 12)} = 5.$$

Un calcolo analogo fornisce

$$o\left(\tau^7\right) = 20$$
$$o\left(\rho^{15}\right) = 4$$

Ora, però, per il Teorema di Lagrange, $o(\alpha)$ divide ognuno di questi tre periodi, e quindi divide $\text{MCD}(5, 20, 4) = 1$. Ne consegue che $o(\alpha) = 1$, ossia α è la permutazione identica. In conclusione, l'intersezione cercata è il sottogruppo banale.

(b) La risposta è **banale**. Basta prendere S_{18} stesso. Questo gruppo non è ciclico, perché non è commutativo.

Variante 1**:** Cerchiamo H ciclico. **(difficoltà media)**

Si determinano potenze $\gamma_1, \gamma_2, \gamma_3$ di $\sigma, \tau,\ \rho,$ rispettivamente, che non siano la permutazione identica e siano a due a due disgiunte. Allora l'insieme

$$H = \{\gamma_1^a \gamma_2^b \gamma_3^c \mid a, b, c \in \mathbb{Z}\}$$

è un sottogruppo (commutativo) di S_{18}. Inoltre, poiché, per ogni $i \in \{1,2,3\},\ \gamma_i \in H,$ è verificata anche la condizione sulle intersezioni. Si può prendere

$$\gamma_1 = (1,2,3) = \sigma^{40}$$
$$\gamma_2 = (13,14,15,16)(17,18) = \tau^{105}$$
$$\gamma_3 = (4,5,6,7,8) = \rho^{36}$$

Questi esponenti sono stati ricavati applicando il procedimento risolutivo contenuto nella dimostrazione del Teorema Cinese del Resto (prima formulazione). Precisamente, per ottenere il primo, si è trovata una soluzione particolare del seguente sistema di congruenze:

$$\begin{cases} x & \equiv & 1 \pmod 3 \\ x & \equiv & 0 \pmod 4 \\ x & \equiv & 0 \pmod 5 \end{cases}$$

(La soluzione 40 si può ricavare anche più velocemente, individuando, tra gli interi positivi, il più piccolo multiplo di 20 che sia congruo ad 1 modulo 3).

In maniera analoga si procede per ricavare i restanti due esponenti, a partire dai sistemi

$$\begin{cases} x & \equiv & 1 \pmod 4 \\ x & \equiv & 0 \pmod 5 \\ x & \equiv & 0 \pmod 7 \end{cases}$$

e

$$\begin{cases} x & \equiv & 1 \pmod 5 \\ x & \equiv & 0 \pmod 3 \\ x & \equiv & 0 \pmod 4 \end{cases}$$

Infine, H è ciclico, in quanto è generato da $\alpha = \gamma_1\gamma_2\gamma_3$. Infatti l'inclusione $\langle\alpha\rangle \subset H$ è banale, per l'inclusione $H \subset \langle\alpha\rangle,$ basta osservare che ciascuno dei γ_i appartiene ad $\langle\alpha\rangle$, in quanto

$$\gamma_1 = \alpha^{40},\ \gamma_2 = \alpha^{45},\ \gamma_3 = \alpha^{36}.$$

La ciclicità di H, ossia la possibilità di reperire gli esponenti precedenti (tramite il Teorema Cinese del Resto) **deriva dal fatto che i periodi di** γ_1, γ_2 **e** γ_3 **sono a due a due coprimi.**

Variante 2**:** Cerchiamo H commutativo e non ciclico. **(difficoltà elevata)**

La costruzione del sottogruppo è basata sul procedimento precedente. Si considerano tre permutazioni δ_1, δ_2 e δ_3 a due a due disgiunte e si definisce l'insieme

$$H = \{\delta_1^a \delta_2^b \delta_3^c \mid a, b, c \in \mathbb{Z}\}.$$

Questo sarà un sottogruppo commutativo di S_{18}. Non sarà ciclico se i periodi di δ_1, δ_2 e δ_3 non sono a due a due coprimi. Inoltre, onde soddisfare la condizione sulle intersezioni, queste permutazioni dovranno essere scelte in modo che potenze non banali di σ, τ, ρ appartengano ad H. Una possibilità consiste nel prendere

$$\delta_1 = (1,2,3) = \sigma^{40} = \rho^{40}$$
$$\delta_2 = (13,14,15,16)$$
$$\delta_3 = (17,18)$$

ove $\delta_2\delta_3 = \tau^{105}$.

