Traccia del 7 novembre 2024

1.

(a) Il sottogruppo $C(\sigma)$ non è commutativo. Infatti vi appartengono le seguenti due permutazioni:

- $\alpha = (1,3,2,4)$, in quanto il suo quadrato $\alpha^2 = (1,2)(3,4)$ è il prodotto di due dei cicli associati a σ;
- $\beta = (1,3)(2,4)$, che commuta con $(1,2)(3,4)$ ed è disgiunta dai restanti cicli di σ.

Ora, $\alpha\beta \neq \beta\alpha$, poiché $\alpha\beta(1) = 2$, mentre $\beta\alpha(1) = 1$.

(b) Un sottogruppo non ciclico di $C(\sigma)$ è, ad esempio,

$$H = \{id,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(3,2)\}.$$

Si noti che ogni elemento di H commuta con $(1,2)(3,4)$ ed è disgiunto dai restanti cicli di σ; inoltre H non è ciclico, poiché i suoi elementi hanno al più periodo 2.

2.

(a) Sia $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_{20} \times \mathbb{Z}_{40}$ un monomorfismo di anelli. Essendo questo, in particolare, un monomorfismo di gruppi additivi, esso conserva i periodi degli elementi. Di conseguenza, posto $(\alpha, \beta) = \varphi([1]_2, [0]_4)$, dovrà essere $o((\alpha, \beta)) = 2$. Ciò significa che

$$(\alpha, \beta) \in \{([10]_{20}, [0]_{40}),\ ([0]_{20}, [20]_{40}),\ ([10]_{20}, [20]_{40})\}.$$

D'altra parte, poiché φ conserva il prodotto, e si ha $([1]_2, [0]_4)^2 = ([1]_2, [0]_4)$, dovrà essere anche $(\alpha, \beta)^2 = (\alpha, \beta)$. Ma quest'ultima condizione non è mai verificata, dato che, in ogni caso, $(\alpha, \beta)^2 = ([0]_{20}, [0]_{40})$. Se ne deduce che non esiste alcun monomorfismo di anelli φ.

(b) Ogni applicazione $\psi : \mathbb{Z}_6 \times \mathbb{Z}_{36} \to \mathbb{Z}_4 \times \mathbb{Z}_{18}$ tale che, per ogni $a, b \in \mathbb{Z}$, $([a]_6, [b]_{36}) \mapsto ([na]_4, [mb]_{18})$, ove n, m sono interi fissati, se è ben definita, è evidentemente un omomorfismo di gruppi additivi. Ora, ψ è ben definita se e solo se, per ogni $a, a' \in \mathbb{Z}$, $6|a - a' \implies 4|n(a - a')$, ossia se e solo se, per ogni intero h, $4|6hn$. Ciò vale, in particolare, per $n = 2$. Ponendo $m = 1$ si ha allora l'omomorfismo di gruppi definito da $([a]_6, [b]_{36}) \mapsto ([2a]_4, [b]_{18})$. La sua immagine è il prodotto diretto $\langle [2]_4 \rangle \times \mathbb{Z}_{18}$, il cui ordine è $2 \cdot 18 = 36$.

3.

(a) Si osserva che

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

Ne consegue che il quoziente cercato è

$$q(x) = (x - \overline{1})^{p^3 - 1} + (x - \overline{1})^{p^2 - 1} + (x - \overline{1})^{p-1} + \overline{1}$$

mentre il resto è $r(x) = \overline{3}$, nullo per $p = 3$.

(b) Sia $\alpha \in \mathbb{Z}_p$. Allora, si ha, in virtù del Piccolo Teorema di Fermat:

$$g(\alpha) = 4\alpha^2 - \overline{1}.$$

Pertanto, se $p = 2$, $g(x)$ non ha radici. Sia allora $p > 2$. In tal caso α è radice di $g(x)$ se e solo se $\alpha^2 = \overline{4}^{-1}$. Ne consegue che le radici di $g(x)$ sono due: $\alpha_1 = \overline{2}^{-1}$ e $\alpha_2 = -\overline{2}^{-1}$. Precisamente, se s è tale che $p = 2s - 1$, si ha che $\alpha_1 = \overline{s}$, $\alpha_2 = -\overline{s}$.

(c) Si applica quanto osservato al punto precedente con $s = 1090$, e si ottengono le radici $\alpha_1 = \overline{1090}$, $\alpha_2 = \overline{1089}$.