Traccia del 27 gennaio 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 3 sotto l'azione delle potenze di σ e di τ si deduce che $2|s$ e $2|t$. Il sottogruppo cercato è dunque $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$, dove

$\sigma^2 = (7,9,11,8,10)(12,14,16,18,13,15,17),$
$\tau^2 = (7,8,11,9,10)(12,17,15,13,18,16,14).$

Ora, $o(\sigma^2) = o(\tau^2) = 35$. Ne consegue che, per il Teorema di Lagrange, posto $d = o(\alpha) = |\langle\sigma^2\rangle \cap \langle\tau^2\rangle|$, d è un divisore di 35. D'altra parte, se $5|d$, allora il gruppo ciclico $\langle\sigma^2\rangle \cap \langle\tau^2\rangle$ contiene un unico sottogruppo di ordine 5. Questo deve coincidere, contemporaneamente, con l'unico sottogruppo di $\langle\sigma^2\rangle$ avente ordine 5 e con l'unico sottogruppo di $\langle\tau^2\rangle$ avente ordine 5. Questi sottogruppi sono, rispettivamente,

$\langle\sigma^{14}\rangle = \langle(7,11,10,9,8)\rangle,$
$\langle\tau^{14}\rangle = \langle(7,11,10,8,9)\rangle.$

Evidentemente, sono distinti. Lo si può verificare facilmente, anche determinando tutti i loro elementi. Ciò esclude che $5|d$. Ne consegue che $d|7$, e dunque $5|s$ e $5|t$. Pertanto il sottogruppo cercato è $\langle\sigma^{10}\rangle \cap \langle\tau^{10}\rangle$, ove

$\sigma^{10} = (12,15,18,14,17,13,16),$
$\tau^{10} = (12,16,13,17,14,18,15).$

Ma σ^{10} e τ^{10} sono una l'inversa dell'altra, quindi generano lo stesso sottogruppo. In conclusione, il sottogruppo cercato è $\langle\sigma^{10}\rangle = \langle\tau^{10}\rangle$, avente ordine 7.

(b) Al sottogruppo $C(\sigma) \cap C(\tau)$ appartengono le permutazioni seguenti:

$\gamma = (1,2),\ \delta_1 = (3,4)(5,6),\ \delta_2 = (3,5)(4,6),\ \delta_3 = (3,6)(4,5),$

insieme ai loro prodotti. Dunque

$$H = \{id,\ \gamma,\ \delta_1,\ \delta_2, \delta_3,\ \gamma\delta_1,\ \gamma\delta_2, \gamma\delta_3\} = \{\gamma^a\delta_i^b \mid a,b \in \mathbb{Z},\ 1 \le i \le 3\}$$

è contenuto in $C(\sigma) \cap C(\tau)$. Inoltre, è un sottogruppo, come si può facilmente verificare mediante la caratterizzazione dei sottogruppi. A tal fine è necessario utilizzare le seguenti note proprietà:

- ognuno degli elementi $\gamma, \delta_1, \delta_2, \delta_3$ è inverso di sé stesso;
- questi elementi commutano a due a due;
- se $\{i,j,k\} = \{1,2,3\}$, allora $\delta_i\delta_j = \delta_k$.

Osservazione aggiuntiva: Si può facilmente verificare, alla luce delle proprietà aritmetiche appena ricordate, che il sottogruppo considerato ammette la seguente definizione equivalente:

$$H = \{\gamma^a\delta_1^b\delta_2^c \mid a,b,c \in \mathbb{Z}\}.$$

2.

(a) Un sottoanello del tipo richiesto è un sottogruppo additivo. Ora, per ogni $(\alpha, \beta) \in \mathbb{Z}_6 \times \mathbb{Z}_{14}$, si ha, in virtù del Teorema di Lagrange, $o(\alpha)|6$ e $o(\beta)|14$, così che $o(\alpha, \beta) = \mathrm{mcm}(o(\alpha), o(\beta))|\mathrm{mcm}(6, 14) = 42$. Di conseguenza, nessun elemento di $\mathbb{Z}_6 \times \mathbb{Z}_{14}$ ha periodo 4, e ciò implica che il sottogruppo cercato non è ciclico. Pertanto, sarà isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, e dunque sarà costituito, oltre che dall'elemento zero $([0]_6, [0]_{14})$, da tre elementi di periodo 2. Questi sono necessariamente $([0]_6, [7]_{14})$, $([3]_6, [0]_{14})$, $([3]_6, [7]_{14})$. Il sottogruppo cercato è dunque $\langle [3]_6 \rangle \times \langle [7]_{14} \rangle$, che è anche un sottoanello di $\mathbb{Z}_6 \times \mathbb{Z}_{14}$, in quanto, come è facile constatare, è chiuso rispetto al prodotto; inoltre, $([3]_6, [7]_{14})$ è il suo elemento uno.

