

$$A = \mathbb{Z}_8$$

$$(\mathbb{Z}_8, +, \circ)$$

$(A, +, \cdot)$  anello  $\Rightarrow$  non si deve evitare perché  $(\mathbb{Z}_n, +, \cdot)$  è un anello  
divisori delle zere  
elementi unitari  
sottogruppi di  $(A, +)$ .

$(\mathbb{Z}_8, +)$  gruppo abeliano

$(\mathbb{Z}_8, \cdot)$  monoido con unità  $[1]_8$  commutativo

$\forall [a]_8, [b]_8, [c]_8 \in \mathbb{Z}_8 \quad [a]_8 \cdot ([b]_8 + [c]_8) = [a]_8 \cdot [b]_8 + [a]_8 \cdot [c]_8$   
vale le proprietà distributive

$[a]_n \in \mathbb{Z}_n$  è divisore delle zere se e solo se M.C.D. ( $a, n$ )  $\neq 1$ .

Def:  $(B, +, \cdot)$  anello

a  $\in B$  è divisore delle zere se

1.  $a \neq 0$   
2.  $\exists b \in B \quad b \neq 0$  tali ch  
 $a \cdot b = 0$

$[2]_8, [4]_8, [6]_8 \rightarrow$  i divisori delle zere di  $(\mathbb{Z}_8, +, \cdot)$

$$[2]_8 \cdot [4]_8 = [8]_8 = [0]_8$$

$$[6]_8 \cdot [4]_8 = [24]_8 = [0]_8$$

gli altri elementi non nulli sono unitari (ovvero sono gli elementi invertibili rispetto a  $\cdot$ ).

$[1]_8, [3]_8, [5]_8, [7]_8$  sono gli elementi unitari di  $(\mathbb{Z}_8, +, \cdot)$

$[a]_n \in \mathbb{Z}_n$  è unitario  $\Leftrightarrow \text{M.C.D.}(a, n) = 1$

gli inversi:

$$[1]_8^{-1} = [1]_8$$

$$[3]_8^{-1} = [3]_8 \quad \text{perché}$$

$$[3]_8 \cdot [3]_8 = [9]_8 = [1]_8$$

$$[5]_8^{-1} = [5]_8 \quad \text{perché}$$

$$[5]_8 \cdot [5]_8 = [25]_8 = [1]_8$$

$$[7]_8^{-1} = [7]_8 \quad \text{perché}$$

$$[7]_8 \cdot [7]_8 = [49]_8 = [1]_8$$

$(\mathbb{Z}_8, +)$  è un gruppo ciclico.

Teorema: Ogni sottogruppo di un gruppo ciclico è ciclico

$$\langle [0]_8 \rangle = \{ [0]_8 \} \quad \text{M.C.D.}(3, 8) = 1 \quad h \cdot [0]_8 = [0]_8$$

$$\langle [1]_8 \rangle = \mathbb{Z}_8 = \langle [3]_8 \rangle = \langle [5]_8 \rangle = \langle [7]_8 \rangle$$

$$\begin{aligned} \langle [2]_8 \rangle &= \{ [2]_8, 2 \cdot [2]_8 = [4]_8, 3 \cdot [2]_8 = [6]_8, 4 \cdot [2]_8 = [8]_8 = [0]_8 \} : \\ &= \{ [2]_8, [4]_8, [6]_8, [0]_8 \} \end{aligned}$$

$$\langle [4]_8 \rangle = \{ [4]_8, 2 \cdot [4]_8 = [8]_8 = [0]_8 \} = \{ [4]_8, [0]_8 \}$$

