1) **INIETTIVA**:

$\forall a, a' \in A \quad f(a) = f(a') \Rightarrow a = a'$

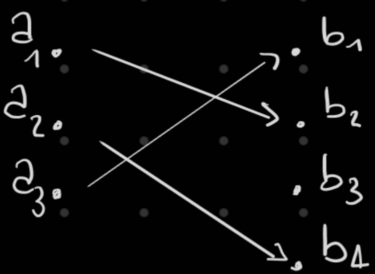
2) **SURIETTIVA**:

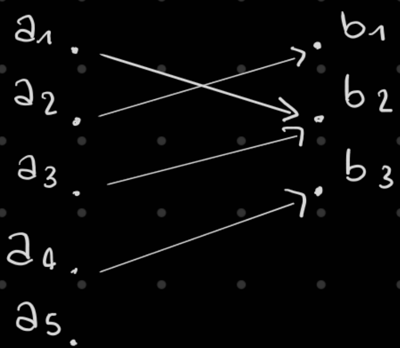
$\mathrm{Im}\, f = B$ ovvero

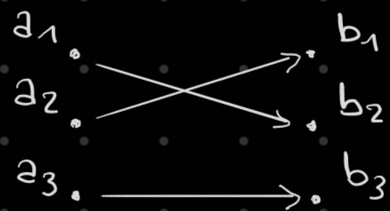
$\forall b \in B \ \exists a \in A \mid f(a) = b$

3) **BIIETTIVA** (o BIUNIVOCA)

iniettiva e suriettiva insieme

① 

② 

③ 

ESERCITAZIONE 1

1) S_3 ha $3!$ elt:

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

↳ identità

cicliche

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

se un numero va in se stesso non c'è bisogno di rappresentarlo: $(1,2)$

tabella moltiplicativa:

$\cdot$	e	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
e	e	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	e	$(1,2,3)$	$(1,2,3)$	$(1,2)$	$(1,3,2)$
$(2,3)$	$(2,3)$	$(1,2,3)$	e	$(1,2,3)$	$(2,3)$	$(1,2)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$(1,2,3)$	e	$(1,3)$	$(1,3,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(1,3,2)$	$(2,3)$	e	e
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,3,2)$	$(1,2)$	$(1,2,3)$	$(1,2,3)$

dovrebbero essere giuste

parto sempre dallo stesso lato.

$$\begin{matrix} 1 & & 2 & & 1 \\ 2 & \to & 1 & \to & 2 & \Rightarrow e \\ 3 & & 3 & & 3 \end{matrix}$$

S_3 è generato da elementi σ, τ tali che:

$\sigma^2 = 1$ e $\tau^3 = 1$ e

$\sigma\tau = \tau^2\sigma = \sigma\tau\tau = \sigma\tau^2\tau = \sigma\tau^2\tau^2 = \sigma\tau^4 = \sigma\tau\tau^3 = \sigma\tau$

2)

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}$$

3) $xyz = 1$. $yzx = 1$? $yxz = 1$?

$\forall\, x, y, z \in G$ gruppo

$(xy)z = 1 \Rightarrow (xy)zz^{-1} = 1z^{-1} \Rightarrow xy = z^{-1}$

$\Rightarrow xyy^{-1} = y^{-1}z^{-1} \Rightarrow x = y^{-1}z^{-1}$

$\Rightarrow xyz = yzy^{-1}z^{-1} \Rightarrow xyz = 1$

procedimento valido anche per l'altro caso.

4) $(G, \cdot), (G^\circ, \circ) \mid a \circ b := b \cdot a$. G° gruppo?

① $a \circ (b \circ c) = (a \circ b) \circ c$

$\Rightarrow a \circ cb = ba \circ c \Rightarrow cba = cba$

② $e \circ a = ae = a \wedge a \circ e = ea = a$

③ $a^{-1} \circ a = a \circ a^{-1} = e$ $\square$

5) $a, b \in G$ gruppo. a ha ordine 5. $a^3 b = b a^3$. $ab = ba$?

