

# Lezione 5

Alessandro Ardizzoni

## Proposizione

*Una funzione è biiettiva  $\Leftrightarrow$  la sua corrispondenza opposta è una funzione.*

## Proof.

Consideriamo una funzione  $f : X \rightarrow Y$ . Poiché  $f$  è, in particolare, una corrispondenza, possiamo considerare la sua corrispondenza opposta  $f^{\text{op}} : Y \rightarrow X$ .

Per definizione, la corrispondenza  $f^{\text{op}} : Y \rightarrow X$  è una funzione  $\Leftrightarrow$

$$\forall y \in Y, \exists! x \in X, (y, x) \in f^{\text{op}}. \quad (1)$$

D'altra parte  $(y, x) \in f^{\text{op}} \Leftrightarrow (x, y) \in f \Leftrightarrow f(x) = y$ . Quindi (1) diventa

$$\forall y \in Y, \exists! x \in X, f(x) = y. \quad (2)$$

Come visto nell'ultima lezione, questo vuol dire che  $f$  è biiettiva. □

## Lemma

Sia  $f : X \rightarrow Y$  una funzione. Allora

$$\text{Id}_X : X \rightarrow X$$

$n \mapsto n$

$$f \circ \text{Id}_X = f \quad \text{e} \quad \text{Id}_Y \circ f = f.$$

## Proof.

Componendo le funzioni  $X \xrightarrow{\text{Id}_X} X \xrightarrow{f} Y$  otteniamo la funzione  $X \xrightarrow{f \circ \text{Id}_X} Y$  che ha lo stesso dominio e codominio di  $f$ .

Per vedere che  $f \circ \text{Id}_X$  ed  $f$  sono uguali resta solo da controllare che  $f \circ \text{Id}_X$  e  $f$  hanno la stessa immagine su tutti gli elementi del proprio dominio.

In effetti, preso  $x \in X$ , abbiamo

$$(f \circ \text{Id}_X)(x) = f(\text{Id}_X(x)) = f(x)$$

e quindi  $f \circ \text{Id}_X = f$ .

Similmente si ottiene che  $\text{Id}_Y \circ f = f$ .



Una funzione  $X \xrightarrow{f} Y$  si dice **invertibile** se esiste una funzione  $Y \xrightarrow{g} X$  tale che  $f \circ g = \text{Id}_Y$  e  $g \circ f = \text{Id}_X$ . In tal caso diremo che  $g$  è **un'inversa** di  $f$ .

### Proposizione (Unicità dell'inversa)

*Una funzione invertibile ha un'unica inversa.*

Proof.

Se  $g$  e  $g'$  sono inverse di  $f$ , si ha in particolare che  $g' \circ f = \text{Id}_X$  e  $f \circ g = \text{Id}_Y$ . Pertanto, per l'associatività otteniamo

$$g \stackrel{\text{lemma}}{=} \text{Id}_X \circ g = (g' \circ f) \circ g \stackrel{\text{ass.}}{=} g' \circ (f \circ g) = g' \circ \text{Id}_Y \stackrel{\text{lemma}}{=} g'.$$



Dato che ci può essere un'inversa sola possiamo chiamarla **l'inversa** di  $f$  ed indicarla con il simbolo  $f^{-1} : Y \rightarrow X$ .

Valgono quindi le seguenti uguaglianze quando  $f$  è invertibile:

$$f \circ f^{-1} = \text{Id}_Y$$

e

$$f^{-1} \circ f = \text{Id}_X.$$

## Osservazione

Le uguaglianze  $f \circ f^{-1} = \text{Id}_Y$  e  $f^{-1} \circ f = \text{Id}_X$  ci dicono che anche  $f^{-1}$  è invertibile e che la sua inversa è proprio  $f$ . In simboli  $(f^{-1})^{-1} = f$ .

