Indice

CAPITOLO 2

Relazioni

In questo capitolo esaminiamo la nozione di *relazione*. Mostreremo svariate operazioni su relazioni e le leggi algebriche che le regolano. Considereremo poi le seguenti quattro proprietà

TOTALE	*SURGETTIVA*
UNIVALENTE	*INIETTIVA*

che sono necessarie per definire i concetti di *funzione* e *biiezione*. Alla fine del capitolo, utilizzeremo questi concetti per introdurre alcune strutture dati fondamentali in Informatica: le n-uple, le sequenze di lunghezza fissata (array) e le sequenze di lunghezza arbitraria (stringhe).

2.1 Nozioni di Base

Definizione 2.1.1 (Relazione)**.** *Una RELAZIONE R tra l'insieme A e l'insieme B è un sottoinsieme del prodotto cartesiano $A \times B$, quindi $R \subseteq A \times B$. Indicheremo l'insieme di tutte le relazioni tra A e B con la notazione $Rel(A, B)$. Per indicare che R è una relazione tra A e B, cioè $R \in Rel(A, B)$, scriveremo spesso $R \colon A \leftrightarrow B$*

Si noti che dalla definizione segue che $Rel(A, B) = \mathcal{P}(A \times B)$.

Data una relazione $R \colon A \leftrightarrow B$ e due elementi $a \in A$ e $b \in B$, se $(a, b) \in R$ diremo che *a è in relazione R con b*.

Esempio 2.1.2.

- *Se $A = \{x, y\}$ e $B = \{a, b, c\}$, il sottoinsieme*

$$\{(x, a), (x, c)\} \subseteq A \times B \tag{2.1}$$

  è una relazione in $Rel(A, B)$.

- *Per tutti gli insiemi A e B, il prodotto cartesiano $A \times B$ è una relazione in $Rel(A, B)$. Questa viene chiamata RELAZIONE COMPLETA.*

- *Per tutti gli insiemi A e B, $\varnothing \subseteq A \times B$ è una relazione in $Rel(A, B)$. Questa viene chiamata RELAZIONE VUOTA, e viene denotata con $\varnothing_{A,B}$.*

In una relazione $R \colon A \leftrightarrow B$, A è detto *INSIEME DI PARTENZA* e B è detto *INSIEME DI ARRIVO*. Talvolta, l'insieme di partenza e l'insieme di arrivo possono coincidere: durante il corso vedremo molte relazioni di questo tipo, che sono anche argomento del Capitolo 4. Illustriamo come esempi prima le relazioni di parentela tra esseri umani e poi la relazione identità su un qualsiasi insieme A.

Esempio 2.1.3. *Sia U l'insieme di tutti gli esseri umani, e consideriamo le seguenti relazioni di parentela:*

- $Madre = \{(x, y) \in U \times U \mid x \text{ è madre di } y\}$,
- $Padre = \{(x, y) \in U \times U \mid x \text{ è padre di } y\}$,
- $Figlia = \{(x, y) \in U \times U \mid x \text{ è figlia di } y\}$,

- $Figlio = \{(x, y) \in U \times U \mid x \text{ è figlio di } y\}$.

A partire da queste quattro relazioni costruiremo nel seguito tutte le comuni relazioni di parentela, tipo sorella, fratello, zia, ...

Osservazione 2.1.4. *Gli autori di queste note credono nella libertà di ogni essere umano di determinare e definire la propria sessualità, i propri affetti e le proprie relazioni familiari. Rigettano quindi ogni forma di discriminazione sessista ed etero-normativa. Tuttavia in queste note le relazioni familiari considerate saranno spesso riferite a quelle della famiglia così detta* tradizionale. *Tali relazioni infatti sono degli esempi molto convenienti delle varie proprietà che desideriamo illustrare.*

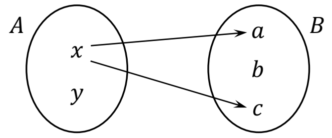
Esempio 2.1.5. *Per tutti gli insiemi A,*

$$\{(x, x) \mid x \in A\} \subseteq A \times A$$

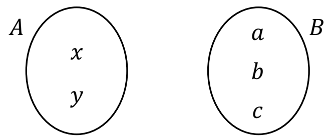
è una relazione. Questa viene chiamata RELAZIONE IDENTITÀ *su A, e viene denotata $Id_A \colon A \leftrightarrow A$.*

Come gli insiemi, anche le relazioni possono essere comodamente visualizzate attraverso dei diagrammi: data una relazione $R \colon A \leftrightarrow B$ questa viene visualizzata disegnando l'insieme A sulla sinistra, l'insieme B sulla destra e inserendo una freccia dall'elemento a all'elemento b per ogni coppia $(a, b) \in R$.

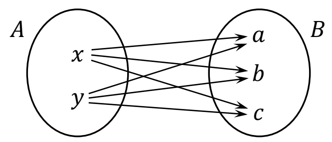
Esempio 2.1.6. *Prendiamo $A = \{x, y\}$ e $B = \{a, b, c\}$ come nell'Esempio 2.1.2. La relazione in (2.1) viene disegnata come*



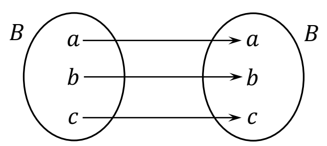
mentre la relazione vuota $\varnothing \colon A \leftrightarrow B$ come



e la relazione completa $A \times B \colon A \leftrightarrow B$ come



Invece, la relazione identità su B, $Id_B \colon B \leftrightarrow B$ è disegnata come



Esercizio 2.1.7. *Sia $A = \{x, y, z\}$ e $B = \{x, y, z, u\}$. Disegnare la relazione $\{(x, x),\ (y, y),\ (z, z)\} \colon A \leftrightarrow B$.*

Quando le relazioni sono molto grandi, o infinite, diventa complicato rappresentarle attraverso diagrammi. Per esempio, per disegnare la relazione $Madre$ su tutti gli esseri umani (Esempio 2.1.3) non basterebbero tutte le pagine di queste dispense. Quando però nelle relazioni c'è una sorta di regola, come per esempio in molte relazioni matematiche si possono usare i punti $(\dots)$ per sottintendere la regola.

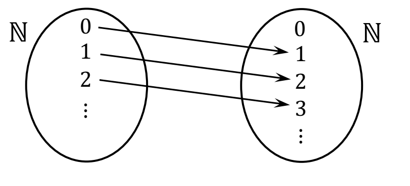
Esempio 2.1.8. *Si consideri la relazione successore*

$$Succ = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x + 1\} \colon \mathbb{N} \leftrightarrow \mathbb{N}$$

dove + denota l'usuale operazione di somma tra numeri. Questa relazione si può anche definire per enumerazione come

$$Succ = \{(0, 1),\ (1, 2),\ (2, 3),\ \dots\} \colon \mathbb{N} \leftrightarrow \mathbb{N}$$

e rappresentare con il seguente diagramma.



Molto spesso l'insieme di partenza è il prodotto cartesiano di due insiemi, cioè $A = A_1 \times A_2$ per qualche insieme A_1, A_2.

Esempio 2.1.9. *Si consideri la relazione*

$$Plus = \{((x, y), z) \mid z = x + y\} \colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$$

dove + denota l'usuale operazione di somma tra numeri. In questo caso l'insieme di partenza è $\mathbb{N} \times \mathbb{N}$*, mentre l'insieme di arrivo è* $\mathbb{N}$.

Questa relazione si può anche definire per enumerazione come

$$\begin{aligned} Plus = \{&((0,0),0),\ ((1,0),1),\ ((2,0),2),\ \dots \\ &((0,1),1),\ ((1,1),2),\ ((2,1),3),\ \dots \\ &\dots \\ \}& \end{aligned}$$

2.2 Operazioni su relazioni

Come gli insiemi, anche le relazioni possono essere combinate in vari modi per ottenere nuove relazioni. In questa sezione illustriamo le principali operazioni su relazioni.

Operazioni insiemistiche su relazioni

Dal momento che ogni relazione è essa stessa un insieme, le relazioni possono essere combinate con tutti gli operatori insiemistici.

Esempio 2.2.1. *Si ricordino le relazioni* $Madre \colon U \leftrightarrow U$ *e* $Padre \colon U \leftrightarrow U$ *dell'Esempio 2.1.3. La relazione* $Genitore \colon U \leftrightarrow U$ *può essere definita come*

$$Genitore = Madre \cup Padre. \tag{2.2}$$

Infatti

$$\begin{aligned} &Madre \cup Padre \\ &= \{(x, y) \in U \times U \mid x \text{ è madre di } y\} \cup \{(x, y) \in U \times U \mid x \text{ è padre di } y\} \\ &= \{(x, y) \in U \times U \mid x \text{ è madre di } y \ \vee \ x \text{ è padre di } y\} \\ &= \{(x, y) \in U \times U \mid x \text{ è madre di } y \text{ oppure } x \text{ è padre di } y\} \\ &= \{(x, y) \in U \times U \mid x \text{ è genitore di } y\} \end{aligned}$$

Esercizio 2.2.2. *Si definisca attraverso unione, la relazione*

$$Figli* = \{(x, y) \in U \times U \mid x \text{ è figlio o figlia di } y\}.$$

Quando si compongono relazioni attraverso le operazioni insiemistiche si deve però fare sempre attenzione agli insiemi di partenza e di arrivo. Per evitare ogni tipo di complicazioni, nel nostro corso consideriamo queste operazioni solo su relazioni che hanno uno stesso insieme di partenza (A) e uno stesso insieme di arrivo (B).

Definizione 2.2.3 (operazioni insiemestiche su relazioni)**.** *Siano date due relazioni* $R\colon A \leftrightarrow B$ *e* $S\colon A \leftrightarrow B$.

- *La relazione* $R \cup S\colon A \leftrightarrow B$ *è detta* UNIONE *di* R *e* S*;*
- *La relazione* $R \cap S\colon A \leftrightarrow B$ *è detta* INTERSEZIONE *di* R *e* S*;*
- *La relazione* $R \setminus S\colon A \leftrightarrow B$ *è detta* DIFFERENZA *di* R *con* S*;*
- *La relazione* $(A \times B) \setminus R\colon A \leftrightarrow B$ *è detta il* COMPLEMENTO *di* R*. Il complemento di una relazione* $R\colon A \leftrightarrow B$ *è denotato da* $\overline{R}$.

Si noti che il complemento di R è definito in maniera apparentemente diversa dal complemento insiemistico: come insieme il complemento di R è $\mathcal{U} \setminus R$, mentre come relazione è $A \times B \setminus R$. L'idea è che quando si considerano relazioni tra A e B si fissa sempre come universo $\mathcal{U}$ l'insieme $A \times B$.

Tutte le leggi nelle Tabelle 1.1, 1.2, 1.3 e 1.4 valgono chiaramente anche per le relazioni tra A e B ma, ancora una volta, si deve prendere $\mathcal{U} = A \times B$.

Composizione

Abbiamo appena visto che quando si combinano relazioni attraverso le operazioni insiemistiche è opportuno restringersi a relazioni con gli stessi insiemi di partenza e di arrivo.

Adesso consideriamo un'operazione che permette di combinare due relazioni, quando l'insieme di arrivo della prima relazione è lo stesso dell'insieme di partenza della seconda.

Definizione 2.2.4. *[composizione di relazioni] Siano* $R\colon A \leftrightarrow B$ *e* $S\colon B \leftrightarrow C$*. La* COMPOSIZIONE *di* R *con* S *è la relazione* $R; S\colon A \leftrightarrow C$ *così definita:*

$$R; S = \{(x, z) \in A \times C \mid \text{esiste almeno un } y \in B \text{ tale che } (x, y) \in R \text{ e } (y, z) \in S\}.$$

Esempio 2.2.5. *Siano dati* $A = \{x, y, z\}$, $B = \{a, b, c, d\}$ *e* $C = \{1, 2\}$*. Consideriamo le relazioni*

$$R = \{(x, a),\ (y, b),\ (z, c),\ (z, d)\}\colon A \leftrightarrow B$$

e

$$S = \{(a, 1),\ (a, 2),\ (c, 2),\ (d, 2)\}\colon B \leftrightarrow C.$$

Le due relazioni possono essere composte in quanto l'insieme di arrivo di R *è uguale all'insieme di partenza di* S*. La loro composizione è la relazione*

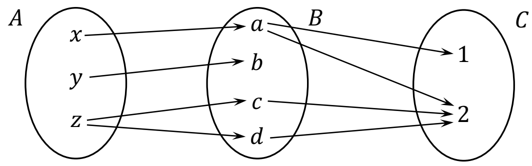
$$R; S = \{(x, 1),\ (x, 2),\ (z, 2)\}\colon A \leftrightarrow C.$$

Infatti $(x, 1) \in R; S$ *perchè per l'elemento* $a \in B$ *si ha che* $(x, a) \in R$ *e* $(a, 1) \in S$*. Similmente,* $(x, 2) \in R; S$ *perchè per l'elemento* $a \in B$ *valgono sia* $(x, a) \in R$ *che* $(a, 2) \in S$.

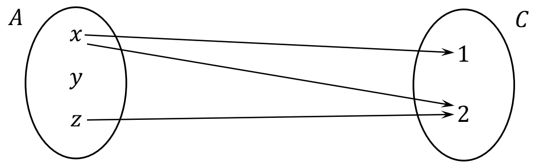
Per vedere che $(z, 2) \in R; S$ *abbiamo due possibili giustificazioni: (1) per l'elemento* $c \in B$ *si ha che* $(z, c) \in R$ *e* $(c, 2) \in S$*; (2) per l'elemento* $d \in B$ *si ha che* $(z, d) \in R$ *e* $(d, 2) \in S$.

