ALGEBRA PER INFORMATICA 2020-21

ESERCITAZIONE GUIDATA - 15/12/2020

Esercizio 1. Si consideri la seguente funzione

$$f : \mathbb{Z}_{35} \times \mathbb{Z}_{22} \longrightarrow \mathbb{Z}_{35} \times \mathbb{Z}_{22}$$
$$(\overline{x}, \overline{y}) \mapsto (\overline{3} \cdot \overline{x}, \overline{3} \cdot \overline{y})$$

(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 $X = \mathbb{Z}_{35} \times \mathbb{Z}_{22}$.

Soluzione. Per prima cosa osserviamo che siccome $\mathrm{MCD}(3,35) = \mathrm{MCD}(3,22) = 1$, la classe di equivalenza di 3 è invertibile in $\mathbb{Z}_{35}$ e in $\mathbb{Z}_{22}$. Con l'algoritmo euclideo, o con un calcolo diretto, si può determinare più precisamente che

$$\overline{3}^{-1} = \overline{12} \text{ in } \mathbb{Z}_{35} \text{ infatti } \overline{3} \cdot \overline{12} = \overline{36} = \overline{1},$$
$$\overline{3}^{-1} = \overline{15} \text{ in } \mathbb{Z}_{22} \text{ infatti } \overline{3} \cdot \overline{15} = \overline{45} = \overline{1}.$$

(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 $(\overline{3} \cdot \overline{x}, \overline{3} \cdot \overline{y}) = (\overline{3} \cdot \overline{a}, \overline{3} \cdot \overline{b})$. Moltiplicando la prima componente per $\overline{12} \in \mathbb{Z}_{35}$ e la seconda componente per $\overline{15} \in \mathbb{Z}_{22}$ si ottiene

$$(\overline{12} \cdot \overline{3} \cdot \overline{x}, \overline{15} \cdot \overline{3} \cdot \overline{y}) = (\overline{12} \cdot \overline{3} \cdot \overline{a}, \overline{15} \cdot \overline{3} \cdot \overline{b})$$

e quindi per quanto detto sopra si ha $(\overline{x}, \overline{y}) = (\overline{a}, \overline{b})$.
Surgettività. Sia $(\overline{a}, \overline{b}) \in X$. Scegliamo $(\overline{x}, \overline{y}) = (\overline{12} \cdot \overline{a}, \overline{15} \cdot \overline{b})$. Per quanto detto sopra si verifica facilmente che $f(\overline{x}, \overline{y}) = f(\overline{12} \cdot \overline{a}, \overline{15} \cdot \overline{b}) = (\overline{3} \cdot \overline{12} \cdot \overline{a}, \overline{3} \cdot \overline{15} \cdot \overline{b}) = (\overline{a}, \overline{b})$.
(2) L'inversa di f è la funzione

$$g : \mathbb{Z}_{35} \times \mathbb{Z}_{22} \longrightarrow \mathbb{Z}_{35} \times \mathbb{Z}_{22}$$
$$(\overline{x}, \overline{y}) \mapsto (\overline{12} \cdot \overline{x}, \overline{15} \cdot \overline{y})$$

La verifica che $f \circ g = g \circ f = \mathrm{Id}_X$ segue da quanto detto prima.

Esercizio 2. Sia $f : \mathbb{Z}^2 \to \mathbb{Z}$ l'applicazione data da $f(x,y) = 7x + 9y$.

(1) Determinare se f è iniettiva e/o surgettiva.
(2) Determinare $f^{-1}(0)$, $f^{-1}(3)$, $f^{-1}\big(f(-1,2)\big)$.
(3) Trovare (se esiste) una funzione $g : \mathbb{Z} \to \mathbb{Z}^2$ tale che $f \circ g = \mathrm{Id}_{\mathbb{Z}}$.

Soluzione. (1) La funzione f è surgettiva. Infatti dato un qualunque $n \in \mathbb{Z}$ esistono sempre due interi x, y tali che $7x + 9y = n$ siccome $\mathrm{MCD}(7,9) = 1 \mid n$.
La funzione f non è iniettiva. Si noti ad esempio che

$$f(8,-6) = 8 \cdot 7 - 6 \cdot 9 = 2 = -7 + 9 = f(-1,1).$$

(2) Si ricordi che 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 $k \in \mathbb{Z}$.

