Traccia dell'8 gennaio 2024

1.

(a) Si ha che $o(\sigma) = \mathrm{mcm}(5,4,3,2) = 60$, $o(\tau) = \mathrm{mcm}(9,5,4,2) = 180$.Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Allora $o(\alpha)$ divide 60. Ne consegue che $3|t$. Dal confronto tra le orbite di 19 sotto le azioni di σ e τ si deduce poi che $2|s$. Dal confronto tra le orbite di 15 risulta, inoltre, che $2|t$. Dunque il sottogruppo cercato è $\langle\sigma^2\rangle \cap \langle\tau^6\rangle$, ove

$$\sigma^2 = (1,3,2)(4,6,5)(7,9,8)(10,12,14,11,13)(19,21)(20,22)$$
$$\tau^6 = (1,3,2)(4,6,5)(7,9,8)(10,12,11,13,14)(15,16)(17,18)$$

Osserviamo che σ^2 muove 19, mentre τ^6, insieme a tutte le sue potenze, lo lascia fisso. Dunque ciò vale anche per $\alpha = \sigma^{2h} = \tau^{6k}$, e pertanto si avrà che $2|h$. In modo analogo, considerando l'elemento 15, si deduce che $2|k$. Pertanto il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^{12}\rangle$, ove

$$\sigma^4 = (1,2,3)\ (4,5,6)(7,8,9)(10,14,13,12,11),$$
$$\tau^{12} = (1,2,3)\ (4,5,6)(7,8,9)(10,11,14,12,13).$$

Queste permutazioni hanno entrambe periodo 15. D'altra parte l'elemento $(1,2,3)(4,5,6)(7,8,9) = \sigma^{40} = \tau^{120}$, di periodo 3, appartiene al sottogruppo cercato, che dunque ha ordine multiplo di 3 e divisore di 15. Ma non può avere ordine 15, poiché $\langle\sigma^4\rangle \neq \langle\tau^{12}\rangle$: infatti nessuna potenza di τ^{12} invia 10 in 14 e 11 in 10. Ne consegue che l'ordine del sottogruppo cercato è 3, e, precisamente, $\langle\sigma\rangle \cap \langle\tau\rangle = \langle(1,2,3)(4,5,6)(7,8,9)\rangle$.

(b) Consideriamo le seguenti permutazioni, a due a due disgiunte:

$$\gamma_1 = (1,2,3)(4,5,6)(7,8,9), \gamma_2 = (15,18,16,17), \gamma_3 = (19,21)(20,22).$$

Ognuna di esse commuta sia con σ, sia con τ, in quanto:
- γ_1 è un prodotto di cicli associati a σ ed è una potenza di un ciclo associato a τ;
- un prodotto di cicli associati a σ è una potenza di γ_2 e γ_2 è un ciclo associato a τ;
- γ_3 è potenza di un ciclo associato a σ ed è un prodotto di cicli associati a τ.

Possiamo dunque considerare il sottogruppo

$$H = \{\gamma_1^a\gamma_2^b\gamma_3^c | a,b,c \in \mathbb{Z}\},$$

il cui ordine è $o(\gamma_1)o(\gamma_2)o(\gamma_2) = 3 \cdot 4 \cdot 2 = 24$.

(c) Sia K un sottogruppo di S_{22} contenente $\{\sigma,\tau\}$. Allora a K appartengono gli elementi $\sigma^{30} = (19,21)(20,22)$ e $\tau^{90} = (15,16)(17,18)$, di periodo 2. Inoltre vi appartengono gli elementi $\sigma^{36} = (10,11,12,13,14)$ e $\tau^{36} = (10,12,11,13,14)$, insieme al loro prodotto,

$$\sigma^{36}\tau^{36} = (10,13)(11,14),$$

anch'esso di periodo 2.

2.

(a) Un omomorfismo del tipo richiesto è l'applicazione $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_{12}$, definita ponendo, per ogni $a, b \in \mathbb{Z}, \varphi([a]_4, [b]_6) = [4b]_{12}$. Infatti, com'è immediato verificare, φ è un omomorfismo di gruppi ben definito e non banale che, inoltre, conserva il prodotto, poiché $4^2 = 16 \equiv 4 \pmod{12}$.

(b) Un omomorfismo del tipo richiesto è l'applicazione $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_4 \times \mathbb{Z}_6$, definita ponendo, per ogni $a \in \mathbb{Z}, \varphi([a]_{12}) = ([a]_4, [3a]_6)$. Si verificano facilmente la buona definizione e la conservazione di somma e prodotto. Inoltre, per ogni $a \in \mathbb{Z}$, $[a]_{12} \in \mathrm{Ker}\varphi$ se e solo se a è multiplo di 4, quindi $\mathrm{Ker}\varphi = \langle [4]_{12} \rangle$, il cui ordine è 3.

3.

(a) Si ha $g(x) = (x - \overline{1})^p$ e $f(x) = x^p \left(x^{p-1} - \overline{1}\right)^p + (x - \overline{1})^2$. Pertanto,

- per $p = 2$, $f(x) = \left(x^2 + \overline{1}\right)(x - 1)^2 = \left(x^2 + \overline{1}\right) g(x)$,
- per $p > 2$,

$$f(x) = (x - \overline{1})^2 \left[x^p (x - \overline{1})^{p-2} \prod_{\alpha \in \mathbb{Z}_p \setminus \{\overline{0}, \overline{1}\}} (x - \alpha)^p + \overline{1} \right].$$

Se $p > 2$, il polinomio tra parentesi quadre non è divisibile per $x - \overline{1}$, in virtù del Teorema di Ruffini, in quanto non si annulla in $\overline{1}$. Ne consegue che, in ogni caso, $\mathrm{MCD}(f(x), g(x)) = (x - \overline{1})^2$.

(b) Poiché $(x + \overline{1})^2$ divide $\left(x^{p-1} - \overline{1}\right)^p$, da (a) si ricava che $f(x) \equiv x^2 - \overline{2}x + \overline{1} \pmod{h(x)}$. Quindi il resto cercato è quello della divisione di $l(x) = x^2 - \overline{2}x + \overline{1}$ per $h(x)$. Si ha $l(x) = (x + \overline{1})^2 - \overline{4}x$. Ne consegue che il resto cercato è il polinomio $-\overline{4}x$, nullo solo per $p = 2$.