Alessio Caminata
Francesco Strazzanti

Algebra per Informatica

Esame 24 gennaio 2024: soluzioni

Svolgere i seguenti esercizi **motivando chiaramente** le risposte.

Esercizio 1. Si consideri la seguente funzione

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\mapsto x^4 + 1 \end{aligned}$$

1. Determinare se f è iniettiva e/o suriettiva.
2. Determinare $f^{-1}(1)$ e $f^{-1}(2)$.

Soluzione.
1. La funzione f non è iniettiva in quanto $f(1) = 2 = f(-1)$. La funzione f è surgettiva. Infatti, dato un qualunque $c \in \mathbb{C}$ esiste sempre un valore $x_0 \in \mathbb{C}$ tale che $f(x_0) = c$ perché per il teorema fondamentale dell'algebra, l'equazione $x^4 + 1 - c = 0$ ha sempre soluzioni in $\mathbb{C}$.
2. Si ha che

$$f^{-1}(1) = \{x \in \mathbb{C} \mid f(x) = 1\} = \{x \in \mathbb{C} \mid x^4 + 1 = 1\} = \{x \in \mathbb{C} \mid x^4 = 0\} = \{0\}.$$

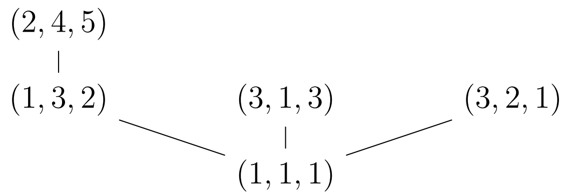
Analogamente, abbiamo

$$f^{-1}(2) = \{x \in \mathbb{C} \mid f(x) = 2\} = \{x \in \mathbb{C} \mid x^4 + 1 = 2\} = \{x \in \mathbb{C} \mid x^4 = 1\}.$$

Pertanto, l'insieme $f^{-1}(2)$ ha come elementi le 4 radici quarte dell'unità, cioè $f^{-1}(2) = \{1, -1, i, -i\}$.

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



Si vede che A ha tre elementi massimali $(2,4,5)$, $(3,1,3)$, e $(3,2,1)$ che non sono confrontabili. Quindi A non ammette massimo. Il minimo di A è $(1,1,1)$, che quindi è anche l'estremo inferiore. Per determinare l'estremo superiore, cerchiamo l'insieme dei maggioranti di A. Esso è dato da

$$\{(x,y,z) \in \mathbb{Z}^3 : \ x \geq 3 \text{ AND } y \geq 4 \text{ AND } z \geq 5\},$$

che ha minimo $(3,4,5)$. Pertanto $\sup A = (3,4,5)$.

2. Sappiamo che $(\mathbb{Z}, \leq)$ è totalmente ordinato, e quindi anche $(\mathbb{Z}^3, \text{LEX})$ è totalmente ordinato. Pertanto anche A è totalmente ordinato. Più precisamente, A è la catena seguente:

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

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

Esercizio 3. 1. Calcolare $\text{MCD}(76,32)$ con l'algoritmo euclideo.
2. Scrivere l'identità di Bézout per 76 e 32.
3. Stabilire se l'equazione $76x + 32y = 8$ ammette soluzioni intere e in tal caso determinarne una.
4. Stabilire se l'equazione $76x + 32y = 2$ ammette soluzioni intere e in tal caso determinarne una.

Soluzione. 1. Nel seguito sono sottolineati i due numeri tra cui facciamo la divisione euclidea.

$$\begin{aligned}
\underline{76} &= 2 \cdot \underline{32} + 12\\
\underline{32} &= 2 \cdot \underline{12} + 8\\
\underline{12} &= 1 \cdot \underline{8} + 4\\
\underline{8} &= 2 \cdot \underline{4} + 0
\end{aligned}$$

Il massimo comun divisore è l'ultimo resto non nullo, quindi $\text{MCD}(76,32) = 4$.