- $f^{-1}(0) = \{(x,y) \in \mathbb{Z}^2 : \ 7x+9y = 0\}$. Siccome una soluzione particolare di $7x+9y=0$ è data da $(x_0,y_0) = (0,0)$, si ha
$$f^{-1}(0) = \{(9k, -7k) : \ k \in \mathbb{Z}\}.$$
- $f^{-1}(3) = \{(x,y) \in \mathbb{Z}^2 : \ 7x+9y = 3\}$. Per determinare una soluzione particolare di $7x+9y=3$ utilizziamo l'algoritmo euclideo
$$9 = 1 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
e la conseguente identità di Bezout $1 = 4 \cdot 7 - 3 \cdot 9$, da cui ricaviamo $3 = 12 \cdot 7 - 9 \cdot 9$. Pertanto $(x_0, y_0) = (12, -9)$ e quindi
$$f^{-1}(3) = \{(12 + 9k, -9 - 7k) : \ k \in \mathbb{Z}\}.$$
- $f^{-1}\big(f(-1,2)\big) = f^{-1}(11) = \{(x,y) \in \mathbb{Z}^2 : \ 7x+9y = 11\}$. Dall'identità di Bezout precedentemente ricavata otteniamo $11 = 44 \cdot 7 - 33 \cdot 9$. Pertanto $(x_0, y_0) = (44, -33)$ e quindi
$$f^{-1}(11) = \{(44 + 9k, -33 - 7k) : \ k \in \mathbb{Z}\}.$$

(3) Prendendo spunto dall'identità di Bezout $1 = 4 \cdot 7 - 3 \cdot 9$, definiamo $g : \mathbb{Z} \to \mathbb{Z}^2$ tale che $g(k) = (4k, -3k)$. Verifichiamo che $f \circ g = \mathrm{Id}_{\mathbb{Z}}$. Per un qualunque $k \in \mathbb{Z}$ abbiamo
$$(f \circ g)(k) = f(g(k)) = f(4k, -3k) = 7 \cdot 4k - 9 \cdot 3k = 28k - 27k = k = \mathrm{Id}_{\mathbb{Z}}(k).$$

Esercizio 3. Si consideri $\mathbb{Z}_{25}$.

(1) Calcolare $\overline{6}^{303}$.

(2) Determinare l'ordine dei seguenti elementi del gruppo degli elementi invertibili $(\mathrm{U}(\mathbb{Z}_{25}), \cdot, \overline{1})$:
$$\overline{6},\ \overline{24},\ \overline{11},\ \overline{7}.$$

Soluzione. Per prima cosa calcoliamo $\varphi(25) = 20$ e ricordiamo che per il teorema di Eulero, dato $x \in \mathbb{Z}$ tale che $\mathrm{MCD}(x, 25) = 1$ allora $\overline{x}^{20} = \overline{1}$ in $\mathbb{Z}_{25}$.

(1) Consideriamo la divisione euclidea $303 = 15 \cdot 20 + 3$, abbiamo pertanto
$$\overline{6}^{303} = \overline{6}^{15 \cdot 20 + 3} = \big(\overline{6}^{20}\big)^{15} \cdot \overline{6}^3 = \overline{1} \cdot \overline{6}^3 = \overline{6}^2 \cdot \overline{6} = \overline{36} \cdot \overline{6} = \overline{11} \cdot \overline{6} = \overline{16}.$$

(2) Ricordiamo che l'ordine moltiplicativo di un elemento in $\mathrm{U}(\mathbb{Z}_{25})$ dev'essere un divisore dell'ordine $|\mathrm{U}(\mathbb{Z}_{25})| = \varphi(25) = 20$.

- Abbiamo già calcolato $\overline{6}^2 = \overline{11}$ e $\overline{6}^3 = \overline{16}$. Calcoliamo $\overline{6}^4 = \overline{6}^3 \cdot \overline{6} = \overline{16} \cdot \overline{6} = \overline{96} = \overline{-4} = \overline{21}$ e $\overline{6}^5 = \overline{6}^4 \cdot \overline{6} = \overline{21} \cdot \overline{6} = \overline{126} = \overline{1}$. Pertanto[1] $\mathrm{ord}(\overline{6}) = 5$.
- Si vede facilmente che $\overline{24} = \overline{-1}$ e quindi $\overline{24}^2 = (\overline{-1}) \cdot (\overline{-1}) = \overline{1}$. Pertanto $\mathrm{ord}(\overline{24}) = 2$.

[1] Notare che sapendo che $\mathrm{ord}(\overline{6}) = 5$ nel punto (1) si sarebbe potuto effettuare la divisione euclidea di 303 per 5 anzichè per 20.

