Traccia del 14 aprile 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 20 sotto l'azione delle potenze di σ e di τ si deduce che $2|s$ e che $2|t$. Il sottogruppo cercato è dunque $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, dove

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

Una volta considerati, nella decomposizione in cicli disgiunti di σ^2, i fattori

$\gamma_1 = (1,3,2),\ \gamma_2 = (4,6)(5,7),\ \gamma_3 = (8,10,12,9,11),\ \gamma_4 = (13,15,17,19,14,16,18),$

si osserva che

$\tau^2 = \gamma_1^2\gamma_2\gamma_3^2\gamma_4^3.$

Dunque $\tau^2 = \left(\sigma^2\right)^k$, se k è soluzione del seguente sistema di congruenze lineari, certamente risolubile in virtù della prima formulazione del Teorema cinese del resto:

$x \equiv 2 \pmod 3$
$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 7$

Una soluzione particolare è 17. Ne consegue che $\langle\tau^2\rangle \subset \langle\sigma^2\rangle$. In realtà vale l'uguaglianza: infatti $o\left(\sigma^2\right) = o\left(\tau^2\right)$, poiché σ^2 e τ^2 hanno la stessa struttura ciclica. Il sottogruppo cercato è dunque $\langle\tau^2\rangle = \langle\sigma^2\rangle$, ed ha ordine 210.

(b) Al sottogruppo $C(\sigma) \cap C(\tau)$ appartengono le permutazioni

$\alpha = (4,5,6,7),\ \beta_1 = (20,21)(22,23),\ \beta_2 = (20,22)(21,23),\ \beta_3 = (20,23)(21,22)$

insieme ai loro prodotti. La prima è disgiunta dalle restanti tre. Ricordiamo che, inoltre, queste tre permutazioni (tutte di periodo 2), formano, insieme alla permutazione identica β_0, un gruppo (abeliano) di ordine 4. Ne consegue che

$H = \{\alpha^a\beta_i | a \in \mathbb{Z},\ 0 \le i \le 3\}$

è un sottogruppo di $C(\sigma) \cap C(\tau)$ avente ordine $o(\alpha) \cdot 4 = 4 \cdot 4 = 16$. Non è ciclico, in quanto possiede più elementi di periodo 2.

2.

(a) Per la seconda formulazione del Teorema cinese del resto, il gruppo $\mathbb{Z}_4 \times \mathbb{Z}_{49}$ è ciclico ed ha come generatore $([1]_4, [1]_{49})$. Se $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_{49} \to \mathbb{Z}_{14} \times \mathbb{Z}_{14}$ è un omomorfismo di gruppi tale che $\varphi([1]_4, [1]_{49}) = (\alpha, \beta)$, allora questa assegnazione lo determina univocamente, in quanto, stante la conservazione dei multipli, per ogni $n \in \mathbb{Z}$ si avrà che $\varphi([n]_4, [n]_{49}) = (n\alpha, n\beta)$. Si può osservare che questa uguaglianza fornisce, per ogni scelta di (α, β), una buona definizione dell'applicazione φ. Infatti, dati $n, m \in \mathbb{Z}$ tali che $([n]_4, [n]_{49}) = ([m]_4, [m]_{49})$, si ha che $4 \cdot 49 | n - m$. In particolare, $14 | n - m$. Poiché, per il Teorema di Lagrange, 14 è multiplo sia di $o(\alpha)$, sia di $o(\beta)$, e quindi lo è a maggior ragione $n - m$, per la caratterizzazione del periodo avremo quindi

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

ossia $\varphi([n]_4,[n]_{49}) = (n\alpha, n\beta) = (m\alpha, m\beta) = \varphi([m]_4,[m]_{49})$. Ciò prova la buona definizione di φ.

D'altra parte, un'applicazione così definita è sempre un omomorfismo di gruppi, com'è immediato verificare. In conclusione, il numero degli omomorfismi di gruppi da $\mathbb{Z}_4 \times \mathbb{Z}_{49}$ a $\mathbb{Z}_{14} \times \mathbb{Z}_{14}$ è pari al numero degli elementi di $\mathbb{Z}_{14} \times \mathbb{Z}_{14}$, ossia 196.

