Traccia del 9 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 9 sotto l'azione delle potenze di σ e di τ si deduce che $2|t$. Il sottogruppo cercato è dunque $\langle\sigma\rangle \cap \langle\tau^2\rangle$, dove

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

Dal confronto tra le orbite di 1 sotto l'azione delle potenze di σ e di τ^2 si deduce ancora che $2|s$. Dunque il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, ove

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

A questo punto si può osservare che $(9,10,11)^2(12,13,14)^2 = (9,11,10)(12,14,13)$ e che $(15,16,17,18,19)^2 = (15,17,19,16,18)$. Pertanto $\sigma^2 = \tau^{2k}$ se k è un intero verificante la seguente terna di congruenze:

$$k \equiv 1 \pmod 2$$
$$k \equiv 2 \pmod 3$$
$$k \equiv 2 \pmod 5$$

Essendo $2, 3$ e 5 a due a due coprimi, un intero siffatto esiste per il Teorema Cinese del resto (ad esempio, si può prendere $k = 17$). Ciò prova che $\sigma^2 \in \langle\tau^2\rangle$, e dunque il sottogruppo cercato è $\langle\sigma^2\rangle = \langle\tau^2\rangle$, di ordine 30.

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

- $\alpha = (1,2,3,4)$, in quanto è un ciclo di σ e l'inverso di un ciclo di τ;
- $\beta = (5,6,7,8)$, in quanto è un ciclo di σ e l'inverso di un ciclo di τ;
- $\gamma = (9,10,11)(12,13,14)$, in quanto è il prodotto di due cicli di σ ed è il quadrato di un ciclo di τ.

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

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

è un sottogruppo di $C(\sigma) \cap C(\tau)$ avente ordine $o(\alpha)o(\beta)o(\gamma) = 4 \cdot 4 \cdot 3 = 48$.

(c) In base a quanto osservato al punto (b), a $C(\sigma)$ appartengono le permutazioni $\alpha = (1,2,3,4)$, $\beta = (5,6,7,8)$, e, di conseguenza, anche il loro prodotto $\alpha\beta = (1,2,3,4)(5,6,7,8)$. Queste sono tre permutazioni di periodo 4, mentre $\phi(4) = 2$. Ciò esclude che $C(\sigma)$ sia ciclico.

2.

(a) Consideriamo un'applicazione $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_{10} \to \mathbb{Z}_2 \times \mathbb{Z}_6$ definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_4, [b]_{10}) = ([\lambda a]_2, [\mu b]_6)$ per opportuni interi λ, μ. Questa è ben definita per ogni valore di λ, e se e solo se $3|\mu$. In tal caso è evidentemente un omomorfismo di gruppi. Sia dunque $\lambda = 1$ e $\mu = 3h$ per qualche intero h. Allora φ è un omomorfismo di anelli se e solo se

conserva il prodotto. Ciò avviene se e solo se l'intero h verifica la condizione $9h^2 \equiv 3h \pmod 6$, ossia se e solo se $6|(3h(3h-1)$, che equivale a $2|h(3h-1)$. Questa condizione è verificata da ogni intero h: infatti i numeri h e $3h-1$ differiscono per un numero dispari, e dunque sono un numero pari e un numero dispari. Per $h=1$ si ottiene l'omomorfismo di anelli definito ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_4, [b]_{10}) = ([a]_2, [3b]_6)$. La sua immagine è $\mathbb{Z}_2 \times \langle [3]_6 \rangle$, il cui ordine è 4.

(b) In base alla seconda formulazione del Teorema cinese del resto, il gruppo di partenza è ciclico, generato da $([1]_3, [1]_{10})$. Sia $\psi : \mathbb{Z}_3 \times \mathbb{Z}_{10} \to \mathbb{Z}_2 \times \mathbb{Z}_{20}$ un omomorfismo di gruppi. Allora è univocamente determinato dall'immagine (α, β) di $([1]_3, [1]_{10})$, in quanto allora, data la conservazione dei multipli, sarà definito ponendo, per ogni $n \in \mathbb{Z}$, $\psi([n]_3, [n]_{10}) = (n\alpha, n\beta)$. Ma sarà ben definito se e solo se $30(\alpha, \beta) = ([0]_2, [0]_{20})$. Poiché $30\alpha = [0]_2$ è verificato per ogni $\alpha \in \mathbb{Z}_2$, la condizione di buona definizione si riduce a $30\beta = [0]_{20}$, che equivale a $o(\beta)|30$. Ma, per il Teorema di Lagrange, $o(\beta)|20$, per ogni $\beta \in \mathbb{Z}_{20}$. Dunque la condizione si traduce infine in $o(\beta)|\mathrm{MCD}(20, 30)$, ossia $o(\beta)|10$, e ciò vale per tutti e soli i $\beta \in \mathbb{Z}_{20}$ che non hanno periodo 4 o 20. I loro numero è $20 - \phi(4) - \phi(20) = 20 - \phi(4) - \phi(4)\phi(5) = 20 - 2 - 2 \cdot 4 = 10$. Quindi 10 sono le possibili scelte di β. Poiché le possibili scelte di α sono 2, si conclude che gli omomorfismi di gruppi fra i gruppi assegnati sono complessivamente $2 \cdot 10 = 20$.

3.

(a) Sia $d(x) = \mathrm{MCD}(f(x), g(x))$. Si ha $g(x) - f(x)^p = -\overline{2}$. Questo è il polinomio nullo per $p = 2$, nel qual caso $f(x)|g(x)$, e dunque $d(x) = f(x)$. Altrimenti, per $p > 2$, essendo $d(x)$ un divisore di $-\overline{2}$, polinomio costante non nullo, si ha $d(x) = \overline{1}$.

(b) Si ha $h(x) = \left(x^p - x\right)^{p^2}$, ove $x^p - x = \prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)$. Ne consegue che $g(x)$ e $h(x)$ sono coprimi se e solo se nessuno dei fattori irriducibili $x - \alpha$ di $h(x)$ divide $g(x)$, ossia, per il Teorema di Ruffini, se e solo se $g(x)$ è privo di radici in $\mathbb{Z}_p$. Ora, per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $g(\alpha) = \alpha^{p^3} + \alpha^{p^2} + \alpha^p - \overline{1} = 3\alpha - \overline{1} = \overline{3}\alpha - \overline{1}$. Se $p \neq 3$, $g(x)$ ha quindi una radice, precisamente $\overline{3}^{-1}$. Per $p = 3$, $g(x)$ è invece privo di radici. Pertanto, $g(x)$ e $h(x)$ sono coprimi se e solo se $p = 3$.