Algebra per Informatica

Esame 25/01/2023

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

Esercizio 1. Si consideri la seguente relazione d'equivalenza sull'insieme[1] $\mathbb{N}^* \times \mathbb{N}^*$:

$$(a,b) \sim (c,d) \iff a+b-2 = c+d-2.$$

Determinare la cardinalità di ciascuna delle seguenti classi d'equivalenza:

$$\overline{(1,1)}, \overline{(2,2)}, \overline{(4,1)}, \overline{(13,7)}.$$

Soluzione. Fissati $a, b \in \mathbb{N}^*$ abbiamo

$\overline{(a,b)} = \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y-2 = a+b-2\} = \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y = a+b\}.$

Pertanto abbiamo

$$\overline{(1,1)} = \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y = 2\} = \{(1,1)\},$$

quindi $\#\overline{(1,1)} = 1$. Analogamente, abbiamo

$$\overline{(2,2)} = \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y = 4\} = \{(3,1),(2,2),(1,3)\},$$

e pertanto $\#\overline{(2,2)} = 3$. Poi abbiamo

$$\overline{(4,1)} = \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y = 5\} = \{(4,1),(3,2),(2,3),(1,4)\},$$

e pertanto $\#\overline{(4,1)} = 4$. Infine, abbiamo

$$\begin{aligned}\overline{(13,7)} &= \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x+y = 13+7 = 20\} \\ &= \{(19,1),(18,2),\dots,(2,18),(1,19)\},\end{aligned}$$

e pertanto $\#\overline{(13,7)} = 19$. In generale, notiamo che vale la formula $\#\overline{(a,b)} = a+b-1$.

Esercizio 2. Sia $f : \mathbb{Z}^2 \to \mathbb{Z}$ l'applicazione data da $f(x,y) = 34x + 31y$.

[1] Ricordiamo che $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1,2,3,\dots\}$.

1. Determinare le seguenti controimmagini:
$$f^{-1}(1), \quad f^{-1}(f(1,-1)).$$
2. Determinare (se esistono) un'inversa sinistra e un'inversa destra per f.

Soluzione. 1. 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 $k \in \mathbb{Z}$.

- Abbiamo
$$f^{-1}(1) = \{(x,y) \in \mathbb{Z}^2 : f(x,y)=1\} = \{(x,y) \in \mathbb{Z}^2 : 34x+31y=1\}.$$
Siccome $\mathrm{MCD}(34,31)=1$, l'equazione diofantea $34x+31y=1$ ha soluzioni, cioè $f^{-1}(1) \neq \emptyset$. Determiniamo una soluzione particolare con l'algoritmo euclideo:
$$\begin{aligned} 34 &= 1 \cdot 31 + 3 \\ 31 &= 10 \cdot 3 + 1. \end{aligned}$$
Percorrendo i passaggi a ritroso otteniamo $1 = 31 - 10 \cdot 3 = 31 - 10 \cdot (34-31) = 11 \cdot 31 - 10 \cdot 34$, cioè l'identità di Bézout $1 = 11 \cdot 31 - 10 \cdot 34$. Quindi una soluzione particolare è $(x_0,y_0)=(-10,11)$, e tutte le soluzioni sono
$$f^{-1}(1) = \{(-10+31k, 11-34k) : \ k \in \mathbb{Z}\}.$$
- Abbiamo
$$\begin{aligned} f^{-1}(f(1,-1)) &= \{(x,y) \in \mathbb{Z}^2 : f(x,y) = f(1,-1)\} \\ &= \{(x,y) \in \mathbb{Z}^2 : 34x+31y=3\}. \end{aligned}$$
Per costruzione, una soluzione particolare dell'equazione diofantea $34x+31y=3$ è data da $(x_0,y_0)=(1,-1)$. Pertanto abbiamo
$$f^{-1}(1) = \{(1+31k, -1-34k) : \ k \in \mathbb{Z}\}.$$

2. • La funzione f non è iniettiva, si consideri ad esempio
$$f(0,0) = 0 = 34 \cdot (-31) + 31 \cdot 34 = f(-31,34).$$
Pertanto f non ammette inverse sinistre.

