Algebra per Informatica

Esame 28/06/2023

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

Esercizio 1. Siano dati i seguenti insiemi

$$A = \{f : \mathbb{Z}_5 \to \mathbb{Z}_5\}, \quad B = \{f : \mathbb{Z}_5 \to \mathbb{Z}_5 \text{ iniettiva}\}, \quad C = \{f : \mathbb{Z}_5 \to \mathbb{Z}_5 \mid f(\overline{0}) = f(\overline{1})\}.$$

Calcolare la cardinalità degli insiemi seguenti: $A \cap B$, $B \cap C$, $B \cup C$, $A \times B$.

Soluzione. Per prima cosa calcoliamo le cardinalità di A, B, e C. L'insieme A è costituito da tutte le funzioni $\mathbb{Z}_5 \to \mathbb{Z}_5$, cioè $A = \mathbb{Z}_5^{\mathbb{Z}_5}$, e quindi $|A| = 5^5 = 3125$. Le funzioni iniettive $\mathbb{Z}_5 \to \mathbb{Z}_5$ sono $|B| = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. Infine, per contare le funzioni in C, consideriamo che abbiamo 5 possibili scelte per il valore di $f(\overline{0}) = f(\overline{1})$, 5 per il valore di $f(\overline{2})$, 5 per $f(\overline{3})$, e 5 per $f(\overline{4})$. Quindi abbiamo $|C| = 5^4 = 625$.

1. Siccome $B \subseteq A$, abbiamo $|A \cap B| = |B| = 120$.
2. Calcoliamo la cardinalità di $B \cap C$. Abbiamo

$$B \cap C = \{f : \mathbb{Z}_5 \to \mathbb{Z}_5 \mid \; f \text{ è iniettiva}, f(\overline{0}) = f(\overline{1})\}.$$

   Siccome una funzione f tale che $f(\overline{0}) = f(\overline{1})$ è necessariamente non iniettiva, abbiamo che $B \cap C = \emptyset$. Pertanto $|B \cap C| = 0$.
3. Calcoliamo $|B \cup C| = |B| + |C| - |B \cap C| = 120 + 5^4 - 0 = 745$.
4. Calcoliamo $|A \times B| = |A| \cdot |B| = 5^5 \cdot 120 = 375\,000$.

Esercizio 2. Sia $f : \mathbb{Z}^2 \to \mathbb{Z}$ l'applicazione data da $f(x, y) = 18x - 27y$.

1. Determinare se f è iniettiva e/o surgettiva.
2. Determinare $f^{-1}(0)$, $f^{-1}(3)$, $f^{-1}(9)$.

Soluzione. Si ricordi che l'equazione diofantea $ax + by = c$ ha soluzioni intere se e soltanto se $\mathrm{MCD}(a, b) \mid c$. Inoltre, se $(x_0, y_0) \in \mathbb{Z}^2$ è una soluzione dell'equazione diofantea $ax + by = c$ con $\mathrm{MCD}(a, b) = 1$, allora tutte le soluzioni si scrivono come $(x, y) = (x_0 + bk, y_0 - ak)$ al variare di $k \in \mathbb{Z}$. In questo caso, siccome $\mathrm{MCD}(18, 27) = 9$ abbiamo che l'equazione diofantea $18x - 27y = c$ ha soluzioni se e soltanto se $9 \mid c$.

1. La funzione f non è surgettiva in quanto $f^{-1}(1) = \{(x, y) \in \mathbb{Z}^2 : 18x - 27y = 1\} = \emptyset$ siccome l'equazione diofantea $18x - 27y = 1$ non ha soluzioni intere per quanto detto precedentemente. Analogamente f non è iniettiva, si consideri ad esempio $f(27, 18) = 0 = f(0, 0)$.

2. Calcoliamo le controimmagini richieste.

   - $f^{-1}(0) = \{(x, y) \in \mathbb{Z}^2 : 18x - 27y = 0\} = \{(x, y) \in \mathbb{Z}^2 : 2x - 3y = 0\}$. Una soluzione particolare dell'equazione diofantea $2x - 3y = 0$ è data da $(x_0, y_0) = (0, 0)$. Pertanto abbiamo
   $$f^{-1}(0) = \{(-3k, -2k) : \ k \in \mathbb{Z}\}.$$
   - Siccome $9 \nmid 3$, l'equazione diofantea $18x - 27y = 3$ non ha soluzioni e quindi $f^{-1}(3) = \emptyset$.
   - $f^{-1}(9) = \{(x, y) \in \mathbb{Z}^2 : 18x - 27y = 9\} = \{(x, y) \in \mathbb{Z}^2 : 2x - 3y = 1\}$. Una soluzione particolare dell'equazione diofantea $2x - 3y = 1$ è data da $(x_0, y_0) = (-1, -1)$. Pertanto abbiamo
   $$f^{-1}(9) = \{(-1 - 3k, -1 - 2k) : \ k \in \mathbb{Z}\}.$$

