UNIVERSITÀ DEGLI STUDI DI VERONA

Facoltà di Scienze
Dipartimento di Informatica — Settore di Matematica

# Matematica di base

ENRICO GREGORIO
FRANCESCA MANTESE

Dispense per il corso di laurea in Informatica

Anno accademico 2006-2007

# Indice

CAPITOLO 1

# Insiemi

## 1. Elementi e Classi

Lo scopo di questo primo capitolo è di introdurre in maniera rigorosa le nozioni di classe e insieme, e di studiarne le principali proprietà. Nel seguito useremo il termine *elemento* per indicare qualcosa a cui si attribuisce identità. Si noti che da un punto di vista matematico, nel definire un elemento si è interessati solo al fatto di potergli attribuire una identità, astraendo da tutte le sue caratteristiche eccetto quella di poter essere distinto da un altro elemento.

DEFINIZIONE 1.1. Si dice *classe* una collezione di elementi su cui si è scelto di fissare la propria attenzione. I singoli elementi considerati si dicono *elementi della classe*.

ESEMPI 1.2. Sono esempi di classe: la classe delle lettere dell'alfabeto italiano; la classe di tutti gli studenti dell'università di Verona; fissato un piano $\alpha$, la classe di tutti i punti di $\alpha$ oppure la classe di tutti i poligoni contenuti in $\alpha$.

NOTAZIONI. Nel seguito indicheremo gli elementi con lettere minuscole, mentre le classi con lettere maiuscole. Per indicare l'appartenenza o la non appartenenza di un elemento a una certa classe si usano rispettivamente i simboli '$\in$' e '$\notin$'; con la scrittura '$a \in A$' si indica che l'elemento $a$ appartiene alla classe $A$, mentre la scrittura '$a \notin A$' indica che l'elemento $a$ non appartiene alla classe $A$.

Per descrivere una classe si possono usare diverse notazioni. Una prima possibilità è di elencare gli elementi della classe tra parentesi graffe separati da virgole. Ad esempio la scrittura $\{2,1,d,b,5,4,7\}$ indica la classe formata dalle lettere $d$ e $b$ e dai numeri 1, 2, 4, 5 e 7. Si possono considerare classi formate da un unico elemento $a$; in tal caso, la classe che si sta considerando si indica con $\{a\}$ e si può scrivere $a \in \{a\}$.

Se invece gli elementi che formano una classe sono tutti quelli che godono di una certa proprietà $P$ si può denotare la classe nel modo seguente: $\{x \mid x \text{ soddisfa } P\}$, dove il simbolo '|' si legge "tale che". Ad esempio per indicare la classe di tutti i numeri naturali pari si può scrivere

$$\{x \mid x \text{ è un numero naturale pari}\}.$$

Analogamente con la scrittura

$$\{x \mid x \text{ è un numero naturale dispari e } x \text{ è minore di } 10\}$$

si indica la classe dei numeri naturali dispari minori di 10; si noti che usando la notazione descritta precedentemente, la stessa classe si può indicare anche con $\{1,3,5,7,9\}$. Spesso il simbolo '|' viene sostituito dal simbolo ':'; in questo modo si scrive $\{x : x \text{ soddisfa } P\}$.

È importante sottolineare che ogni classe è determinata dagli elementi che la compongono, indipendentemente da come essi vengono descritti. Questa proprietà del concetto di classe viene detta *estensionalità*: infatti per individuare una classe guardiamo a quali elementi si estende e non al modo in cui questi vengono descritti. Perciò due diverse descrizioni indicano la stessa classe se la classe individuata dalla prima descrizione ha gli stessi elementi di quella individuata dalla seconda. In altre parole, due classi coincidono se e solo se hanno gli stessi elementi. Ad esempio la classe $\{0,6,9,3\}$, la classe $\{3,0,6,9,3,6\}$ e la classe $\{x \mid x \text{ è un multiplo di 3 minore di } 10\}$ sono tutte coincidenti.

## 2. Sottoclassi e classe complementare

DEFINIZIONE 2.1. Date due classi $X$ e $Y$, $Y$ è una *sottoclasse* di $X$ se tutti gli elementi di $Y$ sono anche elementi di $X$. In tal caso diciamo che $Y$ è contenuta in $X$ e si scrive $Y \subseteq X$; diciamo anche che $X$ contiene $Y$ e si scrive $X \supseteq Y$.

Si osservi che ogni classe è sottoclasse di sé stessa, cioè $X \subseteq X$ per ogni classe $X$. Inoltre date due classi $X$ e $Y$, se $X \subseteq Y$ e anche $Y \subseteq X$, possiamo concludere che $X = Y$; infatti le due inclusioni ci dicono esattamente che $X$ e $Y$ hanno gli stessi elementi e quindi, per la proprietà dell'estensionalità, le due classi coincidono. Se $Y$ è la sottoclasse di $X$ formata da tutti gli elementi di $X$ che godono di una certa proprietà $P$, si scrive

$$Y = \{x \mid x \in X \text{ e } x \text{ soddisfa } P\}.$$

Ad esempio se $\mathbb{N}$ è la classe dei numeri naturali, la classe $\{x \mid x \in \mathbb{N} \text{ e } x \text{ è multiplo di } 2\}$ è la sottoclasse dei numeri naturali pari.

Un'altra classe molto importante è la classe che non contiene elementi; si consideri per esempio la classe $\{x \mid x \text{ è un numero reale e } x^2 = -1\}$, oppure la classe dei mesi dell'anno con meno di 20 giorni.

DEFINIZIONE 2.2. Una classe che non contiene elementi si dice *classe vuota*; essa si indica con il simbolo $\emptyset$.

Si noti che, poiché una classe è determinata dai suoi elementi e due classi coincidono se hanno gli stessi elementi, la classe vuota è unica. Inoltre la classe vuota è sottoclasse di ogni altra classe.

Per concludere, data una classe $X$, introduciamo la classe formata da tutti gli elementi che non appartengono a $X$.

DEFINIZIONE 2.3. Data una classe $X$, la classe $\{x \mid x \notin X\}$ è detta la classe *complementare* di $X$ e si indica con $\complement X$.

Ad esempio, se $X$ è la classe formata dalle lettere dell'alfabeto italiano, la classe complementare di $X$ è $\complement X = \{x \mid x \text{ non è una lettera dell'alfabeto italiano}\}$; pertanto $\pi \in \complement X$ e anche $7 \in \complement X$.

## 3. Operazioni tra classi

In questa sezione, date due classi $Y_1$ e $Y_2$, introduciamo alcune nuove classi che si ottengono a partire da esse. Si consideri ad esempio la classe formata dagli elementi che appartengono sia a $Y_1$ che a $Y_2$.

DEFINIZIONE 3.1. La classe $\{x \mid x \in Y_1 \text{ e } x \in Y_2\}$ è detta *intersezione* delle classi $Y_1$ e $Y_2$ e si indica con $Y_1 \cap Y_2$.

Si noti che dalla definizione di intersezione, segue che $Y_1 \cap Y_2 = Y_2 \cap Y_1$. Inoltre $Y_1 \cap Y_2$ è una sottoclasse sia di $Y_1$ che di $Y_2$. Se $Y_1 \cap Y_2 = \emptyset$, allora le classe $Y_1$ e $Y_2$ si dicono *disgiunte*.

Analogamente, introduciamo la classe formata dagli elementi che appartengono o a $Y_1$ oppure a $Y_2$.

DEFINIZIONE 3.2. La classe $\{x \mid x \in Y_1 \text{ oppure } x \in Y_2\}$ è detta *unione* delle classi $Y_1$ e $Y_2$ e si indica con $Y_1 \cup Y_2$.

Dalla definizione di unione segue che $Y_1 \cup Y_2 = Y_2 \cup Y_1$. Si osservi che, data una qualsiasi classe $Y$, l'unione tra $Y$ e la sua classe complementare $\complement Y$ individua la classe $\{x \mid x \text{ è un elemento}\}$, cioè la classe formata da tutti gli elementi. Tale classe è detta *classe universale* e nel seguito sarà indicata con $\mathscr{U}$. Quindi, per ogni classe $Y$, si ha che $Y \cup \complement Y = \mathscr{U}$.

Si noti che le operazioni di intersezione e unione tra classi possono essere ripetute successivamente. Ad esempio, date tre classi $X$, $Y$ e $Z$, la classe $X \cap Y \cap Z$ si ottiene calcolando prima $X \cap Y$ e poi $(X \cap Y) \cap Z$. Analogamente si costruisce la classe $X \cup Y \cup Z$.

Per finire, date due classi $Y_1$ e $Y_2$ consideriamo la classe formata dagli elementi che appartengono a $Y_1$ ma non a $Y_2$.

DEFINIZIONE 3.3. La classe $\{x \mid x \in Y_1 \text{ e } x \notin Y_2\}$ è detta *differenza* tra $Y_1$ e $Y_2$ o, equivalentemente, *complementare* di $Y_2$ *in* $Y_1$, e si indica con $Y_1 \setminus Y_2$.