## Lemma

Se  $f : X \rightarrow Y$  una funzione invertibile, allora  $\forall x \in X, y \in Y$  si ha che

$$f^{-1}(y) = x \quad \Leftrightarrow \quad y = f(x). \quad (3)$$

Inoltre  $f^{-1} = f^{\text{op}}$ . Quindi se  $f$  è invertibile allora  $f^{\text{op}}$  è una funzione.

DIMOSTRAZIONE. Per verificare (3), basta suddividerla nelle due implicazioni. Ne dimostriamo una (l'altra si fa similmente):

$$f^{-1}(y) = x \Rightarrow f(f^{-1}(y)) = f(x) \Rightarrow (f \circ f^{-1})(y) = f(x) \Rightarrow \text{Id}(y) = f(x) \Rightarrow y = f(x).$$

Riguardando  $f$  e  $f^{-1}$  come corrispondenze, possiamo riscrivere (3) come  $(y, x) \in f^{-1} \Leftrightarrow (x, y) \in f$ . Ciò significa  $f^{-1} = f^{\text{op}}$ .

## Teorema

Sia  $f$  una funzione ed  $f^{\text{op}}$  la sua corrispondenza opposta.

LSAE (=Le seguenti affermazioni sono equivalenti).

- ①  $f$  è biiettiva;
- ②  $f^{\text{op}}$  è una funzione;
- ③  $f$  è invertibile.

Se vale una di queste condizioni, si ha anche  $f^{-1} = f^{\text{op}}$ .

SOLUZIONE. Avendo già dimostrato  $\textcircled{1} \Leftrightarrow \textcircled{2} \Leftarrow \textcircled{3}$ , per concludere basta verificare  $\textcircled{1} \Rightarrow \textcircled{3}$ . Se  $X \xrightarrow{f} Y$  è biiettiva, allora  $f^{\text{op}} : Y \rightarrow X$  è una funzione. Vediamo che è l'inversa di  $f$ . Per ogni  $x \in X, y \in Y$  si ha che

$$\boxed{f^{\text{op}}(y) = x} \Leftrightarrow (y, x) \in f^{\text{op}} \Leftrightarrow (x, y) \in f \Leftrightarrow \boxed{f(x) = y}.$$

Allora,  $\forall x$  possiamo porre  $y := f(x)$  e ottenere

$$(f^{\text{op}} \circ f)(x) = f^{\text{op}}(f(x)) = f^{\text{op}}(y) = x.$$

Similmente,  $\forall y$ , posto  $x := f^{\text{op}}(y)$ , otteniamo  $(f \circ f^{\text{op}})(y) = y$ .

Di conseguenza  $f^{\text{op}} \circ f = \text{Id}_X$  e  $f \circ f^{\text{op}} = \text{Id}_Y$  e quindi  $f$  è invertibile. □

## Osservazione

*Dal teorema precedente segue che ogni funzione invertibile è biiettiva. Questo si può dimostrare direttamente nel modo seguente. Si ha che*

$$\begin{aligned} f \circ f^{-1} = \text{Id}_Y &\Rightarrow f \circ f^{-1} \text{ suriettiva} \Rightarrow f \text{ suriettiva,} \\ f^{-1} \circ f = \text{Id}_X &\Rightarrow f^{-1} \circ f \text{ iniettiva} \Rightarrow f \text{ iniettiva.} \end{aligned}$$

*Pertanto  $f$  è sia suriettiva sia iniettiva e quindi biiettiva.*

## Osservazione

*Abbiamo già osservato, nel definirla, che  $\text{Id}_X : X \rightarrow X$  è biiettiva. Ma allora è anche invertibile. In effetti da*

$$\text{Id}_X \circ \text{Id}_X = \text{Id}_X$$

*deduciamo che la sua inversa è ancora  $\text{Id}_X$ . In simboli*

$$(\text{Id}_X)^{-1} = \text{Id}_X.$$

## Proposizione

Siano  $X \xrightarrow{g} Y$  e  $Y \xrightarrow{f} Z$  delle funzioni invertibili. Allora  $f \circ g$  e  $g^{-1} \circ f^{-1}$  sono invertibili e sono l'una l'inversa dell'altra. In simboli

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}, \quad (g^{-1} \circ f^{-1})^{-1} = f \circ g.$$

Proof.