Per vedere che nessun'altra coppia $(u, w) \in A \times C$ *appartiene a* $R; S$ *si deve mostrare che non esiste alcun elemento* $v \in B$ *tale che* $(u, v) \in R$ *e* $(v, w) \in S$*. Per esempio, per vedere che* $(y, 1) \notin R; S$ *si può osservare che: per* $a \in B$, $(y, a) \notin R$*; per* $b \in B$, $(b, 1) \notin S$*; per* $c \in B$, $(y, c) \notin R$*; e per* $d \in B$, $(y, d) \notin R$.

L'operazione di composizione di relazioni può sembrare un po' complicata, ma in realtà risulta estremamente naturale quando si visualizza attraverso diagrammi. Per visualizzare la composizione di $R\colon A \leftrightarrow B$ e $S\colon B \leftrightarrow C$, prima di tutto si disegnano gli insiemi A (a sinistra), B (al centro) e C (a destra), nonché le relazioni R e S, utlizzando la solita modalità delle frecce. Per esempio il seguente diagramma



visualizza le relazioni R e S dell'Esempio 2.2.5. Poi per ottenere il diagramma della relazione composta è sufficiente seguire le frecce da sinistra a destra e vedere per ogni elemento a di A e ogni elemento c di C se c'è un "percorso" da a a c. In tal caso, si aggiunge una freccia da a a c. Una volta fatto ciò per tutte le coppie $(a, c) \in A \times C$ si cancella l'insieme B dal centro e tutte le frecce ad esso collegate. Il seguente diagramma visualizza la relazione $R; S$ dell'Esempio 2.2.5.



.

Esercizio 2.2.6. *Si consideri la relazione* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$. *Si disegni il diagramma della relazione* $Succ; Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$. *Definire prima per enumerazione e poi per proprietà tale relazione.*

Abbiamo finora mostrato degli esempi di composizione su entità piuttosto astratte. In realtà l'operazione di composizione di relazioni ci permette di formalizzare concetti della vita quotidiana.

Esempio 2.2.7. *Si ricordi la relazione* $Padre\colon U \leftrightarrow U$ *dell'Esempio 2.1.3 e la relazione* $Genitore\colon U \leftrightarrow U$ *dell'Esempio 2.2.1. La relazione* $Nonno\colon U \leftrightarrow U$ *può essere definita come*

$$Nonno = Padre; Genitore.$$

Esercizio 2.2.8. *Definire per proprietà la relazione* $Genitore; Genitore$.

Esercizio 2.2.9. *Definire attraverso composizione la relazione* $Nonna = \{(x, y) \in U \times U \mid x \text{ è nonna di } y\}$.

Esercizio 2.2.10. *Definire utilizzando solamente la composizione la relazione* $Nonn * Patern* = \{(x, y) \in U \times U \mid x \text{ è nonno paterno o nonna paterna di } y\}$.

I quantificatori

Nella definizione dell'operazione di composizione (Definizione 2.2.4) abbiamo utilizzato l'espressione italiana *esiste almeno*:

$$\{(x, z) \in A \times C \mid \text{esiste almeno un } y \in B \text{ tale che } (x, y) \in R \text{ e } (y, z) \in S\}$$

Questa espressione riveste un ruolo speciale nel linguaggio matematico e viene denotata dal simbolo $\exists$, chiamato *QUANTIFICATORE ESISTENZIALE*. La formula

$$(\exists a \in A \,.\, P(a))$$

si legge

esiste almeno un elemento di A <u>tale che</u> la proprietà P è vera.

Pertanto la composizione di relazioni può essere scritta in formule come

$$R;S = \{(x,z) \in A \times C \mid (\exists y \in B\,.\,(x,y) \in R \wedge (y,z) \in S)\}.$$

Un altro simbolo di fondamentale importanza è $\forall$, chiamato *QUANTIFICATORE UNIVERSALE*, che si legge in italiano *per ogni*. La formula

$$(\forall a \in A\,.\,P(a))$$

si legge

per tutti gli elementi di A <u>vale che</u> la proprietà P è vera.

Per dimostrare che la formula $(\exists a \in A\,.\,P(a))$ è vera è sufficiente esibire un elemento $a \in A$ per cui vale la proprietà P. Dimostrare che la formula $(\forall a \in A\,.\,P(a))$ è vera è molto più laborioso in generale: infatti si deve dimostrare che P vale per tutti gli $a \in A$. È importante notare che in questo caso, quando A è vuoto, non c'è niente da dimostrare: quindi la formula $(\forall a \in A\,.\,P(a))$ è banalmente vera.

I quantificatori $\exists$ e $\forall$ saranno studiati in profondità nel Capitolo 9 dove presenteremo la logica del primo ordine. Fino ad allora, utilizzeremo di tanto in tanto questi simboli con il significato che abbiamo appena descritto.

Relazione opposta

Definizione 2.2.11 (relazione opposta)**.** *Sia $R\colon A \leftrightarrow B$ una relazione. La* RELAZIONE OPPOSTA *di R è la relazione $R^{op}\colon B \leftrightarrow A$ definita come*

$$R^{op} = \{(y,x) \in B \times A \mid (x,y) \in R\}.$$

Esempio 2.2.12. *Si considerino le relazioni R e S dell'Esempio 2.2.5. Si ha che*

$$R^{op} = \{(a,x),\ (b,y),\ (c,z),\ (d,z)\}\colon B \leftrightarrow A$$

e

$$S^{op} = \{(1,a),\ (2,a),\ (2,c),\ (2,d)\}\colon C \leftrightarrow B.$$

È importante notare che R^{op} non può essere composta con S^{op} perché l'insieme di arrivo di R^{op} è A, mentre quello di partenza di S^{op} è C. Comunque si possono comporre le relazioni nel senso inverso, cioè come $S^{op};R^{op}$ perché sia l'insieme di arrivo di S^{op} che quello di partenza di R^{op} sono l'insieme B.

Esercizio 2.2.13. *Si considerino le relazioni R, S ed $R;S$ nell'Esempio 2.2.5 e le relazioni R^{op} e S^{op} nell'Esempio 2.2.12. È vera la seguente uguaglianza?*

$$(R;S)^{op} = S^{op};R^{op}$$

Esempio 2.2.14. *Si consideri la relazione $Genitore\colon U \leftrightarrow U$ introdotta nell'Esempio 2.2.1. Si ha che*

$$Genitore^{op} = Figli*$$

dove $Figli*$ è la relazione dell'Esempio 2.2.2. Infatti si ha che

$$\begin{aligned} Genitore^{op} &= \{(y,x) \in U \times U \mid (x,y) \in Genitore\} \\ &= \{(y,x) \in U \times U \mid x \text{ è madre o padre di } y\} \\ &= \{(y,x) \in U \times U \mid y \text{ è figlio o figlia di } x\} \\ &= \{(x,y) \in U \times U \mid x \text{ è figlio o figlia di } y\} \\ &= Figli* \end{aligned}$$

Esercizio 2.2.15. *È vero che*

$$Figli*^{op} = Genitore?$$

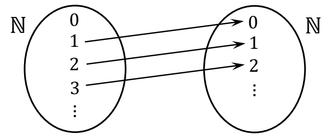
Esempio 2.2.16. *Si consideri la relazione*

$$Succ\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = x+1\}$$

introdotta nell'Esempio 2.1.8. Si ha che

$$\begin{aligned} Succ^{op} &= \{(y,x) \in \mathbb{N} \times \mathbb{N} \mid (x,y) \in Succ\} \\ &= \{(y,x) \in \mathbb{N} \times \mathbb{N} \mid y = x+1\} \\ &= \{(y,x) \in \mathbb{N} \times \mathbb{N} \mid y-1 = x\} \\ &= \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x-1 = y\} \\ &= \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = x-1\} \end{aligned}$$

Chiamiamo questa relazione Pred che sta per "predecessore".



È importante osservare come si può ottenere il diagramma per $Succ^{op}$ a partire da quello di $Succ$: dato il diagramma di una qualsiasi relazione R, il diagramma di R^{op} è ottenuto come l'immagine allo specchio (cioè girandolo di 180 gradi) e invertendo la direzione delle frecce.

Mostriamo adesso un po' di esempi ben noti dalla matematica.

Esempio 2.2.17.

$$Double\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = 2 \times x\}$$

$$Double^{op} = Half\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = x/2\}$$

Esercizio 2.2.18. *Disegnare il diagramma delle relazioni* $Double\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *e* $Double^{op} = Half\colon \mathbb{N} \leftrightarrow \mathbb{N}$

Esempio 2.2.19.

$$Square\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = x^2\}$$

$$Square^{op} = Sqrt\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = \sqrt{x}\}$$

Esercizio 2.2.20. *Disegnare il diagramma delle relazioni* $Square\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *e* $Square^{op} = Sqrt\colon \mathbb{N} \leftrightarrow \mathbb{N}$

Esempio 2.2.21.

$$Exp\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = 2^x\}$$

$$Exp^{op} = Log\colon \mathbb{N} \leftrightarrow \mathbb{N} = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = log_2(x)\}$$

Esercizio 2.2.22. *Disegnare il diagramma delle relazioni* $Exp\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *e* $Exp^{op} = Log\colon \mathbb{N} \leftrightarrow \mathbb{N}$

Esercizio 2.2.23. *Definire attraverso le relazioni e le operazioni viste finora, la relazione* $Fratello = \{(x,y) \in U \times U \mid x \text{ è fratello di } y\}$. *Per "fratello" si intende il figlio di almeno uno dei genitori. Per esempio, due uomini sono considerati fratelli, anche se hanno la stessa madre ma non lo stesso padre.*

Esercizio 2.2.24. *Definire attraverso le relazioni e le operazioni viste finora, la relazione* $Sorella = \{(x,y) \in U \times U \mid x \text{ è sorella di } y\}$. *Anche qui per "sorella" si intende la figlia di almeno uno dei genitori.*

Esercizio 2.2.25. *Definire attraverso le relazioni e le operazioni viste finora, le relazioni* $Zia = \{(x,y) \in U \times U \mid x \text{ è zia di } y\}$ *e* $Zio = \{(x,y) \in U \times U \mid x \text{ è zio di } y\}$.

Concludiamo mostrando un'applicazione immediata delle operazioni su relazioni all'Informatica.

Esempio 2.2.26. *Uno tra i più noti linguaggi di interrogazione di database, SQL (Structured Query Language), è basato sulle operazioni tra relazioni: un database è pensato come una collezione di relazioni e le interrogazioni (queries) al database come operazioni su tali relazioni. Questi argomenti verranno trattati in modo esaustivo nel corso di Basi di Dati; in questo corso ci limitiamo a mostrare un esempio giocattolo per dare un'intuizione più concreta.*

Immaginiamoci una piccola Università con pochi studenti, corsi e professori.

- $Studenti = \{Lucia,\ Mario,\ Franca,\ Luisa,\ Gino,\ Marco,\ Marco,\ Gaia,\ Carlo\}$;
- $Corsi = \{PA,\ LAB,\ FDI,\ ANA\}$;
- $Professori = \{Paperino,\ Pippo,\ Pluto,\ Paperone\}$.

Il database dell'Università consiste delle seguenti due tabelle.

$Segue$

$Studenti$	$Corsi$
$Lucia$	FDI
$Lucia$	PA
$Mario$	ANA
$Franca$	FDI
$Franca$	LAB
$Luisa$	PA
$Luisa$	ANA
$Luisa$	LAB
$Gino$	LAB
$Marco$	FDI
$Marco$	LAB
$Gaia$	FDI
$Gaia$	ANA

$Insegna$

$Professori$	$Corsi$
$Paperino$	PA
$Paperino$	LAB
$Pippo$	FDI
$Pluto$	ANA
$Paperone$	FDI

La tabella di sinistra rappresenta la relazione $Segue\colon Studenti \leftrightarrow Corsi$: $(x, y) \in Segue$ *se e solo se lo studente* x *segue il corso* y. *Ad esempio Lucia segue* FDI *e* PA. *In modo analogo la tabella di destra rappresenta la relazione* $Insegna\colon Professori \leftrightarrow Corsi$.

Una interrogazione tipica per questo database potrebbe essere:

Quali professori ha ciascun studente?

La risposta a tale interrogazione è data calcolando la relazione $Segue; Insegna^{op}$

$Segue; Insegna^{op}$

$Studenti$	$Professori$
$Lucia$	$Pippo$
$Lucia$	$Paperone$
$Lucia$	$Paperino$
$Mario$	$Pluto$
$Franca$	$Pippo$
$Franca$	$Paperone$
$Franca$	$Paperino$
$Luisa$	$Paperino$
$Luisa$	$Pluto$
$Gino$	$Paperino$
$Marco$	$Pippo$
$Marco$	$Paperone$
$Marco$	$Paperino$
$Gaia$	$Pippo$
$Gaia$	$Pluto$
$Gaia$	$Paperone$

2.3 Leggi

Come per gli insiemi, anche per le relazioni esistono delle utili leggi che regolano il comportamento delle varie operazioni. Abbiamo già anticipato che per le operazioni insiemistiche valgono le stesse leggi studiate nella Sezione 1.4, con l'accorgimento di prendere, per una relazione $R\colon A \leftrightarrow B$, l'insieme $\mathcal{U} = A \times B$ come insieme universo.