$$\langle [6]_8 \rangle$$

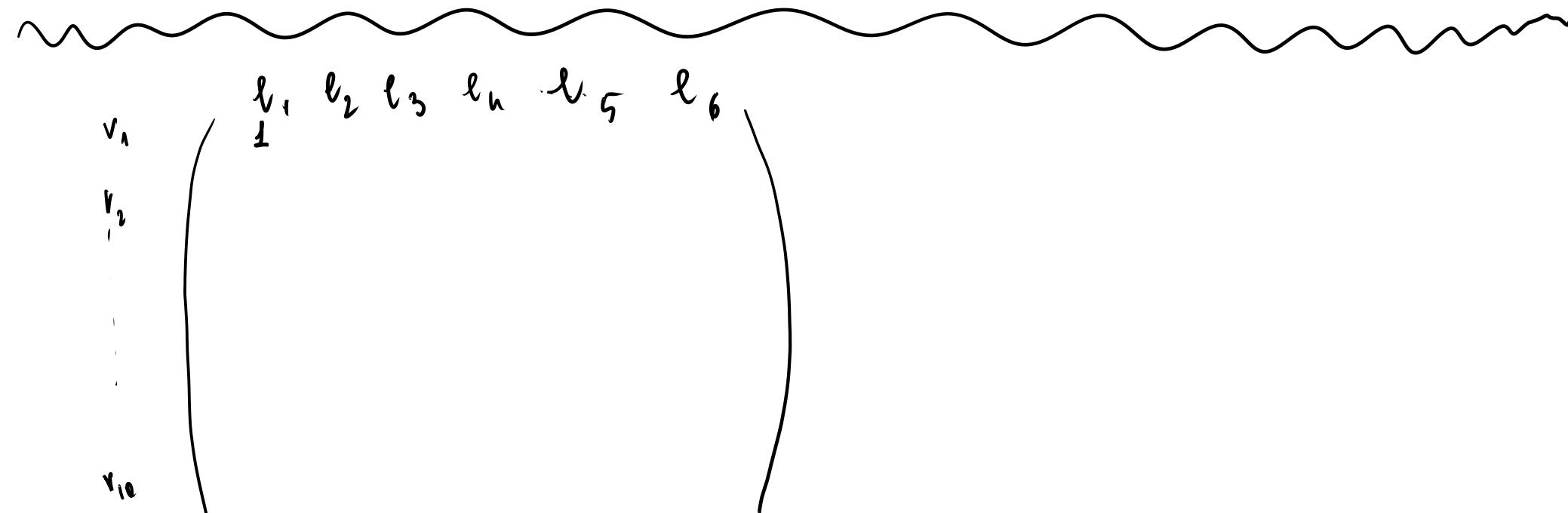
$$[6]_8 = 6 \cdot [1]_8$$

$$|\Sigma [6]_8| = \frac{8}{\text{M.C.D.}(6,8)} = \frac{8}{2} = 4$$

quindi  $\langle [6]_8 \rangle = \langle [2]_8 \rangle$  perche'  $|\Sigma [6]_8| = |\Sigma [2]_8|$

Teorema (inverso del Teorema di Lagrange nei gruppi ciclici)

Sia  $(G, +)$  un gruppo ciclico  $|G|=n$ , allora per ogni  $h \in \mathbb{N}^*$  con  $h|n$  esiste un unico sottogruppo  $H$  di  $(G, +)$  tale che  $|H|=h$ .



Album  $G = (V, L)$  avente

3	5	$ V  = 18 + x$
3	4	$ L  = 11 + x$
2	3	
4	9	
x	1	

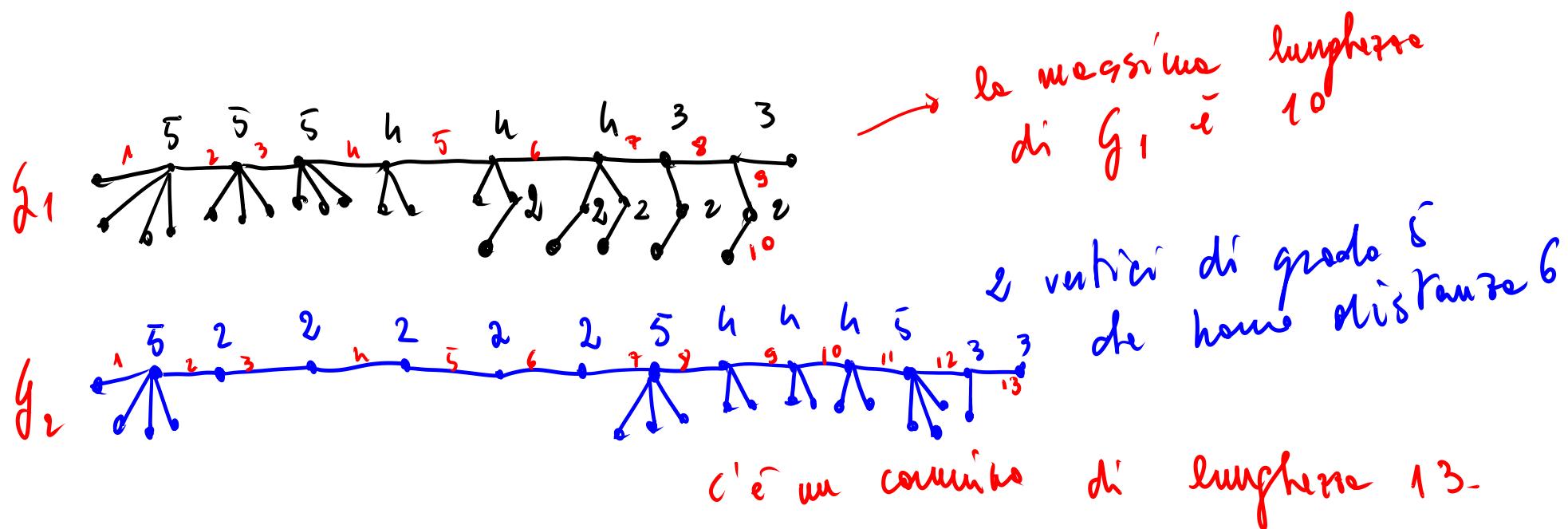
$$2(11+x) = \sum_{v \in V} d(v) = 3 \cdot 5 + 3 \cdot 4 + 2 \cdot 3 + 4 \cdot 2 + x \cdot 1 = \\ = 15 + 12 + 6 + 8 + x = 41 + x$$

