

## Chapter 2

# Insiemi, relazioni e funzioni

In questo capitolo introdurremo altre due importanti nozioni della teoria degli insiemi, quella di *relazione su un insieme* e quella di *funzione tra due insiemi*.

Per dare delle definizioni rigorose, abbiamo bisogno di introdurre prima una nuova operazione che si può fare per ottenere un nuovo insieme a partire da due insiemi dati, quella di *prodotto cartesiano*.

**Definizione 2.1.** Dati due insiemi  $A$  e  $B$ , si dice il *prodotto cartesiano di  $A$  per  $B$*  e si denota  $A \times B$  l'insieme di tutte le *coppie ordinate*  $(a, b)$  dove  $a$  è un elemento di  $A$  e  $b$  è un elemento di  $B$ : in simboli

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Dare una coppia ordinata  $(a, b)$  significa dare non solo due elementi  $a$  e  $b$  ma significa anche specificare che  $a$  è il primo e  $b$  è il secondo: in questo  $(a, b)$  si differenzia da  $\{a, b\}$  (l'insieme degli elementi  $a$  e  $b$ ) nel quale non importa l'ordine di  $a$  e  $b$  ma solo la loro appartenenza all'insieme dato<sup>1</sup>. Quindi, in generale,  $(a, b) \neq (b, a)$  (a meno che non sia  $a = b$ ).

**Esempio 2.2.** Siano  $A = \{0, 1, 2, 3\}$  e  $B = \{3, 4\}$ . Ad esempio, la coppia  $(0, 3)$  appartiene a  $A \times B$  in quanto la sua prima componente, 0, appartiene ad  $A$  e la seconda, 3, appartiene a  $B$ . Si ha in effetti

$$A \times B = \{(0, 3), (0, 4), (1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$$

Si noti che il numero degli elementi di  $A \times B$  è dato dal prodotto del numero degli elementi di  $A$  per il numero degli elementi di  $B$  (infatti, per ogni

---

<sup>1</sup>Se volessimo dare una definizione insiemistica e rigorosa della coppia  $(a, b)$ , questa potrebbe essere  $(a, b) = \{\{a, b\}, \{a\}\}$ : l'insieme con due elementi ci dice chi sono i due elementi che compongono la coppia, l'insieme con un solo elemento ci dice chi è il primo della coppia. Tuttavia, non useremo mai tale definizione rigorosa.

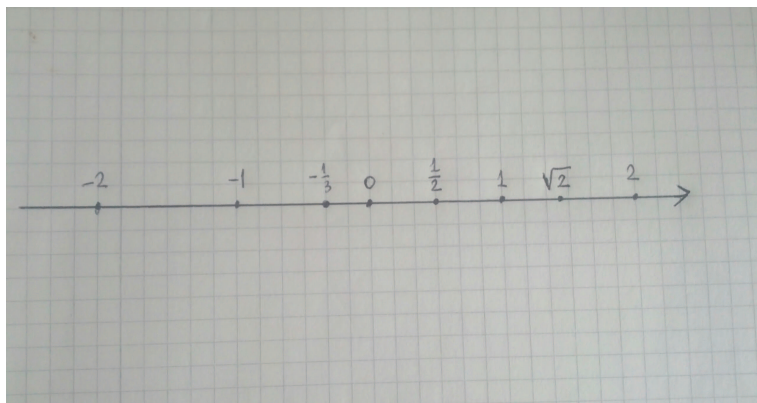
elemento di  $A$  scelto come primo elemento della coppia, il secondo elemento può essere scelto tra uno qualunque degli elementi di  $B$ ).

Si può anche considerare il prodotto di un insieme per se stesso, ad esempio se  $A = \{1, 2, 3\}$  si ha

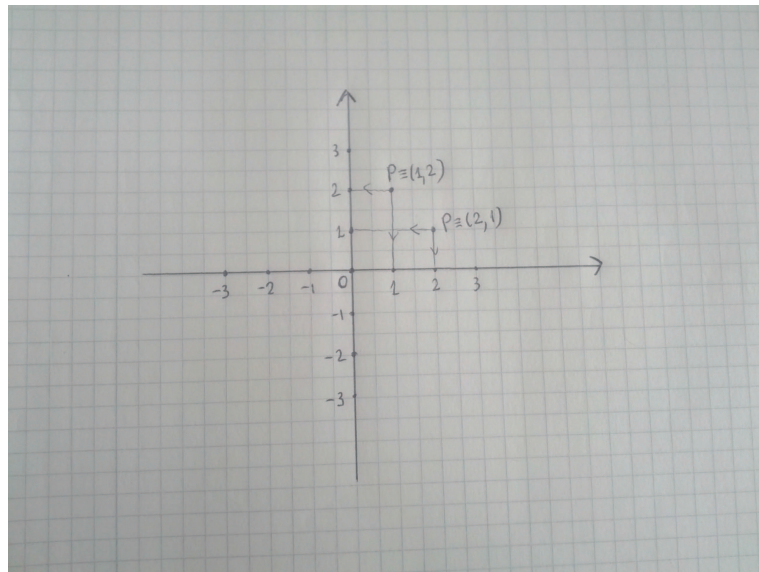
$$A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

Il prodotto cartesiano  $A \times A$  di un insieme con se stesso si denota anche  $A^2$ , con una notazione presa in prestito da quella usata per il prodotto usuale tra numeri dove effettivamente si denota  $a \cdot a = a^2$ .

**Osservazione 2.3.** Il prodotto cartesiano  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  ha particolare importanza in geometria in quanto, fissato un sistema di coordinate cartesiane, rappresenta l'insieme dei punti del piano: più precisamente, sappiamo che i numeri reali si possono rappresentare come i punti di una retta scegliendo prima un punto per rappresentare lo 0, poi a distanza fissata (da noi scelta come unità di misura) gli interi, positivi da un lato e negativi dall'altro (quindi la retta risulta orientata), poi inserendo le frazioni tra i numeri interi e infine i restanti numeri reali che non possono essere rappresentati come frazioni (gli *irrazionali*, ovvero i numeri decimali con infinite cifre dopo la virgola, non periodici):



A questo punto, se nel piano scegliamo due rette orientate, perpendicolari tra loro e che si incontrano nel punto scelto per lo 0 (dette *assi cartesiani*), a ogni punto  $P$  si può assegnare una coppia di numeri reali (le sue *coordinate*) che sono determinati proiettando  $P$  sui due assi.



Si noti che è importante che le coordinate siano rappresentate mediante una coppia ordinata, in quanto ad esempio il punto di coordinate  $(1, 2)$  è diverso dal punto di coordinate  $(2, 1)$ .

Il prodotto cartesiano può anche essere definito per più di due insiemi: ad esempio, per 3 insiemi  $A, B, C$  basta usare invece della nozione di coppia ordinata quella di *terna ordinata*  $(a, b, c)$ , nella quale, analogamente a quanto fatto per la coppia, diamo tre elementi in un ordine assegnato, e definire

$$A \times B \times C = \{(a, b, c) \mid a \in A \wedge b \in B \wedge c \in C\}$$

In generale, possiamo generalizzare tale definizione a un numero arbitrario di insiemi  $A_1, A_2, \dots, A_n$ : in tal caso, useremo la nozione di *n-upla ordinata*  $(a_1, a_2, \dots, a_n)$  (che coincide con una coppia per  $n = 2$  e con una terna per  $n = 3$ ) e definiremo

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}$$

Analogamente a quanto già detto per il prodotto tra due insiemi, denoteremo  $A^n$  il prodotto cartesiano  $A \times A \times \dots \times A$  di  $A$  con se stesso  $n$  volte.

Vedremo in un capitolo successivo che il prodotto  $\mathbb{R}^n$  ha una particolare importanza in algebra vettoriale.

Siamo ora pronti a definire in modo rigoroso cosa è una *relazione* su un insieme.

## 2.1 Relazioni

Introduciamo la definizione rigorosa di relazione su un insieme tramite un esempio concreto: supponiamo che  $X$  sia un insieme i cui elementi sono persone, e supponiamo che alcuni elementi dell'insieme siano figli di altri sempre appartenenti all'insieme dato: in altre parole, alcuni elementi dell'insieme  $X$  sono legati dalla relazione padre-figlio ad altri elementi di  $X$ .

Per raccogliere l'informazione su quali sono gli elementi di  $X$  in tale relazione tra loro, si può fare ricorso proprio alla nozione di coppia ordinata: ogniqualevolta si ha che  $x$  è figlio di  $x'$  per due elementi  $x, x' \in X$ , formiamo la coppia ordinata  $(x, x')$ : l'insieme delle coppie così costruite è un sottoinsieme del prodotto cartesiano  $X \times X$  che ci dice esattamente chi è figlio di chi all'interno dell'insieme.

Si noti che per avere l'informazione giusta è necessario usare la coppia *ordinata*, perchè distinguendo tra la prima componente e la seconda ci dice quale dei due elementi è figlio dell'altro (informazione che perderemmo se usassimo solo l'insieme  $\{x, x'\}$ , che ci direbbe solo che tra  $x$  e  $x'$  uno è figlio dell'altro senza specificare chi).

Questo ci porta alla seguente definizione generale:

**Definizione 2.4.** Una relazione su un insieme  $X$  è un sottoinsieme del prodotto cartesiano  $X \times X$ .

**Esempio 2.5.** Consideriamo sull'insieme dei numeri naturali la relazione “essere minore di”: allora tale relazione è rappresentata dal sottoinsieme  $S$  (infinito) di tutte le coppie  $(n, m)$  di numeri naturali in cui  $n < m$ :

$$S = \{(0, 1), (0, 2), \dots, (1, 2), (1, 3), \dots\}$$

Se invece la relazione fosse quella di uguaglianza, il sottoinsieme sarebbe

$$S = \{(0, 0), (1, 1), (2, 2), (3, 3) \dots\}$$

in cui ogni elemento è in relazione solo con se stesso (in quanto uguale solo a se stesso).

