Traccia del 17 aprile 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 1 sotto l'azione delle potenze di σ e di τ si deduce che $2|s$ e $2|t$. Quindi $s = 2h$, $t = 2k$, per opportuni interi h, k e il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, dove

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

Dal confronto tra le orbite di 5 sotto l'azione delle potenze di σ^2 e di τ^2 si ricava ancora che $2|k$. Quindi il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^4\rangle$, dove

$$\tau^4 = (17,21,19)(18,22,20).$$

Ma, allora, poiché σ^s deve lasciare fisso 9, si ha che $2|h$, ove

$$\sigma^4 = (17,19,21)(18,20,22).$$

Poiché queste permutazioni sono l'una l'inversa dell'altra, il sottogruppo cercato è allora $\langle\sigma^4\rangle \cap \langle\tau^4\rangle = \langle\sigma^4\rangle = \langle\tau^4\rangle$, di ordine 3.

(b) Con σ e con τ commutano le permutazioni $\alpha = (1,2)(3,4)$ e $\beta = (1,3)(2,4)$, che sono dunque due distinti elementi di periodo 2 in $C(\sigma) \cap C(\tau)$. Ciò esclude che $C(\sigma) \cap C(\tau)$ sia ciclico.

(c) A $C(\sigma)$ appartengono $\delta = (1,2)$ e $\varepsilon = (1,3,2,4)$, ma non commutano tra di loro, infatti $\delta\varepsilon(1) = 3 \neq 4 = \varepsilon\delta(1)$. La risposta al quesito è dunque negativa.

2.

(a) Dati due interi n, m, l'applicazione $\varphi : \mathbb{Z}_{10} \times \mathbb{Z}_{28} \to \mathbb{Z}_{20} \times \mathbb{Z}_{56}$ tale che, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_{10}, [b]_{28}) = ([na]_{20}, [mb]_{56})$ è un omomorfismo ben definito se e solo se $2|n$ e $2|m$. Siano dunque λ, μ interi tali che $n = 2\lambda$ e $m = 2\mu$. Allora φ è un omomorfismo di anelli se e solo se conserva il prodotto, ossia se e solo se $20|\ 4\lambda^2 - 2\lambda$ e $56|\ 4\mu^2 - 2\mu$. Queste condizioni equivalgono, rispettivamente, a $10|\ \lambda(2\lambda - 1)$ e $28|\ \mu(2\mu - 1)$. La prima è soddisfatta se

$$\lambda \equiv 0 \pmod 2$$
$$2\lambda \equiv 1 \pmod 5$$

e ciò vale per $\lambda = 8$. In modo analogo si trova che la seconda vale per $\mu = 4$. Si ricava così un omomorfismo di anelli definito ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_{10}, [b]_{28}) = ([16a]_{20}, [8b]_{56})$. La sua immagine è $\langle[16]_{20}\rangle \times \langle[8]_{56}\rangle$, il cui ordine è $o([16]_{20})o([8]_{56}) = 5 \cdot 7 = 35$, come volevasi.

(b) Il gruppo di partenza dell'omomorfismo deve essere $\mathbb{Z}_7 \times \mathbb{Z}_{40}$, che è ciclico, in quanto 7 e 40 sono coprimi. L'immagine di un gruppo ciclico secondo un omomorfismo di gruppi è anch'essa un gruppo ciclico, ma tale non è $\mathbb{Z}_{20} \times \mathbb{Z}_{14}$, in quanto il massimo periodo dei suoi elementi è $\mathrm{mcm}(20,14) = 140 \neq 20 \cdot 14 = 280$. Ne consegue che la risposta al quesito è negativa.

3.

(a) Si ha $g(x) = \left(x^p - x\right)^p = x^p\left(x^{p-1} - \overline{1}\right)^p$. Questo polinomio ammette dunque in $\mathbb{Z}_p[x]$ la seguente decomposizione in fattori lineari

$$g(x) = x^p \prod_{\alpha \in \mathbb{Z}_p^*} (x - \alpha)^p.$$

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,

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

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 $f(x)$. Si noti che

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

ove ciascuno dei tre addendi è divisibile per $(x + \overline{1})^p$. Ma questa è la massima potenza di $x + \overline{1}$ che divide $g(x)$. Ne consegue che, per $p \neq 2$, $MCD(f(x), g(x)) = (x + \overline{1})^p = x^p + \overline{1}$. Sia allora $p = 2$. In questo caso $f(x) = x^4 + x^2 + x^2 + \overline{1} = x^4 + \overline{1} = (x + \overline{1})^4$, $g(x) = x^2(x + \overline{1})^2$, e, di nuovo, $MCD(f(x), g(x)) = (x + \overline{1})^2 = x^p + \overline{1}$.

(b) Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $f(x)$ per $h(x)$. Allora $f(x) = q(x)h(x) + r(x)$, dove $r(x)$ è il polinomio nullo oppure un polinomio di grado 0 o 1. Innanzitutto osserviamo che $r(x)$ non è il polinomio nullo, in quanto

$$\overline{1} = f(\overline{0}) = q(\overline{0})h(\overline{0}) + r(\overline{0}) = r(\overline{0}), \qquad (*)$$

pertanto ha $\overline{1}$ come termine noto. Inoltre

$$\overline{4} = f(\overline{1}) = q(\overline{1})h(1) + r(\overline{1}) = r(\overline{1}). \qquad (**)$$

Se $p \neq 3$, allora $r(\overline{0}) \neq r(\overline{1})$, e quindi $r(x)$ non è costante. Dunque è di grado 1, e precisamente, da $(*)$ e $(**)$ segue che $r(x) = \overline{3}x + \overline{1}$. Sia ora $p = 3$. Allora

$$f(x) = x^9 + x^6 + x^3 + \overline{1} = \left(x^3 + x^2 + x + \overline{1}\right)^3 = \left(x^3 - x^2 + \overline{2}x^2 - \overline{2}x + \overline{1}\right)^3 =$$
$$(xh(x) + \overline{2}h(x) + \overline{1})^3 = h(x)^3(x + \overline{2})^3 + \overline{1},$$

da cui segue che $r(x) = \overline{1}$. Di nuovo si ha $r(x) = \overline{3}x + \overline{1}$.