Allora $|H| = 3 \cdot 4 \cdot 2 = 24$, mentre il periodo di ogni elemento di H è al più 12.

<u>Traccia dell'11 settembre 2020</u>

(a) Sia α un generatore del sottogruppo intersezione cercato, e siano s, t interi tali che $\alpha = \sigma^s = \tau^t$. Allora $o(\alpha)$ divide

$$o(\sigma) = \mathrm{mcm}(9,5,4,3) = 180$$
e
$$o(\tau) = \mathrm{mcm}(6,3) = 6$$

e dunque divide $\mathrm{MCD}(180,6) = 6$. Ora

$$o(\sigma^s) = \frac{180}{\mathrm{MCD}(180,s)}$$ divide 6 se e solo se s è multiplo di 30, diciamo $30h$. Dunque $\langle\alpha\rangle = \langle\sigma^{30}\rangle \cap \langle\tau\rangle$, ove

$$\sigma^{30} = (6,8)(7,9)(13,16,19)(14,17,20)(15,18,21).$$

Confrontando le orbite di 6 sotto l'azione di σ^{30} e di τ si conclude che, sotto l'azione di α, tale orbita deve essere banale. Quindi t è multiplo di 6. Ma $\tau^6 = id$. Ciò prova che l'intersezione cercata è il gruppo banale.

(b) Si ricordi che ogni permutazione commuta con ognuno dei suoi cicli, e dunque con tutti i loro prodotti e tutte le loro potenze. In particolare,

- $\gamma = (13,14,15,16,17,18,19,20,21)$ commuta con σ;
- $\delta = (13,14,16,17,19,20)$ commuta con τ.

Consideriamo le loro seguenti potenze:

$$\gamma^3 = (13,16,19)(14,17,20)(15,18,21),$$
$$\delta^2 = (13,16,19)(14,17,20).$$

In base a quanto ricordato sopra, γ^3 commuta con σ e δ^2 commuta con τ. Ma con τ commuta anche $(15,18,21)$, essendo un suo ciclo. Quindi con τ commuta anche $\gamma^3 = \delta^2(15,18,21)$. Infine, con σ e τ commuta $\varepsilon = (10,11,12)$, ciclo associato ad entrambe. Commutano quindi con σ e τ tutti gli elementi dell'insieme

$$H = \{ \left(\gamma^3\right)^a \varepsilon^b \mid a, b \in \mathbb{Z} \}.$$

Questo è un sottogruppo di S_{21}, dato che γ^3 ed ε sono permutazioni disgiunte. Non è però ciclico, in quanto il suo ordine è $o\left(\gamma^3\right)o(\varepsilon) = 3^2 = 9$, mentre ogni suo elemento diverso dalla permutazione identica, essendo un prodotto di 3-cicli disgiunti, ha periodo 3.

Traccia del 17 febbraio 2020

(a) Il centralizzante di un elemento in un gruppo è sempre un sottogruppo del gruppo. Ora, $C(\sigma)$ non è commutativo, in quanto vi appartengono i seguenti due elementi, che non commutano:

$$\alpha = (1, 2, 3, 4)$$
$$\beta = (1, 5, 2, 6, 3, 7, 4, 8)$$

Il primo elemento è un ciclo di σ, il secondo è tale che $\beta^2 = (1, 2, 3, 4)(5, 6, 7, 8)$, che è il prodotto di due cicli di σ. Ora: β commuta con ogni sua potenza, e quindi, in particolare, con questo prodotto. Ma commuta anche con i restanti cicli di σ, in quanto è da essi disgiunto, e dunque commuta con σ. Ciò prova che $\alpha, \beta \in C(\sigma)$. Per provare che $\alpha\beta \neq \beta\alpha$ è sufficiente osservare che $\alpha\beta(1) = 5$, mentre $\beta\alpha(1) = 6$.