Quando un elemento  $x \in X$  è nella relazione data con un altro  $x' \in X$ , useremo la simbologia  $x \sim x'$ .

Come abbiamo osservato sopra, abbiamo usato le coppie ordinate per formalizzare la definizione di relazione perchè in generale può essere  $x \sim x'$  ma non  $x' \sim x$ : ad esempio, per la relazione “essere figlio di”, se  $x$  è figlio di  $x'$  sicuramente  $x'$  non è figlio di  $x$ .

Tuttavia, per alcune relazioni succede che

$$x \sim x' \Rightarrow x' \sim x \quad (2.1)$$

In tal caso, si dice che la relazione è *simmetrica*.

Ad esempio, la relazione di uguaglianza è simmetrica in quanto se  $x = x'$  sicuramente possiamo anche scrivere  $x' = x$ .

Un'altra proprietà soddisfatta dalla relazione di uguaglianza ma non dalle relazioni in generale, è che per ogni  $x \in X$  si ha

$$x \sim x \quad (2.2)$$

ovvero ogni elemento è in relazione con se stesso (nel caso dell'uguaglianza, chiaramente questo vale in quanto  $x = x$ ); la relazione “essere minore di” non soddisfa questa proprietà in quanto  $x < x$  non è verificata.

Quando vale questa proprietà, si dice che la relazione è *riflessiva*.

Infine, l'uguaglianza soddisfa una terza importante proprietà:

$$x \sim x' \text{ e } x' \sim x'' \Rightarrow x \sim x'' \quad (2.3)$$

ovvero se un elemento è in relazione con un secondo, e questo secondo in relazione con un terzo, allora il primo è in relazione con il terzo.

Quando vale ciò, la relazione si dice *transitiva*.

L'uguaglianza è chiaramente una relazione transitiva in quanto se  $x = x'$  e  $x' = x''$ , allora  $x = x''$ ; anche la relazione “essere minore di” soddisfa tale proprietà in quanto  $x < x'$  e  $x' < x''$  implica  $x < x''$ ; la relazione “essere figlio di” invece non è neanche transitiva, in quanto se  $x$  è figlio di  $x'$  e  $x'$  è figlio di  $x''$ , non è vero che  $x$  è figlio di  $x''$  (sarà semmai il nipote di  $x''$ ).

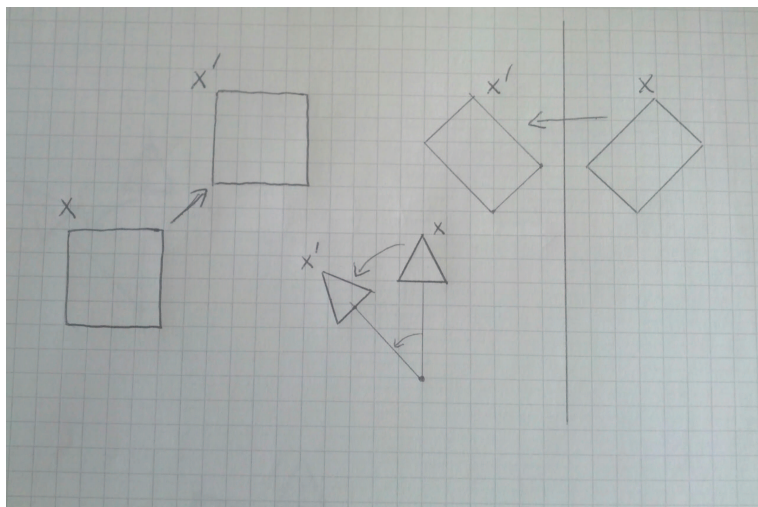
Diamo allora la seguente

**Definizione 2.6.** Una relazione su un insieme  $X$  che sia riflessiva, simmetrica e transitiva si dice *relazione di equivalenza*.

Quindi la relazione di uguaglianza è una relazione di equivalenza. In generale, una relazione di equivalenza è una sorta di “uguaglianza in senso largo”, che ci dice come identificare, ovvero considerare in un qualche senso uguali, oggetti che uguali non sono.

Come esempio significativo di questa affermazione, consideriamo l'esempio seguente: sia  $X$  l'insieme delle *figure* del piano, ovvero quadrati, triangoli, circonferenze e in generale qualunque insieme di punti.

Definiamo su tale insieme la seguente relazione: date due figure  $x$  e  $x'$ , diciamo che  $x \sim x'$  se  $x'$  può essere ottenuta da  $x$  traslando, ruotando o riflettendo  $x$  rispetto a qualche retta (ovvero applicando quelli che si chiamano *movimenti rigidi*), come nel disegno seguente



Vediamo che si tratta di una relazione di equivalenza (che si chiama *congruenza*): se  $x \sim x'$ , ovvero  $x'$  si ottiene da  $x$  mediante traslazioni, rotazioni o riflessioni, allora anche  $x' \sim x$ , in quanto  $x$  si può riottenere da  $x'$  applicando le trasformazioni inverse nell'ordine inverso: quindi abbiamo la simmetria.

Inoltre, se  $x \sim x'$  e  $x' \sim x''$ , questo significa che  $x'$  si ottiene da  $x$  mediante certi movimenti rigidi, e  $x''$  si ottiene da  $x'$  mediante altri movimenti di tale tipo: ma allora anche  $x''$  si ottiene da  $x$  mediante movimenti rigidi (e quindi  $x \sim x''$ ): basta applicare in sequenza quelli che servono prima per ottenere  $x'$  e poi quelli che servono per ottenere  $x''$  da  $x'$ . Quindi abbiamo anche la transitività.

Quanto alla riflessività, ovvero  $x \sim x$ , possiamo dire che vale in quanto  $x$  si ottiene da se stesso applicando per esempio una rotazione di angolo 0.

Ora, questo esempio fa capire perché, come abbiamo detto sopra, una relazione di equivalenza può essere considerata come una sorta di uguaglianza in senso largo: i due quadrati della figura precedente, così come i due triangoli o i due rettangoli, pur essendo figure diverse (non sono formate dagli stessi punti, quindi non possiamo dire che siano veramente uguali), tuttavia rappresentano tutte in un certo senso “la stessa figura”.

**Esempio 2.7.** Tra le relazioni di parentela, un esempio di relazione di equivalenza è “essere fratello di”, nel senso di avere gli stessi genitori. La riflessività è chiara, in quanto ogni  $x$  ha gli stessi genitori di se stesso; la simmetria anche, dal momento che se  $x$  è fratello di  $x'$ , anche  $x'$  è fratello di  $x$ ; e infine si ha anche la transitività, in quanto se  $x$  è fratello di  $x'$  e  $x'$  è fratello di  $x''$ , allora è chiaro che  $x$  è fratello di  $x''$ .

Quando si ha una relazione di equivalenza, tutti gli elementi equivalenti tra loro possono essere raggruppati insieme, in quella che si chiama *classe di equivalenza*. Più precisamente, sia  $X$  un insieme sul quale è definita una relazione, e sia  $x \in X$ . Si chiama classe di equivalenza di  $x$  l'insieme

$$[x] = \{y \in X \mid y \sim x\} \quad (2.4)$$

ovvero l'insieme di tutti gli elementi  $y$  che stanno in relazione con (ovvero che sono equivalenti a)  $x$ .

Elementi diversi  $x$  e  $x'$  possono dar luogo alla stessa classe di equivalenza, ovvero  $[x] = [x']$ : questo accade esattamente quando  $x \sim x'$ , come affermato nella seguente

**Proposizione 2.8.** Data una relazione di equivalenza  $\sim$  su un insieme  $X$ , e dati  $x, x' \in X$ , si ha  $[x] = [x'] \Leftrightarrow x \sim x'$ .

*Proof.* Trattandosi di una doppia implicazione, dobbiamo dimostrare sia  $[x] = [x'] \Rightarrow x \sim x'$  che  $x \sim x' \Rightarrow [x] = [x']$ .

Per dimostrare la prima implicazione, ricordiamoci che, per definizione di uguaglianza tra insiemi,  $[x] = [x']$  significa che ogni elemento della classe  $[x]$  sta anche nella classe  $[x']$  e viceversa ogni elemento di  $[x']$  appartiene anche a  $[x]$ . Ma nella classe  $[x]$  c'è sicuramente  $x$  stesso, perchè essendo la relazione di equivalenza riflessiva vale  $x \sim x$ , e quindi  $x \in \{y \in X \mid y \sim x\} = [x]$ . Quindi, essendo  $x \in [x]$  e  $[x] = [x']$ , si ha anche  $x \in [x']$ , ovvero  $x \sim x'$ , come volevamo.

Per dimostrare l'implicazione inversa  $x \sim x' \Rightarrow [x] = [x']$ , dobbiamo far vedere che (sotto l'ipotesi  $x \sim x'$ ), ogni elemento di  $[x]$  appartiene anche a  $[x']$  e viceversa.