Si osservi che, dalla definizione di differenza tra classi, segue che $Y_1 \setminus Y_2 = Y_1 \cap \complement Y_2$. Si noti inoltre che $Y_1 \setminus Y_2$ è una sottoclasse di $Y_1$ ma non di $Y_2$.

## 4. Insiemi

Tra tutte le classi che possiamo costruire ce ne sono alcune che possono essere considerate come una cosa singola; ad esempio, la classe formata da tutti i giocatori della nostra squadra di calcio preferita può essere considerata come una cosa singola, cioè la squadra stessa. A sua volta la nostra squadra preferita può essere vista come un elemento della classe di tutte le squadre di calcio che partecipano al campionato italiano. In generale, quando una classe può essere considerata come una cosa singola, essa può essere elemento di qualche altra classe.

DEFINIZIONE 4.1. Le classi che possono essere considerate come una cosa singola, cioè che a loro volta possono essere considerate come elementi, si dicono *insiemi*. Le classi che non sono insiemi sono dette *classi proprie*.

ESEMPI 4.2. La classe degli studenti dell'Università di Verona è un insieme; infatti tale classe può essere considerata come un elemento, cioè l'Università di Verona stessa, che a sua volta appartiene alla classe di tutti gli Atenei italiani.

La classe di tutti gli esseri umani è un insieme; infatti può essere considerato come l'elemento "genere umano", appartenente alla classe di tutte le specie animali.

Si fissi un piano $\alpha$ e una circonferenza $\gamma$ contenuta in $\alpha$. La classe di tutti i punti che appartengono alla circonferenza $\gamma$ è un insieme; infatti tale classe può essere considerata come la circonferenza $\gamma$ stessa, che a sua volta è un elemento della classe delle figure contenute nel piano $\alpha$.

ESEMPIO 4.3. Un esempio importante di classe propria, cioè di classe che non è un insieme, è la classe degli insiemi che non appartengono a sé stessi, cioè la classe

$$R = \{X \mid X \text{ è un insieme e } X \notin X\}.$$

Se infatti tale classe fosse un insieme, $R$ potrebbe essere visto come elemento o come classe. Dato che tra elementi e classi sussiste la relazione di appartenenza e un dato elemento appartiene o non appartiene a una data classe, sicuramente $R$ dovrebbe verificare una e una sola delle seguenti: $R \in R$ oppure $R \notin R$. Nel primo caso, se $R \in R$, $R$ dovrebbe soddisfare la proprietà che caratterizza gli elementi della classe $R$, cioè $R \notin R$. Nel secondo caso, sappiamo che $R$ è un insieme e $R \notin R$; pertanto potremmo dire che $R$, come elemento, soddisfa la proprietà che caratterizza la classe $R$, e quindi dovremmo concludere che $R \in R$. In entrambi i casi si trova una contraddizione che deriva dall'aver assunto che $R$ sia un insieme. Pertanto si conclude che $R$ *non è* un insieme.

OSSERVAZIONE 4.4. Come risulta evidente dagli esempi precedenti, dato che un insieme può essere visto come elemento, esso può a sua volta appartenere ad altre classi. Al contrario, le classi proprie non possono appartenere ad altre classi, dato che l'appartenenza è prerogativa degli elementi.

Sottolineiamo inoltre che l'Esempio 4.3 è molto significativo non solo perché mostra come ci sia una profonda differenza tra il concetto di classe e di insieme, ma anche perché in esso si è applicato un tipo di ragionamento, detto ragionamento *per assurdo*, molto usato nelle dimostrazioni matematiche.

Si osservi che, poiché gli insiemi sono classi, per essi vale tutto quanto detto finora sulle classi per quanto riguarda notazioni, operazioni e simboli introdotti.

## 5. Assiomi sugli insiemi

Nella sezione precedente abbiamo visto che non tutte le classi sono insiemi. Sorge quindi il problema di riconoscere quali classi sono insiemi. Si può stabilire che una classe è un insieme ogni qual volta questa assunzione non porta a contraddizioni, come nel caso dell'Esempio 4.3. È quindi necessario trovare un metodo per stabilire se l'assumere che una certa classe sia un insieme implichi o meno una contraddizione. Un possibile criterio è quello di partire da alcuni classi che evidentemente sono insiemi e fissare delle regole per costruire nuovi insiemi a partire da queste classi iniziali. Pertanto fissiamo i seguenti *assiomi* sugli insiemi, cioè affermazioni che non sono dimostrabili ma che decidiamo di assumere come vere.

(1) Ogni classe finita è un insieme.
(2) Una sottoclasse di un insieme $X$ è un insieme, detta *sottoinsieme* di $X$.
(3) L'unione di due insiemi è un insieme.
(4) Se $X$ è un insieme e la classe $Y$ ha tanti elementi quanti $X$, allora anche $Y$ è un insieme.
(5) Se $X$ è un insieme, si costruisca la classe di tutti i sottoinsiemi di $X$, cioè $P(X) = \{ Y \mid Y \subseteq X \}$. Allora $P(X)$ è un insieme, detto *insieme delle parti* di $X$.
(6) La classe dei numeri naturali, indicata con $\mathbb{N}$, è un insieme.
(7) Non esistono successioni di insiemi $X_0, X_1, \ldots, X_n$ tali che $X_0 \in X_1 \in \cdots \in X_n \in X_0$.

Dagli assiomi introdotti seguono alcune importanti conseguenze.

(a) Dal secondo assioma si ottiene che, dati due insiemi $X$ e $Y$, sia $X \cap Y$ che $X \setminus Y$ sono insiemi, essendo entrambi sottoclassi di $X$.
(b) Sempre dal secondo assioma, segue che la classe universale $\mathscr{U}$ non è un insieme. Se infatti lo fosse, la sottoclasse $R$ introdotta nell'Esempio 4.3 (si dimostri per esercizio che $R \subseteq \mathscr{U}$!) per il secondo assioma sarebbe un insieme. Invece abbiamo già visto che $R$ non è un insieme.
(c) La classe vuota è sottoclasse di ogni classe, e in particolare di ogni insieme. Quindi, di nuovo dal secondo assioma, concludiamo che $\emptyset$ è un insieme. Nel seguito lo chiameremo *insieme vuoto*.
(d) Se $X$ è un insieme, il suo complementare $\complement X$ non è un insieme. Se infatti lo fosse, dal terzo assioma si concluderebbe che $X \cup \complement X = \mathscr{U}$ è un insieme, ma abbiamo già osservato che la classe universale è una classe propria.
(e) Nel quarto assioma, se si considerano insiemi con infiniti elementi, il concetto di "avere tanti elementi quanti" può risultare confuso: chiariremo nei capitoli successivi cosa si intende con questa espressione.
(f) Se $X$ è un insieme finito con $n$ elementi, allora anche $P(X)$ è un insieme finito con $2^n$ elementi. (Si veda l'Esercizio 1.5.)
(g) Il fatto che i numeri naturali siano un insieme, chiaramente infinito, implica che anche la classe dei numeri interi, dei numeri razionali, dei numeri reali e dei numeri complessi sono insiemi; una dimostrazione di ciò sarà vista successivamente. Nel seguito, indicheremo tali insiemi rispettivamente con le lettere $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.
(h) Per ogni insieme $X$, possiamo affermare che $X \notin X$.

Nel seguito, tranne quando esplicitamente specificato, tutte le classi su cui lavoreremo si intenderanno insiemi.

## 6. Unione e intersezione su classi e insiemi

Siano $Y_1, Y_2, \ldots, Y_n$ insiemi; allora possiamo costruire l'insieme $Y_1 \cap Y_2 \cap \cdots \cap Y_n$. Questa intersezione si può indicare anche con $\bigcap X$, dove $X$ è l'insieme $X = \{Y_1, Y_2, \ldots, Y_n\}$; in altre parole, $\bigcap X = \{ x \mid x \in Y \text{ per ogni } Y \in X \}$. Questo modo di descrivere l'intersezione tra più insiemi può essere generalizzato al caso in cui $X$ sia un insieme infinito, o una classe, i cui elementi siano a loro volta insiemi. Pertanto estendiamo la definizione di intersezione tra insiemi nel modo seguente.

DEFINIZIONE 6.1. Se $X$ è una classe i cui elementi sono insiemi, allora $\bigcap X$ è la classe $\{ x \mid x \in Y \text{ per ogni } Y \in X \}$.

ESEMPIO 6.2. Si noti che, se $X$ non è l'insieme vuoto, allora $\bigcap X \subseteq Y$ per ogni insieme $Y$ appartenente a $X$ e quindi $\bigcap X$ è un insieme. Analizziamo invece nel dettaglio il caso in cui $X = \emptyset$ e quindi

$$\bigcap \emptyset = \{x \mid x \in Y \text{ per ogni } Y \in \emptyset\}.$$

Possiamo riscrivere $\bigcap \emptyset$ nella forma equivalente: $\{x \mid \text{se } Y \in \emptyset \text{ allora } x \in Y\}$; poiché $\emptyset$ non contiene alcun elemento, dato un qualsiasi elemento $x$ esso sicuramente appartiene a $\bigcap \emptyset$; questo perché non è richiesta alcuna verifica sull'elemento $x$ affinché appartenga a $\bigcap \emptyset$. Concludiamo quindi che $\bigcap \emptyset = \mathscr{U}$, dove $\mathscr{U}$ è la classe universale.

