Traccia del 3 novembre 2025

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 15 sotto l'azione di σ e di τ si deduce che $2|s$ e $4|t$. Il sottogruppo cercato è dunque $\langle\sigma^2\rangle \cap \langle\tau^4\rangle$, dove

$$\sigma^2 = (1,3,2)(4,6,5)(7,9,8)(10,12,14,11,13),$$
$$\tau^4 = (1,5,9,2,6,7,3,4,8)(10,13,11,14,12).$$

A questo punto si può osservare che $(1,5,9,2,6,7,3,4,8)^6 = (1,3,2)(4,6,5)(7,9,8)$ e che $(10,13,11,14,12)^4 = (10,12,14,11,13)$. Pertanto $\sigma^2 = \tau^{4k}$ se k è un intero verificante la seguente coppia di congruenze:

$$k \equiv 6 \pmod 9$$
$$k \equiv 4 \pmod 5$$

Essendo 9 e 5 coprimi, un intero siffatto esiste per il Teorema Cinese del resto (ad esempio, si può prendere $k = 24$). Ciò prova che $\sigma^2 \in \langle\tau^4\rangle$, e dunque il sottogruppo cercato è $\langle\sigma^2\rangle$, di ordine 15.

(b) La permutazione $\alpha = (19,20)(21,22)$ commuta con σ, in quanto prodotto di due dei suoi cicli, e con τ, in quanto è il quadrato di $(19,21,20,22)$, uno dei suoi cicli associati. Inoltre $\beta = (15,17)(16,18)$ commuta con τ, essendo il quadrato del ciclo $(15,16,17,18)$ associato a τ, e commuta con σ, in quanto commuta con il prodotto $(15,16)(17,18)$ di due dei suoi cicli ed è disgiunta dagli altri suoi cicli. Pertanto α, β sono entrambi elementi di $C(\sigma) \cap C(\tau)$. Essendo di periodo 2, ciò esclude che questo gruppo sia ciclico.

(c) A $C(\sigma)$ appartengono le permutazioni $\gamma = (1,2,3)$, che è uno dei suoi cicli, e $\delta = (1,4,2,5,3,6)$, poiché $\delta^2 = (1,2,3)(4,5,6)$ è il prodotto di due dei cicli di σ e δ è disgiunta dagli altri suoi cicli. Ma $\gamma\delta(1) = 4$, mentre $\delta\gamma(1) = 5$. Ciò prova che $\delta\gamma \neq \gamma\delta$, escludendo che $C(\sigma)$ sia abeliano.

2.

(a) L'applicazione da $\mathbb{Z}_{16}$ a $\mathbb{Z}_8$ definita da $[a]_{16} \mapsto [a]_8$ per ogni $a \in \mathbb{Z}$ è evidentemente un omomorfismo di anelli surgettivo. Se ne deduce immediatamente che l'applicazione $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_{16} \to \mathbb{Z}_8 \times \mathbb{Z}_8$ definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_4, [b]_{16}) = ([0]_8, [b]_8)$ è un omomorfismo di anelli la cui immagine è $\{[0]_8\} \times \mathbb{Z}_8$, avente esattamente 8 elementi.

(b) L'applicazione $\psi : \mathbb{Z}_4 \times \mathbb{Z}_{30} \to \mathbb{Z}_{10} \times \mathbb{Z}_{12}$ definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\psi([a]_4, [b]_{30}) = ([b]_{10}, [3a]_{12})$ è evidentemente un omomorfismo di gruppi. La sua immagine è $\mathbb{Z}_{10} \times \langle[3]_{12}\rangle$, dove il secondo fattore diretto è un gruppo ciclico di ordine 4. Il prodotto diretto di due gruppi finiti di ordini 10 e 4 ha ordine 40, ma i periodi dei suoi elementi sono minori o uguali a $\mathrm{mcm}(10,4) = 20$. Ciò esclude che $\mathrm{Im}\psi$ sia un gruppo ciclico.

3.

(a) Sia $\alpha \in \mathbb{Z}_p$. Se α è radice di $f(x)$ o di $g(x)$, allora $\alpha \neq \overline{0}$ e dunque, in virtù del Teorema di Eulero e del Piccolo Teorema di Fermat,

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

$$g(\alpha) = \alpha^{p^3+p^2+p+1} - \alpha^{p^2(p-1)} - \alpha^{p(p-1)} - \alpha^{p-1} + \overline{1} = \alpha^4 - \overline{1} - \overline{1} - \overline{1} + \overline{1} = \alpha^4 - \overline{2}. \qquad (2)$$

Da $f(\alpha) = g(\alpha) = \overline{0}$ segue quindi $\alpha^4 = \overline{9} = \overline{2}$, così che $p = 7$. In tal caso la condizione $\alpha^2 + \overline{3} = \overline{0}$ si può riscrivere come $\alpha^2 = \overline{4}$, che vale se e solo se $\alpha \in \{\overline{2}, -\overline{2}\}$. Questi due elementi di $\mathbb{Z}_7$ verificano anche la condizione $\alpha^4 - \overline{2} = \overline{0}$, e quindi sono le radici comuni di $f(x)$ e di $g(x)$ quando $p = 7$.

(b) Si ha $h(x) = (x + \overline{1})(x - \overline{3})$. Ora, per il Teorema di Ruffini, $x + \overline{1}$ divide $f(x)$ se solo se $f(-\overline{1}) = \overline{0}$, e, alla luce della (1), ciò vale se e solo $p = 2$. In tal caso $f(x) = x^6 + x^3 + x + \overline{1}$ e $h(x) = x^2 + \overline{1}$. Ma $f(x) = x\left(x^2 + \overline{1}\right) + x^6 + \overline{1} = \left(x^2 + \overline{1}\right)\left(x^4 + x^2 + x + \overline{1}\right)$. Dunque, per $p = 2$, $\mathrm{MCD}(f(x), h(x)) = h(x)$. Nei restanti casi, come abbiamo visto, $x + \overline{1}$ non divide $f(x)$, e $x - \overline{3}$ divide $f(x)$ se e solo se $f(\overline{3}) = \overline{0}$. Ciò non può valere per $p = 3$, dato che $f(\overline{0}) \neq \overline{0}$. D'altra parte, se $p > 3$, allora $f(\overline{3}) = \overline{12} \neq \overline{0}$. In conclusione, per $p \neq 2$, $\mathrm{MCD}(f(x), h(x)) = \overline{1}$.