Traccia del 10 settembre 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 20 e di 23 sotto l'azione delle potenze di σ e di τ si deduce che $5|s$ e $6|t$, ossia $s = 5h$, $t = 6k$ per opportuni interi h, k.
Il sottogruppo cercato è dunque $\langle \sigma^5 \rangle \cap \langle \tau^6 \rangle$, dove

$\sigma^5 = (1,2,3,4)(5,6,7,8)(9,10,11,12)(13,18,16,14,19,17,15)$,
$\tau^6 = (1,4,3,2)(5,8,7,6)(9,11)(10,12)(13,18,16,14,19,17,15)$.

Dal confronto tra le orbite di 9 sotto l'azione delle potenze di σ^5 e di τ^6 si deduce ancora che $2|h$, ossia che $s = 10u$, per qualche intero u. Quindi il sottogruppo cercato è $\langle \sigma^{10} \rangle \cap \langle \tau^6 \rangle$, dove

$\sigma^{10} = (1,3)(2,4)(5,7)(6,8)(9,11)(10,12)(13,16,19,15,18,14,17)$.

Dal confronto tra le orbite di 1 sotto l'azione delle potenze di σ^{10} e di τ^6 si deduce inoltre che $2|k$, così che $t = 12v$, per qualche intero v, e il sottogruppo cercato è $\langle \sigma^{10} \rangle \cap \langle \tau^{12} \rangle$, dove

$\tau^{12} = (1,3)(2,4)(5,7)(6,8)(13,16,19,15,18,14,17)$.

Ora, τ^{12}, insieme a tutte le sue potenze, lascia fisso 9. Ma tra le sue potenze si trova, in particolare, $\alpha = \sigma^{10u}$. Ne consegue che $u = 2w$, per qualche intero w e il sottogruppo cercato è $\langle \sigma^{20} \rangle \cap \langle \tau^{12} \rangle$, dove

$\sigma^{20} = (13,19,18,17,16,15,14)$.

Ma allora $\alpha = \tau^{12v}$ deve lasciare fisso 1, ossia $2|v$. Il sottogruppo cercato è dunque $\langle \sigma^{20} \rangle \cap \langle \tau^{24} \rangle$, ove

$\tau^{24} = (13,19,18,17,16,15,14)$.

Ora, $\sigma^{20} = \tau^{24}$ e quindi $\langle \sigma^{20} \rangle = \langle \tau^{24} \rangle$ è il sottogruppo cercato.

(b) Con σ e τ commutano le seguenti permutazioni

- $\alpha = (1,2,3,4)(5,6,7,8)$, che è il prodotto di due cicli di σ, ed è il quadrato del ciclo $(1,5,2,6,3,7,4,8)$ di τ;
- $\beta = (9,10,11,12)$, che è un ciclo di σ e l'inverso di un ciclo di τ.

Pertanto a $C(\sigma) \cap C(\tau)$ appartengono tre elementi di periodo $4:$ $\alpha,\ \beta,\ \alpha\beta$. Tuttavia, $\phi(4) = 2$. Ciò prova che $C(\sigma) \cap C(\tau)$ non è ciclico.

2.

(a) Cerchiamo due omomorfismi di anelli non banali $\varphi_1 : \mathbb{Z}_6 \to \mathbb{Z}_{15}$ e $\varphi_2 : \mathbb{Z}_{12} \to \mathbb{Z}_{10}$ definiti nel modo seguente, per opportuni interi $\lambda, \mu :$

per ogni $a, b \in \mathbb{Z}$, poniamo $\varphi_1([a]_6) = [\lambda a]_{15}$, $\varphi_2([b]_{12}) = [\mu b]_{10}$. Queste applicazioni sono ben definite se e solo se $5|\lambda$ e $5|\mu$. Siano dunque $\lambda = 5s$, $\mu = 5t$. Allora φ_1 e φ_2 conservano il prodotto se e solo se $15|25s^2 - 5s$ e $10|25t^2 - 5t$. La prima condizione è verificata per $s = 2$, la seconda per $t = 1$. Sostituendo questi valori nelle definizioni di φ_1 e φ_2 abbiamo così, per ogni $a, b \in \mathbb{Z}$, $\varphi_1([a]_6) = [10a]_{15}$, $\varphi_2([b]_{12}) = [5b]_{10}$. Queste applicazioni conservano, oltre al prodotto, anche la somma, e sono quindi omomorfismi di anelli, chiaramente non nulli. Tale è dunque anche l'applicazione

$$\varphi = \varphi_1 \times \varphi_2 : \mathbb{Z}_6 \times \mathbb{Z}_{12} \to \mathbb{Z}_{15} \times \mathbb{Z}_{10} \text{ definita ponendo, per ogni } a, b \in \mathbb{Z},\ \varphi([a]_6, [b]_{12}) = ([10a]_{15}, [5b]_{10}).$$

Questo è un omomorfismo del tipo cercato. Lo sono anche le applicazioni definite da $([a]_6, [b]_{12}) \mapsto ([10a]_{15}, [0]_{10})$ e da $([a]_6, [b]_{12}) \mapsto ([0]_{15}, [5b]_{10})$.

