Traccia del 10 febbraio 2023

1.

(a) Si ha $o(\sigma) = \mathrm{mcm}(6,5,3,2) = 30$, $o(\tau) = \mathrm{mcm}(11,7,5,2) = 770$. L'intersezione cercata è un sottogruppo ciclico, sia α un suo generatore. Allora sarà $\alpha = \sigma^s = \tau^t$ per opportuni interi s, t. D'altra parte, per il Teorema di Lagrange, $o(\alpha)$ divide $\mathrm{MCD}(30,770) = 10$. Ciò implica in particolare che $11|t$. Allora τ^t lascia fissi 12 e 13, e quindi lo stesso vale per σ^s. Ne consegue che $30|s$. Ma allora $\alpha = \sigma^s = \mathrm{id}$. L'intersezione cercata è quindi il sottogruppo banale.

(b) Determiniamo H come il sottogruppo generato da un 12-ciclo ρ di S_{25} tale che $\rho^2 = \gamma\delta$, essendo γ un 6-ciclo per il quale $\gamma^3 = (1,2)(3,4)(5,6)$ e $\delta = (7,8,9,10,11,12)$. In tal caso, infatti, γ e δ commutano con σ: δ è un ciclo di σ, e, d'altra parte, γ commuta con γ^3, che è prodotto di alcuni cicli di σ, mentre è disgiunto dai restanti suoi cicli. Dunque si avrà che $\rho^2 \in H \cap C(\sigma)$. Si può prendere $\gamma = (1,3,5,2,4,6)$. Allora $\rho = (1,7,3,8,5,9,2,10,4,11,6,12)$ è un 12-ciclo con la proprietà richiesta.

(c) Siano

$$U = \{\mu \in S_{25} | Supp(\mu) \subset \{1,2\}\}$$
$$V = \{\nu \in S_{25} | Supp(\nu) \subset \{3,4,5\}\}.$$

Questi sono sottogruppi di S_{25} isomorfi, rispettivamente, a S_2 e a S_3. Inoltre ogni elemento di U è disgiunto da ogni elemento di V. Ne discende che $K = \{\mu\nu | \mu \in U, \nu \in V\}$ è un sottogruppo di S_{25} avente ordine $|U| \cdot |V| = 2 \cdot 6 = 12$. Non è commutativo, in quanto vi appartengono le permutazioni $(3,4)$ e $(4,5)$, che tra loro non commutano. Inoltre vi appartiene $(1,2) = \tau^{385}$.

2.

(a) Se esistesse un omomorfismo siffatto, la sua immagine sarebbe un sottoanello A di $\mathbb{Z}_{100}$ isomorfo a $\mathbb{Z}_{20}$. In particolare, A sarebbe un sottogruppo di $\mathbb{Z}_{100}$ avente ordine 20. Questo sottogruppo è unico, precisamente, $A = \langle [5]_{100} \rangle$. Si può notare, però, che A, che pure è un sottoanello di $\mathbb{Z}_{100}$, non è dotato di elemento neutro del prodotto. Infatti, nessun elemento della forma $[5x]_{100}$, con x intero, verifica l'equazione $[5x]_{100}[5]_{100} = [5]_{100}$: questa equivale a $25x \equiv 5 \pmod{100}$, una congruenza lineare non risolubile. Ciò prova che A non è un anello unitario, e dunque non può essere isomorfo a $\mathbb{Z}_{20}$. Essendo pervenuti ad una contraddizione, dobbiamo concludere che la risposta al quesito è negativa.

(b) Sia $(\alpha, \beta) \in \mathbb{Z}_{20} \times \mathbb{Z}_{100}$. Allora $o((\alpha,\beta)) = \mathrm{mcm}(o(\alpha), o(\beta))$. Poiché $o(\alpha)$ e $o(\beta)$ sono entrambi divisori di 100, tale è anche $o((\alpha,\beta))$. D'altra parte, detto d un divisore positivo di 100, e posto $100 = dq$, si ha che $o(([0]_{20}, [q]_{100})) = d$. Quindi i possibili valori di $o((\alpha,\beta))$ sono tutti e soli i divisori positivi di 100, ossia: $1, 2, 4, 5, 10, 20, 25, 50, 100$.

3.

(a) Si ha $h(x) = (x - \overline{1})^{p^3}$. Quindi il massimo comune divisore cercato è la massima potenza di $x - \overline{1}$, con esponente minore o uguale a p^3, che divide $f(x)$. Ora

$$f(x) = x^{p^4} - \overline{1} - \left(x^p - x\right)^p = (x - \overline{1})^{p^4} - x^p\left(x^{p-1} - \overline{1}\right)^p.$$

Nell'ultima espressione, il primo addendo è divisibile per $(x - \overline{1})^{p^3}$, quindi il massimo comune divisore cercato è la massima potenza di $x - \overline{1}$ che divide il secondo addendo, ossia

$\mathrm{MCD}(f(x),\ h(x)) = (x-\overline{1})^p = x^p - \overline{1}$. A tal proposito, si ricorda che $x^{p-1} - \overline{1} = \prod_{\alpha \in \mathbb{Z}_p^*} (x-\alpha)$.

(b) Si ha

$$g(x) = x^{p^2}\left(x^{p-1} - \overline{1}\right)^{p^2} - \left(x^2 - \overline{1}\right) = (x-\overline{1})(x^{p^2}\left(x^{p-1} - \overline{1}\right)^{p^2-1} \prod_{\alpha \in \mathbb{Z}_p^* \setminus \{\overline{1}\}} (x-\alpha)\ - (x+\overline{1})).$$

Per $p > 2$, la massima potenza di $x - \overline{1}$ che divide $g(x)$ è $x - \overline{1}$: ciò è conseguenza del Teorema di Ruffini, in quanto $\overline{1}$ non è radice del secondo fattore dell'ultima espressione. Pertanto, $\mathrm{MCD}(g(x),\ h(x)) = x - \overline{1}$. Per $p = 2$, essendo $h(x) = x^8 + \overline{1} = \left(x^2 + \overline{1}\right)^4$ e

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

si ha, invece, $\mathrm{MCD}(g(x),\ h(x)) = x^2 + \overline{1}$.