2. Per calcolare l'identità di Bézout dobbiamo ripercorrere a ritroso l'algoritmo euclideo, partendo dalla penultima uguaglianza sostituiamo la terzultima e così via fino

alla prima; ricordiamoci di trattare i numeri sottolineati come fossero delle variabili, quindi non dobbiamo mai sommarli o moltiplicarli.

$$\begin{aligned}4 &= \underline{12} - \underline{8} = \underline{12} - (\underline{32} - 2 \cdot \underline{12}) = -\underline{32} + 3 \cdot \underline{12} \\ &= -\underline{32} + 3 \cdot (\underline{76} - 2 \cdot \underline{32}) = 3 \cdot \underline{76} - 7 \cdot \underline{32}.\end{aligned}$$

Dunque abbiamo ottenuto che $3 \cdot \underline{76} - 7 \cdot \underline{32} = 4$, che è l'identità di Bézout che cercavamo.

3. Moltiplicando per 2 l'identità di Bézout $4 = 3 \cdot \underline{76} - 7 \cdot \underline{32}$ ottenuta al punto precedente otteniamo
$$2 \cdot 4 = 2 \cdot (3 \cdot \underline{76} - 7 \cdot \underline{32}) = 6 \cdot \underline{76} - 14 \cdot \underline{32},$$
cioè l'uguaglianza $8 = 6 \cdot \underline{76} - 14 \cdot \underline{32}$. Ciò mostra che $(x, y) = (6, -14)$ è una soluzione dell'equazione $76x + 32y = 8$.
4. Ricordiamo che l'equazione diofantea $ax + by = c$ ha soluzioni intere se e soltanto se $\mathrm{MCD}(a, b) \mid c$. In questo caso, abbiamo $\mathrm{MCD}(76, 32) = 4 \nmid 2$, pertanto l'equazione $76x + 32y = 2$ non ammette soluzioni intere.

Esercizio 4. Si consideri il gruppo $\big(\mathrm{U}(\mathbb{Z}_{42}), \cdot, \overline{1}\big)$.
1. Calcolare la cardinalità di $\mathrm{U}(\mathbb{Z}_{42})$.
2. Stabilire quali dei seguenti insiemi sono sottogruppi di $\mathrm{U}(\mathbb{Z}_{42})$:
$$\begin{aligned}A &= \{\overline{0}, \overline{21}\}, \\ B &= \{\overline{1}, \overline{5}, \overline{25}, \overline{31}, \overline{41}\}, \\ C &= \{\overline{1}, \overline{13}\}.\end{aligned}$$

Soluzione. 1. La cardinalità di $\mathrm{U}(\mathbb{Z}_{42})$ è $|\mathrm{U}(\mathbb{Z}_{42})| = \varphi(42)$, dove φ denota la funzione di Eulero. Siccome $42 = 2 \cdot 3 \cdot 7$, con $2, 3, 7$ numeri primi, abbiamo che
$$\varphi(42) = 42\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 12.$$
Quindi $\mathrm{U}(\mathbb{Z}_{42})$ ha 12 elementi.
2. Ricordiamo che per il Teorema di Lagrange, l'ordine di un sottogruppo divide l'ordine del gruppo. Quindi il sottoinsieme B che ha cardinalità $5 \nmid 12 = |\mathrm{U}(\mathbb{Z}_{42})|$ non è un sottogruppo. Inoltre, un sottogruppo deve sempre contenere l'elemento neutro del gruppo, in questo caso $\overline{1}$. Pertanto A non è un sottogruppo perché $\overline{1} \notin A$.
Infine, dimostriamo invece che il sottoinsieme C è un sottogruppo. Per provare che è un sottogruppo, dobbiamo verificare che contiene l'elemento neutro (che è vero in quanto $\overline{1} \in C$), che è chiuso rispetto all'operazione del gruppo e che contiene

Alessio Caminata
Francesco Strazzanti

gli inversi dei suoi elementi. Siccome C ha soltanto due elementi, e $\overline{1}$ è l'elemento neutro, ci basta controllare il risultato dell'operazione

$$\overline{13} \cdot \overline{13} = \overline{169} = \overline{4 \cdot 42 + 1} = \overline{1}.$$

Questo ci dice che C è chiuso rispetto all'operazione e che $\overline{13}^{-1} = \overline{13}$. Pertanto C è un sottogruppo di $\big(\mathrm{U}(\mathbb{Z}_{42}), \cdot, \overline{1}\big)$.