Sia  $y \in [x]$ : questo significa che  $y \sim x$ ; ma poiché abbiamo  $x \sim x'$ , possiamo applicare la transitività delle relazioni di equivalenza e concludere che  $y \sim x'$ , ovvero  $y \in [x']$ : abbiamo allora dimostrato che ogni elemento di  $[x]$  sta anche in  $[x']$ , ovvero che  $[x] \subseteq [x']$ . Per dimostrare che vale proprio l'uguaglianza, prendiamo viceversa un  $y \in [x']$ : questo significa che  $y \sim x'$ . Combinando con  $x' \sim x$  (l'ipotesi sarebbe  $x \sim x'$ , ma è la stessa cosa visto che una relazione di equivalenza è anche simmetrica) e applicando la transitività si ottiene  $y \sim x$ , ovvero  $y \in [x]$ . Quindi è vero anche che ogni elemento di  $[x']$  sta in  $[x]$ , cioè abbiamo finalmente  $[x] = [x']$ .  $\square$

Le classi di equivalenza hanno l'importante proprietà di ripartire l'insieme  $X$  su cui è definita la relazione in sottoinsiemi non vuoti e disgiunti, come affermato nella seguente

**Proposizione 2.9.** Data una relazione di equivalenza  $\sim$  su un insieme  $X$ , le classi di equivalenza hanno le seguenti tre proprietà:

- (i) per ogni  $x \in X$ , si ha  $[x] \neq \emptyset$
- (ii) l'unione  $\bigcup_{x \in X} [x]$  di tutte le classi di equivalenza è uguale a tutto  $X$
- (iii) due classi di equivalenza diverse sono disgiunte, ovvero  $[x] \neq [x'] \Rightarrow [x] \cap [x'] = \emptyset$

*Proof.* La (i) si dimostra semplicemente ricordando (lo abbiamo visto nella dimostrazione della Proposizione 2.8) che  $x$  appartiene sempre alla sua classe di equivalenza  $[x]$ , quindi questa non è sicuramente vuota.

Per dimostrare la (ii), in base alla definizione di unione basta mostrare che ogni elemento di  $X$  sta in almeno una classe di equivalenza: ma questo è vero per quanto appena detto, in quanto ogni elemento  $x$  sta almeno nella sua classe  $[x]$ .

Per dimostrare la (iii), dimostriamo la sua contronominale

$$[x] \cap [x'] \neq \emptyset \Rightarrow [x] = [x'] \quad (2.5)$$

che come sappiamo dal capitolo precedente è equivalente all'implicazione in (iii).

L'ipotesi  $[x] \cap [x'] \neq \emptyset$  significa che esiste un  $z$  che appartiene sia a  $[x]$  che a  $[x']$ : ma questo per definizione di classe vuol dire che valgono sia  $z \sim x$  (o, equivalentemente visto che la relazione è simmetrica,  $x \sim z$ ) che  $z \sim x'$ : mettendo insieme  $x \sim z$  e  $z \sim x'$ , per la transitività abbiamo  $x \sim x'$ . Ma la Proposizione 2.8 ci dice che allora  $[x] = [x']$ , e la (2.5) è dimostrata.  $\square$

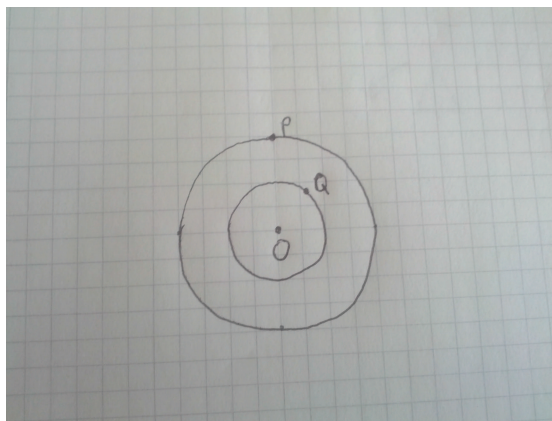
In generale, una famiglia di sottoinsiemi di un insieme dato  $X$  che sia fatta di sottoinsiemi non vuoti, disgiunti e la cui unione sia tutto  $X$  si chiama una *partizione di  $X$* . Quindi, la proposizione appena dimostrata afferma che una relazione di equivalenza su  $X$  determina una partizione di  $X$  (in classi di equivalenza).

**Esempio 2.10.** Ad esempio, si consideri l'insieme  $X$  dei punti del piano, si fissi un punto  $O$  e per ogni  $P, P' \in X$ , si ponga  $P \sim P'$  quando  $|OP| = |OP'|$  (cioè quando i due punti sono alla stessa distanza da  $O$ ).

È facile vedere che si tratta di una relazione di equivalenza: si ha  $P \sim P$  in quanto ovviamente  $|OP| = |OP|$ ; inoltre  $P \sim P'$  implica  $P' \sim P$  in quanto  $|OP| = |OP'|$  implica (per simmetria della relazione di uguaglianza)  $|OP'| = |OP|$ , e infine se  $P \sim P'$  e  $P' \sim P''$ , ovvero  $|OP| = |OP'|$  e

$|OP'| = |OP''|$ , visto che l'uguaglianza gode della proprietà transitiva si ha  $|OP| = |OP''|$ , ovvero  $P \sim P''$ .

Chi sono le classi di equivalenza di questa relazione? Dato un punto  $P$ , che dista  $|OP| = R$  da  $O$ , la sua classe di equivalenza è data da tutti i punti che distano anch'essi  $R$  da  $O$ , ovvero è la circonferenza centrata in  $O$  su cui si trova  $P$



Questo esempio illustra quindi bene come le classi di equivalenza diano una partizione dell'insieme dato, in questo caso il piano: due circonferenze di raggio diverso sono disgiunte e la loro unione, al crescere del raggio, ci dà tutto il piano<sup>2</sup>.

**Esempio 2.11.** Se la relazione di equivalenza è l'uguaglianza, ogni classe di equivalenza contiene un solo elemento, cioè  $[x] = \{x\}$ : in questo caso la partizione è quella in singoli elementi.

**Osservazione 2.12.** Notiamo che se definissimo anche per una relazione  $\sim$  che non sia di equivalenza le classi mediante la (2.4), ovvero dicendo che la classe  $[x]$  di  $x$  è l'insieme di tutti gli elementi in relazione con  $x$ , non sarebbe più vero che tali classi determinano una partizione.

Ad esempio, consideriamo un insieme di quattro individui  $a_1, a_2, a_3, a_4$  nel quale  $a_2$  e  $a_3$  sono figli di  $a_1$  e  $a_4$  è figlio di  $a_2$ .

Rispetto alla relazione “essere figlio di”, allora, la classe di  $a_1$  (cioè l'insieme degli  $x$  tali che  $x$  è figlio di  $a_1$ ) è  $\{a_2, a_3\}$ , la classe di  $a_2$  è  $\{a_4\}$ , mentre le classi di  $a_3$  e  $a_4$  sono vuote, in quanto non esistono figli di  $a_3$  e  $a_4$  nell'insieme dato.

---

<sup>2</sup>Si noti che la classe di equivalenza di  $O$  contiene solo  $O$ , ovvero è una circonferenza di raggio 0.

Quindi non vale la (i) della Proposizione 2.9 (ci sono classi vuote) e neanche la (iii), in quanto unendo le classi  $\{a_2, a_3\}$ ,  $\{a_4\}$  e le due classi vuote si ottiene  $\{a_2, a_3, a_4\}$ , che non è tutto l'insieme.

Per vedere invece un esempio di relazione non di equivalenza in cui non vale la (iii) della Proposizione 2.9, si prenda ad esempio l'insieme  $\mathbb{N}$  dei numeri naturali e la relazione  $<$  (minore).

Allora, la classe di 0 è vuota (non esiste nessun  $x < 0$ ), la classe di 1 è  $\{0\}$  (zero è l'unico numero naturale per cui  $x < 1$  è verificata), la classe di 2 è  $\{0, 1\}$ , di 3 è  $\{0, 1, 2\}$  e così via: come si vede, ci sono classi diverse che non sono disgiunte, diversamente da quanto affermato dalla (iii) della Proposizione 2.9 nel caso di relazioni di equivalenza.

Nel prossimo capitolo studieremo un'altra importante relazione di equivalenza sull'insieme  $\mathbb{Z}$  degli interi che ci porterà a comprendere alcuni moderni metodi crittografici.

Per dare un'anticipazione, illustrata da un esempio concreto, prendiamo l'insieme degli interi  $\mathbb{Z}$  e supponiamo che lo 0 rappresenti la mezzanotte di un dato giorno fissato, mentre ogni intero positivo (risp. negativo) rappresenti il numero di ore successive (risp. precedenti) alla mezzanotte.

Decidiamo di considerare equivalenti due interi  $x$  e  $y$  se essi corrispondono alla stessa ora del giorno (eventualmente di giorni diversi): definiamo cioè la relazione (nel capitolo successivo, dimostreremo che si tratta di una relazione di equivalenza<sup>3</sup>)  $x \sim y$  se e solo se la differenza tra  $x$  e  $y$  è un multiplo di 24. Ad esempio, 0, 24, 48, -24 sono equivalenti in quanto rappresentano la mezzanotte (rispettivamente del giorno in questione, del giorno successivo, di due giorni dopo e del giorno precedente). +1, +25, +49, -23 sono equivalenti in quanto rappresentano l'una del mattino (rispettivamente del giorno in questione, del giorno successivo, di due giorni dopo e del giorno precedente). Si noti che se al posto di 24 avessimo scelto 2, ovvero avessimo definito due numeri sono equivalenti se e solo se la loro differenza è un multiplo di 2, avremmo avuto due sole classi di equivalenza: la classe di 0, data da  $\{0, \pm 2, \pm 4, \pm 6 \dots\}$ , e la classe di 1, data da  $\{\pm 1, \pm 3, \pm 5, \pm 7 \dots\}$ : in altre parole, la partizione di  $\mathbb{Z}$  determinata da questa relazione è quella in numeri pari e numeri dispari.

---

<sup>3</sup>Anzi dimostreremo più in generale che, fissato un qualunque  $k$ , se per due interi  $n, m$  si definisce  $n \sim m$  se e solo se la differenza  $n - m$  è un multiplo di  $k$  questo dà una relazione di equivalenza.

## 2.2 Funzioni

Vedremo ora un'altra nozione fondamentale per tutta la matematica, quella di *funzione*.