Possiamo verificare l'asserzione anche in un altro modo. Quando un elemento $x$ non appartiene a $\bigcap X$? Precisamente quando esiste un elemento $Y \in X$ tale che $x \notin Y$. Ora, di quali elementi $x$ possiamo asserire che $x \notin \bigcap \emptyset$? Di nessuno, perché non possiamo trovare $Y \in \emptyset$ tale che $x \notin Y$. Dunque di nessun elemento $x$ possiamo dire che $x \notin \bigcap \emptyset$ e perciò di ogni elemento $x$ dobbiamo dire che appartiene a $\bigcap \emptyset$, cioè $\bigcap \emptyset = \mathscr{U}$.

Alla luce di quanto osservato, si verifica facilmente che se $X$ e $Z$ sono due classi e $X \subseteq Z$, allora $\bigcap X \supseteq \bigcap Z$ (si veda l'Esercizio 1.6).

In modo analogo a quanto fatto per l'intersezione, dati gli insieme $Y_1$, $Y_2$,..., $Y_n$, allora possiamo costruire l'insieme $Y_1 \cup Y_2 \cup \cdots \cup Y_n$. Questa unione si può indicare anche con $\bigcup X$, dove $X$ è l'insieme $X = \{Y_1, Y_2, \ldots, Y_n\}$; in altre parole, $\bigcup X = \{x \mid \text{esiste } Y \in X \text{ tale che } x \in Y\}$. Questo modo di descrivere l'unione tra più insiemi può essere generalizzato al caso in cui $X$ sia un insieme infinito, o una classe, i cui elementi siano a loro volta insiemi. Pertanto estendiamo la definizione di unione tra insiemi nel modo seguente.

DEFINIZIONE 6.3. Se $X$ è una classe i cui elementi sono insiemi, allora $\bigcup X$ è la classe

$$\{x \mid \text{esiste } Y \in X \text{ tale che } x \in Y\}.$$

Consideriamo il caso $X = \emptyset$; allora $\bigcup \emptyset = \{x \mid \text{esiste } Y \in \emptyset \text{ tale che } x \in Y\}$. Poiché $\emptyset$ non contiene elementi, dato un elemento $x$ non esiste alcun $Y \in \emptyset$ che lo contenga. Quindi $\bigcup \emptyset = \emptyset$.

Se invece $X = \mathscr{U}$, $\bigcup \mathscr{U} = \{x \mid \text{esiste } Y \in \mathscr{U} \text{ tale che } x \in Y\}$. Si osservi che per ogni elemento $x$ possiamo costruire l'insieme $\{x\}$, dove $x \in \{x\}$; poiché l'insieme $\{x\}$, in quanto a sua volta elemento, è sicuramente contenuto nella classe universale, concludiamo che $x \in \bigcup \mathscr{U}$. Quindi $\bigcup \mathscr{U} = \mathscr{U}$. Questo mostra che in generale, al contrario di quanto sussiste per l'intersezione, l'unione di una classe, o di un insieme infinito, di insiemi non è in generale un insieme. Tuttavia assumiamo che se $X$ è un insieme, allora $\bigcup X$ è un insieme; si consideri questo un assioma da aggiungere alla lista descritta nella Sezione 5.

Si verifica facilmente dalla definizione di unione che, se $X$ e $Z$ sono due classi e $X \subseteq Z$, allora $\bigcup X \subseteq \bigcup Z$ (si veda l'Esercizio 1.6).

## 7. Insiemi ordinati

Spesso è utile considerare gli elementi di un dato insieme con un certo ordine. Ad esempio, le lettere della parola 'mela' formano l'insieme $\{a, e, l, m\}$, ma se vogliamo distinguere la parola 'mela' dalla parola 'lame', dobbiamo indicare l'ordine delle lettere. Si introduce così il concetto di insieme ordinato.

DEFINIZIONE 7.1. Un *insieme ordinato* finito è un insieme finito in cui è messo in evidenza un ordine degli elementi.

In generale un insieme ordinato si indica tra parentesi tonde; ad esempio se si considera l'insieme ordinato delle lettere parole 'mela', si scriverà (m,e,l,a), mentre l'insieme ordinato delle lettere della parola 'lame' sarà (l,a,m,e). Si osservi che mentre nella usuale notazione insiemistica gli insiemi $\{a, b, c\}$, $\{b, c, a\}$, $\{b, a, c\}$ e $\{a, b, a, c, b\}$ coincidono, se si considerino insiemi ordinati gli insiemi $(a, b, c)$, $(b, c, a)$, $(b, a, c)$ e $(a, b, a, c, b)$ sono insiemi tra loro diversi.

In particolare spesso consideriamo il caso di insiemi ordinati formati da due elementi, detti *coppie ordinate*, cioè insiemi del tipo $(a, b)$. Si osservi che mentre gli insiemi $\{a, b\}$ e $\{c, d\}$ coincidono sia nel caso in cui $a = c$ e $b = d$ che nel caso in cui $a = d$ e $b = c$, le coppie ordinate $(a, b)$ e $(c, d)$ coincidono se e solo se $a = c$ e $b = d$.

ESEMPIO 7.2. Dovendo rappresentare da un punto di vista insiemistico le targhe automobilistiche italiane, dobbiamo ricorrere a insiemi ordinati con 7 elementi, dove i primi due elementi sono lettere, i successivi tre sono numeri, gli ultimi due lettere; per esempio $(A,W,1,2,3,F,G)$ e $(W,A,1,2,3,F,G)$ sono due targhe diverse, mentre $(A,1,W,2,3,F,G)$ non rappresenta alcuna targa.

Si osservi che gli insiemi ordinati possono essere descritti usando la notazione insiemistica classica, senza introdurre cioè il concetto di ordine su un insieme. Ad esempio, la coppia ordinata $(a,b)$ si può indicare anche con l'insieme $\{\{a\},\{a,b\}\}$; infatti in questo insieme si è indicato il fatto che $a$ "viene prima" di $b$ semplicemente ripetendolo due volte, la prima volta formando l'insieme $\{a\}$, la seconda come elemento dell'insieme $\{a,b\}$. Si faccia attenzione che l'insieme $\{\{a\},\{a,b\}\}$, l'insieme $\{\{a\},\{b,a\}\}$ e l'insieme $\{\{a,b\},\{a\}\}$ sono uguali, in quanto in questa notazione non è rilevante l'ordine in cui gli elementi compaiono tra parentesi graffe. Analogamente l'insieme ordinato $(a,b,c)$ si può indicare anche con $\{\{a\},\{a,b\},\{a,b,c\}\}$; l'insieme così fatto fornisce informazioni su quale elemento va considerato come primo, quale come secondo e quale come terzo. Allo stesso modo si possono denotare insiemi ordinati finiti arbitrari.

## 8. Prodotto di insiemi

Date due classi $A$ e $B$ consideriamo la classe i cui elementi sono le coppie ordinate in cui il primo elemento appartiene alla classe $A$, il secondo alla classe $B$. Tale classe si dice *prodotto* delle classi $A$ e $B$.

DEFINIZIONE 8.1. Date due classi $A$ e $B$ il *prodotto di $A$ per $B$* è la classe $\{(a,b) \mid a \in A \text{ e } b \in B\}$ e si indica con $A \times B$.

Si noti che gli elementi del prodotto sono coppie ordinate. Pertanto in generale l'operazione prodotto non è commutativa, cioè date due classi $A$ e $B$ in generale $A \times B$ è diverso da $B \times A$; questo perché gli elementi di $A \times B$ hanno come primo termine della coppia elementi di $A$ e come secondo termine elementi di $B$, mentre gli elementi di $B \times A$ hanno come primo termine della coppia elementi di $B$ e come secondo termine elementi di $A$.

ESEMPIO 8.2. Se $A = \{1,2,3\}$ e $B = \{a,b,c\}$, il prodotto $A \times B$ è la classe $\{(1,a),\ (1,b),\ (1,c),\ (2,a),\ (2,b),\ (2,c),\ (3,a),\ (3,b),\ (3,c)\}$, mentre il prodotto $B \times A$ è la classe $\{(a,1),\ (a,2),\ (a,3),\ (b,1),\ (b,2),\ (b,3),\ (c,1),\ (c,2),\ (c,3)\}$.

Se una delle due classi $A$ e $B$ che si stanno considerando è l'insieme vuoto, allora il prodotto $A \times B$ è l'insieme vuoto: infatti non si possono costruire coppie ordinate con il primo o il secondo termine appartenente all'insieme vuoto, dato che $\emptyset$ non contiene alcun elemento. Inoltre, se $A' \subseteq A$ e $B' \subseteq B$, è facile verificare che $A' \times B' \subseteq A \times B$.