Per associatività della composizione, abbiamo

$$(g^{-1} \circ f^{-1}) \circ (f \circ g) = g^{-1} \circ \textcolor{red}{f^{-1}} \circ \textcolor{red}{f} \circ g = g^{-1} \circ \text{Id} \circ g = g^{-1} \circ g = \text{Id}.$$

Quindi  $(g^{-1} \circ f^{-1}) \circ (f \circ g) = \text{Id}$ .

Similmente si vede che  $(f \circ g) \circ (g^{-1} \circ f^{-1}) = \text{Id}$ .

Queste due uguaglianze ci dicono che  $f \circ g$  e  $g^{-1} \circ f^{-1}$  sono invertibili e sono l'una l'inversa dell'altra. □



## Esercizio

Per ognuna delle seguenti funzioni, dire se è iniettiva e/o suriettiva. Se è biiettiva, determinare la funzione inversa.

- ①  $f : \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto n^3 + 1$ ;
- ②  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}, (m, n) \mapsto m - n$ ;
- ③  $f : \mathbb{Z} \rightarrow \mathbb{Z}^2, n \mapsto (n - 1, n + 1)$ ;
- ④  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2, (m, n) \mapsto (m - 2, n + 1)$ .

SOLUZIONE. Trattiamo tutti i casi uno alla volta.

①  $f : \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto n^3 + 1$ .

Iniettiva. Siano  $m, n \in \mathbb{Z}$ . Se  $f(m) = f(n)$  allora  $m^3 + 1 = n^3 + 1$  da cui  $m^3 = n^3$ . Di qui deduciamo  $m = n$  (l'Analisi ci dice che la funzione  $f(x) := x^3$  è strettamente crescente perché ha derivata prima  $f'(x) = 3x^2 > 0$  per  $x \neq 0$ ; pertanto è iniettiva). Quindi  $f$  è iniettiva.

Suriettiva. Non è suriettiva perché non tutti gli interi sono della forma  $n^3 + 1$ . Ad esempio, se  $\exists n \in \mathbb{Z}$  per cui  $3 = n^3 + 1$  allora si avrebbe  $2 = n^3$  e quindi  $n$  sarebbe necessariamente pari. Allora potremmo scrivere  $n = 2k$  da cui  $2 = n^3 = (2k)^3 = 8k^3$  il che è assurdo perché  $8 > 2$ .

②  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}, (m, n) \mapsto m - n$ .

Iniettiva. Siano  $(m_1, n_1)$  e  $(m_2, n_2)$  tali che  $f((m_1, n_1)) = f((m_2, n_2))$  cioè  $m_1 - n_1 = m_2 - n_2$ . In questo caso non possiamo dedurre che  $(m_1, n_1) = (m_2, n_2)$ . Ad esempio  $2 - 1 = 1 - 0$  ma  $(2, 1) \neq (1, 0)$ . Pertanto  $f$  non è iniettiva.

Suriettiva. Se  $k \in \mathbb{Z}$ , allora  $k = k - 0 = f((k, 0))$  e dunque  $f$  è suriettiva.

---

③  $f : \mathbb{Z} \rightarrow \mathbb{Z}^2, n \mapsto (n - 1, n + 1)$ .

Iniettiva. Siano  $m, n \in \mathbb{Z}$ . Se  $f(m) = f(n)$  allora  $(m - 1, m + 1) = (n - 1, n + 1)$  da cui  $m - 1 = n - 1$  e  $m + 1 = n + 1$ . Semplificando, otteniamo  $m = n$  e dunque  $f$  è iniettiva.