- Siccome $\mathrm{MCD}(34, 31) = 1$, l'equazione diofantea $34x + 31y = c$ ha sempre soluzioni per ogni $c \in \mathbb{Z}$. Pertanto f è suriettiva, e quindi ammette inverse destre. Per trovare un'inversa destra, motivati dai conti fatti per determinare $f^{-1}(1)$ al punto precedente e dall'identità di Bézout $1 = 11 \cdot 31 - 10 \cdot 34$ definiamo $g : \mathbb{Z} \to \mathbb{Z}^2$ come $g(n) = (-10n, 11n)$. Verifichiamo che $f \circ g = \mathrm{Id}_{\mathbb{Z}}$. Per un qualunque $n \in \mathbb{Z}$ abbiamo

$$\begin{aligned}(f \circ g)(n) &= f(g(n)) = f(-10n, 11n) = 34 \cdot (-10n) + 31 \cdot (11n) \\ &= -340n + 341n = n = \mathrm{Id}_{\mathbb{Z}}(n).\end{aligned}$$

Esercizio 3. Si consideri il poset $(\mathbb{N}^*, |)$, cioè l'insieme $\mathbb{N}^*$ con la relazione d'ordine:

$$a \lhd b \iff a \mid b \ \ (\text{cioè esiste } k \in \mathbb{Z} \text{ tale che } b = ka).$$

Sia $A = \{4, 6, 10, 60, 120, 240\} \subseteq \mathbb{N}^*$. Si determinino (se esistono) massimo, minimo, elementi minimali ed elementi massimali, estremo inferiore ed estremo superiore di A.

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

$$\begin{tikzcd}
 & 240 \arrow[d, dash] & \\
 & 120 \arrow[d, dash] & \\
 & 60 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
6 & 10 & 4
\end{tikzcd}$$

Si vede che A ha un unico elemento massimale 240, che è pertanto anche il massimo e l'estremo superiore: $\max A = \sup A = 240$. Inoltre, A ha tre elementi minimali non confrontabili 4, 6, e 10. Pertanto A non ammette minimo: $\nexists \min A$.
Per determinare l'estremo inferiore di A, troviamo prima l'insieme dei minoranti di A

$$\{n \in \mathbb{N}^* : \ n \mid a \ \forall a \in A\} = \{n \in \mathbb{N}^* : \ \ n \mid 4, \ n \mid 6, \ n \mid 10\} = \{1, 2\}.$$

Questo insieme ha un massimo in 2 che è pertanto l'estremo inferiore di A: $\inf A = 2$.

Esercizio 4. Si considerino i gruppi $(\mathbb{Z}_4, +, \overline{0})$, $(\mathbb{Z}_6, +, \overline{0})$ e il corrispondente gruppo prodotto $G = \mathbb{Z}_4 \times \mathbb{Z}_6$.

1. Determinare l'elemento neutro del gruppo G.

2. Calcolare l'ordine dei seguenti elementi di G: $(\overline{7},\overline{0})$, $(\overline{2},\overline{2})$.
3. Determinare l'elemento inverso di $(\overline{2},\overline{4})$.

Soluzione. Ricordiamo che l'operazione nel gruppo prodotto $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ si effettua componente per componente, cioè $(\overline{x},\overline{y}) + (\overline{a},\overline{b}) = (\overline{x}+\overline{a},\overline{y}+\overline{b})$, dove $\overline{x}+\overline{a} \in \mathbb{Z}_4$ e $\overline{y}+\overline{b} \in \mathbb{Z}_6$.

1. L'elemento neutro di G è la coppia $(\overline{0},\overline{0})$.
2. Ricordiamo che dato un gruppo $(G,*,\lambda)$ e $g \in G$, l'ordine di g è il più piccolo intero positivo n, se esiste, per cui
$$\underbrace{g * g * \cdots * g}_{n \text{ volte}} = \lambda.$$
Per l'elemento $(\overline{7},\overline{0}) = (\overline{3},\overline{0})$ abbiamo
$$\begin{aligned} (\overline{3},\overline{0}) + (\overline{3},\overline{0}) &= (\overline{2},\overline{0}); \\ (\overline{3},\overline{0}) + (\overline{3},\overline{0}) + (\overline{3},\overline{0}) &= (\overline{1},\overline{0}); \\ (\overline{3},\overline{0}) + (\overline{3},\overline{0}) + (\overline{3},\overline{0}) + (\overline{3},\overline{0}) &= (\overline{0},\overline{0}). \end{aligned}$$
Pertanto $\operatorname{ord}(\overline{3},\overline{0}) = 4$.
Per l'elemento $(\overline{2},\overline{2})$ abbiamo
$$\begin{aligned} (\overline{2},\overline{2}) + (\overline{2},\overline{2}) &= (\overline{0},\overline{4}); \\ (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) &= (\overline{2},\overline{0}); \\ (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) &= (\overline{0},\overline{2}). \\ (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) + (\overline{2},\overline{2}) &= (\overline{2},\overline{4}) \\ \underbrace{(\overline{2},\overline{2}) + \cdots + (\overline{2},\overline{2})}_{6 \text{ volte}} &= (\overline{0},\overline{0}) \end{aligned}$$
Pertanto $\operatorname{ord}(\overline{2},\overline{2}) = 6$.
3. L'inverso di $(\overline{2},\overline{4})$ è $(\overline{2},\overline{2})$, infatti
$$(\overline{2},\overline{4}) + (\overline{2},\overline{2}) = (\overline{4},\overline{6}) = (\overline{0},\overline{0}).$$