

Algebra per Informatica

Esame 13 febbraio 2024: soluzioni

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

Esercizio 1. Siano dati gli insiemi $A = \{1, 2, 3\}$ e $B = \{\alpha, \beta\}$. Determinare la cardinalità degli insiemi seguenti:

1. $R = \{f : A \rightarrow B\}$;
2. $S = \{f : B \rightarrow A \mid f \text{ iniettiva}\}$;
3. $T = \{f : A \rightarrow B \mid f(1) = f(3)\}$;
4. $Z = (A \cup B) \times \mathcal{P}(B)$.

Soluzione. 1. Si noti che $R = B^A$ e quindi si ha che $|B^A| = |B|^{|A|} = 2^3 = 8$.

2. Per contare le funzioni iniettive $f : B \rightarrow A$ dobbiamo trovare quali sono le possibili immagini degli elementi di B . L'immagine di α può essere 1, 2 oppure 3, mentre per l'immagine di β abbiamo solo due scelte, in quanto la sua immagine non può essere uguale a $f(\alpha)$. Di conseguenza $|S| = 3 \cdot 2 = 6$, che si poteva anche ottenere utilizzando direttamente un teorema dimostrato a lezione.
3. Le immagini di 1 e 2 possono essere α o β , mentre, una volta fissata $f(1)$, l'immagine di 3 può essere soltanto $f(1)$. Di conseguenza $|T| = 2 \cdot 2 \cdot 1 = 4$.
4. $A \cup B = \{1, 2, 3, \alpha, \beta\}$ ha cardinalità 5, mentre $|\mathcal{P}(B)| = 2^{|B|} = 2^2 = 4$, quindi $|Z| = |A \cup B| \cdot |\mathcal{P}(B)| = 5 \cdot 4 = 20$.

Esercizio 2. Calcolare la seguente espressione in \mathbb{Z}_{36} :

$$\bar{5}^{50} + \bar{6} \cdot \bar{12} + (\bar{-3})^3 + \bar{7}^{-1}.$$

Scrivere il risultato come una classe \bar{x} con x compreso tra 0 e 35.

Soluzione. Calcoliamo ogni addendo separatamente. La fattorizzazione in numeri primi di 36 è $36 = 2^2 \cdot 3^2$, quindi abbiamo $\varphi(36) = 36(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12$. Poiché 5 e 36 sono coprimi, grazie al Teorema di Eulero otteniamo

$$\bar{5}^{50} = \bar{5}^{4 \cdot 12 + 2} = (\bar{5}^{12})^4 \cdot \bar{5}^2 = \bar{1}^4 \cdot \bar{25} = \bar{25}.$$

Inoltre si ha

$$\begin{aligned}\bar{6} \cdot \bar{12} &= \bar{72} = \bar{0}, \\ (\bar{-3})^3 &= \bar{-27}.\end{aligned}$$

Infine, per calcolare l'inverso di $\bar{7}$ iniziamo applicando l'algoritmo euclideo a 36 e 7:

$$\begin{aligned} 36 &= 5 \cdot 7 + 1 \\ 7 &= 7 \cdot 1 + 0. \end{aligned}$$

Quindi $\text{MCD}(7, 36) = 1$, il che significa che l'inverso di $\bar{7}$ esiste. Adesso ci serve l'identità di Bézout tra 36 e 7, ma siamo fortunati perché c'è solo un'uguaglianza con resto non nullo nell'algoritmo euclideo e quindi otteniamo subito $36 - 5 \cdot 7 = 1$, che in \mathbb{Z}_{36} diventa $\overline{-5} \cdot \bar{7} = \bar{1}$. Quindi $\bar{7}^{-1} = \overline{-5}$.

Invece di usare l'algoritmo euclideo, era anche possibile notare che $\bar{7} \cdot \bar{5} = \overline{35}$, quindi $\bar{7} \cdot \overline{-5} = \bar{1}$ e di conseguenza l'inverso di $\bar{7}$ è $\overline{-5}$.

Mettendo insieme tutto ciò che abbiamo trovato finora otteniamo:

$$\bar{5}^{50} + \bar{6} \cdot \bar{12} + (\overline{-3})^3 + \bar{7}^{-1} = \overline{25} + \bar{0} + \overline{-27} + \overline{-5} = \overline{-7} = \overline{29}.$$

Esercizio 3. Determinare tutte le radici terze complesse di -27 . Scrivere ciascuna radice nella forma $a + ib$ con $a, b \in \mathbb{R}$.

