Traccia del 26 gennaio 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 7 sotto l'azione delle potenze di σ e di τ si deduce che $3|s$ e $4|t$. Dal confronto tra le orbite di 10 si deduce inoltre che $5|s$. Il sottogruppo cercato è dunque $\langle\sigma^{15}\rangle \cap \langle\tau^4\rangle$, dove

$\sigma^{15} = (15, 16)(17, 18)$.
$\tau^4 = (1, 3, 2)(4, 6, 5)$.

Poiché queste due permutazioni hanno supporti disgiunti, la loro unica potenza comune è la permutazione identica. Pertanto l'intersezione cercata è il sottogruppo banale.

(b) Con σ e con τ commutano le seguenti permutazioni:

- $\alpha = (1, 4, 2, 5, 3, 6)$, in quanto $\alpha^2 = (1, 2, 3)(4, 5, 6)$ è il prodotto di due cicli di σ e l'inverso del prodotto di due cicli di τ;
- $\beta = (15, 16)(17, 18)$, in quanto è il prodotto di due cicli di σ e commuta con $(15, 17)(16, 18)$, prodotto di due cicli di τ.

Queste due permutazioni sono inoltre disgiunte. Se ne deduce che l'insieme

$$H = \{\alpha^a\beta^b \mid a, b \in \mathbb{Z}\}$$

è un sottogruppo di $C(\sigma) \cap C(\tau)$ avente ordine $o(\alpha)o(\beta) = 6 \cdot 2 = 12$.

(c) In base a quanto osservato al punto (b), a $C(\sigma)$ appartiene la permutazione $\alpha = (1, 4, 2, 5, 3, 6)$. Inoltre vi appartiene anche $\gamma = (1, 2, 3)$, che è uno dei suoi cicli. Ma queste due permutazioni non commutano, in quanto $\alpha\gamma(1) = 5$, mentre $\gamma\alpha(1) = 4$. Ciò esclude che $C(\sigma)$ sia abeliano.

2.

(a) Supponiamo che esista un monomorfismo di anelli $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_{20} \times \mathbb{Z}_{40}$. Allora φ, essendo un monomorfismo di gruppi additivi, invia $([1]_2, [0]_4)$ in un elemento $(\alpha, \beta) \in \mathbb{Z}_{20} \times \mathbb{Z}_{40}$ avente lo stesso periodo, ossia tale che $o(\alpha, \beta) = 2$. Segue che

$$(\alpha, \beta) \in \{([10]_{20}, [20]_{40}),\ ([10]_{20}, [0]_{40}),\ ([0]_{20}, [20]_{40})\}.$$

Ora, però, poiché φ conserva anche il prodotto, l'elemento (α, β) dovrà essere, come $([1]_2, [0]_4)$, idempotente. Ma nessuno degli elementi elencati sopra lo è, in quanto i loro quadrati sono tutti uguali a $([0]_{20}, [0]_{40})$. Ne consegue che il monomorfismo richiesto non esiste.

(b) Un sottogruppo di $\mathbb{Z}_8 \times \mathbb{Z}_{10}$ avente ordine $20 = 4 \cdot 5$ è $H = \langle[2]_8\rangle \times \langle[2]_{10}\rangle$. D'altra parte, un'applicazione $\psi : \mathbb{Z}_8 \times \mathbb{Z}_{10} \to \mathbb{Z}_4 \times \mathbb{Z}_{20}$ che, dati opportuni numeri interi λ, μ, sia definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\psi([a]_8, [b]_{10}) = ([\lambda a]_4, [\mu b]_{20})$, è ben definita se e solo se $2|\mu$. In tal caso è un omomorfismo di gruppi. Per $\lambda = 2$ e $\mu = 10$ si avrà, come richiesto, $\mathrm{Ker}\psi = H$.

3.

(a) Si ha $g(x) = \left(x^2\left(x^p - x\right)\right)^p$, ove $x^p - x = \prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)$. Ne consegue che i fattori irriducibili comuni a $f(x)$ e $g(x)$ saranno tutti e soli quelli della forma $(x - \alpha)$ con α radice di $f(x)$ in $\mathbb{Z}_p$. Tra questi fattori non figurerà, naturalmente, il polinomio x, non essendo $\overline{0}$ radice di $f(x)$. Ora, per ogni $\alpha \in \mathbb{Z}_p^*$ si ha, in virtù del Piccolo Teorema di Fermat e del Teorema di Eulero:

$$f(\alpha) = \alpha^{(p-1)p^2} + \alpha^{(p-1)p} + \alpha^p + \overline{1} \;=\; \alpha^{p-1} + \alpha^{p-1} + \alpha + \overline{1} = \alpha + \overline{3}.$$

Ne consegue che, se $p = 3$, $f(x)$ è privo di radici, e quindi $\mathrm{MCD}(f(x), g(x)) = \overline{1}$. Alttrimenti $f(x)$ ha esattamente una radice, precisamente $\alpha = -\overline{3}$. Quindi l'unico fattore irriducibile comune a $f(x)$ e $g(x)$, per $p \neq 3$ è $x + \overline{3}$. Tuttavia, occorre tener conto del fatto che esso compare nella fattorizzazione di $g(x)$ con molteplicità p. D'altra parte, $f(x)$ è, a sua volta, la p – esima potenza di un polinomio, precisamente, $f(x) = \left(x^{p^2-p} + x^{p-1} + x + \overline{1}\right)^p$. Dunque, nella fattorizzazione di $f(x)$, il fattore irriducibile $x + \overline{3}$ compare con molteplicità pari ad un multiplo di p. Ne consegue che, per $p \neq 3$, $\mathrm{MCD}(f(x), g(x)) = (x + \overline{3})^p = x^p + \overline{3}$.

(b) Si ha $f(x) - h(x)^p = -x^{p^2} + x^p$. Il grado di questo polinomio è maggiore di $\deg h(x)$. Proseguiamo dunque sottraendo un opportuno multiplo di $h(x)$ avente grado p^2: $f(x) - h(x)^p + x^p h(x) = -x^{p^2} + x^p + x^{p^2} + x^{2p-1} + x^{2p} + x^p = x^{2p} + x^{2p-1} + \overline{2}x^p$.
Osserviamo che il grado di questo polinomio è $2p$, ed è dunque minore di $p^2 - p = p(p-1)$ se $p > 3$. In tal caso $r(x) = x^{2p} + x^{2p-1} + \overline{2}x^p$ è il resto cercato. Altrimenti il calcolo va proseguito. Consideriamo singolarmente i rimanenti due valori di p. Per $p = 2$, abbiamo ottenuto $x^4 + x^3$, mentre $h(x) = x + \overline{1}$. Quindi, essendo $x^4 + x^3 = x^3 h(x)$, il resto è nullo. Per $p = 3$ abbiamo ottenuto il polinomio $x^6 + x^5 + \overline{2}x^3$, mentre $h(x) = x^6 + x^2 + x^3 + \overline{1}$. In tal caso il resto è $r(x) = x^5 + x^3 - x^2 - \overline{1}$.