~~$22 + x = 41 + x$~~

$x = 41 - 22 = 19 \quad \text{vertici di grado 1}$

$|V| = 18 + 19 = 37$

$|L| = 30$



$$\sum_{i=1}^n \frac{1}{h i^2 - 1} = \frac{n}{2n+1}$$

$n \in \mathbb{N}^*$

Passo base :  $P(1)$  vero

$n=1$  :

$$\sum_{i=1}^1 \frac{1}{h i^2 - 1} = \frac{1}{h \cdot 1^2 - 1} = \frac{1}{h-1} = \frac{1}{3}$$

$$\frac{1}{2n+1} = \frac{1}{2 \cdot 1 + 1} = \frac{1}{3} \quad \text{OK}$$

Passo induttivo :  $P(n)$  vero

$P(n+1)$  vero

$$\sum_{i=1}^m \frac{1}{h i^2 - 1} = \frac{m}{2n+1} \quad \text{ipotesi d'induz.}$$

$$\sum_{i=1}^{m+1} \frac{1}{h i^2 - 1} = \frac{m+1}{2(n+1)+1} = \frac{m+1}{2n+3} \quad \text{ten}$$

$$\sum_{i=1}^{m+1} \frac{1}{h i^2 - 1} = \sum_{i=1}^m \frac{1}{h i^2 - 1} + \frac{1}{h(n+1)^2 - 1} \stackrel{\text{ipotesi d'induz.}}{=} \frac{m}{2n+1} + \frac{1}{h(n+1)^2 - 1}$$

$$= \frac{m}{2n+1} + \frac{1}{h(m^2+2n+1) - 1} = \frac{m}{2n+1} + \frac{1}{h n^2 + 8n + h - 1} = \frac{m}{2n+1} + \frac{1}{h n^2 + 8n + 3} =$$

$$\begin{aligned} & \frac{h n^2 + 8n + 3}{h n^2 - 2n} \quad \frac{1}{2n+3} \\ & \underline{- h n^2 - 2n} \\ & \underline{6n + 3} \\ & \underline{- 6n - 3} \\ & \underline{\underline{11}} \end{aligned}$$

$$h n^2 + 8n + 3 = (2n+1)(2n+3)$$

$$(2n+1)(2n+3) = h n^2 + 6n + 2n + 3 = h n^2 + 8n + 3 \quad \text{OK!}$$

$$\frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} = \frac{n(2n+3) + 1}{(2n+1)(2n+3)} = \frac{2n^2 + 3n + 1}{(2n+1)(2n+3)} \stackrel{(x)}{=} \frac{1}{}$$

$$n_1, n_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-3 \pm \sqrt{9 - 4 \cdot 2 \cdot 1}}{4} = \frac{-3 \pm \sqrt{9 - 8}}{4} = \frac{-3 \pm 1}{4}$$

