Traccia del 25 settembre 2024

1.

(a) Dal confronto tra le orbite di 5 sotto l'azione delle potenze di σ e di τ si deduce che $\langle\sigma\rangle \cap \langle\tau\rangle = \langle\sigma^2\rangle \cap \langle\tau^2\rangle$, ove

$\sigma^2 = (1,3)(2,4)(9,11,13,15,10,12,14)(16,18,20,17,19)$,
$\tau^2 = (9,13,10,14,11,15,12)(16,19,17,20,18)$.

Poiché τ lascia fisso 1, si deduce ancora che il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^2\rangle$, ove

$\sigma^4 = (9,13,10,14,11,15,12)(16,20,19,18,17)$.

A questo punto si osserva che $(16,20,19,18,17)^2 = (16,19,17,20,18)$. Dunque sarà $\sigma^{4k} = \tau^2$ per ogni intero k tale che

$k \equiv 1 \pmod 7$
$k \equiv 2 \pmod 5$

In virtù del Teorema Cinese del Resto un intero siffatto esiste (ad esempio, $k = 22$). Ne consegue che $\tau^2 \in \langle\sigma^4\rangle$, e quindi il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^2\rangle = \langle\tau^2\rangle$, di ordine 35.

(b) A $C(\sigma) \cap C(\tau)$ appartengono le seguenti permutazioni, a due a due disgiunte:

- $\alpha_1 = (1,2,3,4)$, poiché è un ciclo di σ e il suo quadrato, $(1,3)(2,4)$, è prodotto di due dei cicli di τ;
- $\alpha_2 = (9,10,11,12,13,14,15)$, perché è un ciclo di σ, e il suo quadrato, $(9,11,13,15,10,12,14)$, è un ciclo di τ;
- $\alpha_3 = (16,17,18,19,20)$, perché è un ciclo di σ, e la sua inversa, $(16,20,19,18,17)$, è un ciclo di τ.

Inoltre vi appartengono

- $\beta_1 = (5,6)(7,8)$, $\beta_2 = (5,7)(6,8)$, $\beta_3 = (5,8)(6,7)$, perché queste commutano tra di loro, quindi in particolare con β_1 (che è prodotto di due cicli di σ) e con β_2 (che è prodotto di due cicli di τ), ed inoltre sono disgiunte dai restanti cicli di σ e τ.

Ne consegue che a $C(\sigma) \cap C(\tau)$ appartengono tutti i prodotti della forma $\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ (il cui numero è $o(\alpha_1)o(\alpha_2)o(\alpha_3) = 4 \cdot 7 \cdot 5 = 140$. A questi si aggiungono i loro prodotti con una tra le permutazioni $\beta_1, \beta_2, \beta_3$, ossia altri $3 \cdot 140 = 420$ prodotti. Ciò prova l'asserto.

(c) Dato un sottogruppo H di S_{20} tale che $\{\sigma, \tau\} \subset H$, ad H appartengono anche le permutazioni $\sigma^{70} = (1,3)(2,4)$ e $\tau^{35} = (1,3)(2,4)(5,7)(6,8)$. Queste sono due distinti elementi di H aventi periodo 2, e ciò esclude che H possa essere ciclico.

2.

(a) Per ogni $a \in \mathbb{Z}$, $a^4 - a^2 = a^2(a-1)(a+1)$ è

- divisibile per 4, in quanto lo è a^2, se a è pari, e lo è $(a-1)(a+1)$, se a è dispari;

- divisibile per 3, perché $(a-1)a(a+1)$ è il prodotto di 3 interi consecutivi.

Dunque, per ogni $a \in \mathbb{Z}$, $\left[a^4 - a^2\right]_{12} = [0]_{12}$. In altri termini, φ_n è, per ogni intero $n \geq 2$, l'omomorfismo (di anelli) banale.

(b) Siano p, q due numeri primi positivi distinti. Per ogni $a \in \mathbb{Z}$, in virtù del Piccolo Teorema di Fermat, si ha:

- $a^{pq} - a^p - a^q \equiv a^q - a - a^q = -a \pmod{p}$,
- $a^{pq} - a^p - a^q \equiv a^p - a^p - a = -a \pmod{q}$.

In conclusione, per ogni $a \in \mathbb{Z}$, il numero intero $a^{pq} - a^p - a^q - (-a)$ è divisibile per entrambi i primi p e q, equivalentemente, è divisibile per il loro prodotto. Ciò prova che, per ogni $a \in \mathbb{Z}$,

$$\left[a^{pq} - a^p - a^q\right]_{pq} = [-a]_{pq}.$$

A questo punto è immediato verificare, sulla base della definizione, che $\psi_{p,q}$ è un omomorfismo di gruppi. Lo è per ogni scelta di p e q.

3.

(a) Sia $\alpha \in \mathbb{Z}_p$. Allora, per il Piccolo Teorema di Fermat, $f(\alpha) = \overline{1} + 102\alpha$. Ne consegue che $f(x)$ ha una radice in $\mathbb{Z}_p$ se e solo se $p \notin \{2, 3, 17\}$, nel qual caso tale radice è $\alpha = -\overline{102}^{-1}$. Analogamente si deduce che $g(x)$ ha una radice in $\mathbb{Z}_p$ se e solo se $p \neq 5$, nel qual caso tale radice è $\beta = -\overline{25}^{-1}$. Di conseguenza, per i valori di p appena indicati. $f(x)$ e $g(x)$ hanno una radice comune se e solo se $\alpha = \beta$, ossia, se e solo se $\overline{102} = \overline{25}$, il che avviene se e solo se p divide $102 - 25 = 77$. In conclusione, $f(x)$ e $g(x)$ hanno una radice comune se e solo se $p = 7$ oppure $p = 11$.

(b) Si osserva che

$$h(x) + h(x)^{p^{34}} + h(x)^{p^{68}} = \overline{3} + \sum_{i=0}^{33} x^{p^i} + \sum_{i=34}^{67} x^{p^i} + \sum_{i=68}^{101} x^{p^i} = \overline{2} + f(x).$$

Pertanto, se $p = 2$, $h(x)$ divide $f(x)$.