$\hookrightarrow a^5 = 1$

$ab = 1ab \Rightarrow ab = a^5 ab \Rightarrow ab = a^6 b \Rightarrow ab = ba^6$

$\Rightarrow ab = ba^5 a \Rightarrow ab = ba$ $\square$

6) a) SI c) NO e) NO

b) SI d) SI

$\rightarrow GL_n(\mathbb{K})$ è gruppo lineare delle $M_{n \times n}$ nell'insieme $\mathbb{K}$ invertibili.

l'inverso di $A \cdot B$ è $B^{-1} A^{-1}$

l'inversa di una $M_{2\times 2}$ la trovo così

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ è invertibile sse $ad - bc \neq 0$

$$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

esercizio:

dimostrare per induzione che
$$\sum_{i=0}^{n} 4i+1 = (n+1)\cdot(2n+1)$$

B.I. $\rightarrow$ $n=0 \Rightarrow 1=1$ ✓

P.I. $\rightarrow$ $n=n+1$

$$\sum_{i=0}^{n+1} 4i+1 = \sum_{i=0}^{n} 4i+1 + 4(n+1)+1 =$$

$$(n+1)(2n+1) + 4(n+1)+1 =$$
$$2n^2+n+2n+1+4n+4+1$$
$$2n^2+7n+6$$
$$(n+2)(2n+2+1) = 2n^2+2n+n+4n+4+2 =$$
$$2n^2+7n+6 \quad \square.$$

es. siano $a,b,c \in \mathbb{Z}$ e $c|a$, $c|b$. verificare che:
$\forall \alpha,\beta \in \mathbb{Z} \quad c|(\alpha a+\beta b)$.

ESERCITAZIONE 2

10) $(3522, 321)$ già fatto a lezione ✓

$(413, 173)$

$413 = 173 \cdot 2 + 67$

$173 = 67 \cdot 2 + 39$

$67 = 39 \cdot 1 + 28$

$39 = 28 \cdot 1 + 11$

$28 = 11 \cdot 2 + 6$

$11 = 6 \cdot 1 + 5$

$6 = 5 \cdot 1 + 1$

$5 = 1 \cdot 5 + 0 \qquad \Rightarrow \text{MCD} = 1$

bezout:

$$\begin{aligned}
1 &= 6 - 5 \cdot 1 \\
&= 6 - (11 - 6 \cdot 1) = 6 \cdot 2 - 11 \\
&= (28 - 11 \cdot 2) \cdot 2 - 11 = 28 \cdot 2 - 11 \cdot 5 \\
&= 28 \cdot 2 - (39 - 28 \cdot 1) \cdot 5 = 28 \cdot 7 - 39 \cdot 5 \\
&= (67 - 39 \cdot 1) \cdot 7 - 39 \cdot 5 = 67 \cdot 7 - 39 \cdot 12 \\
&= 67 \cdot 7 - (173 - 67 \cdot 2) \cdot 12 = 67 \cdot 31 - 173 \cdot 12 \\
&= (413 - 173 \cdot 2) \cdot 31 - 173 \cdot 12 = 413 \cdot 31 - 173 \cdot 74 \\
&= 12803 - 12801 = 1
\end{aligned}$$

$\Rightarrow \alpha = 31, \quad \beta = -74$

9) $p := x^3 - 6x^2 + x + 4 \qquad q := x^5 - 6x + 1$

$x^5 - 6x + 1 = (x^3 - 6x^2 + x + 4)(ax^2 + bx + c) + dx + h$

$\Rightarrow ax^5 + bx^4 + cx^3 - 6ax^4 - 6bx^3 - 6cx^2$
$\quad + ax^3 + bx^2 + cx + 4ax^2 + 4bx + 4c + dx + h$

$\Rightarrow ax^5 + x^4(b - 6a) + x^3(c - 6b + a) + x^2(-6c + b + 4a)$
$\quad + x(c + 4b + d) + 4c + h$???