Teorema 2.3.1. *Per tutti gli insiemi A, B e relazioni $R, S, T\colon A \leftrightarrow B$ valgono le uguaglianze nelle Tabelle 2.1, 2.2 e 2.3.*

associatività	$R \cup (S \cup T) = (R \cup S) \cup T$	$R \cap (S \cap T) = (R \cap S) \cap T$
unità	$R \cup \varnothing = R$	$R \cap (A \times B) = R$
commutatività	$R \cup S = S \cup R$	$R \cap S = S \cap R$
idempotenza	$R \cup R = R$	$R \cap R = R$
assorbimento	$R \cup (A \times B) = (A \times B)$	$R \cap \varnothing = \varnothing$

Tabella 2.1: Leggi per le operazioni insiemistiche

distributività di $\cup$ su $\cap$	$R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
distributività di $\cap$ su $\cup$	$R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$
assorbimento di $\cup$ su $\cap$	$R \cup (R \cap S) = R$
assorbimento di $\cap$ su $\cup$	$R \cap (R \cup S) = R$
complemento per $\cup$	$R \cup \overline{R} = (A \times B)$
complemento per $\cap$	$R \cap \overline{R} = \varnothing$

Tabella 2.2: Leggi per le operazioni insiemistiche (2)

differenza	$R \setminus S = R \cap \overline{S}$

Tabella 2.3: Leggi per le operazioni insiemistiche (3)

La validità del Teorema 2.3.1 è garantita dai risultati della Sezione 1.4, che valgono per tutti gli insiemi e quindi, in particolare, anche per tutte le relazioni.

Il seguente teorema illustra invece alcune utili leggi per la composizione e la relazione opposta.

Teorema 2.3.2. *Per tutti gli insiemi A, B, C, D e relazioni $R\colon A \leftrightarrow B$, $S\colon B \leftrightarrow C$ e $T\colon C \leftrightarrow D$ valgono le uguaglianze nelle Tabelle 2.4 e 2.5.*

associatività	$R; (S; T) = (R; S); T$
unità	$Id_A; R = R = R; Id_B$
assorbimento	$R; \varnothing_{B,C} = \varnothing_{A,C} = \varnothing_{A,B}; S$

Tabella 2.4: Leggi per composizione di relazioni

La notazione grafica che abbiamo introdotto per le relazioni può fornire un'intuizione chiara riguardo alla validità di tali leggi. In queste note forniamo una dimostrazione discorsiva per l'associatività della composizione e lasciamo le dimostrazioni delle altre leggi come esercizio.

Dimostrazione di $R; (S; T) = (R; S); T$. Anziché dimostrare l'uguaglianza direttamente possiamo dimostrare separatamente le inclusioni

$$R; (S; T) \subseteq (R; S); T \quad \text{e} \quad R; (S; T) \supseteq (R; S); T$$

convoluzione	$(R^{op})^{op} = R$
op-id	$Id_A^{op} = Id_A$
op-compl	$(A \times B)^{op} = B \times A$
op-vuoto	$\varnothing_{A,B}^{op} = \varnothing_{B,A}$

Tabella 2.5: Leggi per relazione opposta

e poi concludere l'uguaglianza utilizzando l'antisimmetria di $\subseteq$ (Proposizione 1.4.13).

- $\underline{R; (S; T) \subseteq (R; S); T}$. Per dimostrare questa inclusione, dobbiamo dimostrare che preso un generico elemento di $R; (S; T)$, tale elemento appartiene anche a $(R; S); T$. Sia $(a, d) \in R; (S; T)$: per definizione della composizione (;) esiste almeno un $b \in B$ tale che (1) $(a, b) \in R$ e (2) $(b, d) \in S; T$. Da (2) e dalla definizione di composizione si ha che esiste almeno un $c \in C$ tale che (2.1) $(b, c) \in S$ e (2.2) $(c, d) \in T$. Da (1) e (2.1) segue che (3) $(a, c) \in R; S$. Da (3) e (2.2) segue che $(a, d) \in (R; S); T$.
- $\underline{R; (S; T) \supseteq (R; S); T}$. Per dimostrare questa inclusione, dobbiamo dimostrare che preso un generico elemento di $(R; S); T$, tale elemento appartiene anche a $R; (S; T)$. La dimostrazione è del tutto analoga a quella dell'inclusione precedente.

■

Esercizio 2.3.3. *Dimostrare in modo discorsivo le leggi nelle Tabelle 2.4 e 2.5.*

L'ultimo teorema illustra le leggi che regolano le interazioni fra le operazioni insiemistiche, la composizione e la relazione opposta.

Teorema 2.3.4. *Per tutti gli insiemi A, B, C, D e relazioni $R\colon A \leftrightarrow B$, $S, T\colon B \leftrightarrow C$ e $U : C \leftrightarrow D$ valgono le uguaglianze nelle Tabelle 2.6.*

distributività di ; su $\cup$ (sinistra)	$R; (S \cup T) = (R; S) \cup (R; T)$
distributività di ; su $\cup$ (destra)	$(S \cup T); U = (S; U) \cup (T; U)$
distributività di $\cdot^{op}$ su ;	$(R; S)^{op} = S^{op}; R^{op}$
distributività di $\cdot^{op}$ su $\cup$	$(S \cup T)^{op} = S^{op} \cup T^{op}$
distributività di $\cdot^{op}$ su $\cap$	$(S \cap T)^{op} = S^{op} \cap T^{op}$
distributività di $\cdot^{op}$ su $\bar{\cdot}$	$(\overline{R})^{op} = \overline{(R^{op})}$

Tabella 2.6: Leggi di distributività

Ancora una volta, forniamo la dimostrazione di una sola delle leggi e lasciamo le altre come esercizio.

Dimostrazione di $(R; S)^{op} = S^{op}; R^{op}$. Anziché dimostrare l'uguaglianza direttamente possiamo dimostrare separatamente le inclusioni

$$(R; S)^{op} \subseteq S^{op}; R^{op} \quad \text{e} \quad (R; S)^{op} \supseteq S^{op}; R^{op}$$

e poi concludere l'uguaglianza utilizzando l'antisimmetria di $\subseteq$ (Proposizione 1.4.13).

- $\underline{(R; S)^{op} \subseteq S^{op}; R^{op}}$. Per dimostrare questa inclusione, dobbiamo dimostrare che preso un generico elemento di $(R; S)^{op}$, tale elemento appartiene anche a $S^{op}; R^{op}$. Sia $(c, a) \in (R; S)^{op}$: per definizione della relazione opposta si ha che $(a, c) \in R; S$. Quindi, Per definizione di composizione, esiste almeno un $b \in B$ tale che (1) $(a, b) \in R$ e (2) $(b, c) \in S$.

  Utilizzando la definizione di relazione opposta, da (1) si deduce che $(b, a) \in R^{op}$ e, da (2) che $(c, b) \in S^{op}$. Per definizione di composizione, $(c, a) \in S^{op}; R^{op}$.

- $\underline{(R;S)^{op} \supseteq S^{op};R^{op}}$. Per dimostrare questa inclusione, dobbiamo dimostrare che preso un generico elemento di $S^{op};R^{op}$, tale elemento appartiene anche a $(R;S)^{op}$. Sia $(c,a) \in S^{op};R^{op}$. Per definizione di composizone si ha che esiste almeno un $b \in B$ tale che (1) $(c,b) \in S^{op}$ e (2) $(b,a) \in R^{op}$. Utilizzando la definizione di relazione opposta da (1) si deduce che $(b,c) \in S$ e da (2) che $(a,b) \in R$.

  Pertanto, per definizione di composizione, $(a,c) \in R;S$ e quindi $(c,a) \in (R;S)^{op}$.

■

Esercizio 2.3.5. *Dimostrare in modo discorsivo le leggi nelle Tabella 2.6.*

Esercizio 2.3.6. *Dimostrare per sostituzione che*

$Genitore;Genitore =$
$(Madre;Madre) \cup (Madre;Padre) \cup (Padre;Madre) \cup (Padre;Padre)$

Esercizio 2.3.7. *Dimostrare in modo discorsivo che per tutti gli insiemi A, B, C e relazioni $R\colon A \leftrightarrow B$ e $S\colon B \leftrightarrow C$ e $T\colon B \leftrightarrow C$ vale che*

$$\textit{se } S \subseteq T, \textit{ allora } R;S \subseteq R;T.$$

Esercizio 2.3.8. *Considera la seguente affermazione: per tutti gli insiemi A, B, C e relazioni $R\colon A \leftrightarrow B$ e $S\colon B \leftrightarrow C$ e $T\colon B \leftrightarrow C$ vale che*

$$\textit{se } R;S \subseteq R;T \textit{ allora } S \subseteq T.$$

Se è vera fornire una dimostrazione, se è falsa fornire un controesempio.

Esercizio 2.3.9. *Dimostrare in modo discorsivo che per tutti gli insiemi A, B e relazioni $R\colon A \leftrightarrow B$ e $S\colon A \leftrightarrow B$ vale che*

$$R \subseteq S \textit{ se e solo se } R^{op} \subseteq S^{op}.$$

2.4 Proprietà di relazioni

In questa sezione illustriamo quattro fondamentali proprietà di relazioni. Queste proprietà appaiono ovunque, sia in Informatica che in Matematica e, nel resto del nostro corso, ci permetteranno di definire importanti concetti, quali funzioni e biiezioni.

Definizione 2.4.1 (relazione totale)**.** *Siano A e B due insiemi e R una relazione tra A e B. $R\colon A \leftrightarrow B$ si dice* TOTALE *se per tutti gli $a \in A$,* esiste almeno *un $b \in B$ tale che $(a,b) \in R$.*

Esempio 2.4.2. *Siano dati $A = \{x,y,z\}$ e $B = \{a,b,c,d\}$. La relazione*

$$R = \{(x,a),\ (x,b),\ (y,a),\ (z,d)\}\colon A \leftrightarrow B$$

è totale, mentre la relazione

$$S = \{(x,c),\ (x,d),\ (z,d)\}\colon A \leftrightarrow B$$

non è totale perchè per l'elemento $y \in A$ non esiste alcun elemento $u \in B$ tale che $(y,u) \in S$.

Esempio 2.4.3. *Per tutti gli insiemi A e B*

- *la relazione identità $Id_A\colon A \leftrightarrow A$ è totale;*
- *la relazione completa $A \times B\colon A \leftrightarrow B$ è totale.*

Esempio 2.4.4. *Per gli insiemi $A = \{x,y,z\}$ e $B = \{a,b,c,d\}$, la relazione vuota $\varnothing\colon A \leftrightarrow B$ non è totale. Per vederlo, basta osservare che per $x \in A$ non esiste alcun $u \in B$ tale che $(x,u) \in \varnothing$.*

Esercizio 2.4.5. *Esiste un insieme A per il quale la relazione vuota $\varnothing\colon A \leftrightarrow B$ è sicuramente totale. Quale insieme è?*

Esercizio 2.4.6. *La relazione* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *è totale? La relazione* $Pred\colon \mathbb{N} \leftrightarrow \mathbb{N}$*? La relazione* $Plus\colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$*?*

Esercizio 2.4.7. *La relazione* $Madre\colon U \leftrightarrow U$ *è totale? La relazione* $Genitore\colon U \leftrightarrow U$*? La relazione* $Figlia\colon U \leftrightarrow U$*? La relazione* $Figli{*}\colon U \leftrightarrow U$*?*

Definizione 2.4.8 (relazione univalente)**.** *Siano* A *e* B *due insiemi e* R *una relazione tra* A *e* B*.* $R\colon A \leftrightarrow B$ *si dice* UNIVALENTE *se per tutti gli* $a \in A$*,* esiste al più *un* $b \in B$ *tale che* $(a, b) \in R$*.*

Esempio 2.4.9. *Sia* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*. La relazione*

$$R = \{(x, a),\ (x, b),\ (y, a),\ (z, d)\}\colon A \leftrightarrow B$$

è totale ma non è univalente perchè per l'elemento $x \in A$ *esistono due elementi in* B *che sono in relazione* R *con* x*: infatti* $(x, a) \in R$ *e* $(x, b) \in R$*. Invece, la relazione*

$$S = \{(x, c),\ (z, d)\}\colon A \leftrightarrow B$$

è univalente ma non è totale.

Esempio 2.4.10. *Per tutti gli insiemi* A *e* B

- *la relazione identità* $Id_A\colon A \leftrightarrow A$ *è univalente;*
- *la relazione vuota* $\varnothing\colon A \leftrightarrow B$ *è univalente.*

Esempio 2.4.11. *Per gli insiemi* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*, la relazione completa* $A \times B\colon A \leftrightarrow B$ *non è univalente. Per vederlo, basta osservare che per* $x \in A$ *si ha sia che* $(x, a) \in A \times B$ *che* $(x, b) \in A \times B$*.*

Esercizio 2.4.12. *Esiste un insieme* A *per il quale la relazione completa* $A \times B\colon A \leftrightarrow B$ *è sicuramente univalente. Quale insieme è?*

Esercizio 2.4.13. *La relazione* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *è univalente? La relazione* $Pred\colon \mathbb{N} \leftrightarrow \mathbb{N}$*? La relazione* $Plus\colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$*?*

Esercizio 2.4.14. *La relazione* $Madre\colon U \leftrightarrow U$ *è univalente? La relazione* $(Madre)^{op}$*?*

È interessante notare che l'unica differenza nelle definizioni di totale e univalente consiste nel *esiste almeno* (totale) e *esiste al più* (univalente). Per una qualche proprietà P, "esiste almeno un elemento x tale che $P(x)$" significa che il numero di elementi che soddisfano P deve essere *maggiore o uguale* ad 1. Invece "esiste al più un elemento x tale che $P(x)$" significa che il numero di elementi che soddisfano P deve essere *minore o uguale* ad 1.

