Traccia del 3 novembre 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 $3|t$, dal confronto tra le orbite di 19 si deduce inoltre che $4|s$ e $4|t$. Quindi $s = 4h,\ t = 12k$, per opportuni interi h, k e il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^{12}\rangle$, dove

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

Dal confronto tra le orbite di 5 sotto l'azione delle potenze di σ^4 e di τ^{12} si deduce ancora che $3|h$ e $3|k$. Pertanto il sottogruppo cercato è $\langle\sigma^{12}\rangle \cap \langle\tau^{36}\rangle$, ove

$$\sigma^{12} = (10,12,14,11,13),$$
$$\tau^{36} = (10,13,11,14,12).$$

Si osservi che queste due permutazioni sono una l'inversa dell'altra. Ne consegue che il sottogruppo cercato è $\langle\sigma^{12}\rangle = \langle\tau^{36}\rangle$, di ordine 5.

(b) A $C(\sigma) \cap C(\tau)$ appartengono le permutazioni $(15,16)(17,18)$ e $(15,17)(16,18)$, entrambe di periodo 2. Ma nessun gruppo ciclico può avere due elementi di periodo 2. La risposta al quesito è dunque negativa.

(c) A $C(\sigma)$ appartengono le permutazioni $(15,16)$ e $(15,17,16,18)$, che, però, non commutano tra loro. Ciò prova che $C(\sigma)$ non è abeliano.

2.

(a) Un omomorfismo del tipo cercato è l'applicazione $\varphi : \mathbb{Z}_{10} \times \mathbb{Z}_{25} \to \mathbb{Z}_5 \times \mathbb{Z}_{20}$ tale che, per ogni $a, b \in \mathbb{Z}$, si abbia $\varphi([a]_{10}, [b]_{25}) = ([a]_5, [4b]_{20})$. La buona definizione e la conservazione della somma sono di facile verifica. L'immagine è il gruppo $\mathbb{Z}_5 \times \langle[4]_{20}\rangle$, il cui ordine è pari a $5 \cdot o([4]_{20}) = 25$.

(b) Cerchiamo un'applicazione $\psi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_{24} \times \mathbb{Z}_{48}$ avente la forma seguente: per ogni $a, b \in \mathbb{Z}$, si deve avere $\psi([a]_4, [b]_6) = ([\lambda a]_{24}, [\mu b]_{48})$ per opportuni interi λ, μ fissati. Troviamo λ e μ imponendo la buona definizione e la conservazione del prodotto. La prima condizione ci fornisce $\lambda = 6h,\ \mu = 8k$ con h, k interi, e la seconda si traduce nelle seguenti due relazioni di divisibilità: $24|6h(6h-1)$ e $48|8k(8k-1)$. Queste sono a loro volta equivalenti alle relazioni $4|h(6h-1)$ e $6|k(8k-1)$. La seconda è soddisfatta, ad esempio, da $k = 2$. Inoltre possiamo prendere $h = 0$. L'omomorfismo di anelli risultante è definito ponendo, per ogni $a, b \in \mathbb{Z}$, $\psi([a]_4, [b]_6) = ([0]_{24}, [16b]_{48})$.

3.

(a) Per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = \alpha^{p^2} + \alpha^p + \alpha + \overline{1} = \overline{3}\alpha + \overline{1}$, e, inoltre, $g(\alpha) = \left(\alpha^{p-1}\right)^{p-1} + \left(\alpha^2\right)^{p^2} - \overline{3} = \left(\alpha^{p-1}\right)^{p-1} + \alpha^2 - \overline{3}$. Se $p = 3$, allora $f(x)$ è evidentemente privo di radici in $\mathbb{Z}_3$. Sia dunque $p \neq 3$. In tal caso $g(\overline{0}) \neq \overline{0}$, pertanto possiamo limitarci a considerare $\alpha \in \mathbb{Z}_p^*$. Allora l'unica radice di $f(x)$ in $\mathbb{Z}_p$ è $\alpha_1 = -(\overline{3})^{-1}$. Per il teorema di Eulero si ha $g(\alpha_1) = \overline{1} + \alpha_1^2 - \overline{3}$, quindi si avrà $g(\alpha_1) = \overline{0}$ se e solo se sarà $\alpha_1^2 = \overline{2}$. Dovendo essere $f(\alpha_1) = \overline{0}$, contemporaneamente si ha, però, anche $\overline{9}\alpha_1^2 = \overline{1}$. Da ciò si deduce che $\overline{18} = \overline{1}$ e quindi necessariamente $p = 17$. In tal caso $\alpha_1 = -\overline{6} = \overline{11}$ è l'unica radice comune a $f(x)$ e $g(x)$ in $\mathbb{Z}_{17}$. Per gli altri valori di p non vi sono radici comuni in $\mathbb{Z}_p$.

(b) Si ha $h(x) = x(x+\overline{1})(x+\overline{2})$, e, per il Teorema di Ruffini, i fattori irriducibili comuni con $f(x)$ sono dunque tutti e soli i binomi $x - \alpha$ con $\alpha \in \{\overline{0}, -\overline{1}, -\overline{2}\}$ tali che $f(\alpha) = \overline{0}$, ossia tali che $\overline{3}\alpha + \overline{1} = \overline{0}$. Ora,

ciò non è mai vero per $\alpha = \overline{0}$, mentre $\overline{3}(-\overline{1}) = \overline{-1}$ vale se e solo se $p = 2$, e $\overline{3}(-\overline{2}) = -\overline{1}$ vale se e solo se $p = 5$. Dunque $\mathrm{MCD}(f(x), h(x)) = x + \overline{1}$ per $p = 2$, $\mathrm{MCD}(f(x), h(x)) = x + \overline{2}$ per $p = 5$, nei restanti casi $\mathrm{MCD}(f(x), h(x)) = \overline{1}$.