Traccia del 25 settembre 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Se il suo ordine fosse multiplo di 4, esso conterrebbe un unico sottogruppo di ordine 4, coincidente con l'unico sottogruppo di ordine 4 di $\langle\sigma\rangle$, che è $\langle(1,2,3,4)(5,6,7,8)\rangle$. Questo dovrebbe, contemporaneamente, coincidere con l'unico sottogruppo di ordine 4 di $\langle\tau\rangle$, che è, però, $\langle(1,4,3,2)(5,6,7,8)\rangle$. I due sottogruppi sono distinti, in quanto l'unico elemento del primo a inviare 1 in 2 invia 5 in 6, mentre l'unico elemento del secondo a inviare 1 in 2 invia 5 in 8. Ne consegue che 4 non divide $o(\alpha)$. Ora, poiché $o(\sigma) = \mathrm{mcm}(7,5,4,3)$, in base alla formula del periodo, si ha che $4 \nmid o(\sigma^s) = \dfrac{o(\sigma)}{\mathrm{MCD}(o(\sigma), s)}$ se e solo se $2 \mid s$. Analogamente, ragionando su τ, si deduce che $2 \mid t$. Dunque $s = 2h$, $t = 2k$ per opportuni interi h, k, e il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, dove

$$\sigma^2 = (1,3)(2,4)(5,7)(6,8)(9,11,13,10,12)(14,16,18,20,15,17,19)(21,23,22)(24,26,25),$$
$$\tau^2 = (1,3)(2,4)(5,7)(6,8)(9,13,12,11,10)(14,19,17,15,20,18,16)(21,22,23)(24,25,26).$$

Confrontiamo adesso le decomposizioni di queste due permutazioni. Guardando la decomposizione di σ^2, poniamo $\gamma_1 = (1,3)(2,4)(5,7)(6,8)$, $\gamma_2 = (9,11,13,10,12)$, $\gamma_3 = (14,16,18,20,15,17,19)$, $\gamma_4 = (21,23,22)(24,26,25)$. Constatiamo che

$$\tau^2 = \gamma_1\gamma_2^2\gamma_3^6\gamma_4^2.$$

Quindi $\tau^2 = \left(\sigma^2\right)^u$ per un qualunque intero u tale che

$$u \equiv 1 \pmod 2$$
$$u \equiv 2 \pmod 5$$
$$u \equiv 6 \pmod 7$$
$$u \equiv 2 \pmod 3$$

Un intero siffatto esiste in virtù della prima formulazione del Teorema Cinese del resto (ad esempio, $u = 167$). Di conseguenza, $\langle\tau^2\rangle \subset \langle\sigma^2\rangle$. Ma allora i due sottogruppi, avendo lo stesso ordine, coincidono. In conclusione, il sottogruppo cercato è $\langle\sigma^2\rangle = \langle\tau^2\rangle$, di ordine 210.

(b) Il ciclo $\alpha = (1,5,2,6,3,7,4,8)$ commuta con σ, in quanto $\alpha^2 = (1,2,3,4)(5,6,7,8)$ è il prodotto di due dei cicli di σ. Tuttavia, α non commuta con τ. Infatti $\tau\alpha(1) = 6$, mentre $\alpha\tau(1) = 8$. Ciò prova che $C(\sigma) \neq C(\tau)$.

(c) Con σ commuta, oltre al ciclo α del punto precedente, anche il suo ciclo $\gamma = (1,2,3,4)$. Ma $\alpha\gamma \neq \gamma\alpha$, dato che $\alpha\gamma(1) = 6$, mentre $\gamma\alpha(1) = 5$. Ciò basta per concludere che $C(\sigma)$ non è abeliano.

2.