È importante capire questa differenza, e cosa significa in termini di dimostrazioni: quando si desidera dimostrare che "esiste almeno un elemento x tale che $P(x)$" si deve esibire un tale x; invece quando si desidera dimostrare che "esiste al più un elemento x tale che $P(x)$" si deve mostrare che, se ci sono due elementi x e y per cui vale sia $P(x)$ che $P(y)$, allora i due elementi sono lo stesso.

Osservazione 2.4.15. *Abbiamo visto che l'espressione italiana* esiste almeno *viene denotata nel linguaggio matematico dal simbolo* $\exists$*. Per l'espressione* esiste al più *non c'è un simbolo corrispondente. La ragione è che* esiste al più *può essere scritta in formule utilizzando* $\forall$ *e* $=$*. Più precisamente,*

$$\textit{esiste al più un } a \in A \textit{ tale che } P(a)$$

si può scrivere come

$$(\forall a \in A\,.\,(\forall b \in A\,.\ \textit{se } P(a) \wedge P(b),\ \textit{allora } a = b)).$$

Adesso consideriamo altre due proprietà. L'unica differenza tra le due consiste ancora nell'*almeno* e nell'*al più*, ma diversamente dalle due proprietà discusse prima, riguardano l'insieme di arrivo e non quello di partenza.

Definizione 2.4.16 (relazione surgettiva)**.** *Siano* A *e* B *due insiemi e* R *una relazione tra* A *e* B*.* $R\colon A \leftrightarrow B$ *si dice* SURGETTIVA *se per tutti i* $b \in B$*,* esiste almeno *un* $a \in A$ *tale che* $(a, b) \in R$*.*

Esempio 2.4.17. *Sia* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*. La relazione*

$$R\colon A \leftrightarrow B = \{(x, a),\ (x, b),\ (y, c),\ (z, d)\}$$

è surgettiva, mentre la relazione

$$S\colon A \leftrightarrow B = \{(x, c),\ (x, b),\ (z, d)\}$$

non è surgettiva perchè per l'elemento $a \in B$ *non esiste alcun elemento* $u \in A$ *tale che* $(u, a) \in S$*.*

Esempio 2.4.18. *Per tutti gli insiemi* A *e* B

- *la relazione identità* $Id_A\colon A \leftrightarrow A$ *è surgettiva;*
- *la relazione completa* $A \times B\colon A \leftrightarrow B$ *è surgettiva.*

Esempio 2.4.19. *Per gli insiemi* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*, la relazione vuota* $\varnothing\colon A \leftrightarrow B$ *non è surgettiva. Per vederlo, basta osservare che per* $a \in B$ *non esiste alcun* $u \in A$ *tale che* $(u, a) \in \varnothing$*.*

Esercizio 2.4.20. *Esiste un insieme* B *per il quale la relazione vuota* $\varnothing\colon A \leftrightarrow B$ *è surgettiva. Quale insieme è?*

Esercizio 2.4.21. *La relazione* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *è surgettiva? La relazione* $Pred\colon \mathbb{N} \leftrightarrow \mathbb{N}$*? La relazione* $Plus\colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$*?*

Esercizio 2.4.22. *La relazione* $Madre\colon U \leftrightarrow U$ *è surgettiva? La relazione* $Genitore\colon U \leftrightarrow U$*? La relazione* $Figlia\colon U \leftrightarrow U$*? La relazione* $Figli{*}\colon U \leftrightarrow U$*?*

Definizione 2.4.23 (relazione iniettiva)**.** *Siano* A *e* B *due insiemi e* R *una relazione tra* A *e* B*.* $R\colon A \leftrightarrow B$ *si dice* INIETTIVA *se per tutti i* $b \in B$*,* esiste al più *un* $a \in A$ *tale che* $(a, b) \in R$*.*

Esempio 2.4.24. *Sia* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*. La relazione*

$$R\colon A \leftrightarrow B = \{(x, a),\ (x, b),\ (y, c),\ (z, d)\}$$

è iniettiva, mentre la relazione

$$S\colon A \leftrightarrow B = \{(x, c),\ (x, b),\ (z, b)\}$$

non è iniettiva perchè per l'elemento $b \in B$ *esistono due elementi in* A *in relazione* S *con* b*:* $(x, b) \in S$ *e* $(z, b) \in S$*.*

Esempio 2.4.25. *Per tutti gli insiemi* A *e* B

- *la relazione identità* $Id_A\colon A \leftrightarrow A$ *è iniettiva;*
- *la relazione vuota* $\varnothing\colon A \leftrightarrow B$ *è iniettiva.*

Esempio 2.4.26. *Per gli insiemi* $A = \{x, y, z\}$ *e* $B = \{a, b, c, d\}$*, la relazione completa* $A \times B\colon A \leftrightarrow B$ *non è iniettiva. Per vederlo, basta osservare che per* $a \in B$*, si ha che* $(x, a) \in A \times B$ *e* $(y, a) \in A \times B$*.*

Esercizio 2.4.27. *Esiste un insieme* B *per il quale la relazione completa* $A \times B\colon A \leftrightarrow B$ *è iniettiva. Quale insieme è?*

Esercizio 2.4.28. *La relazione* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *è iniettiva? La relazione* $Pred\colon \mathbb{N} \leftrightarrow \mathbb{N}$*? La relazione* $Plus\colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$*?*

Esercizio 2.4.29. *La relazione* $Madre\colon U \leftrightarrow U$ *è iniettiva? La relazione* $Genitore\colon U \leftrightarrow U$*? La relazione* $Figlia\colon U \leftrightarrow U$*? La relazione* $Figli{*}\colon U \leftrightarrow U$*?*

La Tabella 2.7 fornisce un modo efficace per riassumere e, soprattutto, capire le quattro proprietà: totale e univalente riguardano l'insieme di partenza, mentre surgettiva e iniettiva l'insieme di arrivo. Le proprietà totale e surgettiva richiedono l'esistenza di almeno un elemento, mentre univalente e iniettiva richiedo l'esistenza di al più un elemento.

	partenza	arrivo
almeno	*TOTALE*	*SURGETTIVA*
al più	*UNIVALENTE*	*INIETTIVA*

Tabella 2.7: Tabella riassuntiva delle quattro principali proprietà

Risultati di dualità

Confrontando le definizioni di relazione totale e surgettiva è facile osservare che queste impongono lo stesso vincolo ma la prima sull'insieme di partenza, mentre la seconda sull'insieme di arrivo. Abbiamo visto che l'operazione $\cdot^{op}$ inverte l'insieme di partenza e di arrivo. Il seguente risultato collega le due proprietà attraverso la relazione opposta.

Proposizione 2.4.30. *Per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$ vale che:*

1. *$R\colon A \leftrightarrow B$ è totale se e solo se $R^{op}\colon B \leftrightarrow A$ è surgettiva.*
2. *$R\colon A \leftrightarrow B$ è univalente se e solo se $R^{op}\colon B \leftrightarrow A$ è iniettiva.*

Dimostrazione. Dimostriamo il primo punto e lasciamo il secondo come esercizio. Trattandosi di un se e solo se, possiamo dividere la dimostrazioni in due parti:

- Se $R\colon A \leftrightarrow B$ è totale, allora $R^{op}\colon B \leftrightarrow A$ è surgettiva. Visto che R è totale allora

  $$\text{per ogni } x \in A \text{ esiste almeno un } y \in B \text{ tale che } (x, y) \in R.$$

  Per definizione di R^{op} questo significa che

  $$\text{per ogni } x \in A \text{ esiste almeno un } y \in B \text{ tale che } (y, x) \in R^{op}.$$

  Questo significa, per definizione, che $R^{op}\colon B \leftrightarrow A$ è surgettiva.

- Se $R^{op}\colon B \leftrightarrow A$ è surgettiva, allora $R\colon A \leftrightarrow B$ è totale. Visto che $R^{op}\colon B \leftrightarrow A$ è surgettiva allora

  $$\text{per ogni } x \in A \text{ esiste almeno un } y \in B \text{ tale che } (y, x) \in R^{op}.$$

  Per definizione di R^{op} questo significa che

  $$\text{per ogni } x \in A \text{ esiste almeno un } y \in B \text{ tale che } (x, y) \in R.$$

  Questo significa, per definizione, che $R\colon A \leftrightarrow B$ è totale.

■

Esercizio 2.4.31. *Dimostrare la Proposizione 2.4.30.2.*

Proposizione 2.4.32. *Per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$ vale che:*

1. *$R\colon A \leftrightarrow B$ è surgettiva se e solo se $R^{op}\colon B \leftrightarrow A$ è totale.*
2. *$R\colon A \leftrightarrow B$ è iniettiva se e solo se $R^{op}\colon B \leftrightarrow A$ è univalente.*

Dimostrazione. Dimostriamo il primo punto, il secondo lo lasciamo come esercizio. Dalla Proposizione 2.4.30.1 R^{op} è totale se e solo se $(R^{op})^{op}$ è surgettiva. Ma, visto che $(R^{op})^{op} = R$, R^{op} è totale se e solo se R è surgettiva. ■

Esercizio 2.4.33. *Dimostrare la Proposizione 2.4.32.2.*

Teorema di caratterizzazione

Le quattro proprietà fondamentali che abbiamo studiato in questa sezione possono essere *caratterizzate* attraverso le operazioni su relazioni introdotte nella Sezione 2.2.

Teorema 2.4.34. *Per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$ vale che:*

1. *R è totale se e solo se $Id_A \subseteq R; R^{op}$;*
2. *R è univalente se e solo se $R^{op}; R \subseteq Id_B$;*
3. *R è surgettiva se e solo se $Id_B \subseteq R^{op}; R$;*
4. *R è iniettiva se e solo se $R; R^{op} \subseteq Id_A$.*

Dimostrazione. Dimostriamo il primo punto. Trattandosi di un se e solo se, possiamo dividere la dimostrazioni in due parti:

- Se R è totale, allora $Id_A \subseteq R; R^{op}$. Assumendo che R sia totale, dobbiamo dimostrare che $Id_A \subseteq R; R^{op}$, cioè che per tutti gli $a \in A$, $(a, a) \in R; R^{op}$.

  Prendiamo un qualsiasi elemento $a \in A$. Visto che R è totale, allora sappiamo che esiste almeno un $b \in B$ tale che $(a, b) \in R$. Per definizione di R^{op} abbiamo inoltre che $(b, a) \in R^{op}$. Pertanto, per definizione della composizione, si ha che $(a, a) \in R; R^{op}$.

- Se $Id_A \subseteq R; R^{op}$, allora R è totale. Assumendo che $Id_A \subseteq R; R^{op}$, dobbiamo dimostrare che R è totale, cioè che per tutti gli $a \in A$, esiste almeno un $b \in B$ tale che $(a, b) \in R$.

  Prendiamo un qualsiasi elemento $a \in A$. Visto che $Id_A \subseteq R; R^{op}$, si ha che $(a, a) \in R; R^{op}$. Per definizione di composizione, questo significa che esiste almeno un $b \in B$ tale che $(a, b) \in R$ e $(b, a) \in R^{op}$.

Dimostriamo ora il secondo punto. Trattandosi di un se e solo se, possiamo dividere la dimostrazioni in due parti:

- Se R è univalente, allora $R^{op}; R \subseteq Id_B$. Assumendo che R sia univalente, dobbiamo dimostrare che $R^{op}; R \subseteq Id_B$, cioè che per tutti gli $(x, y) \in R; R^{op}$, si ha che $(x, y) \in Id_B$, vale a dire che $x = y$.

  Prendiamo una qualsiasi coppia $(x, y) \in R^{op}; R$. Per definizione di composizione, esiste un $a \in A$ tale che $(x, a) \in R^{op}$ e $(a, y) \in R$. Visto che $(x, a) \in R^{op}$, si ha che $(a, x) \in R$. Essendo R univalente, da $(a, x) \in R$ e $(a, y) \in R$ si può concludere che $x = y$.

- Se $R^{op}; R \subseteq Id_B$, allora R è univalente. Assumendo che $R^{op}; R \subseteq Id_B$, dobbiamo dimostrare che R è univalente, cioè che per tutti gli $a \in A$, esiste al più un $b \in B$ tale che $(a, b) \in R$.

  Prendiamo un qualsiasi elemento $a \in A$ ed assumiamo che $(a, x) \in R$ e $(a, y) \in R$ per qualche $x, y \in B$. Per definizione di R^{op}, si ha che $(x, a) \in R^{op}$ e, per definizione di composizione, che $(x, y) \in R^{op}; R$. Visto che $R^{op}; R \subseteq Id_B$, si ha che $x = y$. Questo prova che R è univalente.

Dimostriamo il terzo punto, utilizzando il primo punto ed i risultati di dualità.

R è surgettiva se e solo se	$R^{op}\colon B \leftrightarrow A$ è totale	(Proposizione 2.4.32.1)
se e solo se	$Id_B \subseteq R^{op}; (R^{op})^{op}$	(primo punto)
se e solo se	$Id_B \subseteq R^{op}; R$	(convoluzione)

Lasciamo la dimostrazione del quarto punto come esercizio. ∎

Esercizio 2.4.35. *Dimostrare il Teorema 2.4.34.4.*

Chiusura per composizione

Il precedente teorema ci fornisce una caratterizzazione che ci sarà utile in più occasioni. Adesso mostriamo come il teorema può essere utile per dimostrare che prese due relazioni che soddisfano una delle quattro proprietà, la loro composizione soddisfa ancora tale proprietà.

