Traccia del 9 febbraio 2026

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Dal confronto tra le orbite di 4 sotto l'azione delle potenze di σ e di τ si deduce che $2|t$. Dal confronto tra le orbite di 10 si deduce inoltre che $2|t$. Quindi $s = 2h,\ t = 2k$, per opportuni interi h, k e il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, dove

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

Dal confronto tra le orbite di 16 sotto l'azione delle potenze di σ e di τ si ricava ancora che $2|h$ e $2|k$. Quindi il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, dove

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

Poiché queste permutazioni sono una l'inversa dell'altra, generano lo stesso sottogruppo. Quindi il sottogruppo cercato è $\langle\sigma^4\rangle = \langle\tau^4\rangle$, di ordine 3.

(b) Con σ e con τ commutano le seguenti permutazioni:

- $\alpha = (1,2,3)$, che è un ciclo di σ e l'inverso di un ciclo di τ;
- $\beta = (4,5,6)(7,8,9)$, in quanto è il prodotto di due cicli di σ ed è il quadrato del ciclo $(4,7,5,8,6,9)$ di τ.

Al sottogruppo $C(\sigma) \cap C(\tau)$ appartengono dunque α, β, insieme al loro prodotto $\alpha\beta$. Queste sono tre permutazioni di periodo 3. Poiché $3 > \varphi(3) = 2$, ciò esclude che $C(\sigma) \cap C(\tau)$ sia ciclico.

2.

(a) In base alla seconda formulazione del Teorema cinese del resto, il gruppo $\mathbb{Z}_{15} \times \mathbb{Z}_{22}$ è ciclico, essendo 15 e 22 coprimi. Precisamente, è generato da $([1]_{15}, [1]_{22})$. Di conseguenza, ogni omomorfismo di gruppi $\varphi : \mathbb{Z}_{15} \times \mathbb{Z}_{22} \to \mathbb{Z}_2 \times \mathbb{Z}_5$ è univocamente determinato da $\varphi([1]_{15}, [1]_{22}) = (\alpha, \beta)$. Infatti, dalla conservazione dei multipli segue che, per ogni $n \in \mathbb{Z}$, $\varphi([n]_{15}, [n]_{22}) = (n\alpha, n\beta)$. Si può facilmente verificare che, per ogni scelta di (α, β), si ottiene un'applicazione ben definita. Risulta, inoltre, che $\mathrm{Im}\varphi$ è il sottogruppo di $\mathbb{Z}_2 \times \mathbb{Z}_5$ generato da (α, β). Pertanto, φ è un epimorfismo se e solo se $\langle(\alpha, \beta)\rangle = \mathbb{Z}_2 \times \mathbb{Z}_5$. Ora, $\mathbb{Z}_2 \times \mathbb{Z}_5$, che è isomorfo a $\mathbb{Z}_{10}$, ha esattamente quattro generatori, e dunque, quattro sono le scelte per (α, β), precisamente

$$(\alpha, \beta) \in \{([1]_2, [1]_5),\ ([1]_2, [2]_5),\ ([1]_2, [3]_5),\ ([1]_2, [4]_5)\}.$$

Quattro sono dunque gli epimorfismi richiesti.

(b) Sia $\psi : \mathbb{Z}_3 \times \mathbb{Z}_{15} \to \mathbb{Z}_{24} \times \mathbb{Z}_{60}$ un monomorfismo di anelli. Poiché è, in particolare, un monomorfismo di gruppi additivi, conserva il periodo di ogni elemento. Inoltre, conservando il prodotto, invia elementi idempotenti in elementi idempotenti. Dunque $\psi([1]_3, [0]_{15})$ sarà un elemento idempotente dell'anello $\mathbb{Z}_{24} \times \mathbb{Z}_{60}$ avente periodo 3, mentre $\psi([0]_3, [1]_{15})$ sarà un elemento idempotente avente periodo 15. Ora, gli elementi di $\mathbb{Z}_{24}$ aventi periodo 3 sono $[8]_{24}$ e $[16]_{24}$. Poiché $16^2 - 16 = 240$, l'elemento $[16]_{24}$ è idempotente nell'anello $\mathbb{Z}_{24}$. Possiamo anche constatare che $[16]_{60}$ è idempotente nell'anello $\mathbb{Z}_{60}$, oltre ad essere un elemento di $\mathbb{Z}_{60}$ avente periodo 15. Se poniamo $\psi([1]_3,[0]_{15}) = ([16]_{24},[0]_{60})$, $\psi([0]_3,[1]_{15}) = ([0]_{24},[16]_{60})$, otterremo l'omomorfismo di gruppi definito da: $\psi([a]_3,[b]_{15}) = ([16a]_{24},[16b]_{60})$ per ogni $a,b \in \mathbb{Z}$. Questo, come si può facilmente verificare, è ben definito, ha nucleo banale e conserva il prodotto, ed è dunque un monomorfismo di anelli.