Suriettiva. Notiamo che  $(n + 1) - (n - 1) = 2$  e quindi ogni elemento  $(a, b) \in \mathbb{Z}^2$  con  $b - a \neq 2$  non sta nell'immagine di  $f$ . In particolare  $(0, 1)$  non sta nell'immagine di  $f$  e quindi  $f$  non è suriettiva.

4  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2, (m, n) \mapsto (m-2, n+1)$ .

Iniettiva. Siano  $(m_1, n_1)$  e  $(m_2, n_2)$  tali che  $f((m_1, n_1)) = f((m_2, n_2))$  cioè  $(m_1 - 2, n_1 + 1) = (m_2 - 2, n_2 + 1)$ . Allora  $m_1 - 2 = m_2 - 2$  e  $n_1 + 1 = n_2 + 1$ . Otteniamo  $m_1 = m_2$  e  $n_1 = n_2$  da cui  $(m_1, n_1) = (m_2, n_2)$ . Pertanto  $f$  è iniettiva.

Suriettiva. Siano  $(a, b) \in \mathbb{Z}^2$ . Per vedere che  $f$  è suriettiva dobbiamo individuare  $(m, n) \in \mathbb{Z}^2$  tale che  $f((m, n)) = (a, b)$  cioè  $(m - 2, n + 1) = (a, b)$ . Ciò vuol dire  $m - 2 = a$  e  $n + 1 = b$  da cui  $m = a + 2$  e  $n = b - 1$ . In effetti  $(a, b) = f((a + 2, b - 1))$ . Quindi  $f$  è suriettiva.

Biiettiva. Visto che  $f$  è sia iniettiva sia suriettiva, allora  $f$  è biiettiva. Pertanto è invertibile, cioè ha l'inversa  $f^{-1}$ . Dobbiamo descriverla esplicitamente. Per farlo, da  $(a, b) = f((a + 2, b - 1))$  deduciamo che  $f^{-1}((a, b)) = (a + 2, b - 1)$ . Dunque l'inversa di  $f$  è

$$f^{-1} : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2, (a, b) \mapsto (a + 2, b - 1).$$

# Immagine e controimmagine

Sia  $f : A \rightarrow B$  una funzione.

- Sia  $A' \subseteq A$ . Allora l'**immagine di  $A'$**  tramite  $f$  è l'insieme

$$f(A') := \{f(a) \mid a \in A'\} \subseteq B.$$

In altri termini è l'insieme di tutte le immagini degli elementi di  $A'$ .

- Sia  $B' \subseteq B$ . Allora la **controimmagine di  $B'$**  tramite  $f$  è l'insieme

NON SIGNIFICA  
CHE  $f$  sia  
invertibile

$$f^{-1}(B') := \{a \in A \mid f(a) \in B'\} \subseteq A.$$

Quindi è l'insieme di tutte le controimmagini degli elementi di  $B'$ .

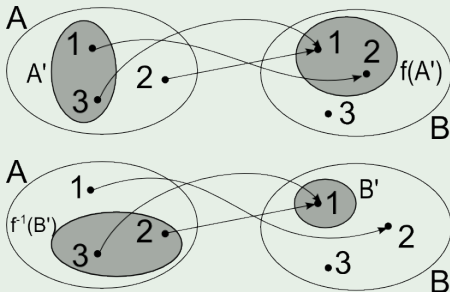
## Osservazione

Si noti che la controimmagine di una funzione **esiste sempre anche se la funzione non è invertibile** e quindi non è detto abbia l'inversa.

Insomma il simbolo  $f^{-1}(B')$  NON vuol dire che l'inversa  $f^{-1}$  esista.

## Esempio

Ecco un esempio di calcolo di  $f(A')$  e di  $f^{-1}(B')$  per una funzione  $f : \{1,2,3\} \rightarrow \{1,2,3\}$  dove  $A' := \{1,3\}$  e  $B' := \{1\}$ .

