

# Esercizio 1

martedì 15 dicembre 2020 09:09



**Esercizio 1.** Si consideri la seguente funzione

$$f : \mathbb{Z}_{35} \times \mathbb{Z}_{22} \longrightarrow \mathbb{Z}_{35} \times \mathbb{Z}_{22}$$

$$\underline{(\bar{x}, \bar{y})} \mapsto (\bar{3} \cdot \bar{x}, \bar{3} \cdot \bar{y})$$

- (1) Determinare se  $f$  è iniettiva e/o surgettiva.  
(2) Trovare (se esiste) l'inversa di  $f$  nel monoide  $(X^X, \circ, \text{Id}_X)$ , dove  $X = \mathbb{Z}_{35} \times \mathbb{Z}_{22}$ .

1)

$f$  iniettiva / surgettiva?

- $\bar{3} \cdot \bar{x}$  in  $\mathbb{Z}_{35}$   $\text{rgd } (3, 35) = 1$  allora  $\bar{3}$  è invertibile in  $\mathbb{Z}_{35}$   
ma quindi  $\exists \bar{3}^{-1} \in \mathbb{Z}_{35} \quad \bar{3}^{-1} \cdot \bar{3} = \bar{1}$   
(inoltre  $\bar{12} \cdot \bar{3} = \bar{36} = \bar{1}$  in  $\mathbb{Z}_{35}$ ,  $\bar{3}^{-1} = \bar{12}$ )
- $\text{rgd } (3, 22) = 1$  allora  $\bar{3}$  è invertibile in  $\mathbb{Z}_{22} \quad \exists \bar{3}^{-1} \in \mathbb{Z}_{22}$   
(diverso dal precedente:  $\bar{3} \cdot \bar{15} = \bar{45} = \bar{1}$  in  $\mathbb{Z}_{22}$ ,  $\bar{3}^{-1} = \bar{15}$ )

$f$  iniettiva siamo  $(\bar{x}, \bar{y}), (\bar{a}, \bar{b}) \in X \quad X = \mathbb{Z}_{35} \times \mathbb{Z}_{22}$

$$\text{d.c. } f(\bar{x}, \bar{y}) = f(\bar{a}, \bar{b}) \quad \text{tesi: } (\bar{x}, \bar{y}) = (\bar{a}, \bar{b})$$

$$(\begin{smallmatrix} \bar{3}\bar{x} \\ \bar{3}\bar{y} \end{smallmatrix}, \bar{3}\bar{y}) \quad (\begin{smallmatrix} \bar{3}\bar{a} \\ \bar{3}\bar{b} \end{smallmatrix}, \bar{3}\bar{b})$$

ovvero  $\left\{ \begin{array}{l} 3\bar{x} = 3\bar{a} \quad \text{in } \mathbb{Z}_{35} \\ 3\bar{y} = 3\bar{b} \quad \text{in } \mathbb{Z}_{22} \end{array} \right.$  possò farlo perché  $\bar{3} \rightarrow$  invertibile  
moltiplico per  $\bar{3}^{-1}$   $\left\{ \begin{array}{l} \bar{x} = \bar{a} \\ \bar{y} = \bar{b} \end{array} \right.$

Quindi  $f$  iniettiva

$$\checkmark \left\{ \begin{array}{l} \bar{x} = \bar{a} \\ \bar{y} = \bar{b} \end{array} \right.$$

$f$  surgettiva si  $\bar{a}, \bar{b}$  in  $X$  tesi  $\exists (\bar{x}, \bar{y}) \in X$  t.c.  $f(\bar{x}, \bar{y}) = (\bar{a}, \bar{b})$

$$\text{scogliamo } (\bar{x}, \bar{y}) = (\bar{3}^{-1}\bar{a}, \bar{3}^{-1}\bar{b}) = (\bar{12}\bar{a}, \bar{15}\bar{b})$$

$$f(\bar{x}, \bar{y}) = (\bar{3} \cdot \bar{12} \cdot \bar{a}, \bar{3} \cdot \bar{15} \cdot \bar{b}) = (1 \cdot \bar{a}, 1 \cdot \bar{b}) = (\bar{a}, \bar{b}) \quad f \text{ surgettiva}$$

posso anche:

$$\exists (\bar{x}, \bar{y}) \text{ d.c. } 3 \cdot \bar{x} = \bar{a} \text{ in } \mathbb{Z}_{35} \iff 3x - a = 35k \iff 3x + 35k = a$$

e allo stesso modo per  $y$

2) L'inversa è unica perché  $f$  bisettiva

$$g: X \rightarrow X \quad g(\bar{x}, \bar{y}) = (\bar{z}^{-1}x, \bar{z}^{-1}y) = (\bar{z}\bar{x}, \bar{z}\bar{y})$$

verifcare che  $g \circ g = g \circ f = Id_X$ , ma  $f$  iniett + suriett. = birettiva, allora la inversa

## Esercizio 2

martedì 15 dicembre 2020 09:10



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

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

1) Dobbiamo dimostrare che  $f$  è iniettiva:

Se  $\pi_{CD}(x, y) \mid \text{immagine}(c)$

$$\rightarrow x \mid c$$

Per  $x$  dividendo  $\forall n \in \mathbb{Z}$ , quindi surgettiva.

