Algebra per Informatica

Esame 14/02/2023

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

Esercizio 1. Siano dati i seguenti insiemi

$$A = \{f : \mathbb{Z}_6 \to \mathbb{Z}_2 \text{ iniettiva}\},\ B = \{f : \mathbb{Z}_2 \to \mathbb{Z}_6 \text{ iniettiva}\},\ C = \{f : \mathbb{Z}_2 \to \mathbb{Z}_6 \mid f(\overline{0}) = \overline{0}\}.$$

Calcolare la cardinalità degli insiemi seguenti: $A \cap B$, $B \cap C$, $B \cup C$, $\mathcal{P}(C)$.

Soluzione. Per prima cosa calcoliamo le cardinalità di A, B, e C. Siccome $|\mathbb{Z}_2| = 2$ e $|\mathbb{Z}_6| = 6$ abbiamo $6 \cdot 5$ possibili funzioni iniettive $\mathbb{Z}_2 \to \mathbb{Z}_6$, e non ci sono funzioni iniettive $\mathbb{Z}_6 \to \mathbb{Z}_2$. Perciò abbiamo $|B| = 6 \cdot 5 = 30$ e $A = \emptyset$, quindi $|A| = 0$. Per contare le funzioni $f : \mathbb{Z}_2 \to \mathbb{Z}_6$ tali che $f(\overline{0}) = \overline{0}$, consideriamo che per l'elemento $\overline{0}$ del dominio è già stata fissata la rispettiva immagine nel codominio. Rimane soltanto da scegliere l'immagine dell'elemento $\overline{1} \in \mathbb{Z}_2$ che può essere scelta in 6 modi diversi possibili, uno per ciascun elemento di $\mathbb{Z}_6$. Pertanto $|C| = 6$.

1. Siccome $A = \emptyset$, abbiamo $A \cap B = \emptyset$ quindi $|A \cap B| = 0$.
2. Calcoliamo la cardinalità di $B \cap C$. Abbiamo

   $$B \cap C = \{f : \mathbb{Z}_2 \to \mathbb{Z}_6 \mid \ f \text{ è iniettiva}, f(\overline{0}) = \overline{0}\}.$$

   Per contare le funzioni in $B \cap C$, considero che l'immagine di $\overline{0} \in \mathbb{Z}_2$ è già stata fissata, rimane da scegliere l'immagine dell'elemento $\overline{1} \in \mathbb{Z}_2$. Questa immagine non può essere $\overline{0} \in \mathbb{Z}_6$ perché altrimenti la funzione non sarebbe iniettiva. Rimangono quindi soltanto 5 possibilità. Perciò $|B \cap C| = 5$.
3. Calcoliamo $|B \cup C| = |B| + |C| - |B \cap C| = 30 + 6 - 5 = 31$.
4. Calcoliamo $|\mathcal{P}(C)| = 2^{|C|} = 2^6 = 64$.

Esercizio 2. Si considerino le seguenti funzioni

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\mapsto x^2 + 4x \end{aligned} \qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto x^2 + 4x \end{aligned}$$

1. Determinare se f è iniettiva e/o suriettiva.
2. Calcolare $f^{-1}(0)$ e $f^{-1}(-5)$.
3. Determinare se g è iniettiva e/o suriettiva.

4. Calcolare $g^{-1}(0)$ e $g^{-1}(-5)$.

Soluzione. 1. La funzione f non è iniettiva in quanto $f(-4) = (-4)^2 + 4 \cdot (-4) = 16 - 16 = 0 = f(0)$. La funzione f è suriettiva se e soltanto se per ogni $c \in \mathbb{C}$ esiste $x \in \mathbb{C}$ tale che $f(x) = c$, cioè $x^2 + 4x = c$. Un tale x esiste sempre in quanto l'equazione $x^2 + 4x - c = 0$ ha sempre soluzioni in $\mathbb{C}$ per il teorema fondamentale dell'algebra. Quindi f è suriettiva.