(b) La prima parte del punto precedente consente di individuare una classe di omomorfismi di gruppi, formata dalle applicazioni

$$\psi_{s,t} : \mathbb{Z}_6 \times \mathbb{Z}_{12} \to \mathbb{Z}_{15} \times \mathbb{Z}_{10} \text{ definite ponendo, per ogni } a, b \in \mathbb{Z},\ \varphi_1([a]_6, [b]_{12}) = ([5sa]_{15}, [5tb]_{10}).$$

Per $s = t = 1$ si ottiene un omomorfismo il cui nucleo è $\langle [3]_6 \rangle \times \langle [2]_{12} \rangle$, di ordine $2 \cdot 6 = 12$. Allo stesso risultato si perviene anche considerando l'omomorfismo φ del punto precedente, corrispondente a $s = 2$, $t = 1$.

(c) La condizione richiesta sarà soddisfatta da un omomorfismo di anelli $\omega : \mathbb{Z}_{15} \times \mathbb{Z}_{10} \to \mathbb{Z}_6 \times \mathbb{Z}_{12}$ la cui immagine sia $\mathbb{Z}_6 \times \{[0]_{12}\}$. Cerchiamo dunque un'applicazione che, per opportuni interi λ, μ, sia definita come segue:

$$\text{per ogni } a, b \in \mathbb{Z},\quad \omega([a]_{15},\ [b]_{10}) = ([\lambda a + \mu b]_6,\ [0]_{12}).$$

Questa applicazione è ben definita se e solo se $2|\lambda$ e $3|\mu$. Siano allora $\lambda = 2s$ e $\mu = 3t$. La conservazione del prodotto richiede, in particolare, che gli elementi $\omega([1]_{15},\ [0]_{10}) = ([2s]_6,\ [0]_{12})$ e $\omega([0]_{15},\ [1]_{10}) = ([3t]_6,\ [0]_{12})$ siano idempotenti, ossia che $6|4s^2 - 2s$ e $6|9t^2 - 3t$. Ciò si verifica per $s = 2$, $t = 1$. Consideriamo dunque l'applicazione definita ponendo

$$\text{per ogni } a, b \in \mathbb{Z},\quad \omega([a]_{15},\ [b]_{10}) = ([4a + 3b]_6,\ [0]_{12}).$$

Si può facilmente verificare che ω è un omomorfismo di anelli. La sua immagine è contenuta in $\mathbb{Z}_6 \times \{[0]_{12}\}$. D'altra parte, all'immagine appartiene l'elemento $([1]_6,\ [0]_{12})$, e quindi essa contiene il sottogruppo generato da questo elemento, che è, per l'appunto, $\mathbb{Z}_6 \times \{[0]_{12}\}$.

(a) Per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = \alpha^3 + \alpha^2 + \alpha + \overline{1}$. Pertanto $f(\alpha)(\alpha - 1) = \alpha^4 - \overline{1}$. Si osservi che $\overline{1}$ è radice di $f(x)$ e solo se $p = 2$, nel qual caso è anche la sua unica radice. Sia dunque $p > 2$. Allora $f(\alpha) = 0$ se e solo se $\alpha^4 - \overline{1}$ e $\alpha \neq \overline{1}$, ossia se e solo $\alpha = -\overline{1}$ oppure α è un elemento di $\mathbb{Z}_p$ avente periodo 4. Questo secondo caso è possibile se e solo se $p \equiv 1 \pmod 4$, e allora gli elementi di periodo 4 sono esattamente 2. In conclusione,

- $f(x)$ ha tre radici se $p \equiv 1 \pmod 4$;
- $f(x)$ ha una sola radice $(-\overline{1})$ nei restanti casi.

(b) Evidentemente, $\overline{0}$ non è radice di $g(x)$. Sia dunque $\alpha \in \mathbb{Z}_p^*$. Allora, in virtù del Teorema di Eulero, si ha

$$g(\alpha) = \alpha^{(p-1)(p^2+1)} + \alpha - \overline{1} = \left(\alpha^{p-1}\right)^{p^2+1} + \alpha - \overline{1} = \overline{1} + \alpha - \overline{1} = \alpha \neq \overline{0}\ .$$

Ne consegue che $g(x)$ è sempre privo di radici in $\mathbb{Z}_p$.