(a) Ogni omomorfismo di anelli conserva gli elementi idempotenti rispetto al prodotto. Pertanto, dato un omomorfismo di anelli $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_4$, gli elementi $\alpha = \varphi([1]_2, [0]_8)$ e $\beta = \varphi([0]_2, [1]_8)$ dovranno essere idempotenti in $\mathbb{Z}_4 \times \mathbb{Z}_4$, ossia appartenere all'insieme

$$\{([0]_4,[0]_4),\ ([0]_4,[1]_4),\ ([1]_4,[0]_4),\ ([1]_4,[1]_4)\}.$$

In virtù della conservazione dello zero e dei multipli, dovrà anche essere $2\alpha = ([0]_4, [0]_4)$, che, nell'elenco precedente, è vero solo per $\alpha = ([0]_4, [0]_4)$, e, inoltre $8\beta = ([0]_4, [0]_4)$, che, invece, vale per ogni scelta di β. Pertanto, per ogni $a, b \in \mathbb{Z}$, si avrà:

$$\varphi([a]_2, [b]_8) = a\alpha + b\beta = b\beta \in \{([0]_4,\ [0]_4),\ ([0]_4,[b]_4), ([b]_4,[0]_4), ([b]_4,[b]_4)\}.$$

Ognuna delle quattro assegnazioni corrisponde ad un omomorfismo di anelli ben definito. Il numero cercato è quindi 4.

(b) In base ad una nota proprietà dei prodotti diretti di anelli unitari, $\mathcal{U}(\mathbb{Z}_6 \times \mathbb{Z}_{12}) = \mathcal{U}(\mathbb{Z}_6) \times \mathcal{U}(\mathbb{Z}_{12})$. D'altra parte, per la seconda formulazione del Teorema cinese del resto, $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$, da cui $\mathcal{U}(\mathbb{Z}_6) \simeq \mathcal{U}(\mathbb{Z}_2 \times \mathbb{Z}_3) = \mathcal{U}(\mathbb{Z}_2) \times \mathcal{U}(\mathbb{Z}_3)$, gruppo di ordine 2, e quindi isomorfo a $\mathbb{Z}_2$. Analogamente si stabilisce che $\mathcal{U}(\mathbb{Z}_{12}) \simeq \mathcal{U}(\mathbb{Z}_3 \times \mathbb{Z}_4) = \mathcal{U}(\mathbb{Z}_3) \times \mathcal{U}(\mathbb{Z}_4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. In conclusione,

$$\mathcal{U}(\mathbb{Z}_6 \times \mathbb{Z}_{12}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

In questo gruppo ogni elemento ha periodo al più 2.
Con la stessa argomentazione si deduce che $\mathcal{U}(\mathbb{Z}_4 \times \mathbb{Z}_{10}) \simeq \mathcal{U}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5) = \mathcal{U}(\mathbb{Z}_4) \times \mathcal{U}(\mathbb{Z}_2) \times \mathcal{U}(\mathbb{Z}_5)$. In questo gruppo, l'elemento $([1]_4, [1]_2, [2]_5)$ ha periodo 4. Ciò basta per concludere che i gruppi $\mathcal{U}(\mathbb{Z}_6 \times \mathbb{Z}_{12})$ e $\mathcal{U}(\mathbb{Z}_4 \times \mathbb{Z}_{10})$ non sono isomorfi.

3.

(a) Per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = 3\alpha^2 - \overline{1}$. Quindi α è radice se e solo se $\alpha^2 = \overline{3}^{-1}$. Si noti che $\overline{3}$ è invertibile in $\mathbb{Z}_p$ per ogni $p \neq 3$. Per $p = 11$, si ha che $\overline{3}^{-1} = \overline{4}$, e quindi il polinomio $f(x)$ ha esattamente due radici in $\mathbb{Z}_{11}$, precisamente $\overline{2}$ e il suo opposto $\overline{9}$.

(b) Sia ora $p = 397$. Poiché $p + 3 = 400 = 20^2$, si ha che $\overline{20}^2 = \overline{3}$. Quindi le radici di $f(x)$ saranno $\overline{20}^{-1}$ e il suo opposto $-\overline{20}^{-1}$. Ora, essendo $\overline{20}^{-1} \cdot \overline{3} = \overline{20} = \overline{397 + 20} = \overline{417} = \overline{139} \cdot \overline{3}$, si ricava che le due radici sono $\overline{139}$ e $\overline{258}$.