Si osservi che se $A$ e $B$ sono entrambi insiemi, allora anche il prodotto $A \times B$ è un insieme. Infatti abbiamo già visto che ogni coppia ordinata $(a,b)$ si può rappresentare tramite l'insieme $\{\{a\},\{a,b\}\}$. Dato che $\{a\}$ e $\{a,b\}$ sono elementi dell'insieme delle parti $P(A \cup B)$, in quanto sottoinsiemi di $A \cup B$, si ottiene che $A \times B \subseteq P(P(A \cup B))$. Quindi applicando il secondo, il terzo e il quinto assioma della Sezione 5, possiamo concludere che $A \times B$ è un insieme.

Per concludere, si può facilmente generalizzare la nozione di prodotto tra due classi a quello tra $n$ classi. Infatti se $A_1, A_2, \ldots, A_n$ sono $n$ classi, il prodotto $A_1 \times A_2 \times \cdots \times A_n$ è l'insieme delle $n$-uple ordinate con il primo termine appartenente a $A_1$, il secondo a $A_2$, e in generale l'$i$-esimo termine appartenente a $A_i$.

## ESERCIZI

ESERCIZIO 1.1. Sia $X$ una classe tale che $X \subseteq Y$ per ogni classe $Y$. Si dimostri che $X = \emptyset$.

ESERCIZIO 1.2. Si dimostri che, date due classi $X$ e $Y$, $X \cap Y$ è la più grande classe contenuta sia in $X$ che in $Y$; analogamente si dimostri che $X \cup Y$ è la più piccola classe contenente sia $X$ che $Y$.

ESERCIZIO 1.3. Date due classi $X$ e $Y$, si dimostri che $X \subseteq Y \Leftrightarrow X \cap Y = X \Leftrightarrow X \cup Y = Y$.

ESERCIZIO 1.4. Sia $X$ la classe dei numeri naturali multipli di 10 e $Y$ la classe dei numeri naturali la cui scrittura decimale ha come ultima cifra lo zero. Si dimostri che $X = Y$.

ESERCIZIO 1.5. Si dimostri che se $X$ è un insieme finito con $n$ elementi, allora l'insieme $P(X)$ ha $2^n$ elementi. (Suggerimento: dato un arbitrario sottoinsieme $Y \subseteq X$ e un arbitrario elemento $x \in X$, sappiamo che $x \in Y$ oppure $x \notin Y$. Quindi i possibili modi per costruire un sottoinsieme $Y$ sono...)

ESERCIZIO 1.6. Si dimostri che se $X$ e $Y$ sono due classi di insiemi e $X \subseteq Y$, allora $\bigcup X \subseteq \bigcup Y$ e $\bigcap X \supseteq \bigcap Y$ (si faccia attenzione al caso in cui $X = \emptyset$).

ESERCIZIO 1.7. Si considerino gli insiemi $X = \{\{a\},\{a,b\}\}$ e $Y = \{\{x\},\{x,y\}\}$. Si dimostri che $X = Y$ se e solo se $a = x$ e $b = y$.

ESERCIZIO 1.8. Si considerino gli insiemi

$$X = \{\{a\},\{a,b\},\{a,b,c\}\} \text{ e } Y = \{\{x\},\{x,y\},\{x,y,z\}\}.$$

Si dimostri che $X = Y$ se e solo se $a = x$, $b = y$ e $c = z$.

ESERCIZIO 1.9. Dati tre insiemi $A$, $B$ e $C$ si dimostrino le seguenti uguaglianze insiemistiche: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

ESERCIZIO 1.10. Si descrivano, in termine di unione, intersezione e differenza di insiemi, i seguenti insiemi:

$\{x \mid x \in \mathbb{N}, x$ è multiplo di 5 e di 3 ma non di $7\}$;

$\{x \mid x \in \mathbb{N}, x$ è minore di 100 oppure è multiplo di 3 e di $5\}$.

CAPITOLO 2

# Relazioni

## 1. Prime proprietà

Il significato comune del concetto di relazione è facilmente intuibile: due elementi sono in relazione se c'è un legame tra loro descritto da una certa proprietà; ad esempio, "essere genitore di...", "essere alto tanto quanto...", "avere la stessa età di...". Da un punto di vista matematico siamo interessati a studiare quali coppie di elementi sono coinvolte in una data relazione, astraendo dalle caratteristiche e dalle proprietà che descrivono la relazione stessa; è pertanto naturale ricorrere al concetto di coppia ordinata.

DEFINIZIONE 1.1. Una *relazione* $R$ è un insieme di coppie ordinate. Se la coppia $(a,b) \in R$, si scrive anche $aRb$ e si dice che $a$ è in relazione con $b$ tramite $R$, o che $b$ corrisponde ad $a$ nella relazione $R$.

Si noti che è essenziale l'ordine con cui si descrivono gli elementi in relazione: ad esempio se si considera la relazione "essere il doppio di", la coppia $(2,1)$ appartiene alla relazione, mentre non ci appartiene la coppia $(1,2)$. Risulta quindi evidente perché si ricorre al concetto di coppia ordinata e non di semplice insieme con due elementi.

Si osservi inoltre che relazioni che a parole si descrivono in modo diverso, possono avere la stessa descrizione in termini di coppie ordinate e quindi essere in realtà la stessa relazione, come mostra l'esempio seguente.

ESEMPIO 1.2. Sia $X = \{x \in \mathbb{N} \mid x = 5^n \text{ per qualche } n \in \mathbb{N}\}$ l'insieme delle potenze di 5. Consideriamo le seguenti relazioni: due elementi di $X$ sono in relazione se il primo è minore o uguale al secondo; due elementi di $X$ sono in relazione se il primo divide il secondo. In termini di coppie ordinate, entrambe individuano lo stesso insieme $R = \{(x,y) \mid x = 5^n, y = 5^m \text{ e } n \leq m\}$ e quindi sono la stessa relazione.

Data una relazione $R$, dato cioè un insieme di coppie ordinate, i primi termini della coppie possono appartenere a un insieme $A$, detto *dominio* della relazione; analogamente i secondi termini delle coppie in $R$ possono appartenere a un insieme $B$, detto *codominio* della relazione. In tal caso l'insieme $R$ è un sottoinsieme del prodotto $A \times B$. Viceversa, dati due insiemi $A$ e $B$, un qualsiasi sottoinsieme $R$ del prodotto $A \times B$ individua una relazione, quella i cui elementi sono esattamente le coppie appartenenti al sottoinsieme scelto. Si osservi che il dominio e il codominio di una relazione non sono univocamente determinati, dato che possiamo considerare come dominio *qualsiasi* insieme contenente i primi elementi delle coppie di $R$, e come codominio *qualsiasi* insieme contenente i secondi elementi delle coppie di $R$. Se gli insiemi $A$ e $B$ coincidono, allora l'insieme $A = B$ viene detto *supporto* della relazione $R$. Si noti che si può sempre assumere che $R$ abbia come supporto l'insieme $A \cup B$, dove $A$ è un qualsiasi dominio e $B$ un qualsiasi codominio.

ESEMPIO 1.3. Si consideri la relazione $R = \{(1,5),(2,7),(6,3)\}$. L'insieme $A = \{1,2,6\}$ è un possibile dominio di $R$ e l'insieme $\{5,7,3\}$ è un possibile codominio; infatti $R \subseteq A \times B$. Anche l'insieme $A' = \{1,2,3,4,5,6\}$ è un possibile dominio e $B' = \{3,4,5,6,7\}$ è un possibile codominio; infatti $R \subseteq A' \times B'$. Se si considera l'insieme $C = \{1,2,3,4,5,6,7\}$, $C$ è un possibile supporto di $R$, dato che sia i primi elementi che i secondi elementi delle coppie in $R$ appartengono a $C$. Per concludere si osservi che anche l'insieme $\mathbb{N}$ dei numeri naturali è un supporto di $R$.

NOTAZIONI. Una relazione $R$ con dominio $A$ e come codominio $B$ si può indicare con la terna $(A,B,R)$; si dice anche che $R$ è una relazione dall'insieme $A$ all'insieme $B$. Con questa

notazione si vuole sottolineare l'insieme in cui si scelgono i primi termini delle coppie e quello in cui si scelgono i secondi. Si noti che questo concetto di relazione da un insieme a un altro è diverso dal concetto di relazione introdotto in 1.1, che è semplicemente un insieme di coppie ordinate. Infatti, la stessa relazione $R$ può essere vista come relazioni tra insiemi diversi, come mostra il seguente esempio.

ESEMPIO 1.4. Si consideri la relazione $R = \{(1,5),(2,7),(6,3)\}$ descritta nell'esempio precedente. Possiamo considerare la relazione $R$ come relazione tra gli insiemi $A$ e $B$ oppure tra gli insiemi $A'$ e $B'$, dove $A$, $B$, $A'$ e $B'$ sono gli insiemi descritti in 1.3. Quindi le scritture $(A,B,R)$ e $(A',B',R)$ indicano due diverse relazioni tra insiemi, anche se $R$ è lo stesso insieme di coppie ordinate.

