Traccia del 10 settembre 2024

1.

(a) In base al Teorema di Lagrange, l'intersezione $\langle\sigma^n\rangle \cap \langle\sigma^m\rangle$ è banale se sono coprimi gli ordini di $\langle\sigma^n\rangle$ e di $\langle\sigma^m\rangle$. Ora, $o(\sigma) = \mathrm{mcm}(9,5,3,2) = 90$. Inoltre, per ogni divisore positivo d di 90, il sottogruppo $\langle\sigma^{\frac{n}{d}}\rangle$ ha ordine d. Basta dunque determinare due divisori propri di 90 che siano tra loro coprimi. Tali sono, ad esempio, 2 e 45. Precisamente $\langle\sigma^{45}\rangle$ ha ordine 2, e $\langle\sigma^2\rangle$ ha ordine 45. Pertanto $(2,45)$ è una coppia del tipo cercato.

(b) A $C(\sigma)$ appartengono le permutazioni $\alpha = (1,2)$ e $\beta = (1,3,2,4)$: entrambe commutano infatti con $(1,2)(3,4)$ e sono disgiunte dai restanti cicli di σ. Tuttavia $\alpha\beta(1) = 3$ e $\beta\alpha(1) = 4$. Dunque $\alpha\beta \neq \beta\alpha$. Ciò prova che $C(\sigma)$ non è abeliano.

(c) Si ha $135 = 3\cdot 5\cdot 9$. A $C(\sigma)$ appartengono le permutazioni $\gamma_1 = (5,6,7)$, $\gamma_2 = (8,9,10,11,12)$ e $\gamma_3 = (13,14,15,16,17,18,19,20,21)$, che sono a due a due disgiunte ed hanno periodi 3, 5 e 9, rispettivamente. Ne consegue che un sottogruppo con le caratteristiche richieste è

$$H = \{\gamma_1^a\gamma_2^b\gamma_3^c | a,b,c \in \mathbb{Z}\}.$$

2.

(a) Sia $\varphi: \mathbb{Z}_3\times\mathbb{Z}_7 \to \mathbb{Z}_{42}$ un monomorfismo di anelli. Allora è, in particolare, un monomorfismo di gruppi additivi, e dunque ha come immagine un sottogruppo di $\mathbb{Z}_{42}$ isomorfo a $\mathbb{Z}_3\times\mathbb{Z}_7$, che, per il Teorema cinese del resto, è ciclico, di ordine 21, generato da $([1]_3,[1]_7)$. Ne consegue che $\varphi([1]_3,[1]_7)$ è un elemento di $\mathbb{Z}_{42}$ avente periodo 21, ossia un elemento della forma $[2n]_{42}$, ove n è coprimo con 21. In virtù della conservazione dei multipli, l'assegnazione $\varphi([1]_3,[1]_7) = [2n]_{42}$ determina univocamente un monomorfismo di gruppi additivi, tale che, per ogni $a\in\mathbb{Z}, \varphi([a]_3,[a]_7) = [2na]_{42}$. Ora, φ è un omomorfismo di anelli se e solo se conserva il prodotto, ossia se e solo, per ogni $a,b\in\mathbb{Z}$, $\left[4n^2ab\right]_{42} = [2nab]_{42}$. Tale condizione equivale a: $4n^2 \equiv 2n \pmod{42}$. Questa, a sua volta, equivale alla relazione di divisibilità $21|(2n-1)n$, che vale in tutti e soli i seguenti quattro casi:

- $n \equiv 0 \pmod{21}$;
- $2n \equiv 1 \pmod{21}$;
- $2n \equiv 1 \pmod 3$ e $n \equiv 0 \pmod 7$;
- $2n \equiv 1 \pmod 7$ e $n \equiv 0 \pmod 3$.

Poiché n deve essere coprimo con 21, il primo, il terzo e il quarto caso sono da scartare. Il secondo caso è verificato se e e solo $n = 11 + 21k$, per qualche intero k, ossia se e solo se $[2n]_{42} = [22]_{42}$. In conclusione, l'unico monomorfismo di anelli $\varphi: \mathbb{Z}_3\times\mathbb{Z}_7 \to \mathbb{Z}_{42}$ è l'applicazione definita ponendo, per ogni $a\in\mathbb{Z}, \varphi([a]_3,[a]_7) = [22a]_{42}$.

(b) Un epimorfismo di gruppi $\psi: \mathbb{Z}_{42} \to \mathbb{Z}_3\times\mathbb{Z}_7$ è univocamente determinato assegnando, al generatore $[1]_{42}$ del gruppo di partenza, uno dei generatori del gruppo di arrivo. Il numero di questi ultimi è $\phi(21) = \phi(3)\phi(7) = 2\cdot 6 = 12$, ove ϕ è la funzione toziente di Eulero. Il numero degli epimorfismi cercati è dunque 12.

3.

(a) Sia $d(x) = \mathrm{MCD}(f(x),\ g(x))$. Se $p = 2$, allora $f(x) = g(x)^2$, e quindi $d(x) = g(x)$. Sia ora $p > 2$. Si osserva che $d(x)$, dividendo $f(x)$ e $g(x)$, divide anche il polinomio

$$f(x) + g(x)^p = x^{p^3} + x^{p^2} + x^p + \overline{1} + x^{p^3} - x^{p^2} - x^p + \overline{1} = \overline{2}x^{p^3} + \overline{2} = \overline{2}(x + \overline{1})^{p^3}.$$

Ma il polinomio $x + \overline{1}$ non divide $f(x)$, per il Teorema di Ruffini, in quanto $f(-\overline{1}) = -\overline{1} - \overline{1} - \overline{1} + \overline{1} = -\overline{2} \neq \overline{0}$. Ne consegue che $d(x) = \overline{1}$.

(b) Si ha

$$f(x) - g(x)^p = x^{p^3} + x^{p^2} + x^p + \overline{1} - x^{p^3} + x^{p^2} + x^p - \overline{1} = \overline{2}x^{p^2} + \overline{2}x^p.$$

Quindi

$$f(x) - g(x)^p - \overline{2}g(x) = \overline{2}x^{p^2} + \overline{2}x^p - \overline{2}x^{p^2} + \overline{2}x^p + \overline{2}x - \overline{2} = \overline{4}x^p + \overline{2}x - \overline{2}.$$

Il resto cercato è dunque $r(x) = \overline{4}x^p + \overline{2}x - \overline{2}$, nullo se $p = 2$.