Non è iniettiva, perché per  $7x + 9y = n$  ottengo  $y$ :

$$\begin{aligned} \pi_{CD}(x, y) : \quad & 3 = 1 \cdot 7 + 2 \\ & = 1 \\ & 7 = 3 \cdot 2 + 1 \\ & 2 = 2 \cdot 1 + 0 \end{aligned}$$

$$\text{es. } f(8, -6) = 8 \cdot 7 - 6 \cdot 3 = 2 = -7 + 3 = f(-1, 1)$$

$$\left\{ \begin{array}{l} x = x_0 + b'k \\ y = y_0 - a'k \end{array} \right. \quad k \in \mathbb{Z} \quad \text{dunque più soluzioni immiate in } n.$$

2) •  $f^{-1}(0)$  ovvero si cerca la controimmagine di 0, ovvero  $x$  e  $y$  che danno immagine 0.

Si traduce nelle soluz. dell'equazione:  $7x + 9y = 0$  → 7 e 9 coprimi

Però  $x$  e  $y$  punti l'eq. le soluzioni:  $(x_0, y_0) = (0, 0)$  soluz. particolare

$$f^{-1}(0) = \{(3k, -7k) \mid k \in \mathbb{Z}\} = \{(0, 0), (3, -7), \dots\} \quad (\text{se } f^{-1}(0) = \{x_0\} \rightarrow f \text{ non iniettiva})$$

•  $f^{-1}(3) \rightarrow 7x + 9y = 3$

Cerco prima  $x$  e  $y$  per  $7x + 9y = 1$

$$\rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3(3 - 7) = 7 - 3 \cdot 3 + 3 \cdot 7 = 4 \cdot 7 - 3 \cdot 3 \quad *$$

$$\text{soluz. } x_0 = 4, y_0 = -3$$

Dunque 7, 9 coprimi, per avere  $7 \cdot 4 + 9(-3) = 3$  moltiplico tutto per 3:

$$3(7 \cdot 4) + 3(9 \cdot -3) = 1 \cdot 3$$

$$7 \cdot 12 + 9(-3) = 3$$

Soluzioni:

$$\left\{ \begin{array}{l} x = 12 + 9k \\ y = -3 - 7k \end{array} \right. \quad k \in \mathbb{Z} \quad \text{ovvero} \quad f^{-1}(3) = \{(7 + 9k, -3 - 7k) \mid k \in \mathbb{Z}\}$$

•  $f^{-1}(-1, 1) = f^{-1}(11)$ ,  $1 \mid 11 \vee$  dato  $7 \cdot 4 - 3 \cdot 3 = 1$

moltiplico tutto per 11:  $7 \cdot 44 - 33 \cdot 3 = 11$

Soluzioni:

perché  $(-1, 1)$  è soluzione di  $f$  (da 11)

$$\begin{cases} x = 4k + 3k \\ y = -3k - 7k \end{cases} \quad k \in \mathbb{Z} \quad = \quad \begin{cases} x = -1 + 3k \\ y = 2 - 7k \end{cases} \quad k \in \mathbb{Z}$$

3) Si dice se  $g$  è inversa di  $f$

In generale,  $f$  ha inv. dx se  $f$  surgettiva;

Per quanto detto sopra ( $\text{rco}(f,g)=1 \quad \forall n \in \mathbb{Z}$ ),  $f$  è surgettiva, allora ha inversa destra.

