Traccia del 5 settembre 2022

1.

(a) Si consideri l'8-ciclo

$$\alpha = (13, 17, 14, 18, 15, 19, 16, 20),$$

il cui quadrato è

$$\alpha^2 = (13, 14, 15, 16)(17, 18, 19, 20).$$

Si può osservare che α commuta con α^2 e con i restanti cicli della permutazione σ, in quanto è da essi disgiunto. Ne consegue che $\alpha \in C(\sigma)$. Con σ commuta anche il suo ciclo $\beta = (7, 8, 9, 10, 11, 12)$. Pertanto $C(\sigma)$ contiene il sottogruppo

$$H_1 = \{\alpha^a \beta^b | a, b \in \mathbb{Z}\},$$

avente ordine $o(\alpha)o(\beta) = 8 \cdot 6 = 48$. In modo analogo, posto $\gamma = (1, 4, 2, 5, 3, 6)$, e osservato che $\gamma^2 = (1, 2, 3)(4, 5, 6)$, si prova che $C(\sigma)$ contiene il sottogruppo

$$H_2 = \{\alpha^a \gamma^c | a, c \in \mathbb{Z}\},$$

anch'esso di ordine 48. Si noti che $H_1 \neq H_2$, in quanto ogni elemento di H_1 lascia fisso 1, mentre ciò non è vero per $\gamma \in H_2$.

<u>Nota</u>: Vi sono diverse altre possibili costruzioni di sottogruppi. Una di queste prevede di prendere $\delta = (1, 2, 3)$, $\varepsilon_1 = (13, 14, 15, 16)$, $\varepsilon_2 = (17, 18, 19, 20)$, e di definire quindi il sottogruppo

$$H_3 = \{\delta^d \varepsilon_1^{e_1} \varepsilon_2^{e_2} | d, e_1, e_2 \in \mathbb{Z}\},$$

avente ordine $3 \cdot 4 \cdot 4 = 48$.

(b) Posto $\tau = (1, 2, 3)(4, 5, 6)(7, 8, 9, 10, 11, 12)$, un gruppo del tipo richiesto è

$$H = \{\tau^t \alpha^a | t, a \in \mathbb{Z}\},$$

nel quale si trova anche $\sigma = \tau\alpha^2$, ed è tale che $|H| = o(\tau)o(\alpha) = 6 \cdot 8 = 48$.

2.

(a) L'applicazione φ è ben definita se e solo se

$$\text{per ogni } a, a', b, b' \in \mathbb{Z}, \quad n|a - a' \implies m|n(a - a'),$$

ossia, se e solo se

$$\text{per ogni } h \in \mathbb{Z}, \quad m|n^2 h$$

ossia, infine, se e solo se $m|n^2$. In conclusione, l'insieme delle coppie cercate è $\{(m, n) | m \text{ divide } n^2\}$.

(b) Poiché φ è evidentemente iniettiva, si ha che $|\mathrm{Im}\varphi| = |\mathbb{Z}_n| = n$.

(c) Se φ è ben definita, è chiaramente un omomorfismo di gruppi additivi. Quindi è un omomorfismo di anelli se e solo se conserva il prodotto. Si verifica facilmente che, nella condizione determinata in (a), ciò avviene se e solo se

$$\text{per ogni } a, b \in \mathbb{Z}, \quad nab \equiv n^2 ab \pmod{m}.$$

In altri termini, φ è un omomorfismo di anelli se e solo se, nell'ipotesi che $m|n^2$, si ha che $n \equiv n^2 \pmod{m}$, ossia si ha che $m|n^2 - n$. Ora, essendo $m|n^2$, la precedente relazione di divisibilità equivale a $m|n$. Pertanto l'insieme cercato è $\{(m, mh) | h \in \mathbb{Z}\}$.

3.

(a) Si ha $f(\overline{1}) = \overline{p^2 - p} = \overline{0}$, quindi $\overline{1}$ è radice di $f(x)$. D'altra parte

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

ove, in virtù del Teorema di Eulero, il polinomio $h(x) = x^{p-1} - \overline{1}$ ha, come radici semplici, tutti gli elementi di $\mathbb{Z}_p^*$. Ne consegue che $f(x)$ ha in $\mathbb{Z}_p$ le seguenti radici:

- ogni $\alpha \in \mathbb{Z}_p^* \setminus \{\overline{1}\}$, di molteplicità p;
- $\overline{1}$, di molteplicità $p - 1$.

(b) Si ha che

$$(x - \overline{1})g(x) = x^n - \overline{1},$$

un polinomio le cui radici in $\mathbb{Z}_p$ sono tutti e soli gli elementi di $\mathbb{Z}_p^*$ il cui periodo sia un divisore di n. Poiché, per il Teorema di Lagrange, ciascuno di tali elementi ha come periodo un divisore di $p - 1$, gli elementi cercati sono tutti e soli quelli il cui periodo divide $d = \mathrm{MCD}(n, p - 1)$. Questi sono gli elementi dell'unico sottogruppo (ciclico) di $\mathbb{Z}_p^*$ avente ordine d. Ora, poiché $g(\overline{1}) = \overline{n}$, $\overline{1}$ è radice di g se e solo se $p|n$. Questo è l'unico caso in cui il numero delle radici di g è d. Negli altri casi è $d - 1$.