Traccia del 26 settembre 2023

1.

(a) Si ha che $o(\sigma) = \text{mcm}(6,5,3,2) = 30 = \text{mcm}(6,5,2) = o(\tau)$. Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Allora, per il Teorema di Lagrange, $o(\alpha)|30$. Se fosse vero che $5|o(\alpha)$, allora $\langle\alpha\rangle$ avrebbe un unico sottogruppo di ordine 5, che dovrebbe coincidere, contemporaneamente, con l'unico sottogruppo di ordine 5 di $\langle\sigma\rangle$ e con l'unico sottogruppo di ordine 5 di $\langle\tau\rangle$. Ma questi due sottogruppi sono distinti: $\langle(1,2,3,4,5)\rangle \neq \langle(1,3,2,4,5)\rangle$. Ne consegue che 5 non divide $o(\alpha)$, e dunque $5|s$, $5|t$. Inoltre, le orbite di 18 sotto l'azione di σ^s e τ^t coincidono, essendo uguali a $\{18\}$, solo se $2|s$, $2|t$. Quindi $\langle\alpha\rangle = \langle\sigma^{10}\rangle \cap \langle\tau^{10}\rangle$, ove

$\sigma^{10} = (6,7,8)(9,10,11)(12,16,14)(13,17,15)$,

$\tau^{10} = (6,8,7)(9,11,10)$.

Ma queste due permutazioni generano due sottogruppi di ordine 3 aventi intersezione banale. In conclusione, l'intersezione cercata è il sottogruppo banale.

(b) Consideriamo le seguenti permutazioni, a due a due disgiunte, il cui prodotto è σ:

$$\gamma_1 = (1,2,3,4,5), \gamma_2 = (6,7,8)(9,10,11),$$
$$\gamma_3 = (12,13,14,15,16,17), \gamma_4 = (18,19)(20,21).$$

Osserviamo preliminarmente che, per ogni indice i, la permutazione γ_i commuta, insieme a tutte le sue potenze, con i cicli di τ disgiunti da γ_i, con i loro prodotti e con tutte le loro potenze. Pertanto, dato un intero k, la permutazione $\sigma^k = \gamma_1^k\gamma_2^k\gamma_3^k\gamma_4^k$ commuta con τ^k se e solo se

- γ_1^k commuta con $\delta_1^k = (1,3,2,4,5)^k$;
- γ_2^k commuta con $\delta_2^k = (6,9,7,10,8,11)^k$;
- γ_3^k commuta con $\delta_3^k = (12,15)^k(13,16)^k(14,17)^k$;
- γ_4^k commuta con $\delta_4^k = (18,20)^k(19,21)^k$.

Osserviamo quanto segue.

- Per ogni intero k non divisibile per 5, la permutazione $\gamma_1^k = (1,2,3,4,5)^k$ ha periodo 5, e quindi è un generatore del sottogruppo ciclico $\langle\gamma_1\rangle$. In particolare, γ_1 è una potenza di γ_1^k. Analogamente, δ_1 è una potenza di δ_1^k. Quindi per tali interi, se γ_1^k commutasse con δ_1^k, allora γ_1 commuterebbe con δ_1, il che, però, non è vero. Ne consegue che γ_1^k commuta con δ_1^k **solo se** 5 **divide** k, nel qual caso $\gamma_1^k = \delta_1^k = id$.
- γ_2 commuta con δ_2, dato che $\gamma_2 = \delta_2^2$, e quindi **per ogni** k, γ_2^k commuta con δ_2^k;
- γ_3 commuta con δ_3, dato che $\gamma_3^3 = \delta_3$ e quindi **per ogni** k, γ_3^k commuta con δ_3^k;
- γ_4 commuta con δ_4, e quindi **per ogni** k, γ_4^k commuta con δ_4^k.

  In conclusione, σ^k commuta con τ^k se e solo se k è multiplo di 5. Il più piccolo valore positivo di k è dunque $k = 5$.

2.

(a) L'immagine di un omomorfismo di gruppi iniettivo da $\mathbb{Z}_4$ a $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ è un sottogruppo di quest'ultimo isomorfo a $\mathbb{Z}_4$, che è un gruppo ciclico di ordine 4. Tuttavia il gruppo $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ non ha elementi di periodo 4: infatti, per ogni $\alpha \in \mathbb{Z}_6$, $o(\alpha) | 6$ e, per ogni $\beta \in \mathbb{Z}_{10}$, $o(\beta) | 10$, così che $o((\alpha, \beta))$ divide $\mathrm{mcm}(6, 10) = 30$. Non esiste dunque un omomorfismo del tipo indicato.

(b) L'immagine di un omomorfismo avente come gruppo di partenza un gruppo ciclico è, a sua volta, un gruppo ciclico. Ma tale non è $\mathbb{Z}_6 \times \mathbb{Z}_{10}$: infatti, come stabilito al punto (a), nessuno dei suoi elementi ha periodo pari all'ordine del gruppo, che è 60. Non esiste dunque un omomorfismo del tipo indicato.

(c) Si consideri l'applicazione $\varphi : \mathbb{Z}_8 \to \mathbb{Z}_6 \times \mathbb{Z}_{10}$ definita ponendo, per ogni $a \in \mathbb{Z}$, $\varphi([a]_8) = ([3a]_6, [0]_{10})$. Questa, com'è facile verificare, è un omomorfismo di gruppi, che è non nullo, in quanto $\varphi([1]_8) = ([3]_6, [0]_{10})$.

3.

(a) Per ogni $\alpha \in \mathbb{Z}_p$ si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = \alpha^4 + \alpha^2 + \overline{1}$. Quindi α è radice di $f(x)$ se e solo se α è radice, distinta da $\overline{1}$ e $-\overline{1}$, del polinomio $h(x) = x^6 - \overline{1} = \left(x^2 - \overline{1}\right)\left(x^4 + x^2 + \overline{1}\right)$. Ciò avviene se e solo se, nel gruppo moltiplicativo $\mathbb{Z}_p^*$, l'elemento α ha come periodo un divisore di 6, distinto da 1 e da 2, ossia ha periodo 3 oppure 6. Un elemento α siffatto esiste in $\mathbb{Z}_p^*$ se e solo se $3 | p - 1$. In tal caso, essendo p dispari, si ha $6 | p - 1$, e dunque in $\mathbb{Z}_p^*$ esistono $\phi(6) = 2$ elementi di periodo 6, diciamo α_1,α_2, ed altri $\phi(3) = 2$ elementi di periodo 3, diciamo α_3, α_4. In totale, $f(x)$ possiede allora 4 radici. Se invece 3 non divide $p - 1$, $f(x)$ è privo di radici.

(b) Il polinomio $g(x) = \left(x^6 - \overline{1}\right)^p$ ha sempre $\overline{1}$ e $-\overline{1}$ come radici (distinte). Le altre radici, ove esistenti, sono gli elementi di $\mathbb{Z}_p^*$ aventi periodo 3 oppure 6. Si applica quanto detto al punto (b) per il polinomio $f(x)$. In conclusione, se 3 non divide $p - 1$, $g(x)$ ha esattamente due radici ($\overline{1}$ e $-\overline{1}$). Altrimenti ha 6 radici.