ESERCITAZIONE 3

1) $(14743,\ 8915)$

$$14743 = 8915 \cdot 1 + 5828$$
$$8915 = 5828 \cdot 1 + 3087$$
$$5828 = 3087 \cdot 1 + 2741$$
$$3087 = 2741 \cdot 1 + 346$$
$$2741 = 346 \cdot 7 + 319$$
$$346 = 319 \cdot 1 + 27$$
$$319 = 27 \cdot 11 + 22$$
$$27 = 22 \cdot 1 + 5$$
$$22 = 5 \cdot 4 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2 + 0 \qquad \Rightarrow MCD = 1$$

bezout:

$$1 = 5 - 2 \cdot 2$$
$$= 5 - (22 - 5 \cdot 4) \cdot 2 = 5 \cdot 9 - 22 \cdot 2$$
$$= -22 \cdot 2 + (27 - 22 \cdot 1) \cdot 9 = 27 \cdot 9 - 22 \cdot 11$$
$$= 27 \cdot 9 - (319 - 27 \cdot 11) \cdot 11 = 27 \cdot 130 - 319 \cdot 11$$
$$= (346 - 319 \cdot 1) \cdot 130 - 319 \cdot 11 = 346 \cdot 130 - 319 \cdot 141$$
$$= 346 \cdot 130 - (2741 - 346 \cdot 7) \cdot 141 = 346 \cdot 1117 - 2741 \cdot 141$$
$$= (3087 - 2741 \cdot 1) \cdot 1117 - 2741 \cdot 141 = 3087 \cdot 1117 - 1258 \cdot 2741$$
$$= 3087 \cdot 1117 - (5828 - 3087 \cdot 1) \cdot 1258 = 2375 \cdot 3087 - 5828 \cdot 1258$$
$$= (8915 - 5828 \cdot 1) \cdot 2375 - 5828 \cdot 1258 = 8915 \cdot 2375 - 3633 \cdot 5828$$
$$= 8915 \cdot 2375 - (14743 - 8915 \cdot 1) \cdot 3633 = 8915 \cdot 6008 - 14743 \cdot 3633$$
$$\alpha = -3633 \qquad \beta = 6008$$

$(10000,\ 642)$

$$10000 = 642 \cdot 15 + 370$$
$$642 = 370 \cdot 1 + 272$$
$$370 = 272 \cdot 1 + 98$$

$272 = 98 \cdot 2 + 76$

$98 = 76 \cdot 1 + 22$

$76 = 22 \cdot 3 + 10$

$22 = 10 \cdot 2 + 2$

$10 = 2 \cdot 5 + 0 \quad \Rightarrow MCD = 2$

bezout:

$2 = 22 - 10 \cdot 2$

$= 22 - (76 - 22 \cdot 3) \cdot 2 = 22 \cdot 7 - 76 \cdot 2$

$= (98 - 76 \cdot 1) \cdot 7 - 76 \cdot 2 = 98 \cdot 7 - 76 \cdot 9$

$= 98 \cdot 7 - (272 - 98 \cdot 2) \cdot 9 = 98 \cdot 25 - 272 \cdot 9$

$= (370 - 272 \cdot 1) \cdot 25 - 272 \cdot 9 = 370 \cdot 25 - 272 \cdot 34$

$= 370 \cdot 25 - (642 - 370 \cdot 1) \cdot 34 = 370 \cdot 59 - 642 \cdot 34$

$= (10000 - 642 \cdot 15) \cdot 59 - 642 \cdot 34 = 10000 \cdot 59 - 642 \cdot 919$

$\alpha = 59 \qquad \beta = -919$

$(5785, 546)$

$5785 = 546 \cdot 10 + 325$

$546 = 325 \cdot 1 + 221$

$325 = 221 \cdot 1 + 104$

$221 = 104 \cdot 2 + 13$

$104 = 13 \cdot 8 + 0 \quad \Rightarrow MCD = 13$

bezout:

$13 = 221 - 104 \cdot 2$

$= 221 - (325 - 221 \cdot 1) \cdot 2 = 221 \cdot 3 - 325 \cdot 2$

$= (546 - 325 \cdot 1) \cdot 3 - 325 \cdot 2 = 546 \cdot 3 - 325 \cdot 5$

$= 546 \cdot 3 - (5785 - 546 \cdot 10) \cdot 5 = 546 \cdot 53 - 5785 \cdot 5$

$\alpha = -5 \qquad \beta = 53$