

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 1 sotto l'azione delle potenze di σ e di τ si deduce che $2|s$ e $2|t$. 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

$$\sigma^2 = (7, 9, 11, 13, 8, 10, 12)(14, 16, 18, 15, 17)$$

$$\tau^2 = (7, 12, 10, 8, 13, 11, 9)(14, 18, 17, 16, 15).$$

Si osserva che, posto $\gamma_1 = (7, 9, 11, 13, 8, 10, 12)$ e $\gamma_2 = (14, 16, 18, 15, 17)$, risulta $\sigma^2 = \gamma_1\gamma_2$, mentre $\tau^2 = \gamma_1^6\gamma_2^2$. Pertanto si avrà che $\tau^2 = \sigma^{2u}$, per ogni intero u tale che

$$u \equiv 6 \pmod{7}$$

$$u \equiv 2 \pmod{5}$$

In base al Teorema Cinese del Resto, un intero u siffatto esiste, e si può prendere $u = 27$. Ne consegue che $\tau^2 \in \langle \sigma^2 \rangle$, e dunque, essendo $o(\tau^2) = o(\sigma^2) = \text{mcm}(7, 5) = 35$, si conclude che $\langle \tau^2 \rangle = \langle \sigma^2 \rangle$ è l'intersezione cercata.

(b) A $C(\sigma)$ appartiene il 6-ciclo $\delta = (1, 3, 5, 2, 4, 6)$, in quanto $\delta^3 = (1, 2)(3, 4)(5, 6)$ è il prodotto di tre cicli di σ , mentre δ è disgiunto dai restanti cicli di σ . Dunque a $C(\sigma)$ appartengono anche δ^2 e δ^4 . Ne consegue che $\langle \delta^2 \rangle = \{id, \delta^2, \delta^4\}$ è un sottogruppo di $C(\sigma)$, di ordine 3.

(c) Osserviamo preliminarmente che con σ commuta ogni permutazione che commuti con $(1, 3)(2, 4)$ e che sia disgiunta dai restanti cicli di σ . Quindi a $C(\sigma)$ appartengono le permutazioni $(1, 2)(3, 4)$, $(1, 4)(2, 3)$, ma anche il 4-ciclo $(1, 3, 2, 4)$, insieme alle sue potenze. Pertanto $C(\sigma)$ contiene i seguenti due sottogruppi di ordine 4:

$$H_1 = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \text{ e } H_2 = \langle (1, 3, 2, 4) \rangle.$$

Entrambi hanno ordine 4, e non sono isomorfi.

2.

(a) Applicando due volte il Teorema Cinese del Resto si ricavano le seguenti relazioni di isomorfismo tra anelli:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{120} \simeq \mathbb{Z}_{10} \times \mathbb{Z}_3 \times \mathbb{Z}_{40} \simeq \mathbb{Z}_{30} \times \mathbb{Z}_{40}.$$

Determiniamo ora un isomorfismo di anelli $\varphi: \mathbb{Z}_{10} \times \mathbb{Z}_{120} \rightarrow \mathbb{Z}_{30} \times \mathbb{Z}_{40}$ definito ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi([a]_{10}, [b]_{120}) = ([\lambda a + \mu b]_{30}, [b]_{40})$, dove λ, μ sono interi opportunamente scelti. L'applicazione φ è ben definita se e solo se λ è multiplo di 3. In tal caso $\lambda = 3s$ e φ è un omomorfismo di gruppi. Imponiamo ora la conservazione del prodotto, che è garantita dalle seguenti tre condizioni:

$$\begin{array}{ll} 30|9s^2 - 3s & 10|s(3s - 1) \\ 30|\mu^2 - \mu & \text{ossia, equivalentemente, } 30|\mu(\mu - 1) \\ 30|3s\mu & 10|s\mu \end{array}$$

I numeri $s = 7, \mu = 10$ verificano tutte le proprietà richieste. Abbiamo dunque determinato un omomorfismo di anelli definito da $\varphi([a]_{10}, [b]_{120}) = ([21a + 10b]_{30}, [b]_{40})$. Si verifica facilmente che il suo nucleo è banale, il che prova la sua iniettività. Poiché i gruppi di partenza e di arrivo

hanno lo stesso ordine, segue che φ è un isomorfismo.

Nota: Volendo provare direttamente la suriettività, si può osservare che ad $\text{Im}\varphi$ appartengono gli elementi

$$([0]_{30}, [1]_{40}) = ([21 \cdot 0 + 10 \cdot 81]_{30}, [81]_{40}) = \varphi([0]_{10}, [81]_{120})$$

e

$$([1]_{30}, [0]_{40}) = ([21 \cdot 1 + 10 \cdot 40]_{30}, [40]_{40}) = \varphi([1]_{10}, [40]_{120}).$$

(b) Si ha $231 = 3 \cdot 7 \cdot 11$, $49 = 7^2$, $363 = 3 \cdot 11^2$. Consideriamo un'applicazione $\psi: \mathbb{Z}_{231} \rightarrow \mathbb{Z}_{49} \times \mathbb{Z}_{363}$ definita ponendo, per ogni $a \in \mathbb{Z}$, $\psi([a]_{231}) = ([\lambda a]_{49}, [\mu a]_{363})$, per opportuni interi λ, μ . Questa è ben definita se e solo se $7|\lambda$ e $11|\mu$, ed in tal caso è un omomorfismo di gruppi. Poniamo allora $\lambda = 7, \mu = 11$. Dato un intero a , si ha $[7a]_{49} = [0]_{49}$ se e solo se $7|a$ e $[11a]_{363} = [0]_{363}$ se e solo se $33|a$. Quindi $[a]_{231} \in \text{Ker}\psi$ implica che $231|a$, ossia $[a]_{231} = [0]_{231}$. Ciò prova che l'applicazione trovata è un monomorfismo, come richiesto.

3.

(a) Si ha:

$$\begin{aligned} f(x) - g(x)^p &= x^{p^4} + x^{p^3} + x^{p^2} + x^p + x + \bar{1} - x^{p^4} + x^{p^2} - x^p + \bar{1} = \\ &= x^{p^3} + \bar{2}x^{p^2} + x + \bar{2}. \end{aligned}$$

Sottraendo ancora $g(x)$, si ottiene:

$$x^{p^3} + \bar{2}x^{p^2} + x + \bar{2} - x^{p^3} + x^p - x + \bar{1} = \bar{2}x^{p^2} + x^p + \bar{3}.$$

Questo è dunque il resto cercato.

(b) Posto $d(x) = \text{MCD}(f(x), g(x))$, si osservi che $d(x)$ divide $r(x) = f(x) - g(x)^p - g(x)$, il resto precedentemente trovato. D'altra parte $r(x) = (\bar{2}x^p + x + \bar{3})^p = (\bar{2}x^p - \bar{2}x + \bar{3}x + \bar{3})^p$. Per $p = 2$ o per $p = 3$ questo polinomio è un prodotto di fattori lineari. Dunque tale è anche $d(x)$, sempre che se non sia uguale a $\bar{1}$. Ma ciò non avviene, nei due casi considerati, perché per $p = 2$ o $p = 3$ $f(x)$ e $g(x)$ hanno radice $\bar{1}$, e quindi sono divisibili per il fattore lineare $x - \bar{1}$.