Per concludere introduciamo la nozione di insieme di definizione e di insieme immagine di una relazione.

DEFINIZIONE 1.5. Data una relazione $R$, l'insieme $\{x \mid \text{esiste } y \text{ tale che } (x,y) \in R\}$ è detto *insieme di definizione* di $R$ e si indica con $\mathrm{Def}(R)$. L'insieme $\{y \mid \text{esiste } x \text{ tale che } (x,y) \in R\}$ è detto *insieme immagine* di $R$ e si indica con $\mathrm{Im}(R)$.

In altre parole, l'insieme di definizione è formato da tutti i primi elementi delle coppie ordinate che appartengono alla relazione, l'insieme immagine dai secondi. Chiaramente se $R$ è una relazione con dominio $A$ e codominio $B$, allora $\mathrm{Def}(R) \subseteq A$ e $\mathrm{Im}(R) \subseteq B$. Se $\mathrm{Def}(R) = A$ allora la relazione $R$ si dice *totale* in $A$; se $\mathrm{Im}(R) = B$, allora $R$ si dice *suriettiva* su $B$.

Si osservi che l'insieme di definizione e l'insieme immagine di una relazione sono univocamente determinati da $R$, dipendono cioè solo dalle coppie che appartengono alla relazione. Invece il concetto di relazione totale o suriettiva assumono significato solo per relazioni da un insieme a un altro, dato che dipendono dal dominio e dal codominio di $R$.

ESEMPIO 1.6. Si consideri la relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$ dove $xRy$ se e solo se $x$ è il doppio di $y$. Il dominio di $R$ è $\mathbb{N}$, mentre l'insieme di definizione è $2\mathbb{N}$, dove $2\mathbb{N}$ indica l'insieme dei numeri naturali pari. La relazione quindi non è totale in $\mathbb{N}$, mentre è suriettiva su $\mathbb{N}$ dato che $\mathrm{Im}(R) = \mathbb{N}$. Al contrario la relazione $(2\mathbb{N},\mathbb{N},R)$, dove di nuovo $xRy$ se e solo se $x$ è il doppio di $y$, è totale in $2\mathbb{N}$, poiché $\mathrm{Def}(R) = 2\mathbb{N}$ coincide con il dominio.

Si consideri la relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$ dove $xRy$ se e solo se $x$ è un terzo di $y$. Il codominio è l'insieme $\mathbb{N}$, mentre $\mathrm{Im}(R) = 3\mathbb{N}$, dove $3\mathbb{N}$ denota l'insieme dei naturali multipli di 3; pertanto $R$ non è suriettiva su $\mathbb{N}$. Invece la relazione tra insiemi $(\mathbb{N},3\mathbb{N},R)$ dove di nuovo $xRy$ se e solo se $x$ è un terzo di $y$, è suriettiva su $3\mathbb{N}$ poiché $\mathrm{Im}(R) = 3\mathbb{N}$ coincide con il dominio.

Si osservi che data una qualsiasi relazione $R$, scegliendo come dominio l'insieme $\mathrm{Def}(R)$ e come codominio l'insieme $\mathrm{Im}(R)$, la relazione descritta dalla terna $(\mathrm{Def}(R),\mathrm{Im}(R),R)$ è totale e suriettiva.

## 2. Proprietà delle relazioni

Vediamo ora alcune rilevanti proprietà di cui possono godere le relazioni. Nel seguito si suppone che $R$ sia una relazione con supporto $A$.

PROPRIETÀ RIFLESSIVA. Una relazione tra insiemi $(A,A,R)$ si dice *riflessiva* se, per ogni $x \in A$, la coppia $(x,x)$ appartiene a $R$.

PROPRIETÀ ANTIRIFLESSIVA. Una relazione tra insiemi $(A,A,R)$ si dice *antiriflessiva* se, per ogni $x \in A$, la coppia $(x,x)$ non appartiene a $R$.

PROPRIETÀ SIMMETRICA. Una relazione tra insiemi $(A,A,R)$ si dice *simmetrica* se, per ogni coppia $(x,y)$ appartenente a $R$, anche la coppia $(y,x)$ appartiene a $R$.

PROPRIETÀ ANTISIMMETRICA. Una relazione tra insiemi $(A,A,R)$ si dice *antisimmetrica* se, ogni qual volta $(x,y) \in R$ e $(y,x) \in R$, si ha $x = y$.

PROPRIETÀ TRANSITIVA. Una relazione tra insiemi $(A,A,R)$ si dice *transitiva* se, ogni qual volta le coppie $(x,y) \in R$ e $(y,z) \in R$, allora $(x,z) \in R$.

ESEMPI 2.1. La relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$, dove $xRy$ se e solo se $x \leq y$, è una relazione riflessiva. Infatti $x \leq x$ per ogni numero naturale $x$.

La relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$, dove $xRy$ se e solo se $x < y$, è una relazione antiriflessiva. Infatti nessun numero naturale $x$ è strettamente minore di se stesso.

La relazione tra insiemi $(\mathbb{Z},\mathbb{Z},R)$, dove $\mathbb{Z}$ è l'insieme dei numeri interi e $xRy$ se e solo se $x$ e $y$ hanno lo segno, è una relazione simmetrica. Infatti se $x$ ha lo stesso segno di $y$, allora anche $y$ ha lo stesso segno di $x$.

La relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$, dove $xRy$ se e solo se $x \leq y$, è una relazione antisimmetrica. Infatti, se $x \leq y$ e $y \leq x$, allora possiamo sicuramente concludere che $x = y$.

La relazione tra insiemi $(X,X,R)$, dove $X$ è l'insieme delle rette del piano e $xRy$ se e solo se la retta $x$ è parallela alla retta $y$, è una relazione transitiva. Infatti se una retta $x$ è parallela alla retta $y$ e inoltre $y$ è parallela alla retta $z$, possiamo concludere che anche $x$ e $z$ sono parallele.

## 3. Relazioni d'equivalenza

DEFINIZIONE 3.1. Una relazione $(A,A,R)$ riflessiva, simmetrica e transitiva è detta *relazione di equivalenza.*

ESEMPI 3.2. Sia $X$ l'insieme delle rette del piano $\alpha$.

La relazione tra insiemi $(X,X,R)$, dove $xRy$ se e solo se la retta $x$ è parallela alla retta $y$, è una relazione d'equivalenza. Infatti è riflessiva, dato che ogni retta è parallela a se stessa; inoltre è simmetrica, poiché se una retta $r$ è parallela alla retta $s$, allora anche $s$ è parallela a $r$. Abbiamo già osservato nell'esempio 2.1 che $R$ è transitiva, quindi concludiamo che $R$ è una relazione d'equivalenza.

La relazione tra insiemi $(X,X,R')$, dove $xR'y$ se e solo se $x$ e $y$ hanno un punto in comune non è una relazione d'equivalenza. Infatti essa è riflessiva e simmetrica ma non transitiva. Infatti siano $x$ e $z$ due rette parallele e $y$ una terza retta incidente sia $x$ che $z$. Allora $xR'y$, $yR'z$ ma $x$ non è in relazione con $z$, dato che due rette parallele non hanno punti di intersezione.

Si consideri una relazione d'equivalenza $(A,A,R)$. Per ogni $x \in A$ possiamo costruire l'insieme di tutti gli elementi di $A$ in relazione con $x$.

DEFINIZIONE 3.3. Il sottoinsieme di $A$ descritto da $\{y \in A \mid xRy\}$ è detto *classe d'equivalenza* dell'elemento $x$ e si denota $[x]_R$.

ESEMPIO 3.4. Si consideri ancora la relazione d'equivalenza $(X,X,R)$, dove $X$ è l'insieme delle rette di un piano $\alpha$ e $xRy$ se e solo se la retta $x$ è parallela alla retta $y$. Data una retta $r$, la classe d'equivalenza di $r$ è l'insieme di tutte le rette del piano parallele a $r$. Si osservi che ogni classe d'equivalenza determinata da $R$ individua una direzione del piano.

Analizziamo ora alcune importanti proprietà delle classi d'equivalenza associate a una relazione d'equivalenza $(A,A,R)$.

PROPOSIZIONE 3.5. *Sia* $(A,A,R)$ *una relazione d'equivalenza.*

(i) *Per ogni* $x \in A$, $x \in [x]_R$.
(ii) *Se* $(x,y) \in R$, *allora* $[x]_R = [y]_R$.
(iii) *Se* $(x,y) \notin R$, *allora* $[x]_R \cap [y]_R = \emptyset$.
(iv) *L'unione di tutte le classe d'equivalenza* $\bigcup_{x\in A}[x]_R$ *è l'insieme* $A$.

DIMOSTRAZIONE. (i) Poiché $R$ riflessiva, per ogni $x \in A$ la coppia $(x,x)$ appartiene a $R$ e pertanto $x \in [x]_R$.

