Traccia del 10 febbraio 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 $2|t$. Dal confronto tra le orbite di 11 sotto l'azione delle potenze di σ e di τ si deduce inoltre che $4|s$. Il sottogruppo cercato è dunque $\langle\sigma^4\rangle \cap \langle\tau^2\rangle$, dove

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

Poiché σ^4 lascia fisso 1, tutte le permutazioni del sottogruppo cercato lo lasceranno fisso. Ne consegue che $4|t$. Pertanto il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, dove

$\tau^4 = (3,5,4)(6,7,8)(15,18,16,19,17).$

Ora, $o(\sigma^4) = 15$, e l'unico sottogruppo di $\langle\sigma^4\rangle$ avente ordine 3 è generato da $(3,4,5)(6,7,8)$. D'altra parte, si ha anche $o(\tau^4) = 15$, ma l'unico sottogruppo di $\langle\tau^4\rangle$ avente ordine 3 è generato da $(3,5,4)(6,7,8)$. Questo sottogruppo è distinto dal precedente. Ne consegue che il sottogruppo $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$ non può avere ordine divisibile per 3. Dunque $3|s$ e $3|t$, e quindi il sottogruppo cercato è $\langle\sigma^{12}\rangle \cap \langle\tau^{12}\rangle$, ove

$\sigma^{12} = (15,17,19,16,18),$
$\tau^{12} = (15,19,18,17,16).$

Poiché $(\sigma^{12})^2 = \tau^{12}$, queste due permutazioni generano lo stesso sottogruppo di ordine 5. In conclusione, l'intersezione cercata è $\langle\sigma^{12}\rangle = \langle\tau^{12}\rangle$.

(b) Al sottogruppo $C(\sigma) \cap C(\tau)$ appartengono le seguenti permutazioni, a due a due disgiunte:

$\alpha_1 = (3,4,5),\ \alpha_2 = (6,7,8),\ \beta = (11,13)(12,14),$

insieme alle loro potenze e ai loro prodotti. Ne consegue che

$H = \{\alpha_1^{a_1}\alpha_2^{a_2}\beta^b \mid a_1, a_2, b \in \mathbb{Z}\}$

è un sottogruppo di $C(\sigma) \cap C(\tau)$ avente ordine $o(\alpha_1)o(\alpha_2)o(\beta) = 3 \cdot 3 \cdot 2 = 18$. Non è ciclico, in quanto nessuno dei suoi elementi ha periodo 18: infatti, per ogni $\delta \in H$, si ha $\delta^6 = id$.

(c) Al sottogruppo K appartengono tutte le potenze di σ e di τ, insieme ai loro prodotti. Quindi a K appartengono gli elementi

$\sigma^{30} = (11,13)(12,14)$
$\tau^{30} = (1,2)(9,10)$
$\sigma^{30}\tau^{30} = (1,2)(9,10)(11,13)(12,14).$

Questi, insieme a id, costituiscono un sottogruppo di ordine 4, isomorfo al gruppo di Klein.

Nota: Lo stesso sottogruppo risponde anche al quesito (b), in quanto è contenuto in $C(\sigma) \cap C(\tau)$.

2.

(a) Supponiamo che esista un epimorfismo di gruppi $\varphi : \mathbb{Z}_3 \times \mathbb{Z}_6 \to \mathbb{Z}_9$. Siano $\lambda, \mu \in \mathbb{Z}$ tali che $\varphi([1]_3,\ [0]_6) = [\lambda]_9$ e $\varphi([0]_3,\ [1]_6) = [\mu]_9$. Allora, dalla conservazione dell'elemento neutro e dei multipli segue che

$$[0]_9 = \varphi([0]_3, [0]_6) = \varphi(3([1]_3, [0]_6)) = 3\varphi([1]_3,\ [0]_6) = [3\lambda]_9.$$

Pertanto $3|\lambda$. In modo analogo si prova che $3|\mu$. Ma da ciò segue facilmente che $\mathrm{Im}\varphi \subset \langle [3]_9 \rangle \neq \mathbb{Z}_9$. Dunque φ non è surgettivo. Si conclude che non esiste un epimorfismo del tipo richiesto.