Proposizione 2.4.36. *Per tutti gli insiemi A, B, C e per tutte le relazioni $R\colon A \leftrightarrow B$, $S\colon B \leftrightarrow C$ vale che:*

1. *Se R e S sono totali, allora $R; S$ è totale.*
2. *Se R e S sono univalenti, allora $R; S$ è univalente.*
3. *Se R e S sono surgettive, allora $R; S$ è surgettiva.*
4. *Se R e S sono iniettive, allora $R; S$ è iniettiva.*

Mostriamo prima una dimostrazione per sostituzione che utilizza la caratterizzazione fornita dal Teorema 2.4.34.

Dimostrazione per sostituzione. Dimostriamo solo il primo punto e lasciamo gli altri per esercizio.

1. Se $Id_A \subseteq R; R^{op}$ e $Id_B \subseteq S; S^{op}$, allora $Id_A \subseteq (R; S); (R; S)^{op}$.

$$\begin{aligned}
Id_A &\subseteq R; R^{op} && (R \text{ totale})\\
&\subseteq R; Id_B; R^{op} && (\text{unità})\\
&\subseteq R; (S; S^{op}); R^{op} && (S \text{ totale})\\
&\subseteq (R; S); (S^{op}; R^{op}) && (\text{associatività})\\
&\subseteq (R; S); (R; S)^{op} && (\text{distributività})
\end{aligned}$$

■

Esercizio 2.4.37. *Dimostrare per sostituzione le Proposizioni 2.4.36.2, 2.4.36.3 e 2.4.36.4.*

Esercizio 2.4.38. *Dimostrare per sostituzione che per tutti gli insiemi A, la relazione identità $Id_A\colon A \leftrightarrow A$ è totale, univalente, surgettiva e iniettiva.*

Esercizio 2.4.39. *Dimostrare per sostituzione che per tutti gli insiemi A, B, la relazione vuota $\varnothing\colon A \leftrightarrow B$ è univalente e iniettiva.*

Esercizio 2.4.40. *Dimostrare per sostituzione che per tutti gli insiemi A, B, la relazione completa $A \times B\colon A \leftrightarrow B$ è totale e surgettiva.*

Mostriamo adesso una dimostrazione discorsiva del Teorema 2.4.36.

Dimostrazione discorsiva. Dimostriamo i primi tre punti. Il quarto lo lasciamo come esercizio.

1. Se R e S sono totali, allora $R; S$ è totale. Assumendo che R e S siano totali, dobbiamo dimostrare che $R; S$ è totale, cioè che per tutti gli $a \in A$, esiste almeno un $c \in C$ tale che $(a, c) \in R; S$.

   Prendiamo un qualsiasi elemento $a \in A$. Visto che R è totale, allora esiste almeno un $b \in B$ tale che $(a, b) \in R$. Visto che S è totale allora esiste almeno un elemento $c \in C$ tale che $(b, c) \in S$. Per definizione di composizione abbiamo che $(a, c) \in R; S$.

2. Se R e S sono univalenti, allora $R; S$ è univalente. Assumendo che R e S siano univalenti, dobbiamo dimostrare che $R; S$ è univalente, cioè che per tutti gli $a \in A$, esiste al più un $c \in C$ tale che $(a, c) \in R; S$.

   Prendiamo un qualsiasi elemento $a \in A$ ed assumiamo che $(a, x) \in R; S$ e $(a, y) \in R; S$ per qualche $x, y \in C$. Per la definizione di composizione, si ha che devono esiste $u, v \in B$ tali che: (1) $(a, u) \in R$, (2) $(u, x) \in S$, (3) $(a, v) \in R$ e (4) $(v, y) \in R$. Visto che R è univalente, da (1) e (3) si può dedurre che $u = v$. Visto che S è univalente, da (2) e (4) e dal fatto che $u = v$ si può dedurre che $x = y$. Pertanto $R; S$ è univalente.

3. Se R e S sono surgettive, allora $R; S$ è surgettiva. Si dimostra questo risultato utilizzando quello di sopra e i risultati di dualità. Se R e S sono surgettive, allora $R^{op}\colon B \leftrightarrow A$ e $S^{op}\colon C \leftrightarrow B$ sono totali. Pertanto, per il risultato appena dimostrato, $S^{op}; R^{op}$ è totale. Quindi, per la Proposizione 2.4.30.1 $(S^{op}; R^{op})^{op}$ è surgettiva. Si osservi che

$$\begin{aligned}(S^{op}; R^{op})^{op} &= (R^{op})^{op}; (S^{op})^{op} && \text{(distributività di } .^{op} \text{ su ;)}\\ &= R; S && \text{(convoluzione)}\end{aligned}$$

Pertanto $R; S$ è surgettiva.

■

Esercizio 2.4.41. *Dimostrare la Proposizione 2.4.36.4.*

Esercizio 2.4.42. *È vero che per tutti gli insiemi A, B e per tutte le relazioni $R, S\colon A \leftrightarrow B$ vale che:*

Se R e S sono totali, allora $R \cup S$ è totale?

In caso affermativo fornire una prova. In caso negativo fornire un controesempio.

Esercizio 2.4.43. *È vero che per tutti gli insiemi A, B e per tutte le relazioni $R, S\colon A \leftrightarrow B$ vale che:*

Se R e S sono totali, allora $R \cap S$ è totale?

In caso affermativo fornire una prova. In caso negativo fornire un controesempio.

Esercizio 2.4.44. *È vero che per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$, $S\colon B \leftrightarrow C$ vale che:*

Se $R; S$ è totale, allora anche R e S sono totali?

In caso affermativo fornire una prova. In caso negativo fornire un controesempio.

2.5 Funzioni

Definizione 2.5.1. *[funzione] Siano A e B due insiemi. Una relazione $R \in Rel(A, B)$ è una* FUNZIONE *se è totale e univalente.*

Esempio 2.5.2. *Sia $A = \{x, y, z\}$ e $B = \{a, b, c, d\}$. La relazione*

$$R = \{(x, a),\ (y, a),\ (z, d)\}\colon A \leftrightarrow B$$

è una funzione, mentre la relazione

$$S = \{(x, c),\ (x, d),\ (y, d),\ (z, d)\}\colon A \leftrightarrow B$$

non è una funzione perché non è univalente.

È fondamentale osservare che per definizione $R\colon A \leftrightarrow B$ è totale se e solo se

per ogni $a \in A$, esiste *almeno un* $b \in B$ tale che $(a, b) \in R$

mentre $R\colon A \leftrightarrow B$ è univalente se e solo se

per ogni $a \in A$, esiste *al più un* $b \in B$ tale che $(a, b) \in R$.

Pertanto $R\colon A \leftrightarrow B$ è una funzione se e solo se

per ogni $a \in A$, esiste *esattamente un* $b \in B$ tale che $(a, b) \in R$.

Notazione 2.5.3. *Solitamente le funzioni vegono denotate da lettere minuscole, tipicamente* $f, g, h, \ldots$ *Anziché dire una funzione* tra A e B, *come nelle relazioni, si dice una funzione* da A a B. *Anziché scrivere* $f\colon A \leftrightarrow B$, *si scrive* $f\colon A \to B$. *Inoltre si scrive* $f(a)$ *per denotare l'unico elemento* $b \in B$ *tale che* $(a, b) \in f$. *Per enfatizzare che tale elemento è* b, *si scrive* $f(a) = b$. *L'insieme di tutte le funzioni da* A *a* B *è denotato da* $Fun(A, B)$, *quindi* $Fun(A, B) = \{f\colon A \to B\}$.

Esempio 2.5.4. *La relazione successore* $Succ\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *è una funzione, così come la relazione* $Plus\colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$ *(Esempio 2.1.9). In virtù di questo, d'ora in avanti, scriveremo* $succ\colon \mathbb{N} \to \mathbb{N}$ *e* $plus\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. *Invece la relazione* $Pred\colon \mathbb{N} \leftrightarrow \mathbb{N}$ *non è una funzione perché non è totale.*

Esempio 2.5.5. *Per tutti gli insiemi* A, *la relazione identità* $Id_A\colon A \leftrightarrow A$ *è una funzione. In virtù di questo, d'ora in avanti, scriveremo* $id_A\colon A \to A$. *La relazione vuota* $\varnothing\colon A \leftrightarrow B$ *e la relazione completa* $A \times B$ *solitamente non sono funzioni.*

Esercizio 2.5.6. *Per quale insieme* A, *la relazione vuota* $\varnothing\colon A \leftrightarrow B$ *e la relazione completa* $A \times B$ *sono sicuramente funzioni?*

La notazione $f(a) = b$ può essere usata anche per definire funzioni: specificando $f(a) = b$ per ogni elemento a dell'insieme di partenza si definisce infatti una funzione.

Esempio 2.5.7. *La funzione* $R\colon A \to B$ *dell'Esempio 2.5.2 può essere definita come*

$$R(x) = a, \quad R(y) = a, \quad R(z) = d.$$

Quando la funzione è chiara dal contesto, piuttosto che scrivere $f(a) = b$, si può scrivere $a \mapsto b$.

Esempio 2.5.8. *La funzione* $R\colon A \to B$ *dell'Esempio 2.5.2 può essere definita come*

$$x \mapsto a, \quad y \mapsto a, \quad z \mapsto d.$$

Nel caso si considerino insiemi di partenza non finiti, questa notazione è abbastanza sconveniente perché necessita la specifica di $f(a) = b$ per gli infiniti elementi a dell'insieme di partenza (o i soliti puntini sospensivi $\ldots$).

Esempio 2.5.9. *La funzione* $succ\colon \mathbb{N} \to \mathbb{N}$ *può essere definita come*

$$succ(0) = 1, \quad succ(1) = 2, \quad succ(2) = 3, \quad \ldots$$

In questi casi un modo conveniente di specificare funzioni è quello di usare delle espressioni con variabili:

$$f(x) = \langle \text{espressione il cui valore può dipendere da } x \rangle$$

L'idea è che per calcolare l'elemento associato ad un certo valore v dalla funzione f basta sostituire v al posto di x nell'espressione e valutare il risultato.

Esempio 2.5.10.

- $f_1(x) = x$
- $f_2(x) = x + 1$
- $f_3(x) = -x$
- $f_4(x) = x/2$
- $f_5(x) = \sqrt{x}$

Ma attenzione: di quale insieme di partenza e di arrivo stiamo parlando? Bisogna sempre chiarire quali siano gli insiemi di riferimento!

Per esempio la funzione f_1 può essere definita per ogni insieme A: questa è difatti la funzione identità $id_A\colon A \to A$. Invece la funzione f_2 non può essere definita per ogni insieme, perchè l'espressione $x + 1$ ha significato solamente negli insiemi di numeri (come $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$). La funzione f_3 necessita dell'operazione di sottrazione $-$ e quindi non può essere definita sui numeri naturali, ma può essere definita sugli interi $\mathbb{Z}$. Similmente, per f_4 non sono sufficienti gli interi ma può essere definita sui razionali $\mathbb{Q}$. Ed infine per f_5 i numeri razionali non sono sufficienti ma questa funzione può essere definita sui reali positivi $\mathbb{R}^+$.

Nel capitolo 3 vedremo come si può definire in modo rigoroso, usando l'*induzione*, una funzione avente come insieme di partenza i numeri naturali. In seguito nel capitolo 7 vedremo come questa tecnica può essere sfuttata per definire funzioni su di un qualunque insieme di partenza che sia stato definito induttivamente.

Le funzioni che solitamente sono studiate nei corsi di Analisi Matematica sono funzioni $f : \mathbb{R} \to \mathbb{R}$ dove l'insieme di partenza e quello di arrivo sono quello dei numeri reali $\mathbb{R}$ (o dei loro sottoinsiemi). Per questa ragione, spesso tali insiemi sono sottointesi e non vengono specificati.

In questo corso invece, e più in generale in tutta l'Informatica, consideriamo spesso funzioni tra insiemi che non sono numerici ed è quindi fondamentale **specificare sempre l'insieme di partenza e di arrivo.** Infatti, i programmi che scriviamo con i linguaggi di programmazione spesso sono funzioni dove l'insieme di partenza rappresenta l'insieme dei possibili valori di input del programma e l'insieme di arrivo l'insieme dei valori di output.

$$\texttt{INPUT} \longrightarrow \boxed{\;f\;} \longrightarrow \texttt{OUTPUT}$$

Di seguito mostriamo un esempio fondamentale nell'informatica.

Esempio 2.5.11. *Si consideri l'insieme dei valori booleani Bool* $= \{\mathsf{t}, \mathsf{f}\}$*. La funzione* $\neg : Bool \to Bool$*, chiamata* NEGAZIONE*, è definita come:*

$$\neg(\mathsf{t}) = \mathsf{f} \qquad\qquad \neg(\mathsf{f}) = \mathsf{t}$$

In una funzione $f : A \to B$, l'insieme di partenza A può essere anche il prodotto cartesiano di due insiemi, vale a dire $A = A_1 \times A_2$ per qualche insieme A_1 e A_2. In tal caso, anziché scrivere $f(\,(a_1, a_2)\,)$ (che, formalmente denota l'elemento associato da f alla coppia $(a_1, a_2) \in A_1 \times A_2$) scriveremo più semplicemente $f(a_1, a_2)$.