(ii) Sia $z \in [x]_R$; allora $(z,x) \in R$. Essendo $R$ transitiva, da $(z,x) \in R$ e $(x,y) \in R$, si conclude che $(z,y) \in R$, cioè $z \in [y]_R$. Si è così verificato che $[x]_R \subseteq [y]_R$; analogamente si dimostra che $[x]_R \supseteq [y]_R$, e di conseguenza si ottiene $[x]_R = [y]_R$.

(iii) Se esistesse $z \in [x]_R \cap [y]_R = \emptyset$, si avrebbe $(z,x) \in R$ e $(z,y) \in R$. Essendo $R$ simmetrica e transitiva, seguirebbe che $(x,z) \in R$ e quindi $(x,y) \in R$, contrariamente alle ipotesi.

(iv) Ogni classe d'equivalenza è un sottoinsieme di $A$, quindi $\bigcup_{x\in A}[x]_R \subseteq A$. Inoltre, poiché $x \in [x]_R$, si ottiene $x \in \bigcup_{x\in A}[x]_R$ per ogni $x \in A$; pertanto $A \subseteq \bigcup_{x\in A}[x]_R$. □

COROLLARIO 3.6. *Data una relazione d'equivalenza* $(A, A, R)$ *e dati* $x, y \in A$, $(x, y) \in R$ *se e solo se* $[x]_R = [y]_R$.

DIMOSTRAZIONE. Segue dalla definizione 3.3 e dalla precedente proposizione. □

Le proprietà (iii) e (iv) ci dicono che l'insieme delle classi d'equivalenza è una *partizione* di $A$; in generale, dato un insieme $X$ una *partizione* di $X$ è un insieme di sottoinsiemi di $X$ a due a due disgiunti tali che la loro unione sia tutto $X$.

Inoltre data una partizione di $A$, ad essa è associata una relazione d'equivalenza nel modo seguente: dati due elementi $x, y \in A$, $xR'y$ se e solo se $x$ e $y$ appartengono allo stesso sottoinsieme della partizione. Si verifica facilmente che $R'$ è riflessiva, simmetrica e transitiva.

ESEMPIO 3.7. Si consideri una relazione d'equivalenza $(A, A, R)$. Data la partizione su $A$ individuata dalla classi d'equivalenza di $R$, si costruisca la relazione $R'$ su $A$ come descritto nel paragrafo precedente. Si verifichi che $R = R'$.

## 4. Relazioni d'ordine stretto

DEFINIZIONE 4.1. Una relazione $(A, A, R)$ antiriflessiva e transitiva è detta *relazione d'ordine stretto*.

ESEMPI 4.2. Si consideri la relazione tra insiemi $(\mathbb{N}, \mathbb{N}, R)$ dove, dati i numeri naturali $n$ e $m$, $nRm$ se e solo se $n < m$; si verifica facilmente che $R$ è una relazione d'ordine stretto.

Sia $X$ un insieme e $(P(X), P(X), R)$ la relazione definita da $Y\ R\ Z$ se e solo se $Y \subsetneq Z$, dove $Y$ e $Z$ sono sottoinsiemi di $X$; allora $R$ è una relazione d'ordine stretto.

Come risulta chiaro dagli esempi precedenti, una relazione d'ordine stretto con supporto l'insieme $A$ determina un criterio per confrontare tra loro gli elementi di $A$. In generale non tutti gli elementi di $A$ possono essere confrontati tramite $R$; ad esempio, dato un insieme $X$ con almeno due elementi $a$ e $b$ e la relazione $(P(X), P(X), \subsetneq)$ i due sottoinsiemi $\{a\}$ e $\{b\}$ non sono confrontabili tra loro, dato che nessuno dei due è contenuto nell'altro.

DEFINIZIONE 4.3. Una relazione d'ordine stretto $(A, A, R)$ gode della proprietà di *tricotomia* se dati due qualsiasi elementi $x$ e $y$ contenuti in $A$, o $xRy$, oppure $yRx$, oppure $x = y$.

ESEMPIO 4.4. La relazione tra insiemi $(\mathbb{Z}, \mathbb{Z}, <)$ gode della proprietà di tricotomia, poiché dati due qualsiasi numeri interi $n$ o $m$, o $n < m$ o $m < n$ oppure $n = m$.

Si consideri ora un sottoinsieme $S \subseteq A$; tramite la relazione di ordine stretto $R$ vogliamo confrontare gli elementi di $S$ tra loro e con gli elementi esterni a $S$. Nell'effettuare questo confronto si possono individuare alcuni elementi con caratteristiche rilevanti, descritti nella discussione che segue.

Data una relazione d'ordine stretto $(A, A, R)$ e $S \subseteq A$, un elemento $u \in A$ è detto *maggiorante* per $S$ se per ogni $x \in S$ si ha $x = u$ oppure $(x, u) \in R$; in altre parole un elemento è un maggiorante per $S$ se è confrontabile con ogni elemento di $S$ e risulta "maggiore", rispetto a $R$, di ogni elemento di $S$.

Un elemento $u \in S$ è detto *massimale* per $S$ se per ogni $x \in S$ si ha $(u, x) \notin R$; in altre parole un elemento è un massimale per $S$ se è un elemento di $S$ e, se è confrontabile rispetto a $R$ con altri elementi di $S$, risulta "maggiore".

Un elemento $u \in S$ è detto *massimo* per $S$ se per ogni $x \in S$ si ha $x = u$ oppure $(x, u) \in R$; in altre parole un elemento è un massimo per $S$ se appartiene a $S$, è confrontabile con ogni altro elemento di $S$, e risulta "maggiore" di ogni altro elemento di $S$. Notiamo che la differenza con la definizione di maggiorante è che qui si impone che l'elemento appartenga a $S$.

In modo analogo, possiamo definire gli elementi *minoranti*, *minimali* e *minimi* di $S$. Un elemento $u \in A$ è detto *minorante* per $S$ se per ogni $x \in S$ si ha $x = u$ oppure $(u, x) \in R$; in altre parole un elemento è un minorante per $S$ se è confrontabile con ogni elemento di $S$ e risulta "minore", rispetto a $R$, di ogni elemento di $S$.

Un elemento $u \in S$ è detto *minimale* per $S$ se per ogni $x \in S$ si ha $(x,u) \notin R$; in altre parole un elemento è un minimale per $S$ se è un elemento di $S$ e, se è confrontabile rispetto a $R$ con altri elementi di $S$, risulta "minore".

Un elemento $u \in S$ è detto *minimo* per $S$ se per ogni $x \in S$ si ha $x = u$ oppure $(u,x) \in R$; in altre parole un elemento è un minimo per $S$ se appartiene a $S$, è confrontabile con ogni altro elemento di $S$, e risulta "minore" di ogni altro elemento di $S$.

Si osservi che massimali, minimali, massimi e minimi sono elementi del sottoinsieme $S$, mentre i maggioranti e i minoranti possono anche non appartenere a $S$. Si noti inoltre che gli elementi massimali, minimali, maggioranti e minoranti, se esistono, possono non essere unici. Si verifica facilmente invece che il massimo e il minimo, se esistono, sono unici (si veda l'Esercizio 2.6).

Si considerino ora tutti gli elementi maggioranti per il sottoinsieme $S$. Essi formano un sottoinsieme di $A$ e pertanto possiamo considerarne il minimo; tale minimo, se esiste, è detto *estremo superiore* di $S$, e l'insieme $S$ si dice *superiormente limitato*. Essendo un minimo, l'estremo superiore se esiste è unico.

Si considerino invece tutti gli elementi minoranti per il sottoinsieme $S$. Essi formano un sottoinsieme di $A$ e pertanto possiamo considerarne il massimo; tale massimo, se esiste, è detto *estremo inferiore* di $S$, e l'insieme $S$ si dice *inferiormente limitato*. Essendo un massimo, l'estremo inferiore se esiste è unico.

Si vedano gli esercizi alla fine del capitolo per alcune importanti connessioni tra massimi, massimali, maggioranti e ed estremo superiore e analogamente tra minimi, minimali, minoranti ed estremo inferiore.

Dopo aver introdotto la nozione di minimo, possiamo studiare un'ulteriore proprietà di cui possono godere le relazioni d'ordine stretto, la proprietà di buon ordinamento.

DEFINIZIONE 4.5. Una relazione d'ordine stretto $(A,A,R)$ si dice un *buon ordine* se ogni sottoinsieme non vuoto di $A$ ammette elemento minimo.

