Note alla traccia del 1° luglio 2025 - Esercizio 1

(a) Il sottogruppo cercato è ciclico, in quanto sottogruppo di gruppi ciclici. Il suo generatore α, appartenendo sia a $\langle\sigma\rangle$ sia a $\langle\tau\rangle$, è, contemporaneamente, una potenza σ^s di σ e una potenza di τ^t di τ. In particolare, dovrà essere $\Omega_{\sigma^s}(21)=\Omega_{\tau^t}(21)$. Analizziamo separatamente queste orbite. Una volta individuato, nella decomposizione in cicli disgiunti di σ, il ciclo $\gamma_1=(21,22)$, al cui supporto appartiene 21, si avrà che, per ogni intero k, $\Omega_{\sigma^k}(21)=\Omega_{\gamma_1^k}(21)$. Precisamente:

$$\gamma_1^{\,k}=\begin{cases} id & \text{se } k \text{ è pari,}\\ (21,22) & \text{se } k \text{ è dispari}\end{cases} \quad\Rightarrow\quad \Omega_{\gamma_1^k}(21)=\begin{cases} \{21\} & \text{se } k \text{ è pari,}\\ \{21,22\} & \text{se } k \text{ è dispari}\end{cases}$$

Analogamente, guardando al ciclo $\gamma_2=(21,23,22,24)$ di τ, si osserva:

$$\gamma_2^{\,k}=\begin{cases} id & \text{se } k\equiv 0 \pmod 4\\ (21,23,22,24) & \text{se } k\equiv 1 \pmod 4\\ (21,22)(23,24) & \text{se } k\equiv 2 \pmod 4\\ (21,24,23,22) & \text{se } k\equiv 3 \pmod 4\end{cases} \quad\Rightarrow\quad \Omega_{\tau^k}(21)=\begin{cases} \{21\} & \text{se } k\equiv 0 \pmod 4\\ \{21,22,23,24\} & \text{se } k\equiv 1 \pmod 4\\ \{21,22\} & \text{se } k\equiv 2 \pmod 4\\ \{21,22,23,24\} & \text{se } k\equiv 3 \pmod 4\end{cases}$$

Dal confronto tra le orbite si deduce quindi che dovrà essere e $t\equiv 0 \pmod 2$. Ora, però, se t è pari, τ^t lascia fisso l'elemento 1. Ma $\tau^t=\sigma^s$, e $\sigma^s(1)=1$ se e solo se s è multiplo della lunghezza dell'orbita di $\Omega_\sigma(1)=\{1,2,3,4\}$, ossia se e solo se $4\mid s$. Ma allora $\sigma^s(21)=21$. Poiché dovrà essere $\tau^t(21)=21$, ne consegue che $4\mid t$. Pertanto nel sottogruppo intersezione saranno presenti solo potenze di σ e τ con esponenti multipli di 4. In conclusione, il sottogruppo cercato è $\langle\sigma^4\rangle\cap\langle\tau^4\rangle$.

(b) Vale la seguente **proprietà generale**:

> Se $\alpha_1,\alpha_2,\dots,\alpha_k\in S_n$ sono permutazioni <u>a due a due disgiunte</u>, allora l'insieme
>
> $$H=\{\alpha_1^{a_1}\alpha_2^{a_2}\cdots\alpha_k^{a_k}\mid a_1,a_2,\dots,a_k\in\mathbb{Z}\}$$
>
> è un sottogruppo <u>commutativo</u> di S_n di ordine $o(\alpha_1)o(\alpha_2)\cdots o(\alpha_k)$.

Osservazione aggiuntiva: Sia $m = \text{mcm}(o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k))$. Allora, per ogni $\delta \in H$, $\delta^m = id$. Se $o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k)$ non sono a due a due coprimi, allora $m < o(\alpha_1)o(\alpha_2)\cdots o(\alpha_k) = |H|$, e dunque nessun elemento di H ha periodo $|H|$, ossia H non è ciclico. Viceversa, si prova che se $o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k)$ sono a due a due coprimi, allora H è ciclico generato da $\alpha_1\alpha_2\cdots\alpha_k$.