(b) Sia $\varphi : \mathbb{Z}_8 \times \mathbb{Z}_9 \to \mathbb{Z}_6$ un epimorfismo di anelli. Essendo φ, in particolare, un omomorfismo di gruppi additivi, esso conserva i multipli, oltre all'elemento zero. Dunque $\varphi([1]_8, [0]_9)$ dovrà essere un elemento $\alpha \in \mathbb{Z}_6$ tale che $8\alpha = [0]_6$. Pertanto $\varphi([1]_8, [0]_9) \in \{[0]_6, [3]_6\}$. Analogamente si deduce che $\varphi([0]_8, [1]_9) \in \{[0]_6, [2]_6, [4]_6\}$. D'altra parte ogni epimorfismo di anelli unitari conserva l'elemento uno, così che

$$[1]_6 = \varphi([1]_8, [1]_9) = \varphi([1]_8, [0]_9) + ([0]_8, [1]_9)) = \varphi([1]_8, [0]_9) + \varphi([0]_8, [1]_9).$$

Si noti che nell'ultima uguaglianza è stata applicata la conservazione della somma. Ma allora si ha necessariamente che $\varphi([1]_8, [0]_9) = [3]_6$ e $\varphi([0]_8, [1]_9) = [4]_6$. Dunque, applicando nuovamente la conservazione della somma, insieme alla conservazione dei multipli, si ottiene la definizione di φ. Precisamente, per ogni $a, b \in \mathbb{Z}$,

$$\varphi([a]_8, [b]_9) = [3a + 4b]_6.$$

Questo è un omomorfismo di gruppi ben definito, ed è surgettivo, dato che $[1]_6 \in \mathrm{Im}\varphi$. Infine, si può facilmente verificare che conserva anche il prodotto. In conclusione, φ è un epimorfismo di anelli.

(c) Sia $\psi : \mathbb{Z}_{60} \to \mathbb{Z}_{30}$ un omomorfismo di gruppi. Allora, se $\psi([1]_{60}) = [\lambda]_{30}$, in virtù della conservazione dei multipli si avrà, per ogni $a \in \mathbb{Z}$, $\psi([a]_{60}) = [\lambda a]_{30}$. D'altra parte, il nucleo richiesto è l'unico sottogruppo di $\mathbb{Z}_{60}$ avente ordine 4, ossia deve essere $\langle [15]_{60} \rangle$. Chiaramente, questo coinciderà con $\mathrm{Ker}\psi$ se $\lambda = 2$.

3.

(a) Sia $\alpha \in \mathbb{Z}_p$. Allora, in virtù del Piccolo Teorema di Fermat, $f(\alpha) = \alpha^q - \overline{1}$, e dunque $f(\alpha) = \overline{0}$ se e solo se, nel gruppo moltiplicativo $\mathbb{Z}_p^*$, si ha che $o(\alpha)|q$. Poiché, per il Teorema di Lagrange, si ha in ogni caso che $o(\alpha)|p-1$, ne deriva che α è radice se e solo se $o(\alpha)|\mathrm{MCD}(q, p-1)$. Posto $d = \mathrm{MCD}(q, p-1)$, si osserva che d è un divisore dell'ordine del gruppo $\mathbb{Z}_p^*$, che è notoriamente ciclico. Ora, per ogni divisore positivo e di d, il numero degli elementi di periodo e in $\mathbb{Z}_p^*$ è pari a $\phi(e)$ (funzione di Eulero). Pertanto, il numero delle radici di $f(x)$ è

$$\sum_{e|d} \phi(e) = d.$$

Si può osservare, per completezza, che, essendo q un numero primo, i casi possibili sono esattamente due:

- se $q|p-1$, allora $d=q$;
- altrimenti $d=1$.

(b) Sia $\alpha \in \mathbb{Z}_{101}$. Allora, in virtù del Piccolo Teorema di Fermat, $g(\alpha)=\alpha^{25}+\overline{1}$, e dunque $g(\alpha)=\overline{0}$ se e solo se $\alpha^{25}=-\overline{1}$, ossia se e solo se $o\left(\alpha^{25}\right)=2$. In tal caso $\alpha^{50}=\overline{1}$ così che, nel gruppo moltiplicativo $\mathbb{Z}_{101}^{*}$, da un lato, $o(\alpha)$ divide 50, dall'altro $o(\alpha)$ non divide 25. Ne consegue che $o(\alpha) \in \{2,10,50\}$. In tutti questi casi si ha, in effetti, la condizione voluta:

$$o\left(\alpha^{25}\right)=\frac{o(\alpha)}{\mathrm{MCD}(o(\alpha),25)}=2.$$

In conclusione, il numero delle radici di $g(x)$ è

$$\phi(2)+\phi(10)+\phi(50)=1+4+20=25.$$

Svolgimento alternativo: Si può osservare che il polinomio $h(x)=x^{100}-\overline{1}$ ha, come radici, tutti i 100 elementi di $\mathbb{Z}_{101}^{*}$. Pertanto si decompone, in $\mathbb{Z}_{101}[x]$, nel prodotto di fattori lineari monici, a due a due distinti. Ora, il polinomio $\ell(x)=x^{25}+\overline{1}$ è un divisore di $h(x)$. Quindi sarà il prodotto di 25 dei suoi fattori lineari, e avrà, dunque, esattamente 25 radici in $\mathbb{Z}_{101}$.