Dati due insiemi  $X$  e  $Y$ , una funzione  $f$  da  $X$  a  $Y$  (si scrive  $f : X \rightarrow Y$ ) è una legge che assegna ad ogni elemento  $x$  di  $X$  un ben preciso elemento di  $Y$ , che si chiama *l'immagine* di  $x$  e si denota  $f(x)$ . Per dire che  $x$  viene mandato dalla funzione in  $f(x)$ , si scrive anche  $x \mapsto f(x)$ . Il tutto si scrive spesso nel modo seguente:

$$f : X \longrightarrow Y \\ x \mapsto f(x)$$

L'insieme  $X$  di partenza si dice *dominio* della funzione, quello  $Y$  di arrivo *codominio*.

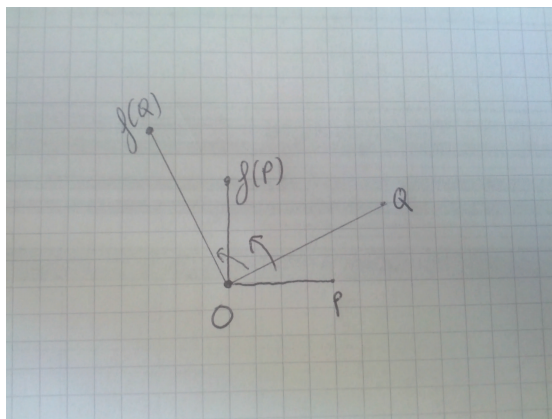
**Esempio 2.13.** Ad esempio, sia  $X$  l'insieme degli studenti presenti in un'aula e sia  $Y$  l'insieme  $\mathbb{N}$  dei numeri naturali. Associando a ogni studente  $x$  il suo numero di matricola, si ottiene una funzione  $X \rightarrow \mathbb{N}$ .

In questo esempio, la funzione rappresenta l'assegnazione di un dato a ogni entrata di una lista.

Le funzioni possono essere anche usate per descrivere l'andamento di un dato fenomeno: si consideri ad esempio un corpo che a un certo istante di tempo parte da un punto  $O$  e inizia a muoversi lungo una traiettoria rettilinea. Identificando i punti della retta con i numeri reali, come descritto nell'Osservazione 2.3, con il punto  $O$  in corrispondenza dello zero, possiamo assegnare a ogni  $t \in \mathbb{R}$  che rappresenti il tempo trascorso dall'istante iniziale (se  $t$  è positivo, altrimenti sia il tempo precedente all'istante iniziale) la posizione  $x(t)$  del corpo sulla retta lungo cui si muove: questo definisce una funzione  $\mathbb{R} \rightarrow \mathbb{R}$  che descrive il moto del corpo.

Ancora, le funzioni possono rappresentare delle operazioni, ad esempio la funzione  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  che assegna a ogni numero intero  $n$  il suo quadrato  $f(n) = n^2$ ; non otteniamo invece una funzione  $\mathbb{Z} \rightarrow \mathbb{Z}$  definendo  $f(n) = \sqrt{n}$ , perché alcuni elementi del dominio non hanno immagine nel codominio, ad esempio se  $n = 2$  o  $n = -1$ , tali elementi non hanno immagine nel codominio in quanto  $f(n) = \sqrt{2}$  e  $f(n) = \sqrt{-1}$  non sono numeri interi (il secondo non è neanche un numero reale).

Infine, come ultimo esempio, le funzioni possono rappresentare trasformazioni di tipo geometrico: se  $X$  è l'insieme dei punti del piano, scelto un punto  $O$  possiamo definire una funzione  $X \rightarrow X$  assegnando a ogni punto  $P$  il punto  $f(P)$  che si ottiene ruotando  $P$  attorno a  $O$  di un angolo di 90 gradi in senso antiorario.



**Osservazione 2.14.** La definizione di funzione data sopra è sufficiente per gli scopi di questo corso ma non è la definizione rigorosa e formale di funzione, che afferma che una funzione da un insieme  $X$  a un insieme  $Y$  è un sottoinsieme  $S$  del prodotto cartesiano  $X \times Y$  che per ogni  $x \in X$  contiene una e una sola coppia  $(x, y)$  che ha  $x$  come prima componente (in simboli<sup>4</sup>,  $\forall x \in X \exists! y \in Y (x, y) \in S$ )

In pratica, l'idea è di rappresentare l'informazione che a  $x$  stiamo assegnando un certo  $y \in Y$  tramite la coppia  $(x, y)$ : la richiesta che per ogni  $x$  esista un'unica coppia che ha  $x$  come primo elemento traduce il fatto che a ogni  $x$  dobbiamo assegnare un ben preciso  $y$  (uno e uno solo).

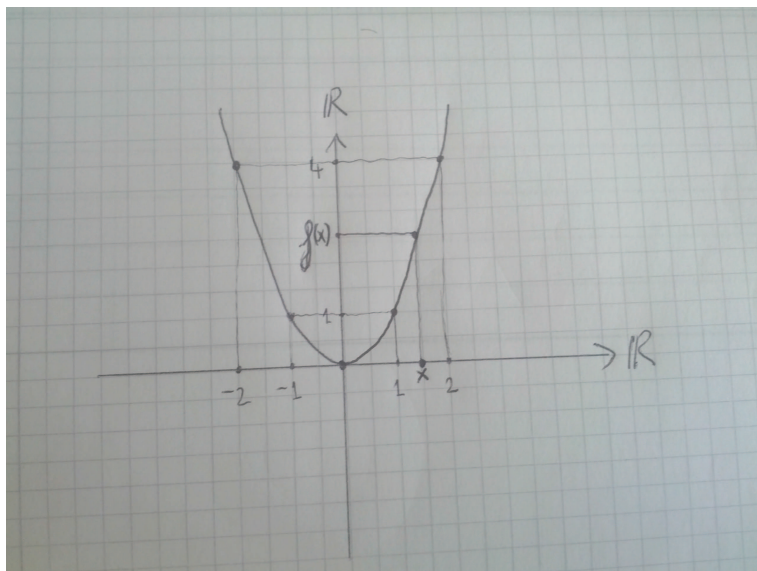
L'idea che una funzione  $f : X \rightarrow Y$  sia definita da un sottoinsieme del prodotto cartesiano  $X \times Y$  non è tanto sorprendente se si pensa che ogni funzione  $f : \mathbb{R} \rightarrow \mathbb{R}$  può essere rappresentata mediante il suo grafico, che può essere pensato proprio come un sottoinsieme del prodotto cartesiano  $\mathbb{R} \times \mathbb{R}$ : più precisamente, se come già descritto nell'Osservazione 2.3 consideriamo un sistema di coordinate per cui a ogni punto del piano corrisponde una coppia  $(x, y)$  di numeri reali e viceversa (e quindi il piano si identifica con il prodotto cartesiano  $\mathbb{R} \times \mathbb{R}$ ), possiamo rappresentare una funzione  $f : \mathbb{R} \rightarrow \mathbb{R}$

disegnando l'insieme dei punti che hanno come prima coordinata  $x$  e come seconda coordinata l'immagine  $f(x)$  (per ogni  $x \in \mathbb{R}$ ).

Ad esempio, se la funzione fosse  $f(x) = x^2$  si avrebbe

---

<sup>4</sup>Il quantificatore universale  $\exists$ , seguito dal punto esclamativo, significa “esiste un unico”.



L'insieme di punti così ottenuto (nel disegno dato la parabola) è quindi un sottoinsieme del piano, che è come dire un sottoinsieme del prodotto cartesiano  $\mathbb{R} \times \mathbb{R}$ , che rappresenta la funzione.

Consideriamo ora alcune proprietà delle funzioni.

Iniziamo con l'osservare che la definizione di funzione non impedisce che due elementi diversi del dominio abbiano la stessa immagine: ad esempio, la funzione quadrato  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  considerata sopra che assegna a ogni  $n \in \mathbb{Z}$  l'intero  $f(n) = n^2$  è tale che  $f(2) = f(-2) = 4$ .

Questo fatto non accade ad esempio invece per la funzione  $X \rightarrow \mathbb{N}$  che assegna a ogni studente di una certa aula il suo numero di matricola, in quanto non è possibile che studenti diversi abbiano lo stesso numero di matricola.

Alla luce di questi due esempi, diamo la seguente

**Definizione 2.15.** Una funzione  $f : X \rightarrow Y$  si dice *iniettiva* se due elementi diversi del dominio hanno sempre immagini diverse, in simboli

$$x \neq x' \Rightarrow f(x) \neq f(x')$$

Quindi, la funzione che assegna a ogni studente il suo numero di matricola è iniettiva, mentre la funzione quadrato da  $\mathbb{Z}$  in  $\mathbb{Z}$  non è iniettiva.

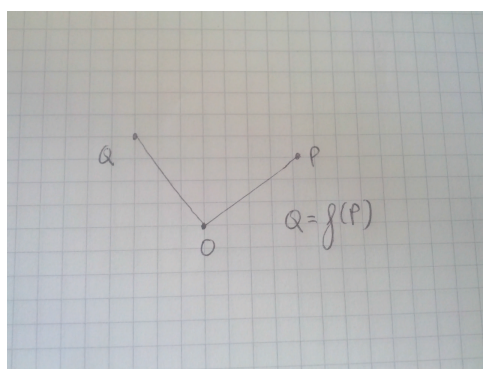
**Osservazione 2.16.** Usando il fatto che ogni implicazione è equivalente alla sua contronominale, possiamo anche dire che una funzione  $f$  è iniettiva se

per ogni  $x, x' \in X$  si ha  $f(x) = f(x') \Rightarrow x = x'$  (ovvero se l'unica possibilità per cui  $x$  e  $x'$  abbiano la stessa immagine sia che  $x = x'$ ).