Se  $g(k) = (4k, -3k)$  insieme a ~~benoit~~

$$(f \circ g)(n) = f(g(n)) = f(4n, -3n) = 7 \cdot 4n - 3 \cdot 3n = 28n - 27n = n = \text{Id}(n)$$

$$f \circ g = \text{Id}_{\mathbb{Z}} \quad g \text{ è inv. da dx} \quad \forall n \in \mathbb{Z}$$

Ma in generale ogni soluzione di  $7x + 3y = 1$  mi dà una inversa destra di  $f$   
(ho infinite inverse)

### Esercizio 3

martedì 15 dicembre 2020 09:10

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

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

(2) Determinare l'ordine dei seguenti elementi del gruppo degli elementi invertibili  $(U(\mathbb{Z}_{25}), \cdot, \bar{1})$ :

$\bar{6}, \bar{24}, \bar{11}, \bar{7}$ .



$$1) \text{ Per il teorema di Eulero } \bar{x}^{\varphi(n)} \equiv 1 \pmod{n} \quad \varphi(25) = \#\{u \in \mathbb{Z}_+ \mid \text{lcm}(25, u) = 1\}$$

$$\varphi(25) = 25(1 - \frac{1}{5}) = \frac{20}{5} = 20 \quad 1 \leq u \leq 25$$

$$\text{quindi } \bar{6}^{20} = \bar{1} \quad \bar{6} \text{ invertibile in } \mathbb{Z}_{25} \quad z_0 = * U(\mathbb{Z}_{25})$$

$$z_0 = 15 \cdot \underline{20} + 3 \quad \text{dunque } \bar{6}^{303} = (\bar{6}^{20})^{15} \cdot \bar{6}^3 = \bar{1} \cdot \bar{6}^3 = \bar{36} \cdot \bar{6}$$

$$= \bar{11} \cdot \bar{6} = \bar{66} = \bar{16}$$

$$2) \text{ Ord e' il piu' piccolo intero t.c. } g * \underbrace{\dots * g}_{n \text{ volte}} = \lambda$$

Per il teorema di Lagrange:  $\# U(\mathbb{Z}_{25}) = 20$  (ord. corrispondente) periodi ord. elem. zero è un divisore di 20:  $1, 2, 4, 5, 10, 20$

$$\bar{6}^2 = \bar{11} + 1, \quad \bar{6}^4 = (\bar{6}^2)^2 = \bar{11}^2 = \bar{121} = -\bar{4} = \bar{21}$$

$$\text{ord}(\bar{6}) = 5 \quad \bar{6}^5 = \bar{6}^4 \cdot \bar{6} = -\bar{4} \cdot \bar{6} = -\bar{24} = \bar{1}$$

$$\text{ord}(\bar{24}) = \text{per Eulero: } \bar{24}^{\varphi(25)} = \bar{24}^{20} = \bar{1}, \quad 20 \text{ e' il piu' piccolo? No; } \text{ord}(\bar{24}) = 2$$

$$\text{ord}(\bar{11}) = " : \bar{11}^{20}, \quad \bar{11}^5 = \bar{11}^4 \cdot \bar{11} = \bar{121} = \bar{1} \quad \text{ord}(\bar{11}) = 5$$

$$\text{ord}(\bar{7}) = " : \bar{7}^{20}, \quad \text{ord}(\bar{7}) = 4$$

$$\bar{7}^4 \text{ con } d \mid 20$$

$$\bar{24}^2 = \bar{576} = \bar{23} \cdot \bar{25} + 1$$

$\bar{24} = \bar{23}$   
allora  $(\bar{23})^2 = \bar{1}$

Oss  $\bar{x}$  non è invertibile allora  $\exists u \in \mathbb{Z}_+ \text{ t.c. } \bar{x}^u = \bar{1}$

$$\text{P.A. } \bar{x}^u = 1 \rightarrow \bar{x} \cdot \bar{x}^{u-1} = \bar{1} \text{ ma allora } \bar{x} \text{ e' invertibile con inverso } \bar{x}^{u-1}$$

Non esiste alcun  $u$ , quindi nessun ord per elementi non invertibili

#### Esercizio 4

martedì 15 dicembre 2020 09:10

**Esercizio 4.** Si consideri il gruppo  $G = \{f : \mathbb{Z} \rightarrow \mathbb{Z} \text{ bigettiva}\}$  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  $g \circ H_k \neq f \circ H_k$ .

1)  $H_3$  sottogruppo se:

$$a) \lambda \in H_3 \text{ dove } \lambda = \text{Id}_{\mathbb{Z}} \text{ allora } f = \text{Id} \in H \iff f(3) = 3 \text{ per } \kappa = 3$$

$$b) \forall g \in H_3 \rightarrow f \circ g \in H_3 \equiv f(f(3)) = \kappa \in H :$$

$$\text{Id}(\text{Id}(3)) = 3 (\kappa = 3), \text{ nessun'altra funzione } g \text{ tale da } f(g(3)) = \kappa \text{ immaginabile.}$$