Esempio 2.5.12. *Si consideri l'insieme dei valori booleani Bool* $= \{\mathsf{t}, \mathsf{f}\}$*. La funzione* $\wedge : Bool \times Bool \to Bool$*, chiamata* CONGIUNZIONE*, è definita come:*

$$\begin{aligned} \wedge(\mathsf{t}, \mathsf{t}) &= \mathsf{t} \\ \wedge(\mathsf{f}, \mathsf{t}) &= \mathsf{f} \\ \wedge(\mathsf{t}, \mathsf{f}) &= \mathsf{f} \\ \wedge(\mathsf{f}, \mathsf{f}) &= \mathsf{f} \end{aligned}$$

La funzione $\vee : Bool \times Bool \to Bool$*, chiamata* DISGIUNZIONE*, è definita come:*

$$\begin{aligned} \vee(\mathsf{t}, \mathsf{t}) &= \mathsf{t} \\ \vee(\mathsf{f}, \mathsf{t}) &= \mathsf{t} \\ \vee(\mathsf{t}, \mathsf{f}) &= \mathsf{t} \\ \vee(\mathsf{f}, \mathsf{f}) &= \mathsf{f} \end{aligned}$$

Esempio 2.5.13. *Un altro esempio di funzione in cui l'insieme di partenza è il prodotto cartesiano è la funzione* $plus : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*. Con la notazione descritta sopra si ha, ad esempio che*

$$plus(2, 1) = 3$$

Le funzioni che hanno come insieme di partenza il prodotto cartesiano di un insieme sono dette *BINARIE*. Per le funzioni binarie, è comune utilizzare la notazione infissa.

Notazione 2.5.14. *Per le funzioni binarie anziché utilizzare la notazione* $f(x, y)$*, chiamata* NOTAZIONE PREFISSA*, si utilizza spesso la* NOTAZIONE INFISSA $x\,f\,y$*. Per esempio,* $plus(2, 1)$ *può essere scritto* $2\,plus\,1$ *(o più comunemente* $2 + 1$*) e* $\wedge(\mathsf{t}, \mathsf{t})$ *come* $\mathsf{t} \wedge \mathsf{t}$*.*

Diversamente dalla Matematica, in Informatica capita spesso di definire funzioni in cui l'insieme di partenza è il prodotto cartesiano di insiemi diversi.

Esempio 2.5.15. *Si consideri la funzione* $f\colon Bool \times \mathbb{N} \to \mathbb{N}$ *che, ad ogni coppia* $(x, y) \in Bool \times \mathbb{N}$*, assegna* 0 *se* $x = \mathtt{f}$ *e* y *se* $x = \mathtt{t}$*. Come sottoinsieme di* $((Bool \times \mathbb{N}) \times \mathbb{N})$ *questa funzione è*

$$f = \{((\mathtt{f}, x), 0) \in (Bool \times \mathbb{N}) \times \mathbb{N} \mid x \in \mathbb{N}\} \cup \{((\mathtt{t}, x), x) \in (Bool \times \mathbb{N}) \times \mathbb{N} \mid x \in \mathbb{N}\}.$$

Altrimenti si può definire con la notazione

$$f(x, y) = \begin{cases} 0 & \text{se } x = \mathtt{f} \\ y & \text{se } x = \mathtt{t} \end{cases}$$

Durante il corso utilizzeremo questa notazione di tanto in tanto.

Proprietà e implicazione

La nozione di funzione ci permette di rendere formale il concetto di *proprietà* che abbiamo utilizzato informalmente nella Sezione 1.1.

Per introdurre questo concetto è conveniente utilizzare degli esempi: *essere più alto di un 1 metro*, *essere nato prima del 1990*, *essere biondo*, o *aver superato l'esame di Fondamenti* sono proprietà sull'insieme degli esseri umani. Intuitivamente questo significa che ogni essere umano può soddisfare oppure non soddisfare una qualunque di queste proprietà.

In modo del tutto analogo, *essere multiplo di 3* o *essere primo* sono proprietà sull'insieme $\mathbb{N}$ dei numeri naturali. Nuovamente, ogni numero naturale o è un multiplo di 3 o non lo è; o è primo oppure non lo è.

A livello intuitivo, una proprietà P su un insieme A è un'entità che, per ogni elemento $a \in A$, ci dice se a soddisfa la proprietà oppure no. Più formalmente una proprietà P su A è una funzione $P\colon A \to Bool$.

Definizione 2.5.16 (proprietà)**.** *Sia* A *un insieme. Una* PROPRIETÀ SU A *è una funzione che ha come insieme di partenza* A *e come insieme di arrivo* $Bool$*. Per ogni elemento* $a \in A$*, si dice che* a soddisfa *la proprietà* P *se* $P(a) = \mathtt{t}$*, mentre si dice che* a non soddisfa *la proprietà* P*, se* $P(a) = \mathtt{f}$*.*

Nel seguito di questo testo, come avviene in generale in Matematica e in Informatica, per una proprietà P spesso scriveremo $P(a)$ al posto di $P(a) = \mathtt{t}$ e $\neg P(a)$ per $P(a) = \mathtt{f}$.

Date due proprietà P e Q definite su uno stesso insieme A, queste possono essere combinate utilizzando le funzioni booleane introdotte negli Esempi 2.5.11 e 2.5.12. Ad esempio la proprietà $P \wedge Q\colon A \to Bool$ è definita per ogni $a \in A$ come

$$P(a) \wedge Q(a)$$

dove $\wedge\colon Bool \times Bool \to Bool$ è la funzione su Booleani definita nell'Esempio 2.5.12. Si noti che $P \wedge Q(a) = \mathtt{t}$ se e solo se entrambi le propriet à sono vere su a, cio è $P(a) = \mathtt{t}$ e $Q(a) = \mathtt{t}$.

In modo del tutto analogo $P \vee Q\colon A \to Bool$ è definita per ogni $a \in A$ come

$$P(a) \vee Q(a)$$

dove $\vee\colon Bool \times Bool \to Bool$ è la funzione su Booleani definita nell'Esempio 2.5.12. In altre parole $P \vee Q(a) = \mathtt{t}$ se e solo se almeno uno tra $P(a)$ e $Q(a)$ vale $\mathtt{t}$.

Infine la proprietà $\neg P\colon A \to Bool$ è definita similmente utilizzando la funzione $\neg\colon Bool \to Bool$ dell'Esempio 2.5.11: $\neg P(a) = \mathtt{t}$ se e solo se $P(a) = \mathtt{f}$.

Esiste un altro modo di combinare proprietà la cui comprensione è di importanza fondamentale. Come nel caso di $\neg$, $\vee$ e $\wedge$ si può definire a partire da una funzione binaria su booleani.

Definizione 2.5.17 (Implicazione)**.** *Si consideri l'insieme dei valori booleani* $Bool = \{\mathtt{t}, \mathtt{f}\}$*. La funzione* $\Rightarrow\colon Bool \times Bool \to Bool$*, chiamata* IMPLICAZIONE*, è definita come:*

$$\Rightarrow (\mathtt{t}, \mathtt{t}) = \mathtt{t}$$

$$\Rightarrow (\mathtt{f}, \mathtt{t}) = \mathtt{t}$$
$$\Rightarrow (\mathtt{t}, \mathtt{f}) = \mathtt{f}$$
$$\Rightarrow (\mathtt{f}, \mathtt{f}) = \mathtt{t}$$

Come nel caso di $\vee$ e $\wedge$, si preferisce spesso utilizzare la notazione infissa. Ad esempio, piuttosto che scrivere $\Rightarrow (\mathtt{t}, \mathtt{t})$ si scrive $\mathtt{t} \Rightarrow \mathtt{t}$.

Si noti come la funzione $\Rightarrow$ restituisca $\mathtt{f}$ in uno solo dei quattro casi possibili: quando il primo argomento è vero ($\mathtt{t}$) ed il secondo è falso ($\mathtt{f}$). Infatti, $\Rightarrow$ cattura il significato intuitivo dell'implicazione: il primo argomento è la *premessa* e il secondo argomento è la *conseguenza*. Un'implicazione è falsa solamente quando la premessa è vera e la conseguenza è falsa.

Il significato dell'implicazione risulta ancora più chiaro quando si utilizza per comporre proprietà: la proprietà $P \Rightarrow Q \colon A \to Bool$ è definita per ogni $a \in A$ come

$$P(a) \Rightarrow Q(a)$$

dove $\Rightarrow \colon Bool \times Bool \to Bool$ è la funzione su Booleani della Definizione 2.5.17. Quando la premessa $P(a)$ è falsa, l'implicazione $P \Rightarrow Q$ assegna automaticamente $\mathtt{t}$ ad a. Quando $P(a)$ è vera, per valutare l'implicazione è necessario conoscere il valore di verità della conseguenza $Q(a)$: quando $Q(a) = \mathtt{t}$, l'implicazione è vera; quando $Q(a) = \mathtt{f}$, l'implicazione è falsa.

Abbiamo detto che $\neg P$, $P \vee Q$ e $P \wedge Q$ in italiano si leggono come *non* P, P *oppure* Q e P e Q. L'implicazione $P \Rightarrow Q$ si legge come

$$\textit{se } P \textit{ allora } Q.$$

Alcuni risultati incontrati fino ad ora (ad esempio nelle Proposizioni 1.4.12, 1.4.13, 1.7.5 2.4.36) utilizzano *se* ... *allora* .... Formalmente questi risultati sono delle implicazioni $P \Rightarrow Q$. Il loro significato intuitivo è che *se* per un elemento a vale la premessa $P(a)$ *allora* deve valere anche la conseguenza $Q(a)$. Altrimenti se $P(a)$ non vale, non sappiamo niente del valore di verità di $Q(a)$.

Lo studente potrà riconoscere le implicazioni tra i risultati che presenteremo d'ora in avanti. Inoltre nel Capitolo 9 torneremo ad approfodire le proprietà e le loro combinazioni.

Composizione di funzioni

In prima approssimazione, dal momento che sono relazioni, le funzioni potrebbero essere combinate con le operazioni su relazioni che abbiamo visto nella Sezione 2.2. Sfortunatamente questo in molti casi non è possibile perché il risultato di tale operazione è una relazione ma non una funzione.

Prendiamo per esempio l'operazione di relazione opposta: la relazione opposta di una funzione è sicuramente una relazione surgettiva e iniettiva (grazie alla Proposizione 2.4.30), ma solitamente questa non è una funzione. Per un esempio concreto, il lettore può osservare che $succ \colon \mathbb{N} \to \mathbb{N}$ è una funzione, mentre $Pred = succ^{op} \colon \mathbb{N} \leftrightarrow \mathbb{N}$ non è una funzione.

In modo del tutto analogo, le operazioni insiemistiche falliscono nel restituire una funzione: se $f \colon A \to B$ e $g \colon A \to B$ sono due funzioni, allora $f \cap g \colon A \leftrightarrow B$ sarà ancora univalente, ma in generale non sarà totale. Similmente $f \cup g \colon A \leftrightarrow B$ sarà totale, ma non univalente.

L'unica operazione che preserva la proprietà di restituire funzioni è l'operazione di composizione.

Proposizione 2.5.18. *Per tutti gli insiemi A, B, C e per tutte le funzioni $f \colon A \to B$ e $g \colon B \to C$, la relazione $f; g$ è una funzione.*

Dimostrazione. Assumendo che f e g siano totali e univalenti, dobbiamo dimostrare che $f; g$ è totale e univalente.

Dalla Proposizione 2.4.36.1, si ha che $f; g$ è totale, visto che f e g sono totali. Dalla Proposizione 2.4.36.2, si ha che $f; g$ è univalente, visto che f e g sono univalenti. ∎

Visto che le leggi illustrate nella Sezione 2.3 valgono per tutte le relazioni, valgono in particolare anche per le funzioni.

Proposizione 2.5.19. *Per tutti gli insiemi A, B, C, D e per tutte le funzioni $f \colon A \to B$, $g \colon B \to C$, $h \colon C \to D$ vale che:*

1. $f;(g;h) = (f;g);h$; *(associatività)*

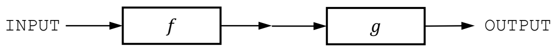
2. $id_A; f = f = f; id_B$. *(unità)*

È importante notare che, come per le relazioni, le funzioni possono essere composte solo se l'insieme di arrivo della prima coincide con l'insieme di partenza della seconda.

Esempio 2.5.20. *La funzione* $f\colon Bool \times \mathbb{N} \to \mathbb{N}$ *dell'Esempio 2.5.15 può essere composta con la funzione* $succ\colon \mathbb{N} \to \mathbb{N}$. *La funzione risultante* $f; succ\colon Bool \times \mathbb{N} \to \mathbb{N}$ *è definita come*

$$(x,y) \mapsto \begin{cases} 1 & se\ x = \mathtt{f} \\ y+1 & se\ x = \mathtt{t} \end{cases}$$

In Informatica si usa spesso la composizione di programmi visti come funzioni: $f;g$ significa intuitivamente che prima viene eseguito il programma f e poi l'output di questo viene passato come input al programma g.



La composizione di funzioni è molto importante anche in Matematica (per esempio, per calcolare le derivate) ma viene spesso utilizzata una notazione diversa.

Notazione 2.5.21. *La composizione* $f;g$ *viene talvolta indicata come* $g \circ f$, *oppure, omettendo* $\circ$, *da* gf. *Inoltre l'elemento* $f;g(a)$ *viene denotato come* $g(f(a))$ *oppure, omettendo le parentesi più esterne, come* $gf(a)$.

Per esempio per dire che f è la composizione della funzione seno $sin\colon \mathbb{R} \to \mathbb{R}$ e della funzione coseno $cos\colon \mathbb{R} \to \mathbb{R}$, si scrive $f(x) = cos(sin(x))$.

Teorema di caratterizzazione

Il Teorema 2.4.34 fornisce una caratterizzazione per le quattro proprietà fondamentali. Grazie a tale teorema, si ottiene banalmente una caratterizzazione delle funzioni.