$(ax^2 + bx + c = a(x-x_1)(x-x_2))$   
 $x_1, x_2$  sono le radici

$$= \frac{-2}{4} = -\frac{1}{2}$$

$$= \frac{-4}{4} = -1$$

$$2n^2 + 3n + 1 = 2(n + \frac{1}{2})(n + 1) = (2n+1)(n+1)$$

$$= \frac{(2n+1)(n+1)}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}$$



$(\mathbb{Z}, *)$

$* : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$$(x, y) \mapsto x * y = x - y + 3$$

(a) \* associative, commutative No

(b) element. neutro non esiste

(c) inversi non ha senso

(d)  $(\mathbb{Z}, *)$  monoid, gruppo (No)

(e)  $\mathbb{N}$  chiuso in  $(\mathbb{Z}, *)$

(f)  $\mathbb{D}$  chiuso in  $(\mathbb{Z}, *)$

$$(a) \quad \forall x, y, z \in \mathbb{Z} \quad x * (y * z) = (x * y) * z \quad ?$$

$$x * (y * z) = x * \underbrace{(y - z + 3)}_{y'} = x - y' + 3 = x - (y - z + 3) + 3 = \\ = x - y + z - \cancel{z} + \cancel{3} = \underline{x - y + z}$$

$$(x * y) * z = \underbrace{(x - y + 3)}_{x'} * z = x' - z + 3 = (x - y + 3) - z + 3 = \\ = x - y + 3 - z + 3 = \underline{x - y - z + 6}$$

pr. es.  $2 * (1 * (-2)) = 2 * (1 - (-2) + 3) = 2 * 6 = 2 - 6 + 3 = \underline{-1}$

$$(2 * 1) * (-2) = (2 - 1 + 3) * (-2) = 4 * (-2) = 4 - (-2) + 3 = \\ = 4 + 2 + 3 = \underline{9}$$

\* nun ist die Regel assoziativ

$$\forall x, y \in \mathbb{Z} \quad x * y = y * x \\ x - y + 3 = y - x + 3 \quad \text{falso}$$

pr. es.:  $1 * 2 = 1 - 2 + 3 = 2$

$$2 * 1 = 2 - 1 + 3 = 4$$

$(\mathbb{Z}, *)$  nun ist die assoziative und kommutative

Cerchiamo, se esiste,  $e \in \mathbb{Z}$  tale che  $\forall x \in \mathbb{Z}$

$$e * x = x * e = x$$

$$e * x = x \Leftrightarrow e - x + 3 = x \Leftrightarrow e = 2x - 3$$

e dipende da  $x$  e quindi non può andare bene

$$x * e = x$$

~~$$x - e + 3 = x$$~~

$$e = 3$$

esiste un elemento neutro a destra

$$3 * x = 3 - x + 3 = 6 - x \neq x$$

3 non funziona come elemento neutro

Allora non ha senso parlare di elementi invertibili

$\mathbb{N}$  chiuse in  $(\mathbb{Z}, *)$

$$\forall n, m \in \mathbb{N}$$

$$n * m \in \mathbb{N}$$

$$m * n \in \mathbb{N}$$

$$0, 4 \in \mathbb{N}$$

$$0 * 4 = 0 - 4 + 3 = -1 \notin \mathbb{N}$$

$\mathbb{N}$  non è chiusa

perché

$$0, 4 \in \mathbb{N} \quad e \quad 0 * 4 \notin \mathbb{N}.$$

Sia pure  $x, y \in \mathbb{P} \Rightarrow \exists h, k \in \mathbb{Z}$  tali che  $x = 2h, y = 2k$

$$x * y = x - y + 3 = 2h - 2k + 3 = 2h - 2k + 2 + 1 = \\ = 2(h - k + 1) + 1 \quad \text{dispari}$$

Sia pure  $x, y \in \mathbb{D} \Rightarrow \exists t, s \in \mathbb{Z}$  tali che  $x = 2t + 1 \quad y = 2s + 1$

$$x * y = x - y + 3 = 2t + 1 - (2s + 1) + 3 = 2t - 2s + 1 + 3 = \\ = 2t - 2s + 2 + 1 \\ = 2(t - s + 1) + 1 \quad \text{dispari}$$

$\forall x, y \in \mathbb{D} \quad x * y \in \mathbb{D}$  puoi con  $\mathbb{D}$  è un sottoinsieme

di  $\mathbb{Z}$  chiuso rispetto ad  $*$ .