Soluzione. Innanzitutto scriviamo -27 in forma trigonometrica. Il suo modulo è $|-27| = \sqrt{(-27)^2 + 0^2} = 27$, mentre il suo argomento è l'angolo θ per cui

$$-27 = 27 \cos(\theta) \quad \text{e} \quad 0 = 27 \sin(\theta),$$

cioè $\cos(\theta) = -1$ e $\sin(\theta) = 0$; quindi $\theta = \pi$. Di conseguenza $-27 = 27(\cos(\pi) + i \sin(\pi))$ e le sue radici terze complesse sono le seguenti z_1, z_2 e z_3 :

$$\begin{aligned} z_1 &= \sqrt[3]{27} \left(\cos\left(\frac{\pi}{3}\right) + i \sin\left(\frac{\pi}{3}\right) \right) = 3 \left(\frac{1}{2} + i \frac{\sqrt{3}}{2} \right) = \frac{3}{2} + i \frac{3\sqrt{3}}{2}, \\ z_2 &= \sqrt[3]{27} \left(\cos\left(\frac{\pi + 2\pi}{3}\right) + i \sin\left(\frac{\pi + 2\pi}{3}\right) \right) = 3 (\cos(\pi) + i \sin(\pi)) = -3 + i 0, \\ z_3 &= \sqrt[3]{27} \left(\cos\left(\frac{\pi + 4\pi}{3}\right) + i \sin\left(\frac{\pi + 4\pi}{3}\right) \right) = 3 \left(\cos\left(\frac{5\pi}{3}\right) + i \sin\left(\frac{5\pi}{3}\right) \right) = \\ &= 3 \left(\frac{1}{2} + i \frac{-\sqrt{3}}{2} \right) = \frac{3}{2} + i \frac{-3\sqrt{3}}{2}. \end{aligned}$$

Esercizio 4. 1. Calcolare l'ordine dei seguenti elementi nel gruppo $(\mathbb{Z}_{34}, +, \bar{0})$:

$$\bar{2}, \bar{3}.$$

2. Calcolare l'ordine dei seguenti elementi nel gruppo $(U(\mathbb{Z}_{34}), \cdot, \bar{1})$:

$$\overline{13}, \overline{25}.$$

Soluzione. 1. L'ordine di $\overline{2}$ è il più piccolo intero positivo n per cui sommando n volte $\overline{2}$ si ottiene $\overline{0}$, cioè il più piccolo intero positivo n per cui $2 \cdot n$ è un multiplo di 34. Chiaramente questo numero è 17 perché $2 \cdot 17 = 34$, mentre se n è più piccolo di 17 si ha $0 < 2 \cdot n < 34$ e quindi $2 \cdot n$ non può essere un multiplo di 34.

Per cercare l'ordine di $\overline{3}$ notiamo che non esiste un intero n per cui $3 \cdot n = 34$ oppure $3 \cdot n = 68$, ma ne esiste uno per cui $3 \cdot n = 102$ ed è $n = 34$. Quindi l'ordine di $\overline{3}$ è proprio 34. Si poteva anche notare che 3 e 34 sono coprimi e quindi, affinché $3 \cdot n$ sia un multiplo di 34, n deve essere un multiplo di 34; di conseguenza il più piccolo n è 34.

2. Innanzitutto notiamo che l'ordine di $U(\mathbb{Z}_{34})$ è $\varphi(34) = \varphi(2 \cdot 17) = 34(1 - \frac{1}{2})(1 - \frac{1}{17}) = 16$. Poiché l'ordine di un elemento divide l'ordine del gruppo, gli ordini di $\overline{13}$ e $\overline{25}$ possono essere solo 2, 4, 8 oppure 16.

Notiamo che $\overline{13}^2 = \overline{169} = \overline{-1}$. Quindi $\overline{13}^4 = (\overline{13}^2)^2 = \overline{-1}^2 = \overline{1}$ e dunque l'ordine di $\overline{13}$ è 4.

Inoltre $\overline{25}^2 = \overline{625} = \overline{13}$. Quindi $\overline{25}^4 = \overline{13}^2 = \overline{-1}$ e $\overline{25}^8 = \overline{13}^4 = \overline{1}$, da cui segue che l'ordine di $\overline{25}$ è 8.