**Traccia dell'8 settembre 2026**

**1.**

**(a)** A $C(\sigma)$ appartengono le permutazioni $(4,5)$ e $(5,6)$, che da $\sigma$ sono disgiunte. Ma queste permutazioni non commutano tra loro. Quindi $C(\sigma)$ non è abeliano.

**(b)** Le permutazioni $\sigma$ e $\tau$ commutano tra loro, in quanto sono disgiunte. Pertanto esse appartengono a $C(\sigma) \cap C(\tau)$, insieme al loro prodotto. Ma nessun gruppo abeliano finito può avere più di due elementi di periodo $3$. Ciò prova che $C(\sigma) \cap C(\tau)$ non è abeliano.

**2.**

**(a)** Sia $\varphi : \mathbb{Z}_{125} \to \mathbb{Z}_{625}$ un monomorfismo di anelli. In virtù della conservazione del prodotto, $\varphi([1]_{125}) = [a]_{625}$ è un elemento idempotente di $\mathbb{Z}_{625}$, ossia $a$ è un intero tale che $625 = 5^4 \mid a^2 - a = a(a-1)$. Poiché $a$ ed $a-1$ non possono essere entrambi divisibili per $5$, la precedente condizione si scinde in due casi: $5^4 \mid a$ oppure $5^4 \mid a-1$. Nel primo caso, $\varphi([1]_{125}) = [0]_{625}$, da cui segue che $\varphi$ non è monomorfismo (perché il nucleo non è banale). D'altra parte, però, nel secondo caso, si avrebbe $\varphi([1]_{125}) = [1]_{625}$, il che, nuovamente, esclude che $\varphi$ sia un monomorfismo (in quanto un monomorfismo di gruppi conserva i periodi). Ciò basta per escludere l'esistenza di un monomorfismo del tipo cercato.

Nota: Si può anche osservare, per maggiore precisione, che, dovendo valere la conservazione del multipli, nel primo dei due casi esaminati, $\varphi$ sarebbe l'omomorfismo nullo, mentre il secondo caso non darebbe luogo ad un omomorfismo di gruppi ben definito.

**(b)** Siano $\lambda, \mu$ interi. Allora l'applicazione $\psi : \mathbb{Z}_{30} \times \mathbb{Z}_3 \to \mathbb{Z}_{15}$ tale che, per ogni $a, b \in \mathbb{Z}$, si abbia $\psi([a]_{30}, [b]_3) = [\lambda a + \mu b]_{15}$ è un omomorfismo di gruppi ogniqualvolta sia ben definita. Ciò vale se e solo se $5 \mid \mu$. Sia dunque $\mu = 5s$, per qualche intero $s$. Allora $\psi$ è un epimorfismo se e solo se $[1]_{15} \in Im\psi = \{[\lambda a + 5sb]_{15} \mid a, b \in \mathbb{Z}\}$. In virtù del Lemma di Bézout, ciò avviene se $\lambda$ e $5s$ sono coprimi. Ponendo $\lambda_1 = 1,\ \mu_1 = 5$ e $\lambda_2 = 1,\ \mu_2 = 10$ si ottengono due distinti epimorfismi di gruppi. La stessa proprietà si verifica anche quando $\lambda$ è coprimo con $15$ e $s = 0$, perché in tal caso $Im\psi = \langle [\lambda]_{15} \rangle = \mathbb{Z}_{15}$. Quindi si ottengono due epimorfismi anche ponendo $\lambda_1 = 1,\ \mu_1 = 0$ e $\lambda_2 = 2,\ \mu_2 = 0$.

**(c)** Se esiste un monomorfismo del tipo indicato, allora $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ possiede un sottogruppo isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_4$. Consideriamo, in entrambi i gruppi, gli elementi di periodo $4$. Sia $\alpha \in \mathbb{Z}_2$, $\beta \in \mathbb{Z}_{16}$. Abbiamo, naturalmente, $o(\alpha, [0]_{16}) = o(\alpha) \mid 2$, mentre, se $\beta \neq [0]_{16}$, allora $o(\alpha, \beta) = \mathrm{mcm}(o(\alpha), o(\beta)) = o(\beta)$, poiché $o(\beta)$, che, per Lagrange, è un divisore di $16$, in questo caso è una potenza di $2$ con esponente positivo, e quindi è un multiplo di $o(\alpha)$. Pertanto, gli elementi di $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ aventi periodo $4$ sono: $([0]_2, [4]_{16})$, $([1]_2, [4]_{16})$, $([0]_2, [12]_{16})$, $([1]_2, [12]_{16})$. Tuttavia, gli elementi di periodo $4$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$ sono in numero maggiore. Sono infatti tutte e sole le coppie aventi una delle seguenti forme: $(\alpha, [1]_4)$, $([1]_4, \beta)$, $(\alpha, [3]_4)$, $([3]_4, \beta)$. Ciò esclude che $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ possieda un sottogruppo isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_4$.

**3.**

**(a)** Si ha $f(x) = \left(x^2 + \overline{3}x + \overline{2}\right)^{p^2} = (x + \overline{1})^{p^2}(x + \overline{2})^{p^2}$, prodotto di fattori lineari, mentre

$$g(x) = \left(x^p - x\right)^{p^3} + \left(x^p - x\right)^p = \left(x^p - x\right)^p \left(\left(x^p - x\right)^{p^3 - p} + \overline{1}\right) = \left(\prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)^p\right) q(x),$$

ove $q(x)$, assumendo ovunque il valore $\overline{1}$, è privo di radici in $\mathbb{Z}_p$ e quindi non ha fattori lineari in $\mathbb{Z}_p[x]$. Ne consegue che $\mathrm{MCD}(f(x),\ g(x)) = (x + \overline{1})^p (x + \overline{2})^p = x^{2p} + \overline{3}x^p + \overline{2}$.

**(b)** Si ha $h(x) = x^6 \left(x^{6(p^3-1)} + x^{6(p^2-1)} + x^{6(p-1)} + \overline{1}\right)$, quindi $h(x)$ ha sempre $\overline{0}$ come radice di

molteplicità $6$. Sia ora $\alpha \in \mathbb{Z}_p^*$. Allora, per il Piccolo Teorema di Fermat, $h(\alpha) = \overline{4}\alpha^6$, che è nullo se e solo se $p = 2$. Questo è l'unico caso in cui $h(x)$ possiede una seconda radice, ossia $\overline{1}$. Ne determiniamo la molteplicità. A tal fine osserviamo che, per $p = 2$,

$$h(x) = \left(x^{6\cdot 8} + \overline{1}\right) + \left(x^{6\cdot 4} + \overline{1}\right) + \left(x^{6\cdot 2} + \overline{1}\right) + \left(x^6 + \overline{1}\right) =$$

$$\left(x^6 + \overline{1}\right)^8 + \left(x^6 + \overline{1}\right)^4 + \left(x^6 + \overline{1}\right)^2 + \left(x^6 + \overline{1}\right) =$$

$$\left(x^6 + \overline{1}\right)\left(\left(x^6 + \overline{1}\right)^7 + \left(x^6 + \overline{1}\right)^3 + \left(x^6 + \overline{1}\right) + \overline{1}\right),$$

ove il secondo fattore non si annulla in $\overline{1}$, e dunque non è divisibile per $x + \overline{1}$. Per contro,

$$\left(x^6 + \overline{1}\right) = \left(x^3 + \overline{1}\right)^2 = (x + \overline{1})^2\left(x^2 + x + \overline{1}\right)^2.$$

Ciò prova che la molteplicità cercata è $2$.