Tale riformulazione è spesso più conveniente quando si vuole dimostrare che una funzione data è iniettiva: se volessi verificare ad esempio che la funzione  $f : \mathbb{N} \rightarrow \mathbb{N}$  data da  $f(n) = n + 1$  è iniettiva, dovrei dimostrare l'implicazione  $f(n) = f(m) \Rightarrow n = m$  ovvero  $n + 1 = m + 1 \Rightarrow n = m$ : ma questo è quasi immediato in quanto da  $n + 1 = m + 1$ , portando l'1 del primo membro a secondo si ottiene subito  $n = m + 1 - 1 = m$ .

Un'altra particolarità sia della funzione  $X \rightarrow \mathbb{N}$  che assegna a ogni studente il suo numero di matricola sia della funzione quadrato  $\mathbb{Z} \rightarrow \mathbb{Z}$  è che non tutti gli elementi del codominio sono immagine di qualche elemento del dominio: non tutti i numeri naturali sono numeri di matricola di qualche studente, esattamente come non tutti gli interi sono quadrati di qualche intero di partenza (ad esempio, 5 non è quadrato, ovvero non è della forma  $n^2$  per nessun  $n \in \mathbb{Z}$ ).

Invece, ad esempio per la rotazione che abbiamo definito nell'Esempio 2.13, cioè la funzione  $f : X \rightarrow X$  dal piano  $X$  in se stesso e che manda ogni punto  $P$  nel punto  $f(P)$  che si ottiene ruotando  $P$  di 90 gradi in senso antiorario, questo non succede in quanto qualunque punto  $Q$  del codominio  $X$  è immagine  $f(P)$  di qualche punto  $P$  del dominio (basta prendere come  $P$  il punto che si ottiene ruotando  $Q$  in senso *orario*, come si vede nel disegno seguente)



Diamo allora la seguente

**Definizione 2.17.** Una funzione  $f : X \rightarrow Y$  si dice *suriettiva* se per ogni  $y \in Y$  esiste un  $x \in X$  tale che  $y = f(x)$ .

Quindi, sia la funzione  $X \rightarrow \mathbb{N}$  che assegna a ogni studente il suo numero di matricola che la funzione quadrato su  $\mathbb{Z}$  sono non suriettive, mentre la rotazione del piano in sè è suriettiva.

In effetti, quest'ultima è anche iniettiva. Tali funzioni sono particolarmente importanti nella teoria:

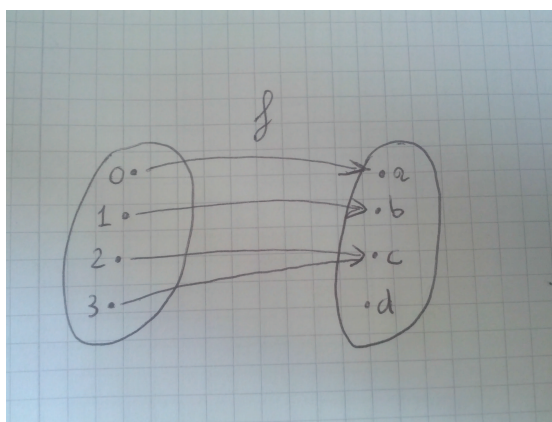
**Definizione 2.18.** Una funzione  $f : X \rightarrow Y$  si dice *biiettiva* se è sia iniettiva che suriettiva.

Una funzione biiettiva si chiama anche *biiezione* o *corrispondenza biunivoca*.

Un modo alternativo di definire l'iniettività è usare il concetto di *controimmagine*. Data una funzione  $f : X \rightarrow Y$ , e dato un elemento  $y \in Y$ , si dice controimmagine di  $y$  (e si denota  $f^{-1}(y)$ ) l'insieme di tutti gli elementi di  $X$  che vanno a finire in  $y$  quando applichiamo la  $f$ , in simboli

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

Ad esempio, si consideri la funzione  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c, d\}$  rappresentata nel seguente disegno



Si ha  $f^{-1}(a) = \{0\}$ ,  $f^{-1}(b) = \{1\}$ ,  $f^{-1}(c) = \{2, 3\}$ ,  $f^{-1}(d) = \emptyset$ .

Questo esempio mostra che la controimmagine di un elemento di  $Y$  potrebbe anche essere vuota (se la funzione non è suriettiva, certamente esistono elementi  $y \in Y$  tali che nessun  $x \in X$  soddisfa  $f(x) = y$ ). Chiaramente, una funzione è iniettiva se non succede mai che  $f^{-1}(y)$  abbia più di un elemento, perchè in tal caso vorrebbe dire che ci sono elementi diversi di  $X$  che vanno a finire in  $y$ . In altre parole, possiamo dire che *una funzione  $f : X \rightarrow Y$  è iniettiva se e solo se tutte le controimmagini degli elementi di  $Y$  hanno al massimo un elemento*.

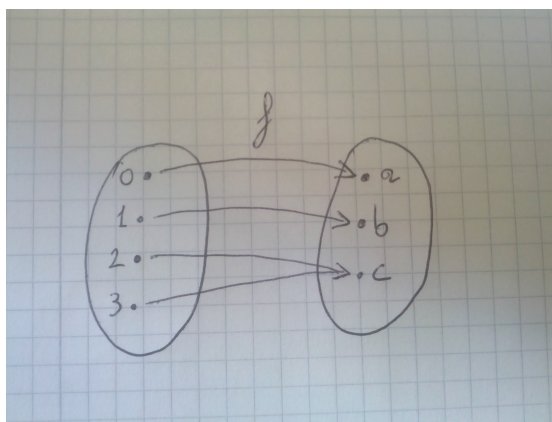
Anche la suriettività ammette una definizione alternativa, basata sul concetto di *immagine della funzione*. L'immagine di una funzione  $f : X \rightarrow Y$  (denotata  $Im(f)$ ) è semplicemente l'insieme di tutte le immagini degli elementi di  $X$ , in simboli

$$Im(f) = \{y \in Y \mid y = f(x) \text{ per qualche } x \in X\}$$

Ad esempio, nella funzione  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c, d\}$  vista sopra si ha  $Im(f) = \{a, b, c\}$  (solo  $d$  non si scrive come immagine di qualche elemento del dominio). Allora, è chiaro che una funzione è suriettiva solo se  $Im(f) = Y$ , in quanto questa uguaglianza si verifica esattamente quando ogni elemento  $y \in Y$  si scrive come  $y = f(x)$  per qualche  $x \in X$ , che è proprio la definizione di suriettività.

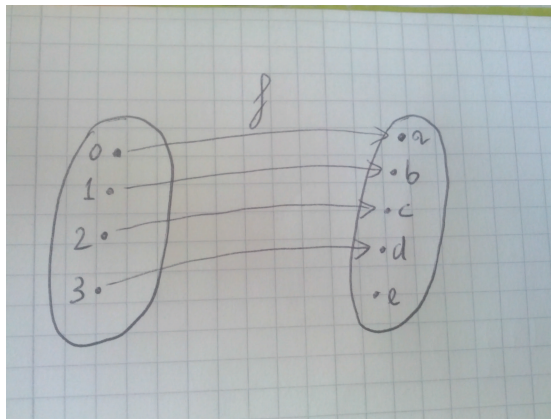
Osserviamo che iniettività e suriettività sono nozioni indipendenti: una funzione può essere iniettiva e non suriettiva, suriettiva e non iniettiva, nessuna delle due o entrambe.

Ad esempio, la funzione  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c\}$  rappresentata dal seguente disegno



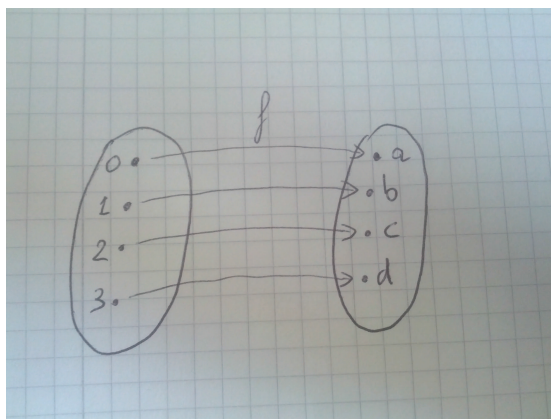
(ovvero  $f(0) = a$ ,  $f(1) = b$ ,  $f(2) = c$ ,  $f(3) = c$ ) è suriettiva (in quanto ogni elemento  $a, b, c$  del codominio è immagine di qualche elemento del dominio) ma non iniettiva in quanto esistono due elementi diversi del dominio (ovvero 2 e 3) che hanno la stessa immagine.

Invece, la funzione  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c, d, e\}$  rappresentata dal seguente disegno



è iniettiva ma non suriettiva (c'è un elemento del codominio, ovvero  $e$ , che non è immagine di nessun elemento del dominio).

Infine, la funzione  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c, d\}$  rappresentata dal seguente disegno



è sia iniettiva che suriettiva, ovvero biiettiva.