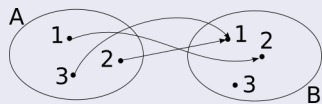


In pratica

- $f(A') = f(\{1,3\}) = \{f(1), f(3)\} = \{1,2\}$  è l'insieme degli elementi su cui arrivano le frecce che partono da  $A'$ ;
- $f^{-1}(B') = f^{-1}(\{1\}) = \{2,3\}$  è l'insieme degli elementi da cui partono le frecce che arrivano in  $B'$ .

## Esercizio

Si consideri la funzione  $f$  qui accanto,  
calcolare  $\mathcal{F} = \{f(S) \mid S \subseteq A\}$  e  
 $\mathcal{G} = \{f^{-1}(S) \mid S \subseteq B\}$



SOLUZIONE. I sottoinsiemi di  $A$  sono  $\emptyset$ ,  $\{1\}$ ,  $\{2\}$ ,  $\{3\}$ ,  $\{1,2\}$ ,  $\{1,3\}$ ,  $\{2,3\}$ ,  $\{1,2,3\}$ . Si ha che

$$\begin{aligned} f(\emptyset) &= \emptyset, & f(\{1\}) &= \{f(1)\} = \{2\}, & f(\{2\}) &= \{f(2)\} = \{1\}, \\ f(\{3\}) &= \{f(3)\} = \{1\}, & f(\{1,2\}) &= \{f(1), f(2)\} = \{1,2\}, \dots \end{aligned}$$

da cui

$$\mathcal{F} = \{\emptyset, \{2\}, \{1\}, \{1\}, \{2,1\}, \{2,1\}, \{1,1\}, \{2,1,1\}\} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}.$$

I sottoinsiemi di  $B$  sono gli stessi di  $A$ . Si ha che

$$\begin{aligned} f^{-1}(\emptyset) &= \emptyset, & f^{-1}(\{1\}) &= \{2,3\}, & f^{-1}(\{2\}) &= \{1\}, & f^{-1}(\{3\}) &= \emptyset, \\ f^{-1}(\{1,2\}) &= \{1,2,3\}, \dots \end{aligned}$$

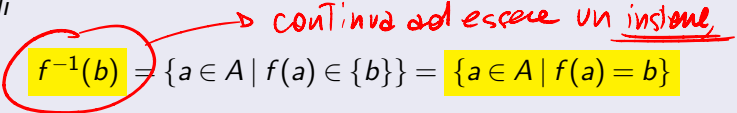
$$\begin{aligned} \text{Quindi } \mathcal{G} &= \{\emptyset, \{2,3\}, \{1\}, \emptyset, \{1,2,3\}, \{2,3\}, \{1\}, \{1,2,3\}\} = \\ &= \{\emptyset, \{1\}, \{2,3\}, \{1,2,3\}\}. \end{aligned}$$



## Osservazione

Vediamo alcuni casi particolari dove  $f : A \rightarrow B$ ,  $A' \subseteq A$  e  $B' \subseteq B$ .

- 1 Se  $A' = A$ ,  $f(A)$  si indica anche con  $\text{Im}(f)$  ed è detta *immagine di  $f$* .
- 2 Se  $B' = B$ ,  $f^{-1}(B) = \{a \in A \mid f(a) \in B\} = A$ .
- 3 Se  $B' = \{b\}$  scriveremo semplicemente  $f^{-1}(b)$  in luogo di  $f^{-1}(\{b\})$ .  
Quindi


$$f^{-1}(b) = \{a \in A \mid f(a) \in \{b\}\} = \{a \in A \mid f(a) = b\}$$

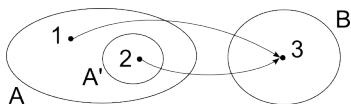
è l'insieme delle controimmagini di  $b$  in  $A$ .