(c) Un sottogruppo di $\mathbb{Z}_6 \times \mathbb{Z}_{80}$ avente ordine 12 è $H = \mathbb{Z}_6 \times \langle [40]_{80} \rangle$. L'applicazione $\omega : \mathbb{Z}_6 \times \mathbb{Z}_{80} \to \mathbb{Z}_{40} \times \mathbb{Z}_{60}$ tale che, per ogni $a,b \in \mathbb{Z}$, $\omega([a]_6,[b]_{80}) = ([b]_{40},\ [0]_{60})$ è un omomorfismo di gruppi ben definito avente H come nucleo.

3.

(a) Si ha $g(x) = \left(x^p - x\right)^2$. Inoltre

$$f(x) = x^{p^3} - x^{p^2} - \left(x^{p^2} - x^p\right) + \overline{1} = \left(x^p - x\right)^{p^2} - \left(x^p - x\right)^p + \overline{1}.$$

Poiché $p \geq 2$, ne consegue che il resto cercato è il polinomio costante $r(x) = \overline{1}$.

(a) Osserviamo che $g(x) = \prod_{\alpha \in \mathbb{Z}_p} (x-\alpha)^2$. Notiamo inoltre che $h(x) = \left(x^2 + \overline{1}\right)^p$. Dato che $g(x)$ si decompone nel prodotto di fattori lineari, $g(x)$ e $h(x)$ saranno coprimi se $x^2 + \overline{1}$ non possiede fattori lineari, in altri termini, tenendo conto del primo corollario al Teorema di Ruffini;

1) se $x^2 + \overline{1}$ non ammette radici in $\mathbb{Z}_p$, allora $MCD(g(x),h(x)) = \overline{1}$.

Supponiamo adesso che $x^2 + \overline{1}$ ammetta radici $\alpha_1, \alpha_2 \in \mathbb{Z}_p$. In tal caso si decompone nel prodotto $(x-\alpha_1)(x-\alpha_2)$. Ora, $x - \alpha_1$ compare nella fattorizzazione di $g(x)$ con molteplicità 2, mentre $h(x) = (x-\alpha_1)^p(x-\alpha_2)^p$. Si noti, però che, se $\alpha_1 = \alpha_2$, allora $x^2 + \overline{1} = (x-\alpha_1)^2$. Si distinguono pertanto i seguenti due casi:

2) se $x^2 + \overline{1}$ ha una radice doppia, allora $MCD(g(x),h(x)) = x^2 + \overline{1}$;

3) se $x^2 + \overline{1}$ ha due radici semplici, allora $MCD(g(x),h(x)) = \left(x^2 + \overline{1}\right)^2$.

Osserviamo anzitutto che 2) vale per $p = 2$. Per $p > 2$, $x^2 + \overline{1}$ ha radici se e solo se esiste $\alpha \in \mathbb{Z}_p$ tale che $\alpha^2 = -\overline{1}$, ossia se e solo se esiste un elemento di $\mathcal{U}(\mathbb{Z}_p)$ avente periodo 4. Poiché $\mathcal{U}(\mathbb{Z}_p)$ è un gruppo ciclico, ciò equivale alla condizione che 4 divida $p-1$, ossia $p \equiv 1 \pmod 4$. In tal caso, le radici α_1, α_2 sono distinte, in quanto sono i due elementi di periodo 4 in $\mathcal{U}(\mathbb{Z}_p)$ (sono, per altro, una l'opposta dell'altra). In tal caso vale 3). In conclusione, 1) vale se 4 non divide $p-1$, ossia se $p \equiv 3 \pmod 4$.