2. Abbiamo $f^{-1}(0) = \{x \in \mathbb{C} \mid f(x) = 0\} = \{x \in \mathbb{C} \mid x^2 + 4x = 0\}$. Cioè $f^{-1}(0)$ è l'insieme delle soluzioni complesse dell'equazione $x^2 + 4x = 0$. Scomponendo $x^2 + 4x = x(x + 4)$, si vede che le soluzioni di $x(x + 4) = 0$ sono $x = 0$ e $x = -4$. Quindi $f^{-1}(0) = \{0, -4\}$. Analogamente

$$f^{-1}(-5) = \{x \in \mathbb{C} \mid f(x) = -5\} = \{x \in \mathbb{C} \mid x^2+4x = -5\} = \{x \in \mathbb{C} \mid x^2+4x+5 = 0\}.$$

Per trovare le soluzioni di $x^2 + 4x + 5 = 0$, usiamo la formula per le equazioni di secondo grado $ax^2+bx+c = 0$. Calcoliamo $\Delta = b^2-4ac = 4^2-4\cdot 5 = 16-20 = -4$. Le due radici quadrate complesse δ_1, δ_2 di -4 sono $\delta_1 = 2i$ e $\delta_2 = -2i$ in quanto $\delta_1^2 = \delta_2^2 = -4$. Pertanto le soluzioni di $x^2 + 4x + 5 = 0$ sono

$$w_1 = \frac{-b + \delta_1}{2a} = \frac{-4 + 2i}{2} = -2 + i, \quad w_2 = \frac{-b + \delta_2}{2a} = \frac{-4 - 2i}{2} = -2 - i.$$

Perciò abbiamo $f^{-1}(-5) = \{-2 + i, -2 - i\}$.

3. La funzione g non è iniettiva in quanto $g(-4) = (-4)^2+4\cdot(-4) = 16-16 = 0 = g(0)$. La funzione g non è suriettiva. Ad esempio, non esiste nessuna $x \in \mathbb{R}$ tale che $g(x) = -5$ siccome le soluzioni dell'equazione x^2+4x+5 non sono reali (come visto al punto precedente).

4. Abbiamo

$$g^{-1}(0) = \{x \in \mathbb{C} \mid g(x) = 0\} = \{x \in \mathbb{R} \mid x^2 + 4x = 0\} = \{0, -4\}.$$

Infine $g^{-1}(-5) = \{x \in \mathbb{R} \mid g(x) = -5\} = \{x \in \mathbb{R} \mid x^2 + 4x = -5\} = \emptyset$ in quanto le soluzioni dell'equazione $x^2 + 4x + 5$ non sono reali.

Esercizio 3. Si consideri la seguente funzione

$$\begin{aligned} f : \mathbb{Z}_{13} \times \mathbb{Z}_{39} &\longrightarrow \mathbb{Z}_{13} \times \mathbb{Z}_{39} \\ (\overline{x}, \overline{y}) &\mapsto (\overline{5} \cdot \overline{x}, \overline{5} \cdot \overline{y}) \end{aligned}$$

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 $X = \mathbb{Z}_{13} \times \mathbb{Z}_{39}$.

Soluzione. Per prima cosa osserviamo che siccome $\mathrm{MCD}(5,13) = \mathrm{MCD}(5,39) = 1$, la classe di equivalenza di 5 è invertibile in $\mathbb{Z}_{13}$ e in $\mathbb{Z}_{39}$. Con l'algoritmo euclideo, o con un calcolo diretto, si può determinare più precisamente che

$$\overline{5}^{-1} = \overline{8} \text{ in } \mathbb{Z}_{13} \text{ infatti } \overline{5}\cdot\overline{8} = \overline{40} = \overline{39} + \overline{1} = \overline{1},$$
$$\overline{5}^{-1} = \overline{8} \text{ in } \mathbb{Z}_{39} \text{ infatti } \overline{5}\cdot\overline{8} = \overline{40} = \overline{39} + \overline{1} = \overline{1}.$$

