Traccia dell'8 novembre 2023

1.

(a) Si ha che $o(\sigma) = \mathrm{mcm}(6,5,4,3) = 60 = o(\tau)$. Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Osserviamo che le potenze di σ che muovono 1, muovono anche 7, inviandoli, rispettivamente, in 2 e in 8, oppure in 3 e in 9. Le stesse potenze di τ inviano 1 e 7, rispettivamente, in 3 e in 8, oppure in 2 e in 9. Ne consegue che potrà essere $\sigma^s = \tau^t$ solo se σ^s e τ^t lasciano entrambi fisso l'elemento 1, ossia solo se s e t sono entrambi multipli di 3. Il sottogruppo cercato è dunque $\langle\sigma^3\rangle \cap \langle\tau^3\rangle$, dove

$\sigma^3 = (10,13,12,11)(14,17)(15,18)(16,19)(20,23,21,24,22)$,
$\tau^3 = (10,11,12,13)(14,15)(16,17)(18,19)(20,22,24,21,23)$.

Pertanto $\alpha = \sigma^{3h} = \tau^{3k}$ per opportuni interi h, k. Dal confronto tra le orbite di 14 sotto le azioni di σ^3 e τ^3 si deduce che h e k sono pari. Dunque il sottogruppo cercato è $\langle\sigma^6\rangle \cap \langle\tau^6\rangle$, ove

$\sigma^6 = (10,12)\,(11,13)(20,21,22,23,24)$,
$\tau^6 = (10,12)\,(11,13)(20,24,23,22,21) = \sigma^{-6}$.

In conclusione, $\langle\alpha\rangle = \langle\sigma^6\rangle = \langle\tau^6\rangle$, un gruppo di ordine 10.

(b) Consideriamo le seguenti permutazioni, a due a due disgiunte, il cui prodotto è σ:

$$\gamma_1 = (1,2,3)(4,5,6), \gamma_2 = (7,8,9), \gamma_3 = (10,11,12,13),$$
$$\gamma_4 = (14,15,16,17,18,19), \gamma_5 = (20,21,22,23,24).$$

Osserviamo preliminarmente che, per ogni indice i, la permutazione γ_i commuta, insieme a tutte le sue potenze, con i cicli di τ disgiunti da γ_i e con i loro prodotti. Pertanto, dato un intero k, la permutazione $\sigma^k = \gamma_1^k\gamma_2^k\gamma_3^k\gamma_4^k\gamma_5^k$ commuta con τ se e solo se

- γ_1^k commuta con $\delta_1 = (1,3,2)(4,6,5)$;
- γ_2^k commuta con $\delta_2 = (7,8,9)$;
- γ_3^k commuta con $\delta_3 = (10,13,12,11)$;
- γ_4^k commuta con $\delta_4 = (14,19,16,15,18,17)$;
- γ_5^k commuta con $\delta_5 = (20,24,23,22,21)$.

Osserviamo quanto segue.

- γ_1 commuta con δ_1, dato che $\gamma_1 = \delta_1^2$, e quindi, **per ogni** k, γ_1^k **commuta con** δ_1;
- $\gamma_2 = \delta_2$, e quindi, banalmente, **per ogni** k, γ_2^k **commuta con** δ_2;
- $\gamma_3 = \delta_3^{-1}$, e quindi, **per ogni** k, γ_3^k **commuta con** δ_3;
- γ_4 non commuta con δ_4, però commuta con δ_4 il suo quadrato, dato che $\gamma_4^2 = \delta_4^2$, e quindi, **per ogni** k **pari**, γ_4^k commuta con δ_4;
- γ_5 commuta con δ_5, essendo il suo inverso, e quindi, **per ogni** k, γ_5^k commuta con δ_5.

In conclusione, σ^k commuta con τ se e solo se k è pari. Quindi l'insieme cercato è il sottogruppo ciclico $\langle\sigma^2\rangle$.

2.

