Traccia dell'8 giugno 2026

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Dal confronto tra le orbite di 9 sotto l'azione delle potenze di σ e di τ si deduce che $4|s$ e $4|t$. Quindi $s = 4h$, $t = 4k$, per opportuni interi h, k e il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, dove

$$\sigma^4 = (13, 14, 15)$$
$$\tau^4 = (13, 15, 14)(16, 18)(20, 22)(21, 23)(17, 19).$$

Ma, allora, poiché τ^t deve lasciare fisso 16, si ha che $2|k$, ove

$$\tau^8 = (13, 14, 15) = \sigma^4.$$

Il sottogruppo cercato è allora $\langle\sigma^4\rangle \cap \langle\tau^8\rangle = \langle\sigma^4\rangle = \langle\tau^8\rangle$, di ordine 3.

(b) Con σ commutano le permutazioni $\alpha = (16, 17, 18, 19)$, che è un suo ciclo, e $\beta = (16, 20, 17, 21, 18, 22, 19, 23)$, in quanto $\beta^2 = (16, 17, 18, 19)(20, 21, 22, 23)$ è prodotto di due suoi cicli. Ora, $\alpha\beta(16) = 20$, mentre $\beta\alpha(16) = 21$. Ciò prova che $\alpha\beta \neq \beta\alpha$, dunque $C(\sigma)$ non è abeliano.

(c) A $C(\sigma)$ appartiene $\gamma = (9, 11, 10, 12)$, che è un ciclo di σ. Ma $\tau\gamma(9) = 10$, mentre $\gamma\tau(9) = 9$. Pertanto, $\gamma \in C(\sigma) \setminus C(\tau)$. Allo stesso modo si vede che $\delta = (9, 12, 11, 10) \in C(\tau) \setminus C(\sigma)$. Quindi la risposta al quesito è negativa.

2.

(a) Un sottogruppo di $\mathbb{Z}_{15} \times \mathbb{Z}_{27}$ avente ordine 81 è $H = \langle[5]_{15}\rangle \times \mathbb{Z}_{27}$. Cerchiamo dunque un omomorfismo di anelli $\varphi : \mathbb{Z}_{15} \times \mathbb{Z}_{27} \to \mathbb{Z}_{10} \times \mathbb{Z}_{54}$ tale che, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_{15}, [b]_{27}) = ([\lambda a]_{10}, [0]_{54})$ per un opportuno intero λ. Questo dovrà essere tale da rendere l'applicazione ben definita, e ciò avviene se e solo se $\lambda = 2\mu$, per qualche intero μ. In tal caso φ è un omomorfismo di gruppi ben definito. Conserverà anche il prodotto se e solo se $10|4\mu^2 - 2\mu$, ossia se e solo se $5|\mu(2\mu - 1)$. Se $5|\mu$, si ottiene, però, l'omomorfismo nullo. Scartando questo caso, si deve dunque imporre che $5|2\mu - 1$, il che si verifica per $\mu = 3$. L'omomorfismo di anelli risultante è definito da $\varphi([a]_{15}, [b]_{27}) = ([6a]_{10}, [0]_{54})$. Si può immediatamente constatare che il suo nucleo è il sottogruppo H.

(b) Il gruppo di partenza del monomorfismo, $\mathbb{Z}_{16} \times \mathbb{Z}_{25}$, è ciclico, in quanto 16 e 25 sono coprimi. L'immagine sarà dunque un gruppo ciclico dello stesso ordine, $16 \cdot 25 = 400$. Tuttavia, il gruppo di arrivo $\mathbb{Z}_{30} \times \mathbb{Z}_{40}$ non ha un sottogruppo ciclico di quell'ordine, in quanto il massimo periodo dei suoi elementi è $\mathrm{mcm}(30, 40) = 120$. Ne consegue che la risposta al quesito è negativa.

3.

(a) Si ha $g(x) = x(x + \overline{1})(x - \overline{1})$.

Sia $\alpha \in \mathbb{Z}_p$. Allora $x - \alpha$ divide $f(x)$ se e solo se $f(\alpha) = \overline{0}$, e in tal caso $\alpha \neq \overline{0}$, così che, per i Teoremi di Eulero e di Fermat,

$$f(\alpha) = \alpha^{p^2} + \alpha^{p-1} + \alpha + \overline{1} = \overline{2}(\alpha + \overline{1}).$$

Se $p \neq 2$, si ha quindi $f(\alpha) = \overline{0}$ se e solo se $\alpha = -\overline{1}$. In tal caso $x + \overline{1}$ è l'unico fattore lineare di $f(x)$. Ne consegue che, per $p \neq 2$, $\mathrm{MCD}(f(x), g(x)) = x + \overline{1}$. Sia allora $p = 2$. In questo caso $f(x) = x^4 + x + x + \overline{1} = x^4 + \overline{1} = (x + \overline{1})^4$, e, d'altra parte, $g(x) = x(x + \overline{1})^2$, così che si ha $\mathrm{MCD}(f(x), g(x)) = (x + \overline{1})^2 = x^2 + \overline{1}$.

(b) Si ha

$$f(x) = \left(x^p + x\right)^p - x^p + x^{p-1} + x + \overline{1} = \left(x^p + x\right)^p - \left(x^p + x\right) + x + x^{p-1} + x + \overline{1} =$$
$$h(x)^p - h(x) + x^{p-1} + \overline{2}x + \overline{1} = \left(h(x)^{p-1} - \overline{1}\right)h(x) + x^{p-1} + \overline{2}x + \overline{1}$$

ove $p - 1 < p = \deg h(x)$. Se ne deduce che il quoziente ed il resto cercati sono, rispettivamente, $q(x) = h(x)^{p-1} - \overline{1}$ e $r(x) = x^{p-1} + \overline{2}x + \overline{1}$.