## Esercizio

Sia  $f : A \rightarrow B$  una funzione,  $A' \subseteq A$  e  $B' \subseteq B$ .

- 1 Dimostrare che  $A' \subseteq f^{-1}(f(A'))$ , che l'uguaglianza non vale in generale ma che vale se  $f$  è iniettiva.
- 2 Dimostrare che  $f(f^{-1}(B')) \subseteq B'$ , che l'uguaglianza non vale in generale ma che vale se  $f$  è suriettiva.

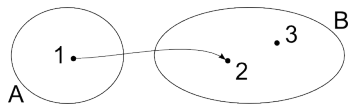
**SOLUZIONE.** ① Vediamo che  $A' \subseteq f^{-1}(f(A'))$ . Si ha  $a' \in A' \Rightarrow f(a') \in f(A') \Rightarrow a' \in f^{-1}(f(A'))$ . L'uguaglianza non vale in generale. Ad esempio, se  $f: \{1, 2\} \rightarrow \{3\}, a \mapsto 3$  e  $A' := \{2\}$ , allora  $f(A') = \{f(2)\} = \{3\}$  da cui  $f^{-1}(f(A')) = f^{-1}(\{3\}) = \{1, 2\} \neq A'$ .



Supponiamo  $f$  iniettiva e dimostriamo  $f^{-1}(f(A')) \subseteq A'$ :

$a \in f^{-1}(f(A')) \Rightarrow f(a) \in f(A') \Rightarrow \exists a' \in A', f(a) = f(a') \stackrel{f \text{ iniet.}}{\Rightarrow} a = a' \Rightarrow a \in A'$ .

② Vediamo che  $f(f^{-1}(B')) \subseteq B'$ . Sia  $b \in f(f^{-1}(B'))$ . Allora esiste  $a \in f^{-1}(B')$  tale che  $b = f(a)$ . D'altra parte  $a \in f^{-1}(B')$  significa  $f(a) \in B'$  e in definitiva  $b \in B'$ . L'uguaglianza non vale in generale. Infatti, se  $f: \{1\} \rightarrow \{2, 3\}, 1 \mapsto 2$  e  $B' := \{2, 3\}$ , allora  $f^{-1}(B') = \{1\}$  e quindi  $f(f^{-1}(B')) = f(\{1\}) = \{2\} \neq B'$ .



Supponiamo  $f$  suriettiva e dimostriamo  $B' \subseteq f(f^{-1}(B'))$ . Se  $b' \in B'$  allora esiste  $a \in A$  tale che  $b' = f(a)$ . Ma allora  $f(a) \in B'$  e quindi  $a \in f^{-1}(B')$ . Pertanto  $b' = f(a) \in f(f^{-1}(B'))$  da cui  $B' \subseteq f(f^{-1}(B'))$ .

*perché surr.*



## Esercizio (per casa)

Sia  $f : A \rightarrow B$  una funzione. Stabilire se  $\{f^{-1}(b) \mid b \in \text{Im}(f)\}$  è una partizione di  $A$ . Dimostrare che  $\{f^{-1}(b) \mid b \in B\}$ , è una partizione di  $A$  se e solo se  $f$  è suriettiva. Stabilire se  $\{f^{-1}(S) \mid S \subseteq \text{Im}(f)\}$  è una partizione di  $A$ .

## Esercizio

Si consideri la funzione  $f : \mathbb{R} \times \mathbb{Z} \rightarrow \mathbb{R}, (x, y) \mapsto x\sqrt{2} + y$ .

- 1 Dire se  $f$  è iniettiva e/o suriettiva.
- 2 Determinare  $f(A)$  dove  $A := \{(\sqrt{2}, a) \mid a \in \mathbb{Z}\}$ .
- 3 Determinare  $f^{-1}(0)$  e  $f^{-1}(\mathbb{Z})$ .