Osserviamo che non c'è nessuna possibile scelta delle immagini di  $0, 1, 2, 3$  nella prima delle tre funzioni precedenti che la renda una funzione iniettiva: infatti, essendoci più elementi nel dominio che nel codominio, almeno due elementi dovranno avere per forza la stessa immagine. In generale, dati due insiemi finiti  $X$  e  $Y$ , il primo con  $|X|$  elementi e il secondo con  $|Y|$  elementi, abbiamo che

$$|X| > |Y| \Rightarrow f : X \rightarrow Y \text{ non è iniettiva} \quad (2.6)$$

o equivalentemente, usando la contronominale,

$$f : X \rightarrow Y \text{ è iniettiva} \Rightarrow |X| \leq |Y| \quad (2.7)$$

**Osservazione 2.19.** La (2.6) si chiama anche *principio della piccionaia* (se  $X$  è un insieme di piccioni e  $Y$  è un insieme di gabbie, e dobbiamo mettere ogni piccione in una gabbia, se ci sono più piccioni che gabbie almeno due piccioni dovranno essere messi nella stessa gabbia), e a dispetto della sua elementarità può essere usato per dimostrare fatti a prima vista non banali. Ad esempio, usando tale principio possiamo dimostrare che nel mondo esistono almeno due persone con lo stesso numero di capelli. Infatti, sia  $X$  l'insieme delle persone del mondo, che quindi diciamo contiene 8 miliardi di elementi, e consideriamo la funzione  $f$  che assegna a ogni persona il numero dei suoi capelli. Stimando che il numero massimo  $N$  di capelli che possono essere contenuti in una testa sia sicuramente minore di 8 miliardi, la funzione  $f$  sarà una funzione  $X \rightarrow Y = \{0, 1, 2, 3, \dots, N\}$  tale che  $|X| > |Y|$ : quindi in base al principio enunciato essa non può essere iniettiva, ovvero esistono almeno due elementi del dominio (due persone) con la stessa immagine (lo stesso numero di capelli).

Analogamente, per quello che riguarda la seconda delle tre funzioni rappresentate nei disegni sopra, ovvero la  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c, d, e\}$ , non c'è nessuna possibile scelta alternativa delle immagini che la renda una funzione suriettiva: infatti, essendoci nel dominio meno elementi che nel codominio, non è possibile raggiungere tutti gli elementi del codominio facendo partire una freccia da tutti gli elementi del dominio. Analogamente a sopra, possiamo dire che in generale dati due insiemi finiti  $X$  e  $Y$ , il primo con  $|X|$  elementi e il secondo con  $|Y|$  elementi, abbiamo che

$$|X| < |Y| \Rightarrow f : X \rightarrow Y \text{ non è suriettiva} \quad (2.8)$$

o equivalentemente, usando la contronominale,

$$f : X \rightarrow Y \text{ è suriettiva} \Rightarrow |X| \geq |Y| \quad (2.9)$$

Dal momento che le funzioni biietive sono sia iniettive che suriettive, combinando la (2.7) e la (2.9) otteniamo

$$f : X \rightarrow Y \text{ è biiettiva} \Rightarrow |X| = |Y| \quad (2.10)$$

**Osservazione 2.20.** La (2.10) ci dice che se esiste una funzione biiettiva tra due insiemi *finiti*, allora essi hanno lo stesso numero di elementi, e non è

difficile verificare anche il viceversa: se il numero di elementi di  $X$  e  $Y$  è lo stesso, allora non è difficile costruire una funzione biettiva  $X \rightarrow Y$ .

Nel caso in cui  $X$  e  $Y$  siano insiemi infiniti, parlare di numero di elementi sembra non avere più senso, o al più verrebbe spontaneo dire che due insiemi infiniti hanno lo stesso numero di elementi (infinito, appunto). Tuttavia, se decidiamo, procedendo per analogia con gli insiemi finiti, di dire anche per due insiemi infiniti  $X$  e  $Y$  che essi hanno lo stesso numero di elementi se esiste una funzione biettiva  $X \rightarrow Y$ , allora scopriremo che *non tutti gli insiemi infiniti hanno lo stesso numero di elementi* (detto anche *cardinalità*). Per illustrare tale affermazione, usiamo come esempi gli insiemi numerici  $\mathbb{N}$  (i numeri naturali),  $\mathbb{Z}$  (i numeri interi),  $\mathbb{Q}$  (i numeri razionali),  $\mathbb{R}$  (i numeri reali), che sono inclusi uno nel successivo:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Iniziamo con il chiederci se esiste una funzione biettiva  $\mathbb{N} \rightarrow \mathbb{Z}$ : questo significherebbe che è possibile associare a ogni naturale un intero in modo da non lasciare scoperto nessun intero e da non ripetere due volte lo stesso intero, o in altre parole mettere gli interi in una successione infinita  $a_0, a_1, a_2, \dots$ .

La risposta è affermativa, ad esempio gli interi possono essere messi in sequenza come segue:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \dots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \dots \end{array}$$

Dunque esiste una corrispondenza biunivoca tra  $\mathbb{N}$  e  $\mathbb{Z}$ , ovvero possiamo dire che i naturali e gli interi hanno lo stesso numero di elementi.

Mentre da una parte questo può risultare banale (si potrebbe pensare che avendo entrambi infiniti elementi, necessariamente questi debbano poter essere messi in corrispondenza biunivoca), dall'altra il risultato ha un aspetto sorprendente: dal momento che  $\mathbb{N}$  si identifica con un sottoinsieme di  $\mathbb{Z}$  (quello degli interi non negativi), stiamo dicendo che  $\mathbb{Z}$  ha lo stesso numero di elementi di un suo sottoinsieme proprio<sup>5</sup>. Questo fatto non è possibile per insiemi finiti: esso caratterizza gli insiemi infiniti ed è spesso assunto come definizione di insieme infinito (ovvero, un insieme si dice infinito se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio).

Anche i razionali  $\mathbb{Q}$  possono essere messi in corrispondenza biunivoca con i naturali. Per mostrare come, consideriamo per facilità solo i razionali posi-

---

<sup>5</sup>Si dice sottoinsieme proprio di un insieme  $X$  un sottoinsieme che non sia  $X$  stesso (in base alla definizione di sottoinsieme, vale sempre l'inclusione  $X \subseteq X$ , ovvero ogni insieme è sottoinsieme di se stesso).

tivi (il ragionamento si riesce ad aggiustare poi per tutti i razionali), che si scrivono come quoziente  $n/m$  di due naturali  $n, m$  (con  $m \neq 0$ ).

Consideriamo la seguente tabella infinita di frazioni dove, nella riga  $n$ -esima, scriviamo le frazioni con numeratore uguale a  $n$ :

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|
| 1/1 | 1/2 | 1/3 | 1/4 | 1/5 | ... |
| 2/1 | 2/2 | 2/3 | 2/4 | 2/5 | ... |
| 3/1 | 3/2 | 3/3 | 3/4 | 3/5 | ... |
| 4/1 | 4/2 | 4/3 | 4/4 | 4/5 | ... |
| ... |     |     |     |     |     |

Chiaramente in questa tabella alcune frazioni rappresentano lo stesso razionale (1/2 e 2/4, oppure 1/1 e 2/2) ma se riusciamo a mostrare che è possibile realizzare una corrispondenza biunivoca tra le entrate della tabella e i naturali, a maggior ragione questo sarà vero per i razionali che corrispondono alle entrate della tabella senza ripetizioni.

La corrispondenza cercata con le frazioni della tabella si può per esempio realizzare scrivendo in sequenza tutte le diagonali della tabella a partire dall'angolo in alto a sinistra: prima 1/1, poi la diagonale adiacente 1/2, 2/1, poi continuando a scendere verso destra la terza diagonale 1/3, 2/2, 3/1 e così via.

$$1/1, 1/2, 2/1, 1/3, 2/2, 3/1, 1/4, 2/3, 3/2, 4/1, \dots$$

In questo modo, si riesce a mettere in una sequenza (ovvero in corrispondenza con i numeri naturali) tutti i razionali, e realizzare una funzione biiettiva  $\mathbb{N} \rightarrow \mathbb{Q}$  che ci dice che anche  $\mathbb{N}$  e  $\mathbb{Q}$  hanno lo stesso numero di elementi.

Questi esempi potrebbero generare l'idea che qualunque insieme infinito possa essere messo in corrispondenza biunivoca con l'insieme dei naturali. In realtà questo è falso: si dimostra che per l'insieme  $\mathbb{R}$  dei numeri reali questa corrispondenza non esiste.

Un'idea della dimostrazione è la seguente: supponiamo per assurdo di poter mettere in una sequenza in corrispondenza biunivoca con i numeri naturali tutti i numeri reali:  $x_0, x_1, x_2, x_3, \dots$

Rappresentando ogni reale con la sua rappresentazione decimale, possiamo riscrivere tale sequenza come

$$x_0 = a_0, b_0 c_0 d_0 \dots$$

$$x_1 = a_1, b_1 c_1 d_1 \dots$$

$$x_2 = a_2, b_2 c_2 d_2 \dots$$

$$x_3 = a_3, b_3 c_3 d_3 \dots$$

...

Ora, mostreremo che in realtà una tale sequenza non può mai contenere tutti i numeri reali, e lo faremo costruendo esplicitamente un numero reale che non è contenuto nella sequenza, il numero

$$x = 0, bcd \dots$$

in cui  $b, c, d, \dots$  sono definiti come segue:  $b = 1$  se  $b_0 = 0$  e  $b = 0$  se  $b_0 \neq 0$  (questo garantisce già che  $x$  non sia il primo numero della sequenza  $x_0$ );  $c = 1$  se  $c_1 = 0$  e  $c = 0$  se  $c_1 \neq 0$  (questo garantisce che  $x$  non sia il secondo numero della sequenza  $x_1$ );  $d = 1$  se  $d_2 = 0$  e  $d = 0$  se  $d_2 \neq 0$  (questo garantisce che  $x$  non sia il terzo numero della sequenza  $x_2$ ) e così via.

Dunque,  $\mathbb{R}$  non ha lo stesso numero di elementi di  $\mathbb{N}$  (pur essendo entrambi gli insiemi infiniti), e poichè  $\mathbb{R}$  contiene  $\mathbb{N}$  possiamo dire che  $\mathbb{R}$  ha una cardinalità strettamente maggiore di quella di  $\mathbb{N}$ .

