Traccia del 1° luglio 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 21 sotto l'azione delle potenze di σ e di τ si deduce che $2|t$. D'altra parte, però, se t è pari, τ^t lascia fisso l'elemento 1. Ne consegue che lo stesso deve valere per σ^s, e quindi $4|s$. Ma allora σ^s, a sua volta, lascia fisso l'elemento 21, così 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 noti che:

$$(9, 10, 11, 12, 13) = (9, 13, 12, 11, 10)^4$$
$$(14, 15, 16, 17, 18, 19, 20) = (14, 18, 15, 19, 16, 20, 17)^2.$$

Pertanto, si avrà $\tau^4 = \sigma^{4k}$ per ogni intero k tale che

$k \equiv 4 \pmod 5$
$k \equiv 2 \pmod 7$

Un intero siffatto è $k = 9$. Ciò prova che $\langle\tau^4\rangle \subset \langle\sigma^4\rangle$. Se ne conclude che il sottogruppo cercato è $\langle\sigma^4\rangle = \langle\tau^4\rangle$, di ordine 35.

(b) Con σ e τ commutano le seguenti permutazioni, a due a due disgiunte:

- $\alpha = (1, 2, 3, 4)$, che è un ciclo di σ, mentre $\alpha^2 = (1, 3)(2, 4)$ è prodotto di due cicli di τ;
- $\beta = (5, 6, 7, 8)$, per un motivo analogo;
- $\gamma = (21, 23, 22, 24)$, che è un ciclo di τ, mentre $\gamma^2 = (21, 22)(23, 24)$ è prodotto di due cicli di σ.

Ne consegue che $H = \{\alpha^a\beta^b\gamma^c | a, b, c \in \mathbb{Z}\}$ è un sottogruppo di $C(\sigma) \cap C(\tau)$. Il suo ordine è pari a $o(\alpha)o(\beta)o(\gamma) = 4^3 = 64$.

2.

(a) Per la seconda formulazione del Teorema cinese del resto, il gruppo $\mathbb{Z}_6 \times \mathbb{Z}_7$ è ciclico ed ha come generatore $([1]_6, [1]_7)$. Se $\varphi : \mathbb{Z}_6 \times \mathbb{Z}_7 \to \mathbb{Z}_{21}$ è un omomorfismo di anelli, e quindi di gruppi additivi, tale che $\varphi([1]_6, [1]_7) = \alpha$, allora questa assegnazione lo determina univocamente, in quanto, stante la conservazione dei multipli, per ogni $n \in \mathbb{Z}$ si avrà che $\varphi([n]_6, [n]_7) = n\alpha$. Si può osservare che questa uguaglianza fornisce, per ogni scelta di α, una buona definizione dell'applicazione φ. Infatti, dati $n, m \in \mathbb{Z}$ tali che $([n]_6, [n]_7) = ([m]_6, [m]_7)$, si ha che $6 \cdot 7 | n - m$. In particolare, $21 | n - m$. Poiché, per il Teorema di Lagrange, 21 è multiplo di $o(\alpha)$, e quindi lo è a maggior ragione $n - m$, per la caratterizzazione del periodo avremo quindi

$$n\alpha - m\alpha = (n - m)\alpha = 0,$$

ossia $\varphi([n]_6, [n]_7) = n\alpha = m\alpha = \varphi([m]_6, [m]_7)$. Ciò prova la buona definizione di φ.

D'altra parte, un'applicazione così definita è sempre un omomorfismo di gruppi, com'è immediato verificare. Resta dunque da imporre a φ la conservazione del prodotto. Questa si traduce nella condizione che, per ogni $n, m \in \mathbb{Z}$, si abbia $\varphi(([n]_6, [n]_7)([m]_6, [m]_7)) = \varphi([n]_6, [n]_7)\varphi([m]_6, [m]_7)$, ovvero $nm\alpha = nm\alpha^2$. Ciò vale se e solo se $\alpha = \alpha^2$, ossia se e solo se α è un elemento idempotente di $\mathbb{Z}_{21}$. Ora, dato $a \in \mathbb{Z}$, si ha che $[a]_{21} = [a]_{21}^2$ se e solo se $21 | a(a - 1)$. Poiché $21 = 3 \cdot 7$, questa condizione si compone dei seguenti quattro casi:

- $21|a$, che equivale a $[a]_{21} = [0]_{21}$;
- $21|a-1$, che equivale a $[a]_{21} = [1]_{21}$;
- $3|a$ e $7|a-1$, che, in base alla prima formulazione del Teorema cinese del resto, equivale a $[a]_{21} = [15]_{21}$;
- $7|a$ e $3|a-1$, che, in base alla prima formulazione del Teorema cinese del resto, equivale a $[a]_{21} = [7]_{21}$.