(b) Abbiamo osservato che β commuta con σ. Analogamente si prova che $\gamma = (9, 11, 13, 10, 12, 14)$ commuta con σ: basta osservare che $\gamma^3 = (9, 10)(11, 12)(13, 14)$, prodotto di cicli di σ. Ora β e γ sono permutazioni disgiunte, di ordini 8 e 6 rispettivamente. Ne consegue che l'insieme

$$H = \{\beta^b \gamma^c \mid b, c \in \mathbb{Z}\}$$

è un sottogruppo di S_{16} di ordine $8 \cdot 6 = 48$, contenuto in $C(\sigma)$.

(c) Consideriamo un 16-ciclo τ tale che $\tau^2 = \tau_1\tau_2$, ove τ_1, τ_2 sono 8-cicli tali che

- $\tau_1 = \beta$
- $\tau_2^4 = (9, 10)(11, 12)(13, 14)(15, 16)$

Allora

- τ_1 commuta con β^2 ed è disgiunto dai restanti cicli di σ;
- τ_2 commuta con $(9, 10)(11, 12)(13, 14)(15, 16)$ ed è disgiunto dai restanti cicli di σ.

Quindi τ_1, τ_2 commutano con σ, insieme al loro prodotto. Ciò prova che τ^2 è un elemento di $C(\sigma)$, e dunque appartiene all'intersezione $\langle\tau\rangle \cap C(\sigma)$, che, pertanto, risulta non banale. Resta da esibire una permutazione τ soddisfacente le condizioni indicate all'inizio. Anzitutto osserviamo che possiamo prendere $\tau_2 = (9, 11, 13, 15, 10, 12, 14, 16)$. E si ha che

$\tau^2 = (1, 5, 2, 6, 3, 7, 4, 8)(9, 11, 13, 15, 10, 12, 14, 16)$ se

$$\tau = (1, 9, 5, 11, 2, 13, 6, 15, 3, 10, 7, 12, 4, 14, 8, 16).$$

Traccia del 31 gennaio 2020

(a) Si ha $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. La somma di questi fattori primi è 41. Detta $(\ell_1, \cdots, \ell_r)$ la struttura ciclica di τ, si deve dunque avere contemporaneamente

(1) $41 = \ell_1 + \cdots + \ell_r$ e $30030 = \mathrm{mcm}(\ell_1, \cdots, \ell_r)$.

Ora, ogni ℓ_i , in quanto divisore di 30030, è prodotto di alcuni fattori della sua fattorizzazione. Sia questa $p_1 \cdots p_r$. Ma se, per qualche i, ℓ_i fosse il prodotto di più primi, diciamo $\ell = p_1 \cdots p_s$, con $s > 1$, sarebbe $\ell_i > p_1 + \cdots + p_s$: poiché la somma dei restanti addendi della (1) è maggiore o uguale a $p_{s+1} + \cdots + p_r$, il secondo membro sarebbe maggiore di 41, una contraddizione.
Ora, elevando τ a potenza, ognuno dei suoi cicli associati, che hanno tutti come lunghezza un numero primo, manterrà la sua lunghezza oppure diventerà la permutazione identica. Dunque, per ogni potenza di τ, i cicli associati non banali avranno lunghezze a due a due distinte, appartenenti all'insieme $\{\ell_1, \cdots \ell_r\}$. Invece, le struttture cicliche delle potenze di σ diverse dalla permutazione identica sono le seguenti:

(14)
$(7, 7)$
$(2, 2, 2, 2, 2, 2, 2)$

Nessuna di queste può essere la struttura ciclica di una potenza di τ distinta dalla permutazione identica. Ciò prova che l'unica permutazione che sia contemporaneamente una potenza di σ e di τ è la permutazione identica. In altri termini, $\langle\sigma\rangle \cap \langle\tau\rangle$ è il sottogruppo banale.