Non esiste dunque un unico “infinito”, ma infiniti di tipo diverso. È lecito chiedersi se  $\mathbb{R}$  sia il maggiore infinito possibile: la risposta è no, infatti, dato un qualunque insieme infinito, ne esiste sicuramente sempre uno di cardinalità più grande. Più precisamente, Cantor (al quale si deve la teoria degli insiemi infiniti che stiamo illustrando) mostrò che dato un insieme  $X$ , l'insieme costituito dai sottoinsiemi di  $X$  (detto *insieme potenza* e denotato  $P(X)$ ) ha sempre cardinalità maggiore di  $X$ . Quindi, ad esempio, se vogliamo un insieme che abbia cardinalità maggiore di  $\mathbb{R}$ , basta prendere l'insieme potenza  $P(\mathbb{R})$  di  $\mathbb{R}$ .

Concludiamo dicendo che si dimostra che la cardinalità di  $\mathbb{R}$  coincide con quella dell'insieme potenza di  $\mathbb{N}$ .

L'affermazione che non esistono insiemi di cardinalità compresa tra quella di  $\mathbb{N}$  e quella di  $\mathbb{R}$  si chiama *ipotesi del continuo*: si dimostra che tale affermazione non è né dimostrabile né confutabile nella teoria assiomatica degli insiemi.

## 2.3 Composizione di funzioni

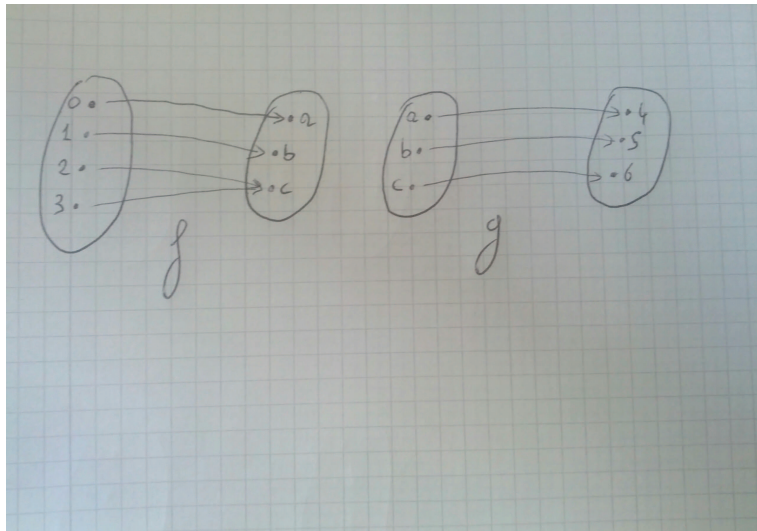
Così come negli insiemi numerici esistono operazioni (somma e prodotto) che dati due numeri ce ne danno un terzo, e nell'algebra di Boole esistono operazioni (le congiunzioni “e” e “o”) che date due proposizioni ne danno una terza, anche per le funzioni, sotto ipotesi opportune, esiste un'operazione che produce una funzione a partire da due funzioni date: tale operazione si chiama *composizione*.

Più precisamente, supponiamo di avere due funzioni  $f : X \rightarrow Y$  e  $g : Y \rightarrow Z$ , tali che *il codominio della prima coincida con il dominio della seconda*. Allora, per ogni elemento  $x \in X$ , possiamo applicare prima  $f$  ottenendo  $f(x) \in Y$ , e poi dal momento che  $Y$  è anche il dominio della  $g$  possiamo applicare la  $g$  a  $f(x)$ , ottenendo  $g(f(x))$ . In questo modo otteniamo una nuova funzione che associa a ogni elemento di  $X$  un elemento di  $Z$ :

$$f : X \longrightarrow Z \\ x \mapsto g(f(x))$$

A causa dell'ordine in cui appaiono le funzioni in  $g(f(x))$ , questa nuova funzione si denota  $g \circ f$  (che si legge “ $g$  composto  $f$ ”).

**Esempio 2.21.** Ad esempio, consideriamo le funzioni  $f : \{0, 1, 2, 3\} \rightarrow \{a, b, c\}$  e  $g : \{a, b, c\} \rightarrow \{4, 5, 6\}$  rappresentate nel seguente disegno



Essendo il codominio di  $f$  uguale al dominio di  $g$ , si può costruire la composizione  $g \circ f$  applicando per ogni elemento di  $\{0, 1, 2, 3\}$  prima  $f$  e poi  $g$ : si ha quindi  $g \circ f : \{0, 1, 2, 3\} \rightarrow \{4, 5, 6\}$ ,

$$(g \circ f)(0) = g(f(0)) = g(a) = 4$$

$$(g \circ f)(1) = g(f(1)) = g(b) = 5$$

$$(g \circ f)(2) = g(f(2)) = g(c) = 6$$

$$(g \circ f)(3) = g(f(3)) = g(c) = 6$$

Si noti che, in questo esempio, la composizione  $f \circ g$  non si può fare, in quanto il codominio di  $g$  non coincide<sup>6</sup> con il dominio di  $f$ : non ha senso provare per esempio a calcolare  $f(g(a)) = f(4)$ .

In alcuni casi hanno senso invece tutte e due le composizioni, ad esempio se  $f : X \rightarrow Y$  e  $g : Y \rightarrow X$  allora hanno senso sia  $g \circ f : X \rightarrow X$  che  $f \circ g : Y \rightarrow Y$ . Chiaramente, se  $X$  e  $Y$  non sono lo stesso insieme si tratta di due funzioni diverse, ovvero si avrà  $g \circ f \neq f \circ g$ , da cui possiamo dire che la composizione di funzioni, quando può essere fatta sia in un ordine che nell'altro, non gode sicuramente della proprietà commutativa.

Questo è vero in generale anche se componiamo due funzioni  $f : X \rightarrow X$  e  $g : X \rightarrow X$ , per le quali si possono fare sia  $g \circ f$  che  $f \circ g$  e sono entrambe funzioni  $X \rightarrow X$ : ad esempio, si considerino le due funzioni

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R}, & f(x) &= x^2 \\ g : \mathbb{R} &\rightarrow \mathbb{R}, & g(x) &= x + 1 \end{aligned}$$

Si ha allora

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1$$

mentre

$$(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1.$$

La composizione di funzioni gode invece sempre della proprietà associativa: più precisamente, date tre funzioni  $f : X \rightarrow Y$ ,  $g : Y \rightarrow Z$ ,  $h : Z \rightarrow W$ , si ha

$$(h \circ g) \circ f = h \circ (g \circ f) \tag{2.11}$$

Infatti, si verifica subito che entrambi i membri di questa uguaglianza sono funzioni  $X \rightarrow W$ ; inoltre, per ogni  $x \in X$ , per definizione di composizione si ha

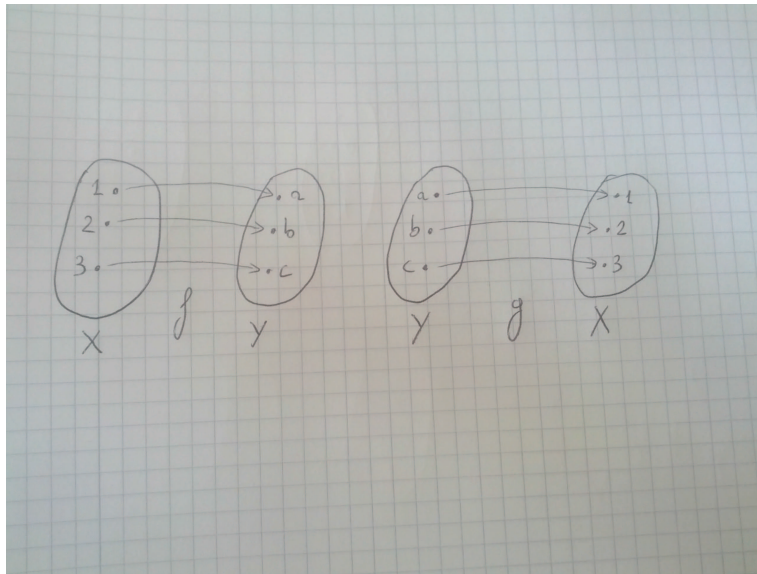
$$\begin{aligned} [(h \circ g) \circ f](x) &= (h \circ g)(f(x)) = h(g(f(x))) \\ [h \circ (g \circ f)](x) &= h((g \circ f)(x)) = h(g(f(x))) \end{aligned}$$

---

<sup>6</sup>In realtà per poter comporre due funzioni  $f : X \rightarrow Y$  e  $g : Y' \rightarrow Z$  basterebbe anche solo che il codominio  $Y$  della prima fosse *contenuto* nel dominio  $Y'$  della seconda: infatti, se  $Y \subseteq Y'$  allora ogni elemento di  $Y$  è anche un elemento di  $Y'$ , quindi  $f(x) \in Y$  sarebbe anche un elemento di  $Y'$  e potremmo applicargli la  $g$  ottenendo  $g(f(x))$ . Tuttavia, per semplicità supporremo sempre che il codominio della prima funzione sia proprio uguale al dominio della seconda.

Grazie a questa proprietà, quando dobbiamo comporre tre (o più) funzioni possiamo scrivere semplicemente  $h \circ g \circ f$ , omettendo le parentesi senza che l'espressione risulti ambigua.