Quindi abbiamo quattro possibili scelte per α, e, precisamente $\alpha \in \{[0]_{21}, [1]_{21}, [7]_{21}, [15]_{21}\}$. Ognuno di esse corrisponde ad un omomorfismo di anelli. In conclusione, il numero degli omomorfismi di anelli è 4.

(b) Osserviamo preliminarmente che $\mathbb{Z}_{25}$ è un gruppo ciclico generato da $[1]_{25}$. Sia $(\alpha, \beta) \in \mathbb{Z}_2 \times \mathbb{Z}_{10}$ tale che $\varphi([1]_{25}) = (\alpha, \beta)$. Allora, per ogni $n \in \mathbb{Z}$, stante la conservazione del multipli, si avrà $\varphi([n]_{25}) = (n\alpha, n\beta)$. Questa è una buona definizione se e solo se, per ogni $n, m \in \mathbb{Z}$ tali che $[n]_{25} = [m]_{25}$ si ha $(n\alpha, n\beta) = (m\alpha, m\beta)$, in altri termini: se e solo se, ogniqualvolta $25|n-m$, si ha $(n-m)\alpha = [0]_2, (n-m)\beta = [0]_{10}$. Ciò si verifica se e solo se $o(\alpha)|25$ e $o(\beta)|25$. D'altra parte, però, in virtù del Teorema d Lagrange, $o(\alpha)|2$ e $o(\beta)|10$. Quindi l'applicazione φ è ben definita se e solo se $o(\alpha) = 1$ e $o(\beta) \in \{1, 5\}$, ossia se e solo se $\alpha = [0]_2$ e $\beta \in \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$. Quindi le possibili scelte per (α, β) sono 5. Ognuna di queste corrisponde ad un'applicazione univocamente determinata, definita come sopra. Essa è, evidentemente, un omomorfismo di gruppi. Il numero degli omomorfismi di gruppi è dunque 5.

(c) Un epimorfismo di anelli $\varphi : \mathbb{Z} \times \mathbb{Z}_2 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_4$ è, ad esempio, l'applicazione definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi(a, [b]_2) = ([b]_2, [a]_4)$. La conservazione di somma e prodotto è di immediata verifica. Facilmente si determina anche il nucleo, che è $\{(4k, [0]_2) | k \in \mathbb{Z}\}$.

3.

(a) Sia $d(x) = \mathrm{MCD}(f(x), g(x))$. Allora $d(x)$ divide $f(x)^p - g(x) = x^p - x = \prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)$. Pertanto $d(x)$ è il prodotto dei fattori lineari $x - \alpha$ che dividono entrambi $f(x)$ e $g(x)$, e per il Teorema di Ruffini, questi sono tutti e soli quelli per i quali α è radice di $f(x)$ e di $g(x)$. Ora, per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = g(\alpha) = 3\alpha + \overline{1}$. Pertanto, per $p = 3$, non vi sono radici, e dunque $d(x) = \overline{1}$. Se, invece, $p \neq 3$, si ha esattamente una radice, ossia $\alpha = -\overline{3}^{-1}$. In tal caso, $d(x) = x + \overline{3}^{-1}$.

(b) Sia $\alpha \in \mathbb{Z}_p$. Come stabilito al punto precedente, se α è radice di $g(x)$, allora è anche radice di $f(x)$, e quindi è radice multipla di $f(x)^p$. Se α fosse radice multipla di $g(x)$, sarebbe dunque radice multipla di $f(x)^p - g(x)$, in quanto $(x - \alpha)^2$ dividerebbe sia $f(x)^p$, sia $g(x)$. Ma ciò è impossibile, in quanto questa differenza, come visto al punto precedente, è prodotto di fattori lineari monici a due a due distinti. La tesi richiesta è stata così provata per assurdo.