(b)

Primo metodo:

Si noti preliminarmente che $4290 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$. Consideriamo una permutazione della forma seguente:
$\tau = (1, 2, 3, 4, 5, 6, 7)\gamma_1 \cdots \gamma_5$, essendo i γ_i i cicli di τ di lunghezze $2, 3, 5, 11, 13$.
Poiché $4290 \equiv -1 \pmod 7$, si ha

$$\tau^{4290} = (1, 2, 3, 4, 5, 6, 7)^{-1} = (1, 7, 6, 5, 4, 3, 2).$$

Ora, σ^2 è il prodotto di due 7-cicli disgiunti. Di conseguenza, σ commuterà con τ^{4290} se uno di questi due cicli è uguale a τ^{4290}, ad esempio se

$$\sigma^2 = (1, 7, 6, 5, 4, 3, 2)(8, 9, 10, 11, 12, 13, 14).$$

Si ha questa uguaglianza se

$$\sigma = (1, 8, 7, 9, 6, 10, 5, 11, 4, 12, 3, 13, 2, 14).$$

Secondo metodo:

Basta prendere σ e τ in modo che σ^2 e τ^{4290} siano disgiunte. Ciò avviene, ad esempio, se $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)$ e il 7-ciclo di τ è $(15, 16, 17, 18, 19, 20, 21)$.

Traccia del 15 gennaio 2020

(a) Osservando le orbite di σ e di τ si conclude che le permutazioni σ^m e τ^n **non** sono disgiunte se e solo se

$(4 \nmid m$ e $5 \nmid n)$ oppure $(3 \nmid m$ e $5 \nmid n)$ oppure $(3 \nmid m$ e $6 \nmid n)$ oppure $(2 \nmid m$ e $6 \nmid n)$.

Pertanto, saranno disgiunte se e solo se

$(4 | m$ oppure $5 | n)$ e $(3 | m$ oppure $5 | n)$ e $(3 | m$ oppure $6 | n)$ e $(2 | m$ oppure $6 | n)$.

Le coppie cercate sono pertanto quelle elencate qui sotto, al variare di $s, t \in \mathbb{Z}$:

$(12s, t), (6s, 5t), (s, 30t)$.

(b) Dal confronto tra le orbite di σ e τ è facile dedurre che l'intersezione è il sottogruppo banale.

(c) Ad H appartengono gli elementi

$\sigma^4 = (5,6,7)$
$\tau^6 = (1,2,3,4,5)$

Quindi vi appartiene anche il loro prodotto

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

Traccia del 15 novembre 2019

(a) Le potenze di σ con esponente dispari inviano 1 in 2, quelle con esponente pari inviano 1 in sé stesso. Quindi $H = \{\sigma^{2s} \mid s \in \mathbb{Z}\} = \langle \sigma^2 \rangle$.

(b) Ogni potenza di τ invia 8 in uno degli elementi dell'insieme $\{8, 9, 10, 11, 12\}$ $(= \Omega_\tau(8))$. Lo invia in sé stesso se e solo se l'esponente è multiplo di 5. Quindi $K = \{\tau^{5t} \mid t \in \mathbb{Z}\} = \langle \tau^5 \rangle$.

(c) Si ha

$\sigma^2 = (3,5,4)(6,8,10,12,7,9,11)$
$\tau^5 = (1,3,2)(4,5,6,7)$

Poiché $o(\sigma^2) = 21$, $o(\tau^5) = 12$, l'ordine del sottogruppo intersezione (che è ciclico) è un divisore di 3. Ma non può essere esattamente 3, poiché l'unico sottogruppo di $\langle \sigma^2 \rangle$ avente ordine 3 è $\langle (3,5,4) \rangle$, distinto da $\langle (1,3,2) \rangle$, unico sottogruppo di $\langle \tau^5 \rangle$ avente ordine 3. Dunque l'intersezione è il sottogruppo banale.

Traccia del 25 settembre 2019

(a) Si ha $\sigma^2 \alpha = \sigma(\alpha \sigma^2) = (\sigma\alpha)\sigma^2 = (\alpha\sigma^2)\sigma^2 = \alpha\sigma^4$. In generale, per induzione, si prova che, per ogni intero positivo n, $\sigma^n \alpha = \alpha \sigma^{2n}$. Se σ fosse di periodo pari, diciamo $2s$, allora si avrebbe $\sigma^{2s} = id$, e dunque $\sigma^s \alpha = \alpha$, da cui, per cancellazione, $\sigma^s = id$. Ma ciò è in contraddizione con l'ipotesi sul periodo.