1. **Iniettività.** Siano $(\overline{x},\overline{y}),(\overline{a},\overline{b}) \in X$ tali che $f(\overline{x},\overline{y}) = f(\overline{a},\overline{b})$, cioè $(\overline{5}\cdot\overline{x},\overline{5}\cdot\overline{y}) = (\overline{5}\cdot\overline{a},\overline{5}\cdot\overline{b})$. Moltiplicando la prima componente per $\overline{8} \in \mathbb{Z}_{13}$ e la seconda componente per $\overline{8} \in \mathbb{Z}_{39}$ si ottiene
$$(\overline{8}\cdot\overline{5}\cdot\overline{x},\overline{8}\cdot\overline{5}\cdot\overline{y}) = (\overline{8}\cdot\overline{5}\cdot\overline{a},\overline{8}\cdot\overline{5}\cdot\overline{b})$$
e quindi, siccome $\overline{5}\cdot\overline{8} = \overline{1}$ in $\mathbb{Z}_{13}$ e $\overline{5}\cdot\overline{8} = \overline{1}$ in $\mathbb{Z}_{39}$, si ha $(\overline{x},\overline{y}) = (\overline{a},\overline{b})$.
Surgettività. Sia $(\overline{a},\overline{b}) \in X$. Scegliamo $(\overline{x},\overline{y}) = (\overline{8}\cdot\overline{a},\overline{8}\cdot\overline{b})$. Per quanto detto sopra si verifica facilmente che $f(\overline{x},\overline{y}) = f(\overline{8}\cdot\overline{a},\overline{8}\cdot\overline{b}) = (\overline{5}\cdot\overline{8}\cdot\overline{a},\overline{5}\cdot\overline{8}\cdot\overline{b}) = (\overline{a},\overline{b})$.

2. L'inversa di f è la funzione
$$\begin{aligned} g : \mathbb{Z}_{13}\times\mathbb{Z}_{39} &\longrightarrow \mathbb{Z}_{13}\times\mathbb{Z}_{39} \\ (\overline{x},\overline{y}) &\mapsto (\overline{8}\cdot\overline{x},\overline{8}\cdot\overline{y}) \end{aligned}$$
La verifica che $f\circ g = g\circ f = \mathrm{Id}_X$ segue da quanto detto prima.

Esercizio 4.
1. Determinare **tutti** i sottogruppi di $\left(\mathbb{Z}_9,+,\overline{0}\right)$.
2. Determinare **tutti** i sottogruppi di $\left(\mathbb{Z}_{11},+,\overline{0}\right)$.

Soluzione. Ricordiamo che per il Teorema di Lagrange, l'ordine di un sottogruppo di un gruppo finito dev'essere un divisore dell'ordine del gruppo.

1. Siccome $|\mathbb{Z}_9| = 9$, un sottogruppo di $\mathbb{Z}_9$ può avere ordine $1, 3$, oppure 9. C'è soltanto un sottogruppo di ordine 1, il sottogruppo triviale $\{\overline{0}\}$. Analogamente, c'è soltanto un sottogruppo di ordine massimo 9, il gruppo stesso $\mathbb{Z}_9$. Rimangono da determinare i possibili sottogruppi di ordine 3. Proviamo a costruire un sottogruppo $H \subseteq \mathbb{Z}_9$ di cardinalità 3. L'elemento neutro $\overline{0}$ deve appartenere ad H. Quindi H sarà della forma $H = \{\overline{0}, x, y\}$. Inoltre, ricordiamo che l'ordine di un elemento deve dividere l'ordine del gruppo, quindi necessariamente x e y devono avere ordine $3 = |H|$. Ci sono soltanto due elementi di ordine 3 in $\mathbb{Z}_9$: $\overline{3}$ e $\overline{6}$. Tutti gli altri elementi (diversi da $\overline{0}$) di $\mathbb{Z}_9$ hanno ordine 9. Pertanto, l'unica possibilità è $H = \{\overline{0},\overline{3},\overline{6}\}$. Si verifica che H è un sottogruppo in quanto chiuso rispetto alla somma:
$$\overline{3}+\overline{3} = \overline{6}, \quad \overline{3}+\overline{6} = \overline{0}, \quad \overline{6}+\overline{6} = \overline{3}.$$
2. Siccome $|\mathbb{Z}_{11}| = 11$, un sottogruppo di $\mathbb{Z}_{11}$ può avere ordine 1 oppure 11. C'è soltanto un sottogruppo di ordine 1, il sottogruppo triviale $\{\overline{0}\}$. Analogamente, c'è soltanto un sottogruppo di ordine massimo 11, il gruppo stesso $\mathbb{Z}_{11}$. Non ci sono altri sottogruppi.