Traccia del 23 gennaio 2024

1.

(a) Si ha che $o(\sigma) = \mathrm{mcm}(5,3) = 15$, $o(\tau) = \mathrm{mcm}(12,5,3) = 60$.Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Allora $o(\alpha)$ divide 15. Ne consegue che $4|t$. Dunque il sottogruppo cercato è $\langle\sigma\rangle \cap \langle\tau^4\rangle$, ove

$$\tau^4 = (1,3,2)(4,6,5)(7,9,8)(10,12,11)(13,15,14)(16,17,18,19,20) = \sigma^{11}.$$

Ma allora il sottogruppo cercato è $\langle\tau^4\rangle = \langle\sigma^{11}\rangle = \langle\sigma\rangle$.

(b) Il gruppo $C(\sigma)$ non è abeliano, in quanto vi appartengono gli elementi $\alpha = (4,5,6)$ e $\beta = (4,7,10,13,6,9,12,15,5,8,11,14)$ (poiché $\beta^8 = (4,5,6)(7,8,9)(10,11,12)(13,14,15)$), ma $\alpha\beta(4) = 7$, mentre $\beta\alpha(4) = 8$.

(c) Il gruppo $C(\tau)$ non è ciclico, in quanto vi appartengono più di $\phi(3) = 2$ elementi di periodo 3, precisamente $(1,2,3)$, $(1,3,2)$ e $(4,6,5)(7,9,8)(10,12,11)(13,15,14)$, quarta potenza del $12-$ciclo β associato a τ.

2.

(a) Un sottogruppo di $\mathbb{Z}_9 \times \mathbb{Z}_{15}$ avente ordine 15 è $K = \langle([3]_9\rangle \times \langle[3]_{15}\rangle$. L'applicazione $\varphi : \mathbb{Z}_9 \times \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_3$ definita ponendo, per ogni $a, b \in \mathbb{Z}$, $\varphi(([a]_9, [b]_{15})) = ([a]_3, [b]_3)$ è, evidentemente, un omomorfismo di anelli ben definito e avente come nucleo K.

(b) L'applicazione $\varphi : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_{15} \times \mathbb{Z}_{21}$, definita ponendo, per ogni $a, b \in \mathbb{Z}, \varphi(([a]_3, [b]_3) = ([\lambda a]_{15}, [\mu b]_{21})$, è ben definita se e solo se $5|\lambda$ e $7|\mu$. In tal caso è un omomorfismo di gruppi. Se $\lambda = 5h$ e $\mu = 7k$, allora φ è un omomorfismo di anelli se e solo se $15|5h(5h-1)$ e $21|7k(7k-1)$, ossia se e solo se $3|h(2h-1)$ e $3|k(k-1)$. Ciò avviene, ad esempio, per $h = 2$ e $k = 1$. Si verifica facilmente che l'omomorfismo di anelli risultante, definito da $\varphi(([a]_3, [b]_3) = ([10a]_{15}, [7b]_{21})$, ha nucleo banale, e quindi è iniettivo.

3.

(a) Per ogni $\alpha \in \mathbb{Z}_p$, si ha, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = n\alpha + \overline{1}$. Questo è sempre uguale a $\overline{1}$ se p divide n. In tal caso l'insieme delle radici di $f(x)$ in $\mathbb{Z}_p$ è vuoto. Se invece p non divide n, allora $[n]_p$ è invertibile nel campo $\mathbb{Z}_p$, e quindi $f(x)$ ha come unica radice $\alpha = -[n]_p^{-1}$.

(b) Poiché $g(x)(x - \overline{1}) = x^p - \overline{1} = (x - \overline{1})^p$, si ha $g(x) = (x - \overline{1})^{p-1}$. Ora, $f(\overline{1}) = \overline{1}$. Quindi, per il Teorema di Ruffini, il fattore irriducibile $x - \overline{1}$ di $g(x)$ non divide $f(x)$. Pertanto, $\mathrm{MCD}(f(x), g(x)) = \overline{1}$.