(b) Si ha $H((1,2)) = \{\sigma \in S_4 \mid \sigma(1,2) = (1,2)\sigma^2\}$. Inoltre, dal punto (a) sappiamo che ogni elemento di H ha periodo

dispari. Infine, osserviamo che ogni $\sigma \in H$ **è necessariamente pari**, in quanto il prodotto a secondo membro è sempre dispari. Gli elementi di A_4 aventi periodo dispari sono, oltre a id, i cicli di lunghezza 3. Ora, se σ è un 3-ciclo, allora $(1,2)\sigma^2 = (\sigma(1,2))^{-1}$. Quindi $\sigma \in H((1,2))$ se e solo se la permutazione $\sigma(1,2)$ è inversa di sé stessa, ossia, non potendo essere id, se e solo se ha periodo 2, ossia, essendo una permutazione dispari di S_4, se e solo se è una trasposizione. Si ha
$(1,2,3)(1,2) = (1,3)$,
$(1,2,4)(1,2) = (1,4)$.

Ciò prova che $(1,2,3)$ e $(1,2,4)$ sono elementi di $H((1,2))$, ma tale non è, tuttavia, il loro prodotto, che non è un 3-ciclo: $(1,2,3)(1,2,4) = (1,3)(2,4)$. Se ne deduce che $H((1,2))$ non è un sottogruppo di S_4.

(c) In base quanto osservato al punto precedente $H((1,2))$ è contenuto in $A_3 = \langle(1,2,3)\rangle$. D'altra parte, sappiamo già che ad $H((1,2))$ appartengono id e $(1,2,3)$. Poiché, inoltre, $(1,3,2)(1,2) = (2,3)$, possiamo concludere che anche $(1,3,2)$ vi appartiene. Dunque $H((1,2)) = A_3$, sottogruppo di S_3.

Traccia del 10 settembre 2019

(a) In base alla caratterizzazione del periodo, gli elementi di A sono tutte e sole le permutazioni di S_6 il cui periodo è un divisore di $32 = 2^5$. L'insieme complementare è dunque formato dalle permutazioni nella cui struttura ciclica compare un numero (necessariamente minore o uguale a 6) avente un fattore primo distinto da 2. Questo può essere soltanto 3 o 5 e le strutture cicliche interessate sono (6), $(3,3)$, $(3,2,1)$, $(3,1,1,1)$ e $(5,1)$. In base ad una nota formula in S_6 vi sono

- $\frac{1}{6}\frac{6!}{0!} = 5! = 120$ cicli di lunghezza 6;
- $\frac{1}{3}\frac{6!}{3!} = \frac{4 \cdot 5 \cdot 6}{3} = 40$ cicli di lunghezza 3;
- $\frac{1}{5}\frac{6!}{1!} = \frac{720}{5} = 144$ cicli di lunghezza 5.

Il numero delle permutazioni di struttura ciclica $(3,3)$ è sempre 40: lo si ottiene, infatti, moltiplicando il numero dei 3-cicli per 2 (i possibili 3-cicli aventi supporto disgiunto da quello considerato), e dividendo nuovamente per 2 (poiché, data la possibilità di scambiare i due cicli, ogni coppia di 3-cicli viene ottenuta due volte). Le permutazioni di struttura ciclica $(3,2,1)$ sono $40 \cdot 3 = 120$ (ad ogni 3-ciclo si possono abbinare 3 trasposizioni da esso disgiunte). In definitiva

$$|A| = |S_6| - 120 - 40 - 144 - 40 - 120 = 720 - 464 = 256.$$

(b) Una permutazione $\sigma \in S_6$ appartiene a B se e solo se $\sigma^{12} \neq id$. Ciò avviene se e solo se nella struttura ciclica di σ compare un numero la cui fattorizzazione contenga la potenza di un primo distinta da 2, $2^2, 3$. L'unica possibilità è che vi compaia il fattore 5, il che equivale al fatto che σ sia un ciclo di lunghezza 5. Dunque, in base ad un calcolo già effettuato, $|B| = 144$.