Traccia del 13 settembre 2023

1.

(a) Consideriamo i cicli associati a τ :

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

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

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

Ora, constatiamo che:

- γ_1 commuta con δ_1, dato che $\gamma_1^2 = \delta_1$, e quindi **ogni potenza** di γ_1 commuta con δ_1;
- γ_2 non commuta con δ_2, mentre invece $\gamma_2^2 = (7,8,9)(10,12,11)$ commuta con δ_2, così che le potenze di γ_2 che commutano con δ_2 sono tutte e sole quelle con **esponente pari**;
- l'unica potenza di γ_3 che commuta con δ_3 è la permutazione identica, coincidente con tutte e sole le potenze di γ_3 aventi **esponente multiplo di** 5;
- le potenze di γ_4 che commutano con δ_4 sono tutte e sole quelle con **esponente pari**, ossia $(18,20)(19,21)$ e la permutazione identica.

In conclusione, τ^k commuta con σ se e solo se k è multiplo di 10. In altri termini, $C(\sigma) \cap \langle\tau\rangle = \langle\tau^{10}\rangle$.

(b) Con τ commutano le seguenti permutazioni, a due a due disgiunte:

- $\alpha = (1,7,4,10,2,8,5,12,3,9,6,11)$, in quanto $\alpha^2 = \gamma_1\gamma_2$ e inoltre α è disgiunto da γ_3 e γ_4;
- $\beta = \gamma_3$;
- $\gamma = \gamma_4$.

Ne consegue che il seguente sottogruppo di S_{21} è contenuto in $C(\tau)$:

$$H = \{\alpha^a\beta^b\gamma^c | a,b,c \in \mathbb{Z}\}.$$

Ma $|H| = o(\alpha)o(\beta)o(\gamma) = 12 \cdot 5 \cdot 4 = 240.$

2.

(a) Si ha che $\mathrm{Im}\varphi = \langle([m]_n,[n]_m)\rangle$, sottogruppo ciclico di $\mathbb{Z}_n \times \mathbb{Z}_m$. Ora, posto $d = \mathrm{MCD}(n,m)$, per la formula del periodo, si ha, rispettivamente, in $\mathbb{Z}_n$ e in $\mathbb{Z}_m$:

$$o([m]_n) = \frac{n}{d}, \qquad o([n]_m) = \frac{m}{d}.$$

Quindi

$$|\mathrm{Im}\varphi| = o(([m]_n, [n]_m)) = \mathrm{mcm}\left(\frac{n}{d}, \frac{m}{d}\right) = \frac{nm}{d^2},$$

ove l'ultima uguaglianza segue dal fatto che $\frac{n}{d}, \frac{m}{d}$ sono coprimi.

(b) Sia $a \in \mathbb{Z}$. Allora $\varphi([a]_{nm}) = ([0]_n, [0]_m)$ se e solo se $n|ma$ e $m|na$, equivalentemente, se e solo se $\frac{n}{d}\Big|\frac{m}{d}a$ e $\frac{m}{d}\Big|\frac{n}{d}a$. Poiché, come già osservato, i numeri interi $\frac{n}{d}$ e $\frac{m}{d}$ sono coprimi, ciò vale se e solo se entrambi questi interi dividono a, ossia, tenendo ancora conto della loro coprimalità, se e solo se il loro prodotto $\frac{nm}{d^2}$ divide a. In altri termini, $\varphi^{-1}([0]_n, [0]_m) = \left\langle \left[\frac{nm}{d^2}\right] \right\rangle$. Pertanto $|\varphi^{-1}([0]_n, [0]_m)| = o\left(\left[\frac{nm}{d^2}\right]\right) = d^2$.

(c) Poiché 3 e 11 sono coprimi, in base a quanto visto al punto (a), l'applicazione è surgettiva, e quindi, in questo caso, invertibile. Dalla dimostrazione della seconda formulazione del Teorema Cinese del resto sappiamo inoltre che il più generale elemento di $\mathbb{Z}_3 \times \mathbb{Z}_{11}$ è della forma $([a]_3, [a]_{11})$, con $a \in \mathbb{Z}$. Tale elemento viene inviato da φ^{-1} nell'elemento $[b]_{33}$ per il quale b è un intero verificante le seguenti condizioni:

$$\begin{aligned} &a \equiv 11b \pmod 3), \quad \text{ossia} \quad a \equiv 2b \pmod 3) \\ &a \equiv 3b \pmod{11} \end{aligned}$$

Ne consegue che

$$\begin{aligned} 11a &\equiv 22b \equiv -11b \pmod{33} \\ 3a &\equiv 9b \pmod{33} \end{aligned}$$

Da qui, determinando una coppia di coefficienti di Bézout per -11 e 9 ($(-5)\cdot(-11) + (-6)\cdot 9 = 1$) ed applicando la compatibilità della congruenza modulo 33 rispetto alle operazioni di somma e prodotto, si deduce che

$(-5)(11a) + (-6)(3a) \equiv b \pmod{33}$, ossia $[b]_{33} = [-73a]_{33} = [26a]_{33}$. Quindi φ^{-1} è definita da $([a]_3, [a]_{11}) \mapsto [26a]_{33}$.

3.

(a) Sia $d(x) = \mathrm{MCD}(f(x), g(x))$. Allora $d(x)$, dividendo entrambi $f(x)$ e $g(x)$, divide anche la loro differenza $f(x) - g(x) = x^2 - \overline{2}x + \overline{1} = (x - \overline{1})^2$. Tuttavia, $x - \overline{1}$ non è un divisore di $f(x)$, in quanto $f(x)$ non ha $\overline{1}$ come radice. Ne consegue che $d(x) = \overline{1}$.

(b) Notiamo che $f(x) = h(x)^p - x^p + x^2 - x - \overline{2}$. Il resto cercato è dunque $r(x) = -x^p + x^2 - x - \overline{2}$.