$(\mathbb{D}, *)$  struttura algebrica.

$$f: \mathbb{N} \rightarrow \mathbb{Q}$$

$$n \mapsto \frac{n-3}{2n+2}$$

$$g: \mathbb{Q} \rightarrow \mathbb{Q}$$

$$x \mapsto -\frac{2}{3}x + 1$$

$$n \in \mathbb{N} \quad 2n+2 \neq 0$$

sempre

f, g      iniettive, surgettive

$$f^{-1}, g^{-1} ?$$

$$g \circ f, f \circ g ?$$

$$f(h), \quad g(\{h, \frac{2}{3}, -1\}) \quad f^{-1}\left(\{\frac{3}{2}, -\frac{2}{3}\}\right)$$

f ist injektiv?       $n, m \in \mathbb{N}$       teilt die  $f(n) = f(m)$

$$f(n) = f(m) \Leftrightarrow \frac{n-3}{2n+2} = \frac{m-3}{2m+2} \Leftrightarrow \frac{(n-3)(2m+2) - (m-3)(2n+2)}{(2n+2)(2m+2)} = 0$$

$$\Leftrightarrow \frac{2nm - 2n - 6m - 6 - (2nm + 2m - 6n - 6)}{(2n+2)(2m+2)} = 0$$

$$\Leftrightarrow 2n - 6m - 2m + 6n = 0 \Leftrightarrow 8n - 8m = 0 \Leftrightarrow n = m$$

$$f(n) = f(m) \Leftrightarrow n = m$$

f ist injektiv.

fi surgettive? Sia  $x \in \mathbb{Q}$ . Cerchiamo se esiste  $n \in \mathbb{N}$  tale che  $f(n) = x$

$$f(n) = x \Leftrightarrow \frac{n-3}{2n+2} = x \Leftrightarrow \frac{n-3 - x(2n+1)}{2n+2} = 0 \Leftrightarrow$$

$$n-3 - 2nx - 2x = 0 \Leftrightarrow n(1-2x) = 3 + 2x \Leftrightarrow$$

$$\Leftrightarrow n = \frac{3+2x}{1-2x} \notin \mathbb{N}$$

$$\text{per es. } x = 4 \quad n = \frac{3+8}{1-8} = -\frac{11}{7} \notin \mathbb{N}.$$

$f$  non è surgettiva e quindi non è bigettiva per cui non è invertibile ( $\nexists f^{-1}$ )

$$g: \mathbb{Q} \rightarrow \mathbb{Q} \leftarrow y \\ x \mapsto -\frac{2}{3}x + 1$$

$g$  è iniettiva? Siano  $x_1, x_2 \in \mathbb{Q}$  tali che  $g(x_1) = g(x_2)$

$$g(x_1) = g(x_2) \Leftrightarrow -\frac{2}{3}x_1 + 1 = -\frac{2}{3}x_2 + 1 \Leftrightarrow -\frac{2}{3}x_1 = -\frac{2}{3}x_2 \Leftrightarrow x_1 = x_2$$

$g$  è iniezione.

$g$  è suriettiva? Sia  $y \in \mathbb{Q}$ : anch'iamo, se esiste,  $x \in \mathbb{Q}$

tale che  $g(x) = y \Leftrightarrow -\frac{2}{3}x + 1 = y \Leftrightarrow -\frac{2}{3}x = y - 1 \Leftrightarrow$

$$x = -\frac{3}{2}(y-1) \in \mathbb{Q}$$

$g$  è suriettiva: se  $y \in \mathbb{Q}$  allora esiste  $x = -\frac{3}{2}y + \frac{3}{2} \in \mathbb{Q}$

tale che  $g(x) = y$

$g$  è bigettiva e quindi è invertibile.

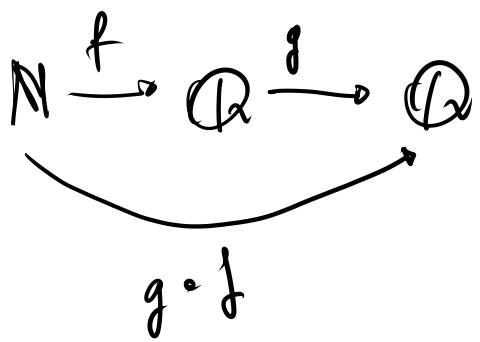
$$\bar{g}^{-1}: \mathbb{Q} \rightarrow \mathbb{Q} \quad \forall y \in \mathbb{Q} \quad \bar{g}^{-1}(y) = -\frac{3}{2}y + \frac{3}{2}$$