Esercizio 3. Si consideri l'insieme $\mathbb{C}$ dotato della seguente relazione d'ordine:
$$z \lhd w \iff (\Re(z) \leq \Re(w) \text{ AND } \Im(z) \leq \Im(w)),$$
dove $\Re(-)$ denota la parte reale e $\Im(-)$ denota la parte immaginaria.
Sia $A = \{i, 2, \sqrt{2}, 5 + 3i, 3i, 1 - 3i\} \subseteq \mathbb{C}$. Si determinino (se esistono) massimo, minimo, elementi minimali ed elementi massimali, estremo inferiore ed estremo superiore di A nel poset $(\mathbb{C}, \lhd)$.

Soluzione. Osserviamo che con l'usuale identificazione di $\mathbb{C}$ con $\mathbb{R}^2$ data da
$$a + ib \in \mathbb{C} \longleftrightarrow (a, b) \in \mathbb{R}^2,$$
l'ordine $\lhd$ coincide con l'ordine prodotto $\leq \times \leq$. Pertanto, abbiamo il seguente diagramma di Hasse che rappresenta la struttura del poset A (dove l'ordine $\lhd$ procede dal basso verso l'alto):

$$\begin{tikzcd}
 & 5+3i \arrow[dl, dash] \arrow[dr, dash] & \\
2 \arrow[d, dash] & & 3i \arrow[d, dash] \\
\sqrt{2} \arrow[d, dash] & & i \\
1-3i & &
\end{tikzcd}$$

Si vede che A ha un massimo in $5+3i$, che è quindi l'unico elemento massimale. Siccome A ammette massimo, esso coincide con l'estremo superiore. Ci sono due elementi minimali non confrontabili $1-3i$ e i, pertanto A non ammette minimo. L'insieme dei minoranti di A è dato da

$$\{z=a+ib \in \mathbb{C} \mid \ (z \triangleleft 1-3i) \text{ AND } (z \triangleleft i)\} = \{z=a+ib \in \mathbb{C} \mid (a \leq 0) \text{ AND } (b \leq -3)\}.$$

Tale insieme ha un massimo in $0-3i=-3i$ che pertanto è l'estremo inferiore. Ricapitolando, abbiamo

$$\max A = \sup A = 5+3i, \qquad \nexists \min A, \qquad \inf A = -3i.$$

Esercizio 4. Si consideri $\mathbb{Z}_{24}$.
1. Calcolare $\overline{11}^{2025}$.
2. Determinare l'ordine dei seguenti elementi del gruppo degli elementi invertibili $(\mathrm{U}(\mathbb{Z}_{24}), \cdot, \overline{1})$:
$$\overline{1},\ \overline{7},\ \overline{11},\ \overline{13}.$$

Soluzione. Per prima cosa calcoliamo $\varphi(24)=8$ e ricordiamo che per il teorema di Eulero, dato $x \in \mathbb{Z}$ tale che $\mathrm{MCD}(x,24)=1$ allora $\overline{x}^8 = \overline{1}$ in $\mathbb{Z}_{24}$.

1. Consideriamo la divisione euclidea $2025 = 253 \cdot 8 + 1$, abbiamo pertanto
$$\overline{11}^{1025} = \overline{11}^{253 \cdot 8 + 1} = \left(\overline{11}^8\right)^{253} \cdot \overline{11}^1 = \overline{1} \cdot \overline{11}^1 = \overline{11}.$$

2. Ricordiamo che l'ordine moltiplicativo di un elemento $\overline{x}$ in $\mathrm{U}(\mathbb{Z}_{24})$ dev'essere un divisore dell'ordine $|\mathrm{U}(\mathbb{Z}_{24})| = \varphi(24) = 8$. Pertanto calcoliamo soltanto le potenze $\overline{x}^d$ con $d=1,2,4,8$.
   - $\overline{1}$ è l'elemento neutro del gruppo $\mathrm{U}(\mathbb{Z}_{24})$, quindi $\mathrm{ord}(\overline{1}) = 1$.
   - Calcoliamo $\overline{7}^2 = \overline{49} = \overline{48} + \overline{1} = \overline{1}$. Pertanto, abbiamo $\mathrm{ord}(\overline{7}) = 2$.
   - Calcoliamo $\overline{11}^2 = \overline{121} = \overline{120} + \overline{1} = \overline{1}$. Pertanto, abbiamo $\mathrm{ord}(\overline{11}) = 2$.
   - Calcoliamo $\overline{13}^2 = \overline{169} = \overline{168} + \overline{1} = \overline{1}$. Pertanto, abbiamo $\mathrm{ord}(\overline{13}) = 2$.