Algebra per Informatica

Esame 19/07/2023

Svolgere nel foglio di consegna i seguenti esercizi **motivando chiaramente** le risposte.

Esercizio 1. Si considerino le seguenti funzioni

$$f : \mathbb{C} \longrightarrow \mathbb{C} \qquad\qquad g : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \mapsto x^4 + 1 \qquad\qquad x \mapsto x^4 + 1$$

1. Determinare se f è iniettiva e/o suriettiva.
2. Calcolare $f^{-1}(0)$.
3. Determinare se g è iniettiva e/o suriettiva.
4. Calcolare $g^{-1}(-1)$.

Soluzione.

1. La funzione f non è iniettiva siccome $f(1) = 2 = f(-1)$. La funzione f è surgettiva, in quanto dato $c \in \mathbb{C}$ per il teorema fondamentale dell'algebra esiste sempre $x \in \mathbb{C}$ tale che $x^4 + 1 - c = 0$, cioè tale che $f(x) = c$.
2. Abbiamo $f^{-1}(0) = \{x \in \mathbb{C} \mid \ x^4 + 1 = 0\} = \{x \in \mathbb{C} \mid \ x^4 = -1\}$, cioè $f^{-1}(0)$ è l'insieme delle radici quarte complesse di $z = -1$. Abbiamo $|z| = 1$ e $\arg(z) = \pi$. Pertanto le radici quarte z_k (per $k = 0, 1, 2, 3$) di z sono date dalla formula

$$z_k = \sqrt[4]{1}\left(\cos\left(\frac{\pi + 2k\pi}{4}\right) + i\sin\left(\frac{\pi + 2k\pi}{4}\right)\right) = \cos\left(\frac{\pi}{4} + \frac{k\pi}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{k\pi}{2}\right).$$

Abbiamo quindi

$$\begin{aligned}
z_0 &= \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,\\
z_1 &= \cos\left(\frac{\pi}{4} + \frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{\pi}{2}\right) = \cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right) = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,\\
z_2 &= \cos\left(\frac{\pi}{4} + \pi\right) + i\sin\left(\frac{\pi}{4} + \pi\right) = \cos\left(\frac{5\pi}{4}\right) + i\sin\left(\frac{5\pi}{4}\right) = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i,\\
z_3 &= \cos\left(\frac{\pi}{4} + \frac{3\pi}{2}\right) + i\sin\left(\frac{\pi}{4} + \frac{3\pi}{2}\right) = \cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right) = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.
\end{aligned}$$

E perciò $f^{-1}(0) = \{z_0, z_1, z_2, z_3\}$.

3. La funzione g non è iniettiva siccome $g(1) = 2 = g(-1)$. La funzione g non è surgettiva, in quanto non esiste nessun valore reale $x \in \mathbb{R}$ per cui $x^4 + 1 = 0$, cioè $g^{-1}(0) = \emptyset$.
4. Abbiamo $g^{-1}(1) = \{x \in \mathbb{C} \mid \ x^4 + 1 = 1\} = \{x \in \mathbb{C} \mid \ x^4 = 0\} = \{0\}$, siccome l'equazione $x^4 = 0$ ha soltanto la soluzione nulla.

Esercizio 2. Sia dato l'insieme $A = \{(-1,-2), (-2,-1), (0,0), (1,1), (1,4), (2,3), (5,3)\}$.
1. Si consideri A come sottoinsieme del poset $(\mathbb{Z} \times \mathbb{Z}, \leq \times \leq)$ e si determinino (se esistono) massimo, minimo, estremo inferiore, ed estremo superiore di A.
2. Si consideri A come sottoinsieme del poset $(\mathbb{Z}\times\mathbb{Z}, \mathrm{LEX})$ e si determinino (se esistono) massimo, minimo, estremo inferiore, ed estremo superiore di A.

Soluzione. 1. Abbiamo il seguente diagramma di Hasse che rappresenta la struttura del poset A (dove l'ordine $\leq \times \leq$ procede dal basso verso l'alto):

$$\begin{tikzcd}
 & & (5,3) \arrow[d, dash] \\
(1,4) \arrow[dr, dash] & & (2,3) \arrow[dl, dash] \\
 & (1,1) \arrow[d, dash] & \\
 & (0,0) \arrow[dl, dash] \arrow[dr, dash] & \\
(-2,-1) & & (-1,-2)
\end{tikzcd}$$

Si vede che A ha due elementi minimali $(-1,-2)$ e $(-2,-1)$ che non sono confrontabili. Quindi A non ammette minimo. Analogamente, A ha due elementi massimali non confrontabili $(1,4)$ e $(5,3)$. Pertanto A non ammette massimo. L'insieme dei maggioranti di A è

$$\{(x,y) \in \mathbb{Z}^2 : \ x \geq 5 \text{ AND } y \geq 4\},$$

che ha minimo $(5,4)$. Pertanto $\sup A = (5,4)$. Analogamente, l'insieme dei minoranti di A è

$$\{(x,y) \in \mathbb{Z}^2 : \ x \leq -2 \text{ AND } y \leq -2\},$$

che ha massimo $(-2,-2)$. Pertanto $\inf A = (-2,-2)$. Ricapitolando, abbiamo

$$\nexists \max A, \quad \nexists \min A, \quad \sup A = (5,4), \quad \inf A = (-2,-2).$$

2. Sappiamo che $(\mathbb{Z}, \leq)$ è totalmente ordinato, e quindi anche $(\mathbb{Z}\times\mathbb{Z}, \mathrm{LEX})$ è totalmente ordinato. Pertanto anche A è totalmente ordinato. Più precisamente, A è la catena seguente:

$$(-2,-1) \leq (-1,-2) \leq (0,0) \leq (1,1) \leq (1,4) \leq (2,3) \leq (5,3).$$

Quindi abbiamo $\min A = \inf A = (-2,-1)$ e $\max A = \sup A = (5,3)$.