SOLUZIONE. ① Se  $x_1, x_2 \in \mathbb{R}, y_1, y_2 \in \mathbb{Z}$ , son tali che  $f((x_1, y_1)) = f((x_2, y_2))$ , allora  $x_1\sqrt{2} + y_1 = x_2\sqrt{2} + y_2$  vale a dire  $(x_1 - x_2)\sqrt{2} = y_2 - y_1$ . Ad esempio  $(\sqrt{2} - 0)\sqrt{2} = 2 - 0$  e quindi  $(\sqrt{2}, 0) \neq (0, 2)$  hanno la stessa immagine. Allora  $f$  non è iniettiva.

$\forall r \in \mathbb{R}$ , abbiamo  $r = \frac{r}{\sqrt{2}}\sqrt{2} + 0 = f\left(\left(\frac{r}{\sqrt{2}}, 0\right)\right)$  e quindi  $f$  è suriettiva.

② Visto che  $f : \mathbb{R} \times \mathbb{Z} \rightarrow \mathbb{R}, (x, y) \mapsto x\sqrt{2} + y$ , abbiamo  
 $f(A) = \{f(z) \mid z \in A\} = \{f((\sqrt{2}, a)) \mid a \in \mathbb{Z}\} = \{2 + a \mid a \in \mathbb{Z}\} = \mathbb{Z}$ .

③ Abbiamo visto che  $f$  non è iniettiva. Pertanto non è invertibile. Allora non esiste  $f^{-1}$ . Invece esiste sempre la controimmagine:

$$f^{-1}(0) = f^{-1}(\{0\}) = \{(x, y) \in \mathbb{R} \times \mathbb{Z} \mid f((x, y)) = 0\}.$$

Ora  $f((x, y)) = 0$  significa  $x\sqrt{2} + y = 0$  da cui  $x = -\frac{y}{\sqrt{2}}$ . Allora  
 $f^{-1}(0) = \{(-\frac{y}{\sqrt{2}}, y) \mid y \in \mathbb{Z}\}$ . Invece:

$$f^{-1}(\mathbb{Z}) = \{(x, y) \in \mathbb{R} \times \mathbb{Z} \mid f((x, y)) \in \mathbb{Z}\}.$$

Ora  $f((x, y)) \in \mathbb{Z}$  significa

$$\exists z \in \mathbb{Z}, x\sqrt{2} + y = z \Leftrightarrow \exists z \in \mathbb{Z}, x\sqrt{2} = \overbrace{z - y}^w \Leftrightarrow \exists w \in \mathbb{Z}, x\sqrt{2} = w.$$

Quindi  $f^{-1}(\mathbb{Z}) = \{(\frac{w}{\sqrt{2}}, y) \mid w, y \in \mathbb{Z}\}$ .

# Assiomi di Peano e dimostrazione per induzione

Finora abbiamo usato l'insieme  $\mathbb{N}$  dei numeri naturali senza introdurlo perché già visto scuola. Vogliamo ora discutere come questo insieme possa essere definito in modo assiomatico attraverso i cosiddetti Assiomi di Peano, pubblicati nel 1889.

## (Assiomi di Peano)

L'insieme  $\mathbb{N}$  è caratterizzato dai seguenti assiomi:

- P1) esiste un elemento 0 in  $\mathbb{N}$  detto **zero**;
- P2) esiste una funzione iniettiva  $s : \mathbb{N} \rightarrow \mathbb{N}$  detta **successore** tale che  $0 \notin \text{Im}(s)$ ;
- P3) se  $X \subseteq \mathbb{N}$  è tale che  $0 \in X$  e **se per ogni  $n \in X$  anche  $s(n) \in X$**  allora **deve risultare  $X = \mathbb{N}$** .

L'assioma P1 garantisce che  $\mathbb{N} \neq \emptyset$ . L'assioma P2 dice che  $s$  è iniettiva ma non suriettiva: come vedremo più avanti, questo implica che  $\mathbb{N}$  non è un insieme finito. L'assioma P3 è detto anche **principio di induzione**.

