Traccia del 26 gennaio 2023

1.

(a) L'intersezione cercata, chiamiamola L, è un gruppo ciclico. Il suo ordine, per il Teorema di Lagrange, divide $|\langle\sigma\rangle| = |\langle\tau\rangle| = \mathrm{mcm}(7,5,4,3) = 420$. Se tale ordine fosse divisibile per 5, allora L avrebbe un unico sottogruppo ciclico di ordine 5, che sarebbe, contemporaneamente, l'unico sottogruppo di ordine 5 di $\langle\sigma\rangle$ e di $\langle\tau\rangle$. Ma l'unico sottogruppo di ordine 5 di $\langle\sigma\rangle$ è $\langle(1,2,3,4,5)\rangle$, e questo è distinto dall'unico sottogruppo di ordine 5 di $\langle\tau\rangle$, che è $\langle(1,3,2,4,5)\rangle$. Si può infatti notare che l'unico elemento del primo sottogruppo ad inviare 2 in 3 è $(1,2,3,4,5)$, mentre l'unico elemento del secondo sottogruppo avente tale proprietà è $(1,5,4,2,3)$. Con considerazioni analoghe si esclude che $|L|$ sia divisibile per 7. Inoltre, si esclude che $|L|$ possa essere divisibile per 2, in quanto gli elementi di ordine 2 in $\langle\sigma\rangle$ e $\langle\tau\rangle$ sono, rispettivamente, $(6,8)(7,9)$ e $(6,7)(8,9)$, chiaramente distinti. Si conclude che $|L|$ divide 3. D'altra parte, il Teorema cinese del resto assicura l'esistenza di un intero k tale che

$$k \equiv 0 \pmod{140} \text{ e } k \equiv 1 \pmod{3},$$

ossia tale che

$$\sigma^k = (17,18,19) = \tau^{-k}.$$

Ne consegue che $\langle(17,18,19)\rangle \subset L$. Alla luce delle precedenti considerazioni sull'ordine, si conclude che $L = \langle(17,18,19)\rangle$.

(b) Sia $H = \{(1,2,3,4)^a(6,7,8,9)^b | a,b \in \mathbb{Z}\}$. Allora H è un sottogruppo di S_{19} avente ordine $4 \cdot 4 = 16$. Inoltre vi appartiene $(6,7,8,9)$, che è anche elemento di $\langle\sigma\rangle$, come si può provare, analogamente a quanto fatto in (a), applicando il Teorema cinese del resto.

(c) Sia $K = \{(6,8)^a(7,9)^a(1,10,11,12,13,14,15,16,17,18,19)^b | a,b \in \mathbb{Z}\}$. Allora K è un sottogruppo di S_{19} avente ordine $2 \cdot 11 = 22$. Inoltre vi appartiene $(6,8)(7,9) = (6,7,8,9)^2$, che, in base a quanto osservato in (b), è anche elemento di $\langle\sigma\rangle$.

2.

(a) Poiché un omomorfismo di gruppi additivi conserva lo zero e i multipli, vale quanto segue:

$$12\varphi(([5]_{20},[7]_{42})) = \varphi(12([5]_{20},[7]_{42})) = \varphi(([0]_{20},[0]_{42})) = [0]_{35}.$$

Pertanto il periodo di $\varphi(([5]_{20},[7]_{42}))$ in $\mathbb{Z}_{35}$ divide 12. Poiché, per il Teorema di Lagrange, divide anche 35, tale periodo deve essere 1. In altri termini, $\alpha = ([5]_{20},[7]_{42}) \in \mathrm{Ker}\varphi$. Si noti che $o(\alpha) = \mathrm{mcm}(4,6) = 12$. La tesi segue allora dal Teorema di Lagrange, applicato a $\mathrm{Ker}\varphi$, che, essendo un sottogruppo di $\mathbb{Z}_{20} \times \mathbb{Z}_{42}$, è un gruppo (abeliano) finito.

(b) Sia $\varphi : \mathbb{Z}_6 \times \mathbb{Z}_{20} \mapsto \mathbb{Z}_8$ un omomorfismo di gruppi. Allora, per ogni $\alpha \in \mathbb{Z}_6 \times \mathbb{Z}_{20}$, si ha $60\alpha = ([0]_6,[0]_{20})$. Ne consegue, come in (a), che $60\varphi(\alpha) = [0]_8$. Ma poiché $60[1]_8 = [4]_8 \neq [0]_8$, se ne deduce che $[1]_8 \notin \mathrm{Im}\varphi$, e dunque φ non è surgettivo. La risposta al quesito è dunque negativa.

3.

(a) Si ha, tenendo conto del Piccolo Teorema di Fermat:

$$f\left(\overline{3}^{-1}\right) = 3\left(-\overline{3}^{-1}\right) + \overline{1} = \overline{3} \cdot \left(-\overline{3}^{-1}\right) + \overline{1} = \overline{0}.$$

Dunque $-\overline{3}^{-1}$ è radice di $f(x)$ in $\mathbb{Z}_p$, e pertanto, in virtù del Teorema di Ruffini, $g(x)$ divide $f(x)$. Il resto

della divisione euclidea è quindi il polinomio nullo.

(b) Si ha

$$f(x) = h(x)^p - x^p + x.$$

Ne consegue che il resto cercato è $r(x) = -x^p + x$. Si noti che il suo grado è minore del grado di $h(x)$.