Traccia del 9 febbraio 2024

1.

(a) Una permutazione del tipo richiesto è, ad esempio, un qualsiasi prodotto $\tau = (1,2,3)\gamma$, ove γ è un $4-$ciclo disgiunto da $(1,2,3)$. In tal caso, infatti, $\tau^4 = (1,2,3)$ commuta con σ.

(b) Il gruppo $C(\sigma)$ non è abeliano, in quanto vi appartengono gli elementi $\alpha = (1,2,3)$ e $\beta = (1,4,2,5,3,6)$ (poiché $\beta^2 = (1,2,3)(4,5,6)$), ma $\alpha\beta(1) = 4$, mentre $\beta\alpha(1) = 5$.

(c) Si osservi anzitutto che, se γ è un $15-$ciclo, per il Teorema di Lagrange $|\langle\sigma\rangle \cap \langle\gamma\rangle| \in \{1,3\}$. Quindi basterà determinare γ in modo che il sottogruppo intersezione non sia banale. Ora, l'unico sottogruppo di ordine 3 di $\langle\sigma\rangle$ è quello generato da

$$\sigma^2 = (1,3,2)(4,6,5)(7,9,8)(10,12,14)(11,13,15).$$

Quindi basterà prendere un $15-$ciclo γ tale che $\gamma^5 = \sigma^2$, ad esempio

$$\gamma = (1,4,7,10,11,3,6,9,12,13,2,5,8,14,15).$$

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 $(\alpha,\beta) \in \mathbb{Z}_8 \times \mathbb{Z}_9$ un generatore di tale immagine. Si avrà allora $6 = o((\alpha,\beta)) = \mathrm{mcm}(o(\alpha), o(\beta))$. Dato che $o(\alpha)|8$ e $o(\beta)|9$, necessariamente $o(\alpha) = 2$ e $o(\beta) = 3$, e quindi $\mathrm{Im}\varphi = \langle[4]_8\rangle \times \langle[3]_9\rangle$. Tuttavia, questo anello non è unitario, in quanto il suo prodotto è banale.

(b) Se esistesse un epimorfismo φ del tipo indicato, φ conserverebbe l'elemento neutro del prodotto, ossia si avrebbe $\varphi([1]_8, [1]_{12}) = [1]_{16}$. Ma, poiché φ, in quanto omomorfismo di gruppi additivi, conserva i multipli, si avrebbe anche

$$\varphi([0]_8, [0]_{12}) = \varphi([24]_8, [24]_{12}) = \varphi(24([1]_8, [1]_{12})) = 24\varphi([1]_8, [1]_{12}) = 24[1]_{16} = [24]_{16} \neq [0]_{16},$$

e ciò è in contrasto con la proprietà di conservazione dell'elemento neutro della somma.

3.

(a) Si noti che, posto $a(x) = x^p + x^{p-1} + \overline{1}$, e $b(x) = x^{p-1} + x + \overline{1}$, si ha $f(x) = a(x)^p$ e $g(x) = b(x)^{p^2}$. Sia $d(x) = \mathrm{MCD}(a(x), b(x))$. Allora

$$d(x)|a(x) - b(x) = x^p - x = \prod_{\alpha \in \mathbb{Z}_p} (x - \alpha).$$

Ne consegue che $d(x)$ è prodotto di fattori lineari monici a due a due distinti, precisamente, di quelli corrispondenti alle radici comuni ad $a(x)$ e $b(x)$. Ora, se α è una siffatta radice, allora $\alpha \neq \overline{0}$, e dunque, per il Teorema di Eulero, $a(\alpha) = b(\alpha) = \alpha + \overline{2}$, da cui si ricava $\alpha = -\overline{2}$. In conclusione, $d(x) = x + \overline{2}$, che è l'unico fattore irriducibile comune ad $a(x)$ e $b(x)$. Dunque $\mathrm{MCD}(f(x), g(x)) = d(x)^p = x^p + \overline{2}$.

(b) Si ha

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

Se $p > 3$, essendo $2p^2 < \deg g(x) = p^3 - p^2 = (p-1)p^2$, ne deduciamo che il quoziente è $q(x) = x^{p^2}$, mentre il resto è $r(x) = -x^{2p^2} - \overline{1}$. Per $p = 3$, $g(x) = x^{18} + x^9 + \overline{1}$, e, proseguendo il calcolo, si ottiene

$$h(x) = x^9 g(x) - x^{18} - \overline{1} = \left(x^9 - \overline{1}\right) g(x) + x^9.$$

In tal caso, si conclude che il quoziente è $q(x) = x^9 - \overline{1}$, mentre il resto è $r(x) = x^9$.