$$g \circ \bar{g}^{-1}: \mathbb{Q} \rightarrow \mathbb{Q} \quad \forall y \in \mathbb{Q} \quad g \circ \bar{g}^{-1} = id_{\mathbb{Q}}$$

$$(g \circ \bar{g}^{-1})(y) = g(\bar{g}^{-1}(y)) = g\left(-\frac{3}{2}y + \frac{3}{2}\right) = -\frac{2}{3}\left(-\frac{3}{2}y + \frac{3}{2}\right) + 1 = \\ = y - 1 + 1 = y$$

verificare  $(\bar{g}^{-1} \circ g)(x) = x$

$$\bar{g}^{-1} \circ g = id_{\mathbb{Q}}$$



l'insieme di arrivo di  $f$ , coincide con l'insieme di partenza di  $g$ , per cui esiste  $g \circ f$

$$g \circ f : \mathbb{N} \rightarrow \mathbb{Q}$$

$$\forall n \in \mathbb{N} \quad (g \circ f)(n) = g(f(n)) = g\left(\frac{n-3}{2n+2}\right) =$$

$$\begin{aligned} &= -\frac{2}{3}\left(\frac{n-3}{2n+2}\right) + 1 = \frac{-2n+6 + 6n+6}{6n+6} = \\ &= \frac{4n+12}{6n+6} = \frac{2(2n+6)}{6n+6} = \frac{2n+6}{3(n+1)} \end{aligned}$$

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{g} & \mathbb{Q} \\ \mathbb{N} & \xrightarrow{f} & \mathbb{Q} \end{array}$$

non esiste  $f \circ f$  perché l'insieme di arrivo di  $g$  è diverso dall'insieme di partenza di  $f$ .

$$f(n) = \frac{n-3}{2n+2} = \frac{1}{8+2} = \frac{1}{10}$$

$$g\left(\{1, \frac{2}{3}, -1\}\right)$$

$$\left. \begin{array}{l} g(1) = -\frac{2}{3} \cdot 1 + 1 = -\frac{2}{3} + 1 = \frac{-2+3}{3} = \frac{1}{3} \\ g\left(\frac{2}{3}\right) = -\frac{2}{3} \cdot \frac{2}{3} + 1 = -\frac{4}{9} + 1 = \frac{-4+9}{9} = \frac{5}{9} \\ g(-1) = -\frac{2}{3} \cdot (-1) + 1 = \frac{2}{3} + 1 = \frac{2+3}{3} = \frac{5}{3} \end{array} \right\} \Rightarrow$$

$$\Rightarrow g\left\{1, \frac{2}{3}, -1\right\} = \left\{\frac{1}{3}, \frac{5}{9}, \frac{5}{3}\right\}.$$

$$f^{-1}\left(\left\{\frac{2}{3}, -\frac{3}{2}\right\}\right) = \left\{n \in \mathbb{N} : f(n) = \frac{2}{3} \vee f(n) = -\frac{3}{2}\right\}$$

such that  $n \in \mathbb{N}$  such that  $f(n) = \frac{2}{3}$

$$f(n) = \frac{2}{3} \Leftrightarrow \frac{n-3}{2n+2} = \frac{2}{3} \Leftrightarrow \frac{3(n-3) - 2(2n+2)}{3(2n+2)} = 0 \Leftrightarrow 3n - 9 - 4n - 4 = 0$$

$$\Leftrightarrow -n - 13 = 0 \Leftrightarrow n = -13 \notin \mathbb{N}$$

Cerchiamo, se esiste  $m \in \mathbb{N}$  tale che  $f(m) = -\frac{3}{2}$

$$f(m) = -\frac{3}{2} \Leftrightarrow \frac{m-3}{2m+2} = -\frac{3}{2} \Leftrightarrow \frac{m-3}{2(m+1)} = -\frac{3}{2} \Leftrightarrow$$

$$\Leftrightarrow \frac{m-3 + 3(m+1)}{m+1} = 0 \Leftrightarrow m-3 + 3m+3 = 0 \Leftrightarrow 4m = 0$$

$$\Leftrightarrow m=0 \in \mathbb{N}$$

$$f(0) = -\frac{3}{2} \Rightarrow f^{-1}\left(\left\{-\frac{3}{2}\right\}\right) = \{0\}$$

$$\text{e risulta: } f^{-1}\left(\left\{\frac{2}{3}\right\}\right) = \emptyset$$