Traccia dell'11 aprile 2024

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo $\langle\sigma\rangle \cap \langle\tau\rangle$. Dal confronto tra le orbite delle potenze di σ e delle potenze di τ, si ricavano le seguenti conclusioni. Considerando

- le orbite di 9, si deduce che $5|t$;
- le orbite di 19, si deduce che $4|t$.

Pertanto $20|t$. Essendo $o(\tau) = 20$, ne consegue che $\alpha = \mathrm{id}$. In altri termini, il sottogruppo cercato è banale.

(b) La permutazione $\beta = (1,3)(2,4)$ appartiene a $C(\sigma) \cap C(\tau)$. Infatti β

- commuta con $(1,2,3,4)$, essendo il suo quadrato, ed è disgiunta dai restanti cicli di σ;
- commuta con $(1,2)(3,4)$, ed è disgiunta dai restanti cicli di τ.

(c) Sia $\gamma = (1,5,2,6,3,7,4,8)(9,12,10,13,11,14)$. Allora $o(\gamma) = \mathrm{mcm}(8,6) = 24$. Inoltre $\gamma \in C(\sigma)$, in quanto

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

2.

(a) Se esistesse un monomorfismo φ del tipo indicato, la sua immagine sarebbe, come $\mathbb{Z}_2 \times \mathbb{Z}_3$, un anello unitario di ordine 6, con gruppo additivo ciclico. Sia dunque $(\alpha,\beta) \in \mathbb{Z}_{10} \times \mathbb{Z}_{45}$ un generatore del sottogruppo immagine. Si avrà allora $6 = o((\alpha,\beta)) = \mathrm{mcm}(o(\alpha), o(\beta))$. Dato che $o(\alpha)|10$ e $o(\beta)|45$, necessariamente $o(\alpha) = 2$ e $o(\beta) = 3$, e quindi $\mathrm{Im}\varphi = \langle[5]_{10}\rangle \times \langle[15]_{45}\rangle$. Tuttavia, questo anello non è unitario, in quanto in tutte le coppie ottenute tramite moltiplicazione il secondo elemento è nullo. Pertanto non esiste un monomorfismo del tipo indicato.

(b) Un monomorfismo φ del tipo indicato ha come immagine un sottoanello B di $\mathbb{Z}_{30}$ avente ordine 6. Questo deve coincidere con l'unico sottogruppo di $\mathbb{Z}_{30}$ avente ordine 6, ossia $B = \langle[5]_{30}\rangle$. Questo sottoanello ha $[25]_{30}$ come elemento uno. Poiché φ stabilisce un isomorfismo di anelli tra $\mathbb{Z}_2 \times \mathbb{Z}_3$ e B, si avrà dunque $\varphi([1]_2,[1]_3) = [25]_{30}$. Dalla proprietà di conservazione dei multipli si deduce allora:

$$\varphi([1]_2,[0]_3) = \varphi(3([1]_2,[1]_3)) = 3\varphi([1]_2,[1]_3) = [75]_{30} = [15]_{30},$$
$$\varphi([0]_2,[1]_3) = \varphi(4([1]_2,[1]_3)) = 4\varphi([1]_2,[1]_3) = [100]_{30} = [10]_{30}.$$

E quindi, si ricava, infine, per ogni $a, b \in \mathbb{Z}$,

$$\varphi([a]_2,[b]_3) = [15a + 10b]_{30}.$$

Questo è il monomorfismo cercato: è univocamente determinato. L'iniettività e la conservazione di somma e prodotto sono di facile verifica.

3.

(a) Si ha

$$f(x) = \left(x^p - \overline{1}\right)\left(x^{p-1} - \overline{1}\right) = (x - \overline{1})^p \prod_{\alpha \in \mathbb{Z}_p^*} (x - \alpha),$$

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

Poiché il fattore lineare $x - \overline{1}$ divide il polinomio $f(x)$ con molteplicità $p + 1 < 2p$, ne consegue che

$$\mathrm{MCD}(f(x), g(x)) = (x - \overline{1})^{p+1} = x^{p+1} - x^p - x + \overline{1}.$$

(b) Per ogni $\alpha \in \mathbb{Z}_p$, in virtù del Piccolo Teorema di Fermat, $h(\alpha) = \alpha^{p^2} + \alpha^p + \overline{1} = 2\alpha + \overline{1}$. Dunque $h(x)$ è privo di radici in $\mathbb{Z}_p$ per $p = 2$, nel qual caso è privo di fattori lineari, e quindi è coprimo con $f(x)$. Altrimenti $h(x)$ ha (esattamente) una radice non nulla $\alpha = -\overline{2}^{-1}$, e quindi è divisibile per il fattore lineare $x - \alpha$. Poiché quest'ultimo divide anche $f(x)$, i polinomi $f(x)$ e $h(x)$ non sono allora coprimi.