Teorema 2.5.22. *Per tutti gli insiemi* A, B *e per tutte le relazioni* $R\colon A \leftrightarrow B$ *vale che:*

$$R \text{ è una funzione se e solo se } id_A \subseteq R; R^{op} \text{ e } R^{op}; R \subseteq id_B.$$

Esercizio 2.5.23. *Dimostrare il Teorema 2.5.22 utilizzando il Teorema 2.4.34.*

Il seguente risultato ci sarà utile in seguito per dimostrare il Teorema 2.6.16.

Proposizione 2.5.24. *Per tutti gli insiemi* A, B *e per tutte le relazioni* $R\colon A \leftrightarrow B$ *e* $S\colon B \leftrightarrow A$ *vale che se* $id_A \subseteq R; S$ *e* $S; R \subseteq id_B$, *allora* $S = R^{op}$.

Dimostrazione. Dimostriamo separatamente $S \subseteq R^{op}$ e $R^{op} \subseteq S$ e concludiamo con l'antisimmetria di $\subseteq$ (Proposizione 1.4.13).

- $S \subseteq R^{op}$. Dobbiamo dimostrare che, presa una generica coppia $(x,y) \in S$, questa appartiene anche a R^{op}.

  Prendiamo $(x,y) \in S$. Si ha che $(y,y) \in id_A$ e, utilizzando l'ipotesi $id_A \subseteq R; S$, possiamo concludere che $(y,y) \in R; S$. Per la defnizione di composizione, esiste almeno un $z \in B$ tale che $(y,z) \in R$ e $(z,y) \in S$.

  Utilizzando la definizione di composizione, da $(x,y) \in S$ e $(y,z) \in R$, possiamo concludere che $(x,z) \in S; R$. Utilizzando l'ipotesi $S; R \subseteq id_B$, da $(x,z) \in S; R$ possiamo conludere che $x = z$. Da $x = z$ e $(y,z) \in R$, possiamo concludere che $(y,x) \in R$. Per defnizione di relazione opposta, $(x,y) \in R^{op}$.

- $R^{op} \subseteq S$. Dobbiamo dimostrare che, presa una generica coppia $(x, y) \in R^{op}$, questa appartiene anche ad S.

  Prendiamo $(x, y) \in R^{op}$. Per definzione di relazione opposta, si ha che $(y, x) \in R$. Si ha che $(y, y) \in id_A$ e, utilizzando l'ipotesi $id_A \subseteq R; S$, possiamo concludere che $(y, y) \in R; S$. Per la definzione di composizione, esiste almeno un $z \in B$ tale che $(y, z) \in R$ e $(z, y) \in S$.

  Utilizzando la definizione di composizione, da $(z, y) \in S$ e $(y, x) \in R$, possiamo concludere che $(z, x) \in S; R$. Utilizzando l'ipotesi $S; R \subseteq id_B$, da $(z, x) \in S; R$ possiamo concludere che $x = z$. Pertanto $(x, y) \in S$.

■

Funzioni Parziali

Abbiamo spiegato a livello intuitivo che un programma calcola una funzione. Talvolta il calcolo può non andare a buon fine: il programma può per esempio restituire un messaggio di errore o addirittura non terminare. In questo caso non è vero che per tutti i valori di input il programma restituisce un output, cioè la funzione calcolata da un programma potrebbe non essere una relazione totale, ma solamente univalente.

Definizione 2.5.25 (funzione parziale)**.** *Siano A e B due insiemi ed R una relazione tra di loro. $R\colon A \leftrightarrow B$ si dice una* FUNZIONE PARZIALE *se R è univalente.*

Se $R\colon A \leftrightarrow B$ è una funzione parziale e $a \in A$, diciamo che R È DEFINITA SU *a se esiste un $b \in B$ tale che $(a, b) \in R$, altrimenti diciamo che R* NON È DEFINITA SU *a.*

Per le funzioni parziali, si utilizza la stessa notazione che abbiamo descritto per le funzioni.

Esempio 2.5.26. *Si consideri $f\colon \mathbb{R} \to \mathbb{R}$ definita come*

$$f(x) = 1/x$$

La divisione di qualunque numero n per 0 non è definita. Per questa ragione f è una funzione parziale.

Come per le funzioni, le funzioni parziali possono essere composte e la loro composizione è associativa.

Proposizione 2.5.27. *Per tutti gli insiemi A, B, C e per tutte le funzioni parziali $f\colon A \to B$ e $g\colon B \to C$, la relazione $f; g$ è una funzione parziale.*

Proposizione 2.5.28. *Per tutti gli insiemi A, B, C, D e per tutte le funzioni parziali $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ vale che:*

1. *$f; (g; h) = (f; g); h$; (associatività)*
2. *$id_A; f = f = f; id_B$. (unità)*

Esercizio 2.5.29. *Dimostrare le Proposizioni 2.5.27 e 2.5.28.*

Funzioni surgettive ed iniettive

Il lettore avrà probabilmente sentito parlare di funzioni surgettive ed iniettive: queste sono relazioni che sono funzioni (quindi totali e univalenti) ed in aggiunta godono della proprietà surgettiva o di quella iniettiva.

Definizione 2.5.30 (funzione surgettiva)**.** *Siano A e B due insiemi ed R una relazione tra di loro. $R\colon A \leftrightarrow B$ si dice una* FUNZIONE SURGETTIVA *se R è totale, univalente e surgettiva.*

Definizione 2.5.31 (funzione iniettiva)**.** *Siano A e B due insiemi ed R una relazione tra di loro. $R\colon A \leftrightarrow B$ si dice una* FUNZIONE INIETTIVA *se R è totale, univalente e iniettiva.*

Come per le funzioni e le funzioni parziali, le funzioni surgettive ed iniettive possono essere composte

Proposizione 2.5.32. *Per tutti gli insiemi A, B, C e per tutte le funzioni surgettive $f : A \to B$ e $g : B \to C$, la relazione $f ; g$ è una funzione surgettiva.*

Proposizione 2.5.33. *Per tutti gli insiemi A, B, C e per tutte le funzioni iniettive $f : A \to B$ e $g : B \to C$, la relazione $f ; g$ è una funzione iniettiva.*

Esercizio 2.5.34. *Dimostrare le Proposizioni 2.5.32 e 2.5.33.*

2.6 Biiezioni

Le funzioni che sono allo stesso tempo surgettive ed iniettive sono particolarmente importanti e vengono dette biiezioni.

Definizione 2.6.1 (Biiezione)**.** *Siano A e B due insiemi ed R una relazione tra di loro. $R : A \leftrightarrow B$ si dice una* BIIEZIONE *se R è totale, univalente, surgettiva ed iniettiva. L'insieme delle biiezioni da A a B è denotato $Bii(A, B)$.*

È importante notare che ogni biiezione è anche una funzione. Per questo utilizzeremo la stessa notazione che abbiamo usato per le funzioni.

Esempio 2.6.2. *Per ogni insieme A, $id_A : A \to A$ è una biiezione.*

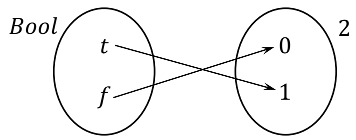
Esempio 2.6.3. *Si consideri l'insieme $Bool = \{\mathsf{t}, \mathsf{f}\}$ e l'insieme $2 = \{0, 1\}$. La relazione $i : Bool \to 2$*

$$\{(\mathsf{f}, 0),\ (\mathsf{t}, 1)\}$$

è una biiezione. Questa può anche essere specificata come

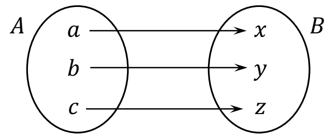
$$i(\mathsf{f}) = 0, \quad i(\mathsf{t}) = 1$$

e illustrata attraverso il seguente diagramma.



Esercizio 2.6.4. *Esiste un'altra biiezione da $Bool$ a 2?*

Esempio 2.6.5. *Si consideri l'insieme $A = \{a, b, c\}$ e l'insieme $B = \{x, y, z\}$. La relazione*



è una biiezione da A a B.

Esercizio 2.6.6. *Siano A e B gli insiemi dell'Esempio 2.6.5. Esistono altre biiezioni da A a B? In caso positivo, quante sono?*

Come per le funzioni, le biiezioni possono essere composte.

Proposizione 2.6.7. *Per tutti gli insiemi A, B, C e per tutte le biiezioni $f : A \to B$ e $g : B \to C$, la relazione $f ; g$ è una biiezione.*

Esercizio 2.6.8. *Dimostrare la Proposizione 2.6.7.*

Esiste però una differenza fondamentale tra funzioni e biiezioni: data una funzione $f : A \to B$ non necessariamente $f^{op} : B \leftrightarrow A$ è una funzione, invece se f è una biiezione, allora anche f^{op} lo è.

Proposizione 2.6.9. *Per tutti gli insiemi A, B e per tutte le biiezioni $f\colon A \to B$, la relazione f^{op} è una biiezione.*

Dimostrazione. Assumendo che f sia totale, univalente, surgettiva ed iniettiva, dobbiamo dimostrare che f^{op} ha le stesse proprietà.

- Grazie alla Proposizione 2.4.30.1, f^{op} è surgettiva perché f è totale.
- Grazie alla Proposizione 2.4.30.2, f^{op} è iniettiva perché f è univalente.
- Grazie alla Proposizione 2.4.32.1, f^{op} è totale perché f è surgettiva.
- Grazie alla Proposizione 2.4.32.2, f^{op} è univalente perché f è iniettiva.

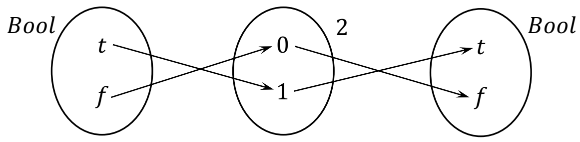
■

Esercizio 2.6.10. *Dimostrare che se f^{op} è una biiezione allora anche f lo è.*

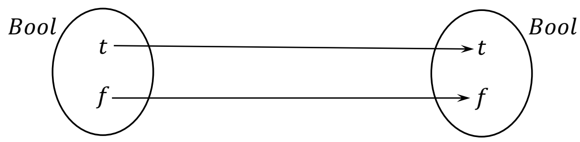
Esercizio 2.6.11. *Si ricordi la biiezione i dell'Esempio 2.6.3. Illustrare la sua biiezione opposta attraverso un diagramma.*

Esercizio 2.6.12. *Si ricordi la biiezione dell'Esempio 2.6.5. Illustrare la sua biiezione opposta attraverso un diagramma.*

Componendo una biiezione $f\colon A \to B$ con la sua biezione opposta $f^{op}\colon B \to A$ si ha che $f; f^{op} = id_A$. Per esempio, componendo la biiezione $i\colon Bool \to 2$ dell'Esempio 2.6.3 con $i^{op}\colon 2 \to Bool$



si ottiene $id_{Bool}\colon Bool \to Bool$.



Similmente componendo $f^{op}\colon B \to A$ con $f\colon A \to B$ si ottiene che $f^{op}; f = id_B$.

Questa proprietà fornisce una caratterizzazione delle biiezioni tra tutte le relazioni.

Teorema 2.6.13. *Per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$ vale che:*

$$R \text{ è una biiezione se e solo se } R; R^{op} = id_A \text{ e } R^{op}; R = id_B.$$

Esercizio 2.6.14. *Dimostrare il Teorema 2.6.13. Suggerimento: si utilizzi il Teorema 2.4.34.*

Teorema di caratterizzazione attraverso relazioni invertibili

La caratterizzazione fornita dal Teorema 2.6.13 può essere resa ancora più forte utilizzando la nozione di relazione inversa.

Definizione 2.6.15 (Relazione inversa). *Siano $R\colon A \leftrightarrow B$ e $S\colon B \leftrightarrow A$ due relazioni. Si dice che S è l'INVERSA di R se $R; S = id_A$ e $S; R = id_B$. Si dice che R è INVERTIBILE se esiste almeno una relazione inversa di R.*

Le trasformazioni invertibili giocano un ruolo chiave in moltissimi campi. Per esempio in Informatica, sono molto studiate per la Crittografia (la materia che studia come cifrare i messagi in modo sicuro) e nelle computazioni quantistiche. Purtroppo, questi argomenti non possono essere trattati in questo corso introduttivo e ci limiteremo quindi a fare funzioni invertibili il loro uso più classico, cioè quello di mettere in biiezione insiemi apparentemente distinti.

Teorema 2.6.16. *Per tutti gli insiemi A, B e per tutte le relazioni $R\colon A \leftrightarrow B$ vale che:*

R è una biiezione se e solo se R è invertibile.

Dimostrazione. Trattandosi di un se e solo se possiamo dimostrare separatamente che

- Se R è una biiezione, allora R è invertibile;
- Se R è invertibile, allora R è una biiezione.

Partiamo dal primo punto. Se R è una biiezione allora, grazie al Teorema 2.6.13, $R; R^{op} = id_A$ e $R^{op}; R = id_B$. Pertanto, prendendo $S = R^{op}$ si ha che R è invertibile.

Dimostriamo adesso il secondo punto. Se esite un S tale che $id_A = R; S$ e $S; R = id_B$, allora per la Proposizione 2.5.24, si ha che $S = R^{op}$. Pertanto, per il Teorema 2.6.13, R è una biiezione. ■

Nel resto delle note scriveremo R^{-1} al posto di R^{op} quando R è una biiezione, per enfatizzare che R^{op} è l'inversa di R.