Esercizio 3. Semplificare la seguente espressione in $\mathbb{Z}_{36}$

$$\overline{7}^{24} + \overline{3}^{4} + \overline{2} \cdot \overline{13}^{13}.$$

smallskip

Soluzione. Ricordiamo che per il teorema di Eulero, se $\overline{x}$ è invertibile in $\mathbb{Z}_n$ allora $\overline{x}^{\varphi(n)} = \overline{1}$, dove $\varphi(n)$ è la funzione φ di Eulero. In questo caso, abbiamo $\varphi(36) = \varphi(4)\varphi(9) = 2 \cdot 6 = 12$. Pertanto $\overline{x}^{12} = \overline{1}$ per ogni $\overline{x}$ invertibile in $\mathbb{Z}_{36}$. Inoltre ricordiamo che $\overline{x}$ è invertibile in $\mathbb{Z}_n$ se e soltanto se $\mathrm{MCD}(x, n) = 1$. In questo caso, $\mathrm{MCD}(7, 36) = \mathrm{MCD}(13, 36) = 1$, quindi sia $\overline{7}$ che $\overline{13}$ sono invertibili in $\mathbb{Z}_{36}$. Siamo adesso pronti per semplificare l'espressione richiesta:

$$\begin{aligned}
\overline{7}^{24} + \overline{3}^{4} + \overline{2} \cdot \overline{13}^{13} &= (\overline{7}^{12})^2 + \overline{81} + \overline{2} \cdot \overline{13}^{12} \cdot \overline{13} \\
&= \overline{1}^2 + \overline{9} + \overline{2} \cdot \overline{1} \cdot \overline{13} \\
&= \overline{1} + \overline{9} + \overline{26} \\
&= \overline{36} = \overline{0}.
\end{aligned}$$

Esercizio 4. Si consideri la seguente funzione

$$\begin{aligned}
f : \mathbb{Z}_{21} &\longrightarrow \mathbb{Z}_{21} \\
\overline{x} &\mapsto \overline{2x+1}
\end{aligned}$$

1. Determinare se f è iniettiva e/o surgettiva.
2. Trovare (se esiste) l'inversa di f nel monoide $(X^X, \circ, \mathrm{Id}_X)$, dove $X = \mathbb{Z}_{21}$.

Soluzione. Per prima cosa osserviamo che siccome $\mathrm{MCD}(2, 21) = 1$, la classe di equivalenza di 2 è invertibile in $\mathbb{Z}_{21}$. Con l'algoritmo euclideo, o con un calcolo diretto, si può determinare più precisamente che

$$\overline{2}^{-1} = \overline{11} \text{ in } \mathbb{Z}_{21} \quad \text{infatti } \overline{2} \cdot \overline{11} = \overline{22} = \overline{1}.$$

1. **Iniettività.** Siano $\overline{x}, \overline{a} \in \mathbb{Z}_{21}$ tali che $f(\overline{x}) = f(\overline{a})$, cioè $\overline{2x+1} = \overline{2a+1}$. Sottraiamo $\overline{1}$ ad entrambi i membri e otteniamo $\overline{2x} = \overline{2a}$. Infine moltiplicando entrambi i membri per $\overline{11} \in \mathbb{Z}_{21}$, che è l'inverso di $\overline{2}$ per quanto detto prima, abbiamo $\overline{x} = \overline{a}$. Pertanto la funzione f è iniettiva.
   Surgettività. Sia $\overline{a} \in \mathbb{Z}_{21}$. Ci chiediamo se esiste $\overline{x} \in \mathbb{Z}_{21}$ tale che $f(\overline{x}) = \overline{a}$, cioè tale che
   $$\overline{2x+1} = \overline{a}.$$

Sottraendo $\overline{1}$ ad entrambi i membri, l'uguaglianza precedente è equivalente a

$$\overline{2x} = \overline{a} - \overline{1}.$$

Moltiplichiamo entrambi i membri per $\overline{2}^{-1} = \overline{11}$ e otteniamo

$$\overline{x} = \overline{11} \cdot \overline{a} - \overline{11}.$$

Pertanto scegliendo $\overline{x}$ come sopra si ha che $f(\overline{x}) = \overline{a}$, cioè f è surgettiva.

2. L'inversa di f è la funzione

$$\begin{aligned} g : \mathbb{Z}_{21} &\longrightarrow \mathbb{Z}_{21} \\ \overline{x} &\mapsto \overline{11} \cdot \overline{x} - \overline{11} \end{aligned}$$

Verifichiamo che $f \circ g = \mathrm{Id}_X$

$$\begin{aligned} (f \circ g)(\overline{x}) &= f(g(\overline{x})) \\ &= f(\overline{11} \cdot \overline{x} - \overline{11}) \\ &= \overline{2}(\overline{11} \cdot \overline{x} - \overline{11}) + \overline{1} \\ &= \overline{x} - \overline{22} + \overline{1} \\ &= \overline{x}. \end{aligned}$$

La verifica che $g \circ f = \mathrm{Id}_X$ è analoga.