- Calcoliamo soltanto le potenze $\overline{11}^d$ con $d \mid 20$.

$$\overline{11}^2 = \overline{121} = \overline{-4},$$
$$\overline{11}^4 = (\overline{-4})^2 = \overline{16},$$
$$\overline{11}^5 = \overline{11}^4 \cdot \overline{11} = \overline{16} \cdot \overline{11} = \overline{176} = \overline{1}.$$

  Pertanto $\text{ord}(\overline{11}) = 5$.
- Calcoliamo soltanto le potenze $\overline{7}^d$ con $d \mid 20$.

$$\overline{7}^2 = \overline{49} = \overline{-1},$$
$$\overline{7}^4 = (\overline{7}^2)^2 = (\overline{-1})^2 = \overline{1}.$$

  Pertanto $\text{ord}(\overline{7}) = 4$.

Esercizio 4. Si consideri il gruppo $G = \{f : \mathbb{Z} \to \mathbb{Z} \text{ bigettiva}\}$ con l'operazione di composizione. Per ogni $k \in \mathbb{Z}$, definiamo il sottoinsieme

$$H_k = \{f \in G : \ f(3) = k\}.$$

(1) Determinare per quali $k \in \mathbb{Z}$ il sottoinsieme H_k è un sottogruppo di G.

Sia $f \in G$ la funzione definita da $f(x) = x + 1 \ \forall x \in \mathbb{Z}$.

(2) Per ciascuno dei $k \in \mathbb{Z}$ determinati in (1), trovare un elemento $h \in G$ diverso da f e appartenente alla classe laterale sinistra $f \circ H_k$.

(3) Per ciascuno dei $k \in \mathbb{Z}$ determinati in (1), trovare un elemento $g \in G$ tale che $g \circ H_k \neq f \circ H_k$.

Soluzione. (1) Affinchè H_k sia un sottogruppo di G è necessario che l'elemento neutro di G, la funzione identità $\text{Id}_\mathbb{Z}$, appartenga ad H_k. Siccome $\text{Id}_\mathbb{Z}(3) = 3$, l'unico $k \in \mathbb{Z}$ per cui $\text{Id}_\mathbb{Z} \in H_k$ è $k = 3$. Sia pertanto $k = 3$, verifichiamo che H_3 è un sottogruppo di G. Abbiamo già verificato che $\text{Id}_\mathbb{Z} \in H_3$. Siano adesso $f, g \in H_3$, verifichiamo che $f \circ g \in H_3$. Ci basta calcolare

$$(f \circ g)(3) = f(g(3)) = f(3) = 3.$$

Infine, consideriamo $f \in H_3$ e la sua inversa $f^{-1} \in G$. Mostriamo che $f^{-1} \in H_3$, cioè che $f^{-1}(3) = 3$. Ricordiamo che per definizione di inversa abbiamo $(f^{-1} \circ f)(3) = \text{Id}_\mathbb{Z}(3) = 3$, ma d'altra parte $(f^{-1} \circ f)(3) = f^{-1}(f(3)) = f^{-1}(3)$ siccome $f(3) = 3$. Mettendo insieme le due uguaglianze otteniamo $f^{-1}(3) = 3$ come richiesto.

(2) Fissiamo $k = 3$. La classe laterale sinistra di f modulo H_3 è definita come

$$f \circ H_3 = \{h \in G : \ h \sim_S f\},$$

dove la relazione d'equivalenza $\sim_S$ è data da

$$h \sim_S f \iff h^{-1} \circ f \in H_3 \iff h^{-1}(f(3)) = 3 \iff h^{-1}(4) = 3.$$

La prima doppia freccia è la definizione di $\sim_S$, la seconda segue dalla definizione di H_3, e la terza doppia implicazione è dovuta al fatto che $f(3) = 3 + 1 = 4$.
Per trovare un elemento $h \in f \circ H_3$ ci basta quindi trovare una funzione $h : \mathbb{Z} \to \mathbb{Z}$ bigettiva la cui inversa h^{-1} assume il valore 3 in 4. Scegliamo $h(x) = -x + 7$. Si verifica facilmente che h è bigettiva con inversa $h^{-1} = h$. Inoltre $h^{-1}(4) = h(4) = -4 + 7 = 3$. Pertanto $h \in f \circ H_3$.

(3) Fissiamo $k = 3$. Dato $g \in G$ si ha che $g \circ H_3 \neq f \circ H_3$ se e soltanto se $g \not\sim_S f$. Ragionando come al punto (2), abbiamo quindi

$$g \not\sim_S f \iff g^{-1} \circ f \notin H_3 \iff g^{-1}(f(3)) \neq 3 \iff g^{-1}(4) \neq 3.$$

Cerchiamo pertanto una funzione bigettiva $g : \mathbb{Z} \to \mathbb{Z}$ per cui $g^{-1}(4) \neq 3$. Scegliamo $g(x) = x+2$. La sua inversa è $g^{-1}(x) = x-2$ e si ha $g^{-1}(4) = 4-2 = 2 \neq 3$. Quindi $g \circ H_3 \neq f \circ H_3$ come richiesto.