Insiemi in biiezione

La caratterizzazione delle biiezioni come relazioni invertibili è molto interessante: dopo aver applicato una relazione invertibile $i\colon A \to B$ ad un qualsiasi elemento in A, è sempre possibile tornare indietro all'elemento originale utilizzando $i^{-1}\colon B \to A$. Viceversa, trasformando prima con $i^{-1}\colon B \to A$ è sempre possibile tornare all'elemento orginale utilizzando i.

$$a \overset{i}{\mapsto} b \overset{i^{-1}}{\mapsto} a$$

$$b \overset{i^{-1}}{\mapsto} a \overset{i}{\mapsto} b$$

Intuitivamente l'esistenza della biiezione $i\colon A \to B$ garantisce che ci possiamo spostare avanti e indietro tra gli elementi di A e gli elementi di B senza perdere alcuna "informazione". Questo permette quasi di identificare gli insiemi A e B come se fossero lo stesso insieme.

Definizione 2.6.17 (Insiemi in biiezione)**.** *Due insiemi A e B si dicono* IN BIIEZIONE *(o in corrispondenza uno a uno) se esiste una biiezione $i\colon A \to B$. In questo caso scriviamo $A \cong B$.*

Esempio 2.6.18. *Abbiamo mostrato che esiste una biiezione dall'insieme $Bool = \{\mathtt{t}, \mathtt{f}\}$ all'insieme $2 = \{0, 1\}$. I due insiemi sono quindi in biiezione: $Bool \cong 2$. È molto comune, in Informatica e in Logica identificare questi due insiemi, identificando $\mathtt{t}$ con 1 e $\mathtt{f}$ con 0.*

Esercizio 2.6.19. *Dimostrare che per tutti gli insiemi A, se $A \cong \varnothing$, allora $A = \varnothing$.*

Nella Definizione 2.5.16 abbiamo introdotto le proprietà su A come funzioni da A in $Bool$. Il seguente risultato ci dice un fatto abbastanza intuitivo: le proprietà su A sono in biiezione con i sottoinsiemi di A.

Proposizione 2.6.20. *Per tutti gli insiemi A, vale che:*

$$\mathcal{P}(A) \cong \mathit{Fun}(A, \mathit{Bool})$$

Dimostrazione. Ricordiamo che $\mathcal{P}(A)$ è l'insieme delle parti di A (Definizione 1.5.2), mentre $\mathit{Fun}(A, \mathit{Bool})$ è l'insieme di tutte le funzioni $f\colon A \to Bool = \{\mathtt{f}, \mathtt{t}\}$ (Notazione 2.5.3). Mostriamo per prima cosa una funzione $i\colon \mathcal{P}(A) \to \mathit{Fun}(A, \mathit{Bool})$. Per ogni insieme $B \subseteq A$, definiamo la sua *FUNZIONE CARATTERISTICA* $\chi_B\colon A \to Bool$ come

$$\chi_B(a) = \begin{cases} \mathtt{t} & \text{se } a \in B \\ \mathtt{f} & \text{se } a \notin B \end{cases}$$

Equivalentemente, possiamo definire questa funzione come una relazione, cioè un sottoinsieme di $A \times Bool$

$$\chi_B = \{(a, \mathtt{t}) \in A \times Bool \mid a \in B\} \cup \{(a, \mathtt{f}) \in A \times Bool \mid a \notin B\}$$

La funzione $i\colon \mathcal{P}(A) \to \mathit{Fun}(A, \mathit{Bool})$ mappa ogni $B \subseteq A$ nella sua funzione caratteristica χ_B.

$$\begin{array}{rccc} i\colon & \mathcal{P}(A) & \to & \mathit{Fun}(A, \mathit{Bool}) \\ & B \subseteq A & \mapsto & \chi_B \end{array}$$

Mostriamo ora una funzione $j\colon \mathit{Fun}(A, \mathit{Bool}) \to \mathcal{P}(A)$. Per ogni funzione $f\colon A \to \mathit{Bool}$, definiamo $\mathit{Sub}(f) \subseteq A$ come

$$\mathit{Sub}(f) = \{x \in A \mid f(x) = \mathtt{t}\}$$

La funzione j associa ad ogni $f\colon A \to \mathit{Bool}$ il sottoinsieme $\mathit{Sub}(f)$.

$$\begin{array}{rccc} j\colon & \mathit{Fun}(A, \mathit{Bool}) & \to & \mathcal{P}(A) \\ & f\colon A \to \mathit{Bool} & \mapsto & \mathit{Sub}(f) \end{array}$$

Per mostrare che i è una biiezione, mostriamo che j è la sua funzione inversa, cioè che

$$i; j = id_{\mathcal{P}(A)} \qquad \text{e} \qquad j; i = id_{\mathit{Fun}(A,\mathit{Bool})}$$

- $\underline{i; j = id_{\mathcal{P}(A)}}$ Dobbiamo dimostrare che per tutti i $B \in \mathcal{P}(A)$ vale che $j(i(B)) = id_{\mathcal{P}(A)}(B)$, cioè che $\mathit{Sub}(\chi_B) = B$. Ma questo è immediato perché per tutti gli $a \in A$

$$a \in \mathit{Sub}(\chi_B) \ \text{ se e solo se } \ \chi_B(a) = \mathtt{t} \ \text{ se e solo se } \ a \in B.$$

- $\underline{j; i = id_{\mathit{Fun}(A,\mathit{Bool})}}$ Dobbiamo dimostrare che per tutte le $f \in \mathit{Fun}(A, \mathit{bool})$ vale che $i(j(f)) = id_{\mathit{Fun}(A,\mathit{bool})}(f)$, cioè che $\chi_{\mathit{Sub}(f)} = f$. Ma questo è immediato perché per tutti gli $a \in A$, vale che:

$$\chi_{\mathit{Sub}(f)}(a) = \mathtt{t} \text{ se e solo se } a \in \mathit{Sub}(f) \text{ se e solo se } f(a) = \mathtt{t}$$

e

$$\chi_{\mathit{Sub}(f)}(a) = \mathtt{f} \text{ se e solo se } a \notin \mathit{Sub}(f) \text{ se e solo se } f(a) = \mathtt{f}.$$

■

Esempio 2.6.21. *Siano $A = \{a, b, c\}$ e $B = \{a, c\}$. La funzione caratteristica $\chi_B\colon A \to \mathit{Bool}$ è*

$$\begin{array}{rccc} \chi_B\colon & A & \to & \mathit{Bool} \\ & a & \mapsto & \mathtt{t} \\ & b & \mapsto & \mathtt{f} \\ & c & \mapsto & \mathtt{t} \end{array}$$

Esercizio 2.6.22. *Sia $A = \{a, b, c, d\}$. Illustrare la funzione caratteristica dei sottoinsiemi $\varnothing \subseteq A$, $A \subseteq A$ e $\{b, d\} \subseteq A$.*

Nell'Esercizio 1.6.5 abbiamo visto che il prodotto cartesiano non è associativo, cioè che in generale

$$A \times (B \times C) \neq (A \times B) \times C$$

Comunque l'associatività vale *a meno di biiezione*, cioè i due insiemi anche se diversi sono in biiezione.

Proposizione 2.6.23. *Per tutti gli insiemi A, B, C vale che*

$$A \times (B \times C) \cong (A \times B) \times C$$

Dimostrazione. La funzione $i \colon A \times (B \times C) \to (A \times B) \times C$ è definita come

$$(a,\ (b,c)) \mapsto ((a,b),\ c)$$

mentre la funzione $j \colon (A \times B) \times C \to A \times (B \times C)$ come

$$((a,b),\ c) \mapsto (a,\ (b,c)).$$

È immediato vedere che j è la funzione inversa di i. ∎

Il seguente risultato illustra un'importante biiezione che sta alla base della programmazione funzionale. Lasciamo la sua dimostrazione come esercizio.

Esercizio 2.6.24. *Dimostrare che per tutti gli insiemi A, B, C, vale che*

$$Fun(A \times B, C) \cong Fun(A, Fun(B, C))$$

Per $\cong$ valgono le stesse proprietà dell'uguaglianza insiemistica.

Proposizione 2.6.25. *Per tutti gli insiemi A, B, C vale che:*

1. $A \cong A$ *(riflessività);*
2. *Se $A \cong B$ e $B \cong C$, allora $A \cong C$ (transitività);*
3. *Se $A \cong B$, allora $B \cong A$ (simmetria).*

Dimostrazione. Dimostriamo i primi due punti e lasciamo il terzo come esercizio.

1. $A \cong A$. Per dimostrare che $A \cong A$ dobbiamo esibire una biiezione $i \colon A \to A$. Visto che l'insieme di arrivo e di partenza sono lo stesso insieme, possiamo prendere $id_A \colon A \to A$ che, come illustrato nell'Esempio 2.6.2, è una biiezione.

2. Se $A \cong B$ e $B \cong C$, allora $A \cong C$; Per dimostrare che $A \cong C$ dobbiamo esibire una biiezione $i \colon A \to C$. Per ipotesi abbiamo una biiezione $f \colon A \to B$ ed una biiezione $g \colon B \to C$. La loro composizione $f; g \colon A \to C$ è una biiezione per la Proposizione 2.6.7. Possiamo quindi prendere $i = f; g$.

∎

Esercizio 2.6.26. *Dimostrare la Proposizione 2.6.25.3*

Esercizio 2.6.27. *Dimostrare che per tutti gli insiemi A, A', B vale che*

$$\textit{se } A \cong A', \textit{ allora } Fun(A, B) \cong Fun(A', B).$$

Esercizio 2.6.28. *Dimostrare che per tutti gli insiemi A, B, B' vale che*

$$\textit{se } B \cong B', \textit{ allora } Fun(A, B) \cong Fun(A, B').$$

Esercizio 2.6.29. *Si ricordi che $1 = \{0\}$. Dimostrare che per tutti gli insiemi A, vale che*

$$A \times 1 \cong A$$

Esercizio 2.6.30. *Dimostrare che per tutti gli insiemi A, B, vale che*

$$A \times B \cong B \times A$$

2.7 n-uple, sequenze di lunghezza fissata e arbitraria

La Proposizione 2.6.23 ci dice che gli insiemi $A \times (B \times C)$ e $(A \times B) \times C$ anche se non sono uguali sono comunque in biiezione. Per questa ragione, prenderemo la libertà di scrivere

$$A \times B \times C$$

senza dover specificare le parentesi. Inoltre, denoteremo gli elementi di questo insieme come delle *TRIPLE*

$$(a, b, c)$$

dove $a \in A$, $b \in B$ e $c \in C$. Formalmente, $A \times B \times C = \{(a, b, c) \mid a \in A,\ b \in B,\ c \in C\}$. Quando il prodotto cartesiano è fra 4 insiemi A, B, C, D scriveremo

$$A \times B \times C \times D$$

e denoteremo gli elementi di questo insieme come delle *QUADRUPLE*

$$(a, b, c, d).$$

Per il prodotto cartesiano per 5 insiemi, faremo la stessa cosa e chiameremo i suo elementi quintuple. Lo stesso procedimento si applica ad un qualsiasi numero $n \in \mathbb{N}$ di insiemi e chiamiamo gli elementi n-uple. Per $n = 0$, esiste una sola 0-upla che denotiamo con $()$.

Le n-uple sono onnipresenti in Informatica. Infatti, mentre in matematica la maggior parte delle funzioni sono unarie o binarie, le funzioni che rappresentano programmi hanno spesso insiemi di partenza che sono il prodotto cartesiano di più di due insiemi.

Esempio 2.7.1. *Mostriamo come esempio una semplice variante dell'Esempio 2.5.15. Consideriamo la funzione $f\colon Bool \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definita come*

$$f(x, y, z) = \begin{cases} 0 & se\ x = \mathtt{f} \\ y + z & se\ x = \mathtt{t} \end{cases}$$

Questa funzione assegna ad ogni tripla $(x, y, z) \in Bool \times \mathbb{N} \times \mathbb{N}$, $y + z$ se $x = \mathtt{t}$ e 0 altrimenti. Si noti che il primo elemento della tripla deve essere un elemento di $Bool$, mentre il secondo e il terzo sono numeri naturali in $\mathbb{N}$.

Un caso di n-upla particolarmente interessante è quello in cui tutti gli insiemi coinvolti nel prodotto cartesiano sono uguali.

Definizione 2.7.2 (sequenze)**.** *Sia A un insieme. Una SEQUENZA SU A DI LUNGHEZZA n è una n-upla $(a_0, a_1, \ldots, a_{n-1})$ dove per tutti gli indici $i \in \{0, \ldots, n-1\}$, $a_i \in A$. L'insieme A^n di tutte le sequenze su A di lunghezza n è definito come:*

$$A^n = \{(a_0, a_1, \ldots, a_{n-1}) \mid (\forall i \in \{0, \ldots, n-1\} \,.\, a_i \in A)\}$$

Esempio 2.7.3. *Sia $A = \{a, b\}$. Allora*

$$\begin{array}{lcl} A^0 & = & \{()\} \\ A^1 & = & \{(a),\ (b)\} \\ A^2 & = & \{(a, a),\ (a, b),\ (b, a),\ (b, b)\} \\ A^3 & = & \{(a, a, a),\ (a, a, b),\ (a, b, a),\ (a, b, b),\ (b, a, a),\ (b, a, b),\ (b, b, a),\ (b, b, b)\} \\ `\ldots & = & \ldots \end{array}$$

Osservazione 2.7.4. *È interessante osservare che $A^0 \cong 1$, $A^1 \cong A$, $A^2 \cong A \times A$, $A^3 \cong A \times (A \times A)$ e, più in generale $A^n \cong A \times (\cdots \times (A \times A) \ldots)$. Questo può essere espresso attraverso l'induzione, un argomento che affronteremo in modo approfondito nel Capitolo 3 (si veda la Proposizione 3.1.4):*

$$\begin{array}{rcl} A^0 & \cong & 1 \\ A^{n+1} & \cong & A \times A^n \end{array}$$