Consideriamo ora  $X = \{1, 2, 3\}$  e  $Y = \{a, b, c\}$  e le funzioni  $f : X \rightarrow Y$  e  $g : Y \rightarrow X$  rappresentate nel disegno seguente:



Come si vede subito, si ha

$$(g \circ f)(1) = g(f(1)) = g(a) = 1$$

$$(g \circ f)(2) = g(f(2)) = g(b) = 2$$

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

ovvero  $g \circ f : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  è la funzione che manda ogni elemento dell'insieme  $X = \{1, 2, 3\}$  in se stesso: tale particolare funzione si chiama *funzione identica di  $X$*  e si denota  $id_X$ . Possiamo quindi scrivere

$$g \circ f = id_X \tag{2.12}$$

Analogamente, si ha

$$(f \circ g)(a) = f(g(a)) = f(1) = a$$

$$(f \circ g)(b) = f(g(b)) = f(2) = b$$

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

ovvero  $f \circ g : \{a, b, c\} \rightarrow \{a, b, c\}$  è la funzione che manda ogni elemento dell'insieme  $Y = \{a, b, c\}$  in se stesso, cioè è la funzione identica  $id_Y$ :

$$f \circ g = id_Y \quad (2.13)$$

Le uguaglianze (2.12) e (2.13) sono analoghe alle uguaglianze

$$a \cdot b = 1, \quad b \cdot a = 1$$

che sussistono quando  $a$  e  $b$  sono due numeri uno l'inverso dell'altro (ad esempio,  $a = 2$  e  $b = \frac{1}{2}$ ). In effetti, per convincersi ulteriormente di quanto questa analogia sia appropriata, osserviamo che così come il numero 1 ha la proprietà di fungere da cosiddetto “elemento neutro per la moltiplicazione”, ovvero  $x \cdot 1 = 1 \cdot x = x$  per ogni numero reale  $x$ , anche le funzioni identiche fungono da elementi neutri per la composizione: più precisamente, se abbiamo una funzione  $f : X \rightarrow Y$ , allora  $f \circ id_X = f$  e  $id_Y \circ f = f$ , in quanto dal momento che la funzione identica manda ogni elemento in se stesso si ha

$$(f \circ id_X)(x) = f(id_X(x)) = f(x)$$

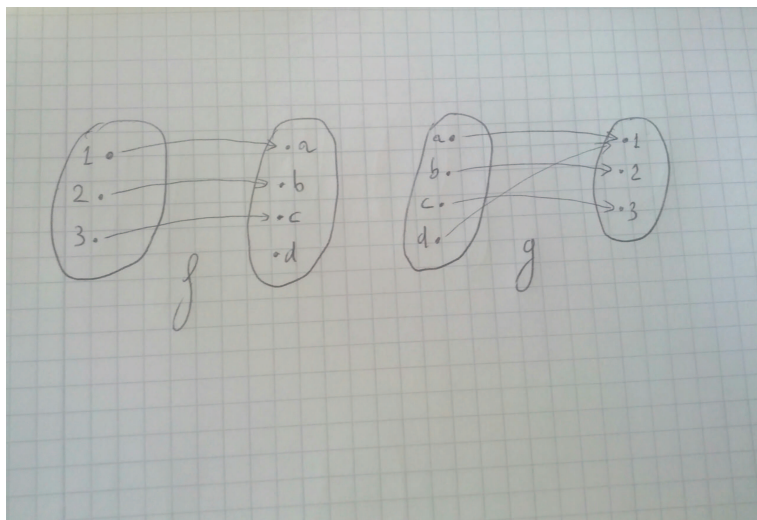
$$(id_Y \circ f)(x) = id_Y(f(x)) = f(x)$$

Questa analogia con quello che accade per numeri uno l'inverso dell'altro ci suggerisce la seguente, importante

**Definizione 2.22.** Una funzione  $f : X \rightarrow Y$  si dice *invertibile* se esiste una funzione  $g : Y \rightarrow X$  per cui  $g \circ f = id_X$  e  $f \circ g = id_Y$ , e in tal caso la funzione  $g$  si dice *inversa di  $f$*  (e la si denota  $f^{-1}$ ).

Mentre nell'insieme dei numeri tutti i numeri sono invertibili tranne lo zero, in quanto non esiste nessun numero reale  $x$  per cui  $x \cdot 0 = 1$ , per le funzioni e la composizione la situazione è un po' più complessa: infatti, esistono funzioni  $f$  per cui vale la  $g \circ f = id_X$  ma  $f \circ g \neq id_Y$ , e in tal caso si dice che  $g$  è solamente un'*inversa sinistra* di  $f$ , oppure funzioni  $f$  per cui viceversa si ha  $f \circ g = id_Y$  ma  $g \circ f \neq id_X$ , e in tal caso si dice che  $g$  è solamente un'*inversa destra* di  $f$ .

Per un esempio di funzione del primo tipo, si prendano  $f : \{1, 2, 3\} \rightarrow \{a, b, c, d\}$  e  $g : \{a, b, c, d\} \rightarrow \{1, 2, 3\}$  definite come nel seguente disegno



Allora, si vede subito che  $g \circ f$  è la funzione identica di  $\{1, 2, 3\}$ , ma  $f \circ g$  non è la funzione identica di  $\{a, b, c, d\}$  in quanto pur essendo  $f(g(a)) = f(1) = a$ ,  $f(g(b)) = f(1) = a$  e  $f(g(c)) = f(2) = b$ , si ha  $f(g(d)) = f(3) = c$ , ovvero  $f \circ g$  non manda  $d$  in se stesso.

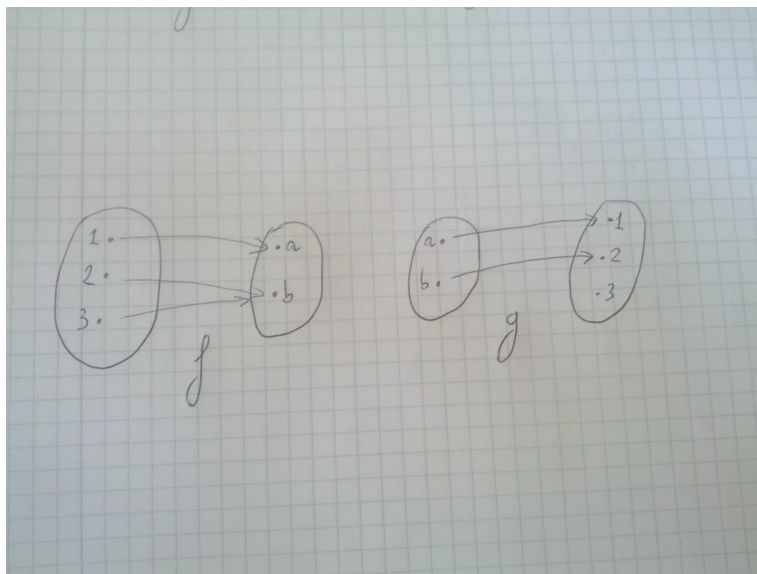
Si osservi che non c'è alcun modo di modificare  $g$  in modo che sia anche un'inversa destra per  $f$ : qualunque valore assegniamo a  $d$  non sarà mai  $f(g(d)) = d$ , perchè  $g(d)$  dovrebbe essere un elemento mandato da  $f$  in  $d$ , ma non esiste nessun elemento di  $\{1, 2, 3\}$  che viene mandato da  $f$  in  $d$ .

In altre parole, il motivo per cui non esiste un'inversa destra di  $f$  è dovuto alla non suriettività di  $f$ . Questo esempio illustra la validità della seguente proposizione, di cui omettiamo la dimostrazione rigorosa.

**Proposizione 2.23.** Una funzione  $f : X \rightarrow Y$  ammette un'inversa destra se e solo se è suriettiva

Analogamente, per un esempio di funzione che ammette un'inversa destra ma non sinistra<sup>7</sup>, si prendano  $f : \{1, 2, 3\} \rightarrow \{a, b\}$  e  $g : \{a, b\} \rightarrow \{1, 2, 3\}$  definite come nel seguente disegno

<sup>7</sup>In realtà basterebbe l'esempio già visto, in cui è  $g$  ad avere  $f$  come inversa destra (ma non sinistra) ma per una maggiore chiarezza facciamo un ulteriore esempio.



Allora, si vede subito che  $f \circ g$  è la funzione identica di  $\{a, b\}$ , ma  $g \circ f$  non è la funzione identica di  $\{1, 2, 3\}$  in quanto pur essendo  $g(f(1)) = g(a) = 1$  e  $g(f(2)) = g(b) = 2$ , si ha  $g(f(3)) = g(b) = 2$ , ovvero  $g \circ f$  non manda 3 in se stesso.

Si osservi che anche qui non c'è alcun modo di modificare  $g$  in modo che sia anche un'inversa sinistra per  $f$ : se avessimo posto  $g(b) = 3$  avremmo sì ottenuto  $g(f(3)) = g(b) = 3$  ma stavolta sarebbe stato  $g(f(2)) = g(b) = 3$ , ovvero  $g \circ f$  non avrebbe mandato 2 in se stesso: come si vede, il problema stavolta è che  $f$  manda i due elementi 2 e 3 entrambi in  $b$ , quindi necessariamente  $g(f(2))$  e  $g(f(3))$  saranno uguali e non potranno mai essere il primo 2 e il secondo 3.

In altre parole, il motivo per cui non esiste un'inversa sinistra di  $f$  è dovuto alla non iniettività di  $f$ . Questo esempio illustra la validità della seguente proposizione, di cui omettiamo la dimostrazione rigorosa.

**Proposizione 2.24.** Una funzione  $f : X \rightarrow Y$  ammette un'inversa sinistra se e solo se è iniettiva

Poiché, per la Definizione 2.22, dire che  $f$  ha un'inversa  $g$  significa dire che  $g$  è sia inversa sinistra che inversa destra, possiamo combinare le due Proposizioni 2.23 e 2.24 ottenendo la

**Proposizione 2.25.** Una funzione  $f : X \rightarrow Y$  ammette un'inversa se e solo se è sia iniettiva che suriettiva (ovvero biiettiva).

Quindi, le funzioni biiettive sono le uniche a essere invertibili.