ESEMPI 4.6. Si consideri l'usuale relazione d'ordine stretto $(\mathbb{N},\mathbb{N},<)$; questo è un buon ordine, dato che ogni sottoinsieme dei numeri naturali ammette minimo. Infatti sia $S \subseteq \mathbb{N}$ e sia $S \neq \emptyset$. Se $0 \in S$, allora chiaramente 0 è il minimo di $S$. Altrimenti, poiché $S$ è non vuoto, esiste un elemento $s_0 \in S$, con $s_0 > 0$; se $s_0$ è l'elemento minimo di $S$, allora $S$ ammette minimo, altrimenti esiste $s_1 \in S$ con $s_1 < s_0$; se $s_1$ è l'elemento minimo di $S$ allora $S$ ammette minimo, altrimenti esiste $s_2 \in S$ con $s_2 < s_1$; procedendo in questo modo, dopo al più un numero finito di passi, in particolare dopo al più $s_0$ passi, si trova l'elemento minimo di $S$. Si consideri invece la stessa relazione, ma tra numeri interi; allora $(\mathbb{Z},\mathbb{Z},<)$ non è un buon ordine. Infatti sia $S$ il sottoinsieme di $\mathbb{Z}$ formato da tutti i numeri negativi: chiaramente $S$ non ammette minimo e pertanto la relazione non può essere un buon ordine.

## 5. Relazioni d'ordine largo

Come abbiamo visto nella sezione precedente, un tipico esempio di relazione d'ordine stretto è la relazione $<$ tra insiemi numerici. Spesso tuttavia è più utile confrontare coppie di numeri tramite la relazione $\leq$. Questa non è una relazione d'ordine stretto, dato che non è antiriflessiva, ma si verifica facilmente che è riflessiva, antisimmetrica e transitiva.

DEFINIZIONE 5.1. Una relazione $(A,A,R)$ riflessiva, antisimmetrica e transitiva è detta *relazione d'ordine largo*.

ESEMPI 5.2. Si consideri la relazione tra insiemi $(\mathbb{N},\mathbb{N},R)$ dove, dati i numeri naturali $n$ e $m$, $nRm$ se e solo se $n \leq m$; si verifica facilmente che $R$ è una relazione d'ordine largo.

Sia $X$ un insieme e $(P(X),P(X),R)$ la relazione definita da $Y\ R\ X$ se e solo se $Y \subseteq Z$, dove $Y$ e $Z$ sono sottoinsiemi di $X$; allora $R$ è una relazione d'ordine largo.

Per chiarire la differenza tra il concetto di ordine stretto e ordine largo, si consiglia di ricordare i due esempi precedenti, confrontandoli con gli analoghi esempi 4.2 della sezione precedente.

Il legame tra le relazioni d'ordine stretto e d'ordine largo è molto forte: ogni relazione d'ordine stretto individua in modo univoco una relazione d'ordine largo, e viceversa.

PROPOSIZIONE 5.3. (a) *Sia* $(A, A, R)$ *una relazione d'ordine stretto e si consideri la relazione* $R' = \{(x, y) \mid (x, y) \in R$ *oppure* $x = y\}$. *Allora* $(A, A, R')$ *è una relazione d'ordine largo.*

(b) *Sia* $(A, A, R)$ *una relazione d'ordine largo e si consideri la relazione* $R' = \{(x, y) \mid (x, y) \in R$ *e* $x \neq y\}$. *Allora* $(A, A, R')$ *è una relazione d'ordine stretto.*

DIMOSTRAZIONE. (a) Dobbiamo verificare che $R'$ è riflessiva, antisimmetrica e transitiva, sapendo che $R$ è antiriflessiva e transitiva. Sia quindi $x \in A$; la coppia $(x, x)$ appartiene a $R'$ per costruzione, quindi $R'$ è riflessiva. Inoltre se $(x, y) \in R'$ e $(y, x) \in R'$, possiamo concludere che $x = y$; se infatti $x \neq y$, dalla costruzione di $R'$ seguirebbe che $(x, y) \in R$ e $(y, x) \in R$. Per la transitività di $R$ si avrebbe quindi che $(x, x) \in R$, contrariamente all'antiriflessività di $R$. Pertanto $R'$ è antisimmetrica. Per finire, siano $(x, y) \in R'$ e $(y, z) \in R'$; se $x = y$ allora ovviamente $(x, z) \in R'$ e analogamente se $y = z$ allora $(x, z) \in R'$. Se $x \neq y$ e $y \neq z$, allora per costruzione $(x, y) \in R$ e $(y, z) \in R$; essendo $R$ transitiva si conclude che $(x, z) \in R$ e quindi $(x, z) \in R'$.

(b) Dobbiamo verificare che $R'$ è antiriflessiva e transitiva sapendo che $R$ è riflessiva, antisimmetrica e transitiva. Sia quindi $x \in A$; la coppia $(x, x)$ non appartiene a $R'$ per costruzione, quindi $R'$ è antiriflessiva. Inoltre siano $(x, y) \in R'$ e $(y, z) \in R'$; dalla costruzione di $R'$ sappiamo che $x \neq y$, $y \neq z$, $(x, y) \in R$ e $(y, z) \in R$. Per la transitività di $R$ otteniamo $(x, z) \in R$; se $x = z$, si avrebbe inoltre $(y, x) \in R$ e quindi per l'antisimmetria di $R$ si concluderebbe che $x = y$, contrariamente al fatto che $(x, y) \in R'$. Quindi otteniamo $(x, z) \in R$ e $x \neq z$, cioè $(x, z) \in R'$. □

## 6. Relazioni $n$-arie

La definizione di relazione data in 1.1 è anche detta relazione *binaria*, poiché coinvolge *coppie* ordinate. Si può generalizzare questa definizione, introducendo il concetto di relazione *n-aria*:

DEFINIZIONE 6.1. Una *relazione n-aria* è un insieme di *n-uple* ordinate.

Una relazione $n$-aria è un sottoinsieme del prodotto $A_1 \times A_2 \times \cdots \times A_n$, dove $A_i$ è un insieme a cui appartengono tutti gli $i$-esimi termini delle $n$-uple. Nel seguito, se non diversamente specificato, col termine relazione intenderemo relazioni binarie

## ESERCIZI

ESERCIZIO 2.1. Descrivere geometricamente la relazione sull'insieme $X = \mathbb{R}$ definita da $xRy$ se $x^2 + y^2 = 1$; si ripeta l'esercizio con la relazione $xRy$ se $x^2 + y^2 \leq 1$.

ESERCIZIO 2.2. Sia $X = \mathbb{N} \times \mathbb{N}$ e si consideri la relazione $R = \{((a, b), (c, d)) \mid (a, b), (c, d) \in X$ e $a + d = b + c\}$. Si dimostri che $R$ è una relazione d'equivalenza.

ESERCIZIO 2.3. Si consideri la relazione su $\mathbb{Z}$ definita da $xRy$ se e solo se $-2 \leq x - y \leq 2$. È una relazione d'equivalenza?

ESERCIZIO 2.4. Si consideri la seguente relazione su $\mathbb{Z}$: $R = \{(a, b) \mid a, b \in \mathbb{Z}, a^2 = b^2$ e $b < a\}$. Dire se si tratta di una relazione di tipo noto; quali sono gli elementi $x \in \mathbb{Z}$ tali che $(3, x) \in R$?

ESERCIZIO 2.5. Si consideri la seguente relazione sull'insieme $\mathbb{Z} \setminus \{0\}$ dei numeri interi diversi da 0:

$$R = \{(a, b) : a, b \in \mathbb{Z}, ab > 0\}.$$

Dire se è una relazione di tipo noto, motivandone la risposta. Quali sono gli elementi in relazione con $-3$?

ESERCIZIO 2.6. Sia $(A, A, R)$ una relazione d'ordine stretto e sia $S \subseteq A$. Si dimostri che, se esiste un minimo di $S$, questo è unico. Si dimostri l'analogo fatto per un massimo.

ESERCIZIO 2.7. Mostrare che $R = \{(a, b), (a, e), (a, d), (a, f), (b, e), (b, f), (c, b), (c, e), (c, f), (d, f), (e, f)\}$ è una relazione d'ordine stretto sull'insieme $\{a, b, c, d, e, f\}$. Determinare gli eventuali elementi massimali, minimali, massimo, minimo, estremo superiore e estremo inferiore del sottoinsieme $\{b, d, e\}$.

ESERCIZIO 2.8. Mostrare che $R = \{(6,5), (6,4), (6,3), (6,2), (6,1), (5,3), (5,4), (5,2), (5,1), (4,3), (4,1), (3,1), (2,1)\}$ è una relazione d'ordine stretto sull'insieme $\{1,2,3,4,5,6\}$. Determinare gli eventuali elementi massimali, minimali, massimo, minimo, estremo superiore e estremo inferiore del sottoinsieme $\{2,3,4\}$.

ESERCIZIO 2.9. Mostrare che $R = \{(7,5), (7,3), (7,2), (7,1), (6,4), (6,3), (6,2), (6,1), (5,3), (5,2), (5,1), (4,3), (4,2), (4,1), (3,2), (3,1)\}$ è una relazione d'ordine stretto sull'insieme {1, 2, 3, 4, 5, 6, 7}. Determinare gli eventuali elementi massimali, minimali, massimo, minimo, estremo superiore e estremo inferiore del sottoinsieme $\{3,4,5\}$.