(a) Per il Teorema cinese del resto, essendo 24 e 25 coprimi, il gruppo $\mathbb{Z}_{24} \times \mathbb{Z}_{25}$ è ciclico. Allora tale è anche l'immagine di un omomorfismo di gruppi che lo abbia come gruppo di partenza. Tuttavia, $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$ non è ciclico, dato che, mentre il suo ordine è 150, tutti i suoi elementi hanno come periodo un divisore di $30 = \mathrm{mcm}(10, 15)$. Non esiste dunque un omomorfismo del tipo indicato.

(b) Il sottogruppo $\langle [2]_{24} \rangle \times \langle [6]_{30} \rangle$ di $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ ha ordine $60 = 12 \cdot 5 = o([2]_{24})o([6]_{30})$. Inoltre è ciclico, generato dalla coppia $([2]_{24}, [6]_{30})$, il cui periodo è pari a $\mathrm{mcm}(12, 5) = 60$. Tale sottogruppo è l'immagine dell'applicazione $\varphi : \mathbb{Z}_{12} \times \mathbb{Z}_{10} \to \mathbb{Z}_{24} \times \mathbb{Z}_{30}$ definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_{12}, [b]_{10}) = ([2a]_{24}, [6b]_{30})$: questa, che è chiaramente ben definita, è un omomorfismo di gruppi.

(c) Se un siffatto omomorfismo esiste, allora esso determina un isomorfismo tra $\mathbb{Z}_{12}$ e un sottoanello di $\mathbb{Z}_{24}$, quello che ne costituisce l'immagine. Tale sottoanello ha ordine 12, e dunque coincide con l'unico sottogruppo di $\mathbb{Z}_{24}$ avente quell'ordine, ossia con $\langle [2]_{24} \rangle$. Questo, però, è un anello non unitario, e dunque non può essere isomorfo a $\mathbb{Z}_{12}$. Ciò impedisce l'esistenza di un omomorfismo del tipo indicato. In effetti, dato $a \in \mathbb{Z}$, se fosse $[2a]_{24}[2]_{24} = [2]_{24}$, si avrebbe che $24 | 4a - 2$, ossia che $12 | 2a - 1$, il che è impossibile, dal momento che il numero $2a - 1$ è dispari. Ciò prova che nessun elemento di $\langle [2]_{24} \rangle$ è elemento neutro del prodotto.

3.

(a) Per ogni $\alpha \in \mathbb{Z}_p$ si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = \overline{3}\alpha + \overline{1}$ e $g(\alpha) = \overline{15}\alpha + \overline{2}$. Quindi, se α è radice comune a $f(x)$ e $g(x)$, allora

$$\overline{0} = \overline{5}f(\alpha) - g(\alpha) = \overline{3}.$$

Ciò avviene solo se $p = 3$. Ma in tal caso $f(\alpha) = \overline{1} \neq \overline{0}$. Ne consegue che $f(x)$ e $g(x)$ non hanno mai radici comuni.

(b) Si ha $f(x) - h(x) = -x^{p^2} + x$. Questo polinomio si annulla in ogni elemento di $\mathbb{Z}_p$. Per il Teorema di Ruffini è dunque divisibile per ogni polinomio della forma $x - \alpha$, con $\alpha \in \mathbb{Z}_p$. Ne consegue che ogni polinomio lineare di $\mathbb{Z}_p[x]$ divide $f(x) - h(x)$. Precisamente, si ha:

$$f(x) - h(x) = x\left(\overline{1} - x^{(p-1)(p+1)}\right) = x\left(\overline{1} - x^{p-1}\right)\left(\overline{1} + \sum_{i=1}^{p} x^{(p-1)i}\right).$$

L'ultimo fattore non ha radici, in quanto la sua valutazione in ogni elemento di $\mathbb{Z}_p$ è pari a $\overline{1}$. Ciò è evidente per $\overline{0}$, mentre per $\alpha \neq \overline{0}$ basta applicare il Teorema di Eulero. Di conseguenza, tale polinomio non ha fattori lineari. D'altra parte, $x\left(\overline{1} - x^{p-1}\right) = -\prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)$, quindi ogni fattore lineare di $f(x) - h(x)$ ha molteplicità uno.