Traccia del 1° luglio 2024

1.

(a) Sia $\sigma^s = \tau^t$ 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 $4|s$, dal confronto tra le orbite di 17 si ricava, in maniera analoga, che $4|t$. Di conseguenza, il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, ove

$$\sigma^4 = (5,9,8,7,6)(10,14,11,15,12,16,13),$$
$$\tau^4 = (5,6,7,8,9)(10,11,12,13,14,15,16).$$

Ora si osserva che $\sigma^4 = \left(\tau^4\right)^4$, e si conclude quindi che il sottogruppo cercato è $\langle\sigma^4\rangle$, il cui ordine è $\mathrm{mcm}(5,7) = 35$.

(b) La permutazione $\alpha = (1,3)(2,4)$ commuta con

- σ, in quanto è il quadrato di $(1,2,3,4)$, uno dei cicli associati a σ;
- τ, in quanto commuta con $(1,2)(3,4)$, prodotto di due dei cicli associati a τ, ed è disgiunta dai restanti cicli associati a τ.

Analogamente si vede che anche $\beta = (17,19)(18,20)$ commuta con entrambi σ e τ. Sono stati così trovati due elementi di $C(\sigma) \cap C(\tau)$ aventi periodo 2, il che è impossibile in un gruppo ciclico. Ne consegue che la risposta al quesito è negativa.

2.

(a) L'immagine di un monomorfismo di anelli da $\mathbb{Z}_4 \times \mathbb{Z}_5$ a $\mathbb{Z}_8 \times \mathbb{Z}_{10}$ sarebbe un sottoanello B di $\mathbb{Z}_8 \times \mathbb{Z}_{10}$ isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_5$. Quindi, per il Teorema cinese del resto, B sarebbe un anello isomorfo a $\mathbb{Z}_{20}$, e quindi un anello unitario, ed un gruppo additivo ciclico di ordine 20. Poiché un isomorfismo tra anelli unitari conserva l'elemento uno, e, in quanto isomorfismo di gruppi, anche il periodo degli elementi, in B, come in $\mathbb{Z}_{20}$, l'elemento uno sarebbe un generatore del gruppo additivo. Sia dunque (α,β) l'elemento uno di B. Allora $20 = o((\alpha,\beta)) = \mathrm{mcm}(o(\alpha), o(\beta))$. Ora, per il Teorema di Lagrange, $o(\beta)$ divide 10. Quindi avremo necessariamente che $o(\alpha) = 4$. In conclusione, sarà $\alpha \in \{[2]_8, [6]_8\}$. D'altra parte, però, essendo (α,β) idempotente rispetto al prodotto, dev'essere $\alpha^2 = \alpha$. Ma nessuno tra $[2]_8$ e $[6]_8$ gode di questa proprietà. Ciò costituisce una contraddizione e prova che non esiste un monomorfismo del tipo richiesto.

(b) Se un siffatto epimorfismo esiste, allora trasforma l'elemento uno dell'anello di partenza nell'elemento uno dell'anello di arrivo. In altri termini, $[1]_{36}$ viene inviato in $([1]_3, [1]_6)$. Poiché questa applicazione è anche un omomorfismo di gruppi additivi, e, in quanto tale, conserva i multipli, la sua immagine è il sottogruppo ciclico $\langle([1]_3, [1]_6)\rangle$ di $\mathbb{Z}_3 \times \mathbb{Z}_6$. Ma tale sottogruppo ha ordine 6. Ne consegue che l'applicazione considerata non è surgettiva, contro la nostra iniziale supposizione. Ciò prova che non esiste un epimorfismo del tipo richiesto.
Svolgimento alternativo (più breve): se il gruppo di partenza di un omomorfismo di gruppi è un gruppo ciclico, tale è anche la sua immagine. Ora: $\mathbb{Z}_{36}$ è ciclico, mentre tale non è $\mathbb{Z}_3 \times \mathbb{Z}_6$. Pertanto tra $\mathbb{Z}_{36}$ e $\mathbb{Z}_3 \times \mathbb{Z}_6$ non esiste nemmeno un epimorfismo di gruppi.

(c) L'anello $\mathbb{Z}_2 \times \mathbb{Z}_8$ ha un sottoanello isomorfo a $\mathbb{Z}_2$, formato dagli elementi $([0]_2, [0]_8)$ e $([1]_2, [0]_8)$. Quest'ultimo elemento è idempotente rispetto al prodotto e, inoltre, ha periodo 2 rispetto

alla struttura di gruppo additivo. Un elemento con le stesse proprietà esiste, naturalmente, in ogni anello isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_8$. Ma $\mathbb{Z}_8 \times \mathbb{Z}_{16}$ non possiede un elemento siffatto: nessuno dei suoi elementi di periodo 2, che sono $([4]_8, [0]_{16}), ([0]_8, [8]_{16}), ([4]_8, [8]_{16})$, è idempotente rispetto al prodotto. Infatti il quadrato di ognuno di essi è la coppia nulla. Ciò esclude che $\mathbb{Z}_8 \times \mathbb{Z}_{16}$ possa avere un sottoanello isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_8$.

3.

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

(a) Tenendo conto che $g(x) = x\left(x^{p-1} - \overline{1}\right)$, dalla precedente decomposizione segue facilmente che $\mathrm{MCD}(f(x),\ g(x)) = x^{p-1} - \overline{1}$.

(b) La stessa decomposizione consente immediatamente di concludere che il resto cercato è $r(x) = x^{p-1} - \overline{1}$.