Traccia del 2 novembre 2022

1.

(a) Si ha $\sigma^5 = (1,6)(2,7)(3,8)(4,9)(5,10)$. Questo elemento di $\langle\sigma\rangle$ appartiene a ciascuno dei seguenti sottogruppi di S_{10}:

$$H = \{(1,6)^a(2,7)^b(3,8)^c(4,9)^c(5,10)^c | a,b,c \in \mathbb{Z}\},$$
$$K = \{(1,6)^a(2,7)^a(3,8)^a(4,9)^b(5,10)^c | a,b,c \in \mathbb{Z}\}.$$

Entrambi hanno ordine $2^3 = 8,$ e sono distinti, in quanto $(1,6) \in H,$ ma $(1,6) \notin K.$

(b) Sia

$$L = \{(1,2,6,7)^a(3,4,5,8,9,10)^b | a,b \in \mathbb{Z}\}.$$

Allora $|L| = 4 \cdot 6 = 24$. Inoltre ad L appartiene

$$\sigma^5 = (1,2,6,7)^2(3,4,5,8,9,10)^3.$$

Ciò prova che $L \cap \langle\sigma\rangle \neq \{id\}$.

(c) Il gruppo $C(\sigma^5)$ non è ciclico, in quanto vi appartengono più elementi di periodo 2, tra cui $(1,6)$ e $(2,7)$.

2.

(a) L'applicazione φ è ben definita se e solo se

$$\text{per ogni } a,a',b,b' \in \mathbb{Z},\ n|a-a' \text{ e } m|b-b' \implies n|a+b-(a'+b') = (a-a')+(b-b'),$$

se e solo se,

$$\text{per ogni } h,k \in \mathbb{Z},\ n|nh+mk. \qquad (1)$$

Se ciò avviene, allora, in particolare, $n|m$. Viceversa, se $n|m,$ allora (1) vale. Quindi l'insieme cercato è $\{(n,nh) | h \in \mathbb{Z}\}$.

(b) Siano $a,b \in \mathbb{Z}$. Allora

$$\varphi([a]_n,[b]_m) = [0]_n \text{ se e solo se } n|a+b \text{ se e solo se } b \equiv -a \pmod{n}.$$

La soluzione generale della congruenza lineare

$$x \equiv -a \pmod{n}$$

è

$$x_k = -a+nk \quad (k \in \mathbb{Z}).$$

Se $m = nh,$ allora $x_0,\ldots,x_{h-1}$ sono le soluzioni a due a due non congrue modulo m. Pertanto, per ognuno degli n elementi α di $\mathbb{Z}_n$ esistono esattamente h elementi β di $\mathbb{Z}_m$ tali che $(\alpha,\beta) \in \varphi^{-1}([0]_n)$. In conclusione, $|\varphi^{-1}([0]_n)| = nh = m$.

(c) Siano $a,b \in \mathbb{Z}$. Allora

$$a = nk - b \quad \text{per qualche } k \in \mathbb{Z}$$

se e solo se

$$([a]_n, [b]_m) = ([-b]_n, [b]_m)$$

se e solo se

$$([a]_n, [b]_m) \in \langle([-1]_n, [1]_m)\rangle.$$

Quest'ultimo è un gruppo ciclico, di ordine pari a $\mathrm{mcm}(n, m) = m$. Quest'ultima osservazione consente di risolvere (b) e (c) insieme.

3. Sia $\alpha \in \mathbb{Z}_p$. Allora, per il Piccolo Teorema di Fermat, $\alpha^{p^n} = \alpha$, per ogni intero nonnegativo n. Dunque

$$\begin{aligned} f(\alpha) &= \alpha^{p^3+p^2+1} + \alpha^{p^2+1} + \alpha^p + \overline{1} \\ &= \alpha^3 + \alpha^2 + \alpha + \overline{1}. \end{aligned}$$

Ora,

$$(\alpha - 1)\left(\alpha^3 + \alpha^2 + \alpha + \overline{1}\right) = \alpha^4 - \overline{1}.$$

Quindi

i) se $p = 2,$ allora $f(x)$ ha, come unica radice, $\overline{1}$;

ii) se $p \neq 2,$ allora $f(\overline{1}) = \overline{4} \neq 0,$ e dunque α è radice di $f(x)$ se e solo se α ha periodo 2 oppure 4 in $\mathbb{Z}_p^*$. L'unico elemento di periodo 2 è $-\overline{1}$. Un elemento di periodo 4 esiste in $\mathbb{Z}_p^*$ se e solo se $4|p-1$ (ossia $p \equiv 1 \pmod 4$), ed in tal caso gli elementi siffatti sono $2,$ uno l'opposto dell'altro.

In conclusione:

- se $p = 2,$ l'unica radice è $\overline{1},$
- se $p \equiv 3 \pmod 4$, l'unica radice è $-\overline{1}$,
- se $p \equiv 1 \pmod 4$, $f(x)$ ha esattamente tre radici: $-\overline{1},\ \alpha,\ -\alpha$.