(b) Se $\psi : \mathbb{Z}_4 \times \mathbb{Z}_{49} \to \mathbb{Z}_{14} \times \mathbb{Z}_{14}$ è un omomorfismo di anelli, allora posto $\varphi([1]_4,[1]_{49}) = (\alpha,\beta)$, la coppia (α,β) deve essere un elemento idempotente, ossia tali sono entrambi α e β. Ora, dato $a \in \mathbb{Z}$, si ha che $[a]_{14}^2 = [a]_{14}$ se e solo se $14|a(a-1)$. Ciò avviene se e solo se uno dei fattori di questo prodotto è divisbile per 14, oppure uno dei fattori è divisibile per 2 e l'altro fattore è divisibile per 7. Dunque gli elementi idempotenti di $\mathbb{Z}_{14}$ sono $[0]_{14}$, $[1]_{14}$, $[7]_{14}$ e $[8]_{14}$, così che gli elementi idempotenti di $\mathbb{Z}_{14} \times \mathbb{Z}_{14}$ sono le coppie ordinate a cui essi danno luogo. Il loro numero è 16. Come dimostrato al punto precedente, l'assegnazione $\psi([1]_4,[1]_{49}) = (\alpha,\beta)$ determina univocamente un omomorfismo di gruppi. D'altra parte, se α,β sono idempotenti, allora ψ conserva il prodotto, ed è dunque un omomorfismo di anelli. Infatti, in tal caso, per ogni $n,m \in \mathbb{Z}$,

$$\psi(([n]_4,[n]_{49})([m]_4,[m]_{49})) = \psi([nm]_4,[nm]_{49}) = (nm\alpha, nm\beta) = \left(nm\alpha^2, nm\beta^2\right) =$$
$$(n\alpha, n\beta)(m\alpha, m\beta) = \psi([n]_4,[n]_{49})(\psi([m]_4,[m]_{49}).$$

In conclusione, 16 è il numero degli omomorfismi di anelli.

(c) L'unico sottogruppo di $\mathbb{Z}_4 \times \mathbb{Z}_{49}$ avente ordine 2 è $\langle([2]_4,[0]_{49})\rangle = \langle([98]_4,[98]_{49})\rangle$. Consideriamo, con la notazione dell'esercizio precedente, un omomorfismo di anelli $\omega : \mathbb{Z}_4 \times \mathbb{Z}_{49} \to \mathbb{Z}_{14} \times \mathbb{Z}_{14}$ definito ponendo, per ogni $n \in \mathbb{Z}$, $\omega([n]_4,[n]_{49}) = (n\alpha, n\beta)$. Supponiamo per assurdo che sia $\ker\omega = \langle([98]_4,[98]_{49})\rangle$. Ciò significa che, per ogni $n \in \mathbb{Z}$, $(n\alpha, n\beta) = ([0]_{14},[0]_{14})$ se e solo se $98|n$. Ma ciò è impossibile, in quanto, comunque siano stati scelti $\alpha,\beta \in \mathbb{Z}_{14}$, si ha certamente $(14\alpha, 14\beta) = ([0]_{14},[0]_{14})$. Ciò prova che non esiste un omomorfismo del tipo indicato.

3.

(a) Poiché $g(x) = f(x)^p + \overline{15}$, il quoziente è $f(x)^{p-1}$, mentre il resto è $\overline{15}$. Il resto è nullo se e solo se $p = 3$ oppure $p = 5$.

(b) In base alla uguaglianza stablita al punto precedente, $f(x)$ e $g(x)$ possono avere radici comuni solo se $p = 3$ oppure $p = 5$. Nel primo caso, però, in virtù del Piccolo Teorema di Fermat, per ogni $\alpha \in \mathbb{Z}_3$, $f(\alpha) = 3\alpha - \overline{2} = -\overline{2}$, quindi $f(x)$ non ha radici. Nel secondo caso, analogamente, per ogni $\alpha \in \mathbb{Z}_5$, $f(\alpha) = g(\alpha) = 3\alpha - \overline{2}$, e quindi $\alpha = \overline{4}$ è la sola radice comune.