$$(f \circ g)(3) \in H_3 \iff (f \circ g)(3) = 3$$

$$(f \circ g)(3) = f(g(3)) = \underset{g \in H_3}{\underset{|}{\cancel{f}}} \underset{g \in H_3}{\underset{|}{\cancel{g}}} = 3$$

$$d) \forall f \in H \rightarrow f^{-1} \in H_3 \iff f^{-1}(3) = 3 \in H$$

$$(f^{-1} \circ f) = \text{Id}_{\mathbb{Z}} \rightarrow (f^{-1} \circ f)(3) = \underset{\|}{\underset{|}{\cancel{f^{-1}(3)}}} = 3$$

$$f^{-1}(f(3)) = f^{-1}(3) \underset{f \in H_3}{\underset{|}{\cancel{f}}} = 3$$

controllo a) :  $\text{Id} \in H_3 ? \quad \text{Id}(3) = \kappa \quad \text{Id} \in H_3 \iff \kappa = 3$

pernodi b) e c)

Se  $\kappa \neq 3$ ,  $H_3$  non è sottogruppo perché  
 $\lambda \notin H_3$  dunque  $\text{Id} \notin H$

dovono essere verificate ma solo per  $\kappa = 3$

$$2) \begin{array}{l} \text{SISTEMA} \\ f(x) = x+1 \quad \forall x \in \mathbb{Z} \end{array} \quad \kappa = 3 \quad H_3 = \{\text{Id}\} \quad f \circ H_3 = \{h \in G \mid h \sim f\} = \{f \circ t \mid t \in H_3\}$$

scegli

$$h \sim f \iff h^{-1} \circ f \in H_3$$

$$\iff h^{-1}(f(3)) = 3 \iff h^{-1}(4) = 3$$

$\underset{\text{DEF } H_3}{\underset{|}{\cancel{h^{-1}(3)}}} = 3+1=4$

Bisognerebbe  $h : \mathbb{Z} \rightarrow \mathbb{Z}$  invertibile t.c.  $h^{-1}(4) = 3$

ad esempio  $h(x) = -x+7$

$h$  bigettiva con inversa se stessa :  $h^{-1}(x) = h(x)$  infatti

$$(h \circ h)(x) = h(-x+7) = -(-x+7) + 7 = x - 7 + 7 = x$$

$$h^{-1}(4) = h(4) = -4+7 = 3$$

$$h \in f \circ H_3$$

$$t \in H_3, t \neq \text{Id}, \text{dove } t \in f \circ H_3$$

• oppure  $t(x) = \begin{cases} 4 & x=3 \\ 5 & x=2 \\ x+2 & x \neq 2, 3 \end{cases}$ ,  $t(x) = \begin{cases} 3 & x=6 \\ 4 & x=3 \\ x & x \neq 3, 4 \end{cases}$ ,  $t(x) = \begin{cases} x & x \neq 0 \text{ e } x \neq 1 \\ 1 & x=0 \\ 0 & x=1 \end{cases}$

$$3) g \in G \quad g \circ h_3 \neq g \circ l_{t_3} \iff g \not\sim_s g \iff \underset{\substack{| \\ \text{DEF} \\ H_3}}{g^{-1} \circ g \not\sim h_3} \iff \underset{\substack{| \\ \text{DEF} \\ H_3}}{g^{-1}(g(3)) \neq 3} \iff \underset{\substack{| \\ f(3)=4}}{g^{-1}(4) \neq 3}$$

Consideriamo  $g : \mathbb{Z} \rightarrow \mathbb{Z}$  BIGETTIVA

$$g^{-1}(4) = 3$$

$$\text{Scegliamo } g(x) = x+2 \quad \text{BIGETTIVA} \quad g^{-1}(x) = x-2 \quad g^{-1}(4) = 4-2=2 \neq 3$$

$$\rightarrow \underline{g \circ h_3} \neq \underline{g \circ l_3}$$

insieme

diversi

$$\begin{aligned} g \circ h_3 &= \{h \in G \mid h \sim_s g\} = [g] \quad \text{con rel.} \\ g \circ l_3 &= \{h \in G \mid h \sim_s g\} = [g] \quad \text{con rel.} \end{aligned}$$

avere classi diverse

$X$  insieme,  $\sim$  rel. d'equiv.,  $x, y \in X$

$$[x] \neq [y] \iff x \not\sim y$$

$$g \circ h_3 \neq g \circ l_3 \iff [g] \neq [g] \iff g \not\sim_s g$$

$$\text{Ad esempio } g \not\sim h_3 \quad g \circ h_3 \neq h_3$$

$$\text{Avremo} \quad \text{se } g \circ h_3 = h_3 \quad g \circ h_3 = h_3 \neq g \circ h_3$$