Traccia del 10 gennaio 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 1 sotto l'azione delle potenze di σ e di τ si deduce che $4|s$. Analogamente, dal confronto tra e le orbite di 5 sotto l'azione delle potenze di σ e di τ si deduce che $4|t$. Il sottogruppo cercato è dunque $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, dove

$\sigma^4 = (9, 13, 12, 11, 10)(14, 18, 15, 19, 16, 20, 17)$,
$\tau^4 = (9, 10, 11, 12, 13)(14, 15, 16, 17, 18, 19, 20)$.

Si nota che
$\sigma^4 = \left(\tau^4\right)^4$.

Ne consegue che $\langle\sigma^4\rangle \subset \langle\tau^4\rangle$, pertanto $\langle\sigma^4\rangle \cap \langle\tau^4\rangle = \langle\sigma^4\rangle$. Questo è il sottogruppo cercato: ha ordine pari a $o\left(\sigma^4\right) = \mathrm{mcm}(5, 7) = 35$. Poiché questo è anche l'ordine di $\langle\tau^4\rangle$, si ha, di fatto, che $\langle\sigma^4\rangle = \langle\tau^4\rangle$.

(b) La permutazione $\gamma = (1, 3)(2, 4)$ commuta con σ. Infatti $\gamma = (1, 2, 3, 4)^2$, quindi γ commuta con uno dei cicli associati a σ, ed è disgiunta dai restanti suoi cicli. Inoltre γ commuta con τ, in quanto commuta con $(1, 2)(3, 4)$, ossia con il prodotto di due dei cicli associati a τ, ed è disgiunta dai restanti suoi cicli. Ciò prova che $\gamma \in C(\sigma) \cap C(\tau)$. In maniera analoga si prova che $\delta = (5, 7)(6, 8) \in C(\sigma) \cap C(\tau)$. Dunque $C(\sigma) \cap C(\tau)$ ha due elementi di periodo 2, e ciò esclude che sia ciclico.

(c) Abbiamo visto, al punto precedente, che a $C(\sigma) \cap C(\tau)$ appartengono γ e δ, permutazioni disgiunte di periodo 2. Ora aggiungiamo che vi appartiene anche $\varepsilon = (21, 23, 22, 24)$. Infatti, da un lato, ε è uno dei cicli di τ, dall'altro $\varepsilon^2 = (21, 22)(23, 24)$ è il prodotto di due dei cicli di σ. Poiché ε è disgiunta da γ e da δ, ne consegue che

$$H = \{\gamma^c \delta^d \varepsilon^e | c, d, e \in \mathbb{Z}\}$$

è un sottogruppo di $C(\sigma) \cap C(\tau)$ avente ordine pari a $o(\gamma)o(\delta)o(\varepsilon) = 2 \cdot 2 \cdot 4 = 16$.

2.

(a) Supponiamo che $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3 \times \mathbb{Z}_{12}$ sia un monomorfismo di anelli. Allora esso induce, per corestrizione, un isomorfismo da $\mathbb{Z}_6$ ad un sottoanello B di $\mathbb{Z}_3 \times \mathbb{Z}_{12}$, che dunque sarà unitario. Precisamente, l'immagine secondo φ dell'elemento uno di $\mathbb{Z}_6$ sarà l'elemento uno di B. Sia $\varphi([1]_6) = ([a]_3, [b]_{12})$. Ora, essendo φ un monomorfismo di gruppi (additivi), φ conserva i periodi degli elementi. Pertanto si avrà che $6 = o(([a]_3, [b]_{12})) = \mathrm{mcm}(o([a]_3), o([b]_{12}))$. Poiché, per Lagrange, $o([a]_3) \in \{1, 3\}$ e $o([b]_{12}) \in \{1, 2, 3, 4, 6, 12\}$, si ha

$$(o([a]_3), o([b]_{12})) \in \{(1, 6),\ (3, 2),\ (3, 6)\}.$$

Ciò implica che $[b]_{12} \in \{[2]_{12}, [10]_{12}, [6]_{12}\}$. D'altra parte, però, $([a]_3, [b]_{12})$ è idempotente rispetto al prodotto, così che, in particolare, $[b]_{12}^2 = [b]_{12}$. Ma nessuno dei tre elementi precedentemente

elencati gode di tale proprietà. Se ne deduce che il monomorfismo considerato non esiste.