(b) Se esiste un monomorfismo di anelli $\psi : \mathbb{Z}_3 \times \mathbb{Z}_9 \to \mathbb{Z}_6 \times \mathbb{Z}_{18}$, allora $\mathrm{Im}\ \psi$ è un sottoanello B di $\mathbb{Z}_6 \times \mathbb{Z}_{18}$ isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_9$, e dunque avente ordine 27. Un sottogruppo di $\mathbb{Z}_6 \times \mathbb{Z}_{18}$ di ordine 27 è il prodotto diretto $\langle [2]_6 \rangle \times \langle [2]_{18} \rangle$, ed è immediato osservare che questo è anche un sottoanello, in quanto evidentemente chiuso rispetto al prodotto. Inoltre è dotato di un elemento neutro del prodotto, che è $([4]_6,\ [10]_{18})$.
Dato che ψ conserva l'elemento uno, si avrà, inoltre:

$$\psi([1]_3, [1]_9) = ([4]_6, [10]_{18}).$$

Ciò suggerisce di definire ψ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$\psi([a]_3, [b]_9) = ([4a]_6, [10b]_{18}).$$

Si può facilmente verificare che, in questo modo, si ottiene effettivamente un monomorfismo di anelli.

3.

(a) Si ha

$$f(x) = \left(x^p + x^2 - x + \overline{1}\right)^p = \left(x\left(x^{p-1} - \overline{1}\right) + x^2 + \overline{1}\right)^p = \ell(x)^p,$$
$$g(x) = \left(x^2 + \overline{1}\right)\left(x^p - \overline{1}\right) = \left(x^2 + \overline{1}\right)(x - \overline{1})^p.$$

Poiché, essendo $p > 2$, $\overline{1}$ non è radice di $f(x)$, il polinomio $f(x)$ non possiede il fattore irriducibile $x - \overline{1}$. Pertanto, Il massimo comune divisore cercato è $d(x) = \mathrm{MCD}\left(\ell(x),\ x^2 + \overline{1}\right)$, e dunque si ha, evidentemente, $d(x) = \mathrm{MCD}\left(x^{p-1} - \overline{1},\ x^2 + \overline{1}\right)$. A questo punto si considera la fattorizzazione di $m(x) = x^2 + \overline{1}$ in $\mathbb{Z}_p[x]$. Come ben noto, $m(x)$ è riducibile se e solo se è dotato di radici in $\mathbb{Z}_p$, ossia se e solo se esiste qualche $\alpha \in \mathbb{Z}_p$ tale che $\alpha^2 = -\overline{1}$, ossia tale che $o(\alpha) = 4$ nel gruppo moltiplicativo $\mathbb{Z}_p^*$, e ciò avviene se e solo se $p \equiv 1 \pmod 4$. In tal caso $m(x)$ ha esattamente due radici (distinte) α_1 e $-\alpha_1$ in $\mathbb{Z}_p$, e dunque $m(x) = (x - \alpha_1)(x - \alpha_2)$ è un divisore di

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

In conclusione, se $p = 1 \pmod 4$, allora $d(x) = m(x) = x^2 + \overline{1}$.
Se, invece, $p \equiv 3 \pmod 4$, allora $m(x)$ è irriducibile, e dunque coprimo con $x^{p-1} - \overline{1}$. Pertanto, in tal caso, $d(x) = \overline{1}$.

(b)
Ogni radice comune a f ed h è non nulla. Sia dunque $\alpha \in \mathbb{Z}_p^*$. Allora, in virtù del Piccolo Teorema di Fermat e del Teorema di Eulero, $f(\alpha) = \alpha^2 + \overline{1}$, mentre $h(\alpha) = \alpha^3 - \overline{2}$. Ora, se α è radice comune, allora, $\alpha^2 = -\overline{1}$ e $\alpha^3 = \overline{2}$. Se ne deduce che $\alpha = -\overline{2}$. Ma questa è una radice di f se e solo se $p = 5$, ed allora è anche radice di h. In conclusione, f ed h non hanno radici comuni se $p \neq 5$, mentre hanno $\overline{3}$ come unica radice comune se $p = 5$.