Il principio di induzione implica che gli elementi

$$0, \quad s(0), \quad s(s(0)), \quad s(s(s(0))), \quad \dots \quad (4)$$

comprendono tutti gli elementi di  $\mathbb{N}$ . Infatti l'insieme  $X$  i cui elementi sono gli elementi di  $\mathbb{N}$  che appaiono in (4) soddisfa le richieste dell'assioma P3:  $0 \in X$  e per costruzione  $X$  contiene il successore di ogni suo elemento. Gli elementi in (4) li indichiamo così

$$0, \quad \underbrace{s(0)}_1, \quad \underbrace{s(s(0))}_2, \quad \underbrace{s(s(s(0)))}_3, \quad \dots$$

$$0 \quad s(0)$$

↓

$$0, s(0), s(s(0))$$

↓

$$0, s(0), s(s(0)), s(s(s(0)))$$

Possiamo dunque scrivere

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

Notiamo inoltre che

$$1 = s(0), \quad 2 = s(1), \quad 3 = s(2), \quad \dots$$

eccetera.

SOMMA. Una volta definito l'insieme  $\mathbb{N}$  possiamo definire la somma  $m + m'$  di numeri naturali  $m, m'$ . Fissato  $m \in \mathbb{N}$ , allora  $m'$  potrà essere 0 oppure il successore  $s(n)$  di un altro numero  $n$ . Distinguiamo dunque questi due casi. Nel primo caso si definisce

$$m + 0 := m.$$

Nel secondo caso, dando per noto  $m + n$ , si definisce

$$m + s(n) := s(m + n).$$

Quello appena dato è un esempio di definizione **ricorsiva** (il cui fondamento teorico si può dimostrare a partire dal principio di induzione).

Chiaramente, come risulta subito ponendo  $n = 0$  nell'ultima formula, la somma è definita in modo che risulti  $s(m) = m + 1$  per ogni  $m \in \mathbb{N}$ .

PRODOTTO. Il prodotto è definito similmente ponendo

$$m \cdot 0 := 0 \quad \text{e} \quad m \cdot s(n) := m \cdot n + m.$$

## Teorema (Dimostrazione per induzione)

Sia  $\mathcal{P}(n)$  una proposizione dipendente da un numero naturale  $n$ .  
Supponiamo che

- PASSO INIZIALE o BASE:

$\mathcal{P}(0)$  è vera.

- PASSO INDUTTIVO:

per ogni numero naturale  $n$ , se  $\mathcal{P}(n)$  è vera allora  $\mathcal{P}(n+1)$  è vera.  
*ipotesi induttiva*

Allora  $\mathcal{P}(n)$  è vera per tutti i numeri naturali  $n$ , in simboli:  $\forall n \in \mathbb{N}, \mathcal{P}(n)$ .

### Proof.

Sia  $X \subseteq \mathbb{N}$  l'insieme dei numeri naturali per cui  $\mathcal{P}(n)$  è vera.

- Il passo iniziale dice che  $0 \in X$ .
- Il passo induttivo dice che se  $n \in X$  allora  $n+1 = s(n) \in X$ .

Dunque per il principio di induzione  $X = \mathbb{N}$ .

In altre parole  $\mathcal{P}(n)$  è vera per ogni  $n \in \mathbb{N}$ . □

# Effetto domino

Visualizziamo la dimostrazione per induzione tramite l'*effetto domino*. Immaginiamo delle tessere del domino allineate e numerate (da 0).

Indichiamo con  $\mathcal{P}(n)$  l'affermazione "la tessera  $n$  cade".

Affinché cadano tutte occorre accertarsi che

- (PASSO INIZIALE) la prima tessera cada ( $\mathcal{P}(0)$  è vera);
- (PASSO INDUTTIVO) ogni tessera che cade faccia cadere quella successiva ( $\forall n \in \mathbb{N}, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ ).