(b) Ogni epimorfismo di anelli unitari conserva l'elemento uno. Dunque, se $\psi : \mathbb{Z}_8 \times \mathbb{Z}_{24} \to \mathbb{Z}_6 \times \mathbb{Z}_{16}$ è un epimorfismo di anelli, allora $\psi([1]_8, [1]_{24}) = ([1]_6, [1]_{16})$. D'altra parte, essendo ψ un omomorfismo di gruppi additivi, ψ conserva anche i multipli. Ne consegue che

$$\psi(24([1]_8, [1]_{24})) = 24([1]_6, [1]_{16}),$$

ossia che

$$\psi(([0]_8, [0]_{24})) = ([0]_6, [8]_{16}).$$

L'ultima uguaglianza, tuttavia, contraddice un'altra proprietà degli omomorfismi di gruppi additivi, ossia la conservazione dell'elemento zero. Ne consegue che non esiste un epimorfismo di anelli del tipo indicato.

3.

(a) Sia $\alpha \in \mathbb{Z}_p$ una radice comune a $f(x)$ e $g(x)$. Allora $\alpha \neq \overline{0}$. Inoltre $f(\alpha) = g(\alpha)$. Ora, in virtù del Piccolo Teorema di Fermat e del Teorema di Eulero, $f(\alpha) = \alpha + \overline{1} + \alpha^{-1} - \overline{1} = \alpha + \alpha^{-1}$, e $g(\alpha) = \alpha + \alpha^{-2}$. Di conseguenza

$$\alpha + \alpha^{-1} = \alpha + \alpha^{-2},$$

da cui

$$\alpha = \alpha^2, \qquad \text{ossia} \qquad \alpha(\alpha - \overline{1}) = \overline{0}.$$

Pertanto, l'unica radice comune possibile è $\alpha = \overline{1}$. Tuttavia si constata immediatamente che questa non è radice di $f(x)$ se $p > 2$. In conclusione, per nessun primo $p > 2$ $f(x)$ e $g(x)$ hanno radici comuni.

(b) Sia $d(x) = \mathrm{MCD}(f(x), h(x))$. Allora, in particolare, $d(x)$ divide

$$f(x)^p - h(x) = x^{p-1} - \overline{1} = \prod_{\alpha \in \mathbb{Z}_p^*} (x - \alpha).$$

Quindi $d(x) = \overline{1}$, oppure $d(x)$ è prodotto di fattori lineari della forma $(x - \alpha)$ per opportuni $\alpha \in \mathbb{Z}_p^*$, precisamente, di tutti e soli quei fattori $(x - \alpha)$ tali che α sia radice di $f(x)$ e di $h(x)$. Ora, per ogni $\alpha \in \mathbb{Z}_p^*$, $f(\alpha) = \alpha + \alpha^{-1} = h(\alpha)$. Dunque gli elementi α in questione sono tutti e soli quelli per i quali $\alpha^2 = -\overline{1}$. Si osservi che questa uguaglianza è verificata se e solo se $o(\alpha) = 4$ nel gruppo moltiplicativo $\mathbb{Z}_p^*$. Ora, il gruppo ciclico $\mathbb{Z}_p^*$ ha un elemento di periodo 4 se e solo se $p \equiv 1 \pmod 4$. In tal caso gli elementi siffatti sono due (dato che $2 = \varphi(4)$), e sono uno l'opposto dell'altro. Questi due elementi α_1 e $-\alpha_1$ sono dunque le radici comuni a $f(x)$ e $h(x)$, e quindi $d(x) = (x - \alpha_1)(x + \alpha_1) = x^2 + \overline{1}$. Se, invece, $p \equiv 3 \pmod 4$, $f(x)$ e $h(x)$ non hanno radici comuni, e pertanto $d(x) = \overline{1}$.