ESERCIZIO 2.10. Si consideri la relazione sull'insieme $\mathbb{N}$ definita da $R = \{(a,b) \mid a,b \in \mathbb{N} \text{ e } b-a \text{ è multiplo di } 5\}$. Si dica se è una relazione di tipo noto.

ESERCIZIO 2.11. Si consideri la relazione sull'insieme $\mathbb{Z}$ definita da $R = \{(a,b) \mid a,b \in \mathbb{Z} \text{ e } b-a \text{ è multiplo di } 5\}$. Si dica se è una relazione di tipo noto.

ESERCIZIO 2.12. Sia $X = \mathbb{Z} \times \mathbb{Z}$ e sia $R = \{((a,b),(c,d)) \mid (a,b),(c,d) \in X \text{ e } a \leq c\}$. Si dica se $R$ è una relazione di tipo noto.

ESERCIZIO 2.13. Sia $X = \mathbb{Z} \times \mathbb{Z}$ e sia $R = \{((a,b),(c,d)) \mid (a,b),(c,d) \in X \text{ e } a < c\}$. Si dica se $R$ è una relazione di tipo noto.

ESERCIZIO 2.14. Sia $R$ una relazione d'ordine stretto. Si costruisca come nella Proposizione 5.3(a) la relazione d'ordine largo $R'$. A partire da $R'$, si costruisca come in 5.3(b) la relazione d'ordine stretto $R''$. Si dimostri che $R = R''$. Si svolga lo stesso esercizio partendo da una relazione $R$ d'ordine largo.

CAPITOLO 3

# Funzioni

## 1. Definizioni e prime proprietà

Il concetto di funzione è di uso comune per esprimere la seguente situazione: due grandezze variano l'una al variare dell'altra secondo una certa legge. Ad esempio, l'area del quadrato varia al variare del lato, la pressione di un gas in un recipiente chiuso varia in funzione della temperatura, il tempo impiegato a percorrere un certo tragitto varia in funzione della velocità. In tutti questi casi si osservi che dato un certo valore del lato, della temperatura, o della velocità possiamo ottenere in modo esatto il valore dell'area, della pressione o del tempo semplicemente conoscendo la formula dell'area del quadrato, la legge di Boyle o la legge oraria del moto.

Procedendo analogamente a quanto è stato fatto per le relazioni, da un punto di vista matematico vogliamo astrarre dal significato e dalle caratteristiche fisiche delle funzioni; siamo invece interessati ad individuare le coppie ordinate che sono coinvolte in esse.

DEFINIZIONE 1.1. Una funzione $f$ è un insieme di coppie ordinate con la seguente proprietà, detta *univocità*: se $(a,b) \in f$ e $(a,c) \in f$, allora $b = c$. Se la coppia $(a,b) \in f$ si scrive $b = f(a)$ e si dice che *$b$ è immagine di $a$ tramite $f$*, o che *$b$ è il valore assunto da $f$ in $a$*.

ESEMPIO 1.2. L'insieme di coppie ordinate $\{(1,2),(2,4),(1,3),(4,1)\}$ non è una funzione; invece l'insieme $\{(1,2),(2,4),(4,1)\}$ è una funzione.

Si noti che le funzioni sono particolari relazioni, in quanto insiemi di coppie ordinate. Inoltre l'univocità esprime matematicamente quanto già osservato: dato un certo valore della grandezza corrispondente al primo elemento delle coppie ordinate, possiamo individuare in maniera univoca il valore della grandezza corrispondente al secondo elemento delle coppie ordinate. Spesso la quantità corrispondente ai primi termini delle coppie della funzione viene detta *variabile indipendente* e quella corrispondente ai secondi termini viene detta *variabile dipendente*. Tuttavia non bisogna dare al termine "variabile" significati che non ha; il concetto di funzione non li richiede.

Poiché le funzioni sono relazioni, ad esse si applicano tutti i concetti descritti nel capitolo precedente. In particolare, si definiscono il dominio, il codominio, l'insieme di definizione e l'insieme immagine di una funzione data. Inoltre una funzione si dice *totale* se il dominio coincide con l'insieme di definizione e *suriettiva* se il codominio coincide con l'insieme immagine. Se gli insiemi $A$ e $B$ sono rispettivamente il dominio e il codominio di una funzione $f$ e $(a,b) \in f$, si usa la notazione $f\colon A \to B$, $a \mapsto b$; questa notazione si legge "$f$ è una funzione da $A$ in $B$ e manda $a$ in $b$".

OSSERVAZIONE 1.3. Per descrivere le coppie ordinate appartenenti a una funzione, spesso si usa la notazione $f = \{(a,b) \mid (a,b) \text{ soddisfa } P\}$, dove $P$ è una data proprietà. Per esempio, si consideri la funzione $f = \{(x,y) \mid x,y \in \mathbb{R} \text{ e } x = (y+1)/2\}$, oppure la funzione $f = \{(x,y) \mid x,y \in \mathbb{R} \text{ e } y = e^x\}$. In maniera più compatta, si scrive anche $y = f(x)$; per esempio, le due funzioni sopra descritte, si scrivono rispettivamente

$$y = 2x - 1 \quad \text{e} \quad y = e^x.$$

Introduciamo ora una nuova importante proprietà di cui possono godere le funzioni.

DEFINIZIONE 1.4. Una funzione $f$ si dice *iniettiva* se gode della seguente proprietà: se $(a,c) \in f$ e $(b,c) \in f$, allora $a = b$.

Si può riformulare la proprietà di iniettività nel modo seguente: dati $x_1, x_2 \in \mathrm{Def}(f)$, se $f(x_1) = f(x_2)$ allora $x_1 = x_2$. Si faccia attenzione a distinguere l'iniettività dall'univocità. Si noti inoltre che, mentre la totalità e la suriettività di una funzione dipendono dal dominio e dal codominio, l'iniettività dipende solo dalla funzione.

ESEMPI 1.5. Si considerino $f = \{(1,2),(3,4),(5,7)\}$ e $f' = \{(1,2),(3,2),(5,7)\}$, insiemi di coppie ordinate che sono funzioni; la funzione $f$ è iniettiva, mentre $f'$ non è iniettiva.

Si consideri la funzione $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 3x+2$; questa è una funzione iniettiva, poiché, se $f(x_1) = f(x_2)$, si ha $3x_1 + 2 = 3x_2 + 2$, da cui si conclude $x_1 = x_2$. Inoltre $f$ è una funzione totale, ma non suriettiva; infatti, per esempio, $4 \notin \mathrm{Im}(f)$.

Si consideri la funzione $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 3x^2+2$; questa è una funzione totale, iniettiva e non suriettiva.

Si consideri la funzione $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x^2+2$; questa è una funzione totale, non suriettiva e non iniettiva.

DEFINIZIONE 1.6. Una funzione $f\colon A \to B$ totale, iniettiva e suriettiva si dice *biiettiva*.

Le funzioni biiettive sono dette anche corrispondenze biunivoche; infatti, data una funzione biiettiva tra due insiemi $A$ e $B$, possiamo far corrispondere a ogni elemento di $A$ uno e un solo elemento di $B$.

ESEMPI 1.7. La funzione $f\colon \mathbb{N} \to 2\mathbb{N}$, $x \mapsto 2x$ è biiettiva.
La funzione $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x-1$ è biiettiva.
La funzione $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$ è biiettiva.

ESEMPIO 1.8. Un importante esempio di funzione biiettiva è la funzione identica: dato un insieme $A$, la funzione $f\colon A \to A$, $a \mapsto a$, è detta *identità su* $A$, e si indica con $id_A$.

Per concludere introduciamo alcune notazione che useremo frequentemente. Si consideri la funzione $f\colon A \to B$; siano $C \subseteq A$ e $D \subseteq B$. L'insieme $\{f(x) \mid x \in C\}$ è detto *immagine di $C$ tramite $f$* e si indica con $f^{\rightarrow}(C)$; l'insieme $\{x \mid f(x) \in D\}$ è detto *controimmagine di $D$ tramite $f$* e si indica con $f^{\leftarrow}(D)$. Si noti che $f^{\rightarrow}(C) \subseteq B$ e $f^{\leftarrow}(D) \subseteq A$. Si osservi inoltre che, in generale, $f^{\leftarrow}(f^{\rightarrow}(C)) \neq C$ e $f^{\rightarrow}(f^{\leftarrow}(D)) \neq D$; si verifichi che $C \subseteq f^{\leftarrow}(f^{\rightarrow}(C))$ per ogni $C \subseteq A$ e $f^{\rightarrow}(f^{\leftarrow}(D)) \subseteq D$ per ogni $D \subseteq B$ (si veda l'Esercizio 3.17).

ESEMPI 1.9. Sia $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, e sia $C \subseteq \mathbb{R}$, $C = \{1,2\}$. Allora $f^{\leftarrow}(f^{\rightarrow}(C)) = \{1,-1,2,-2\}$. Sia $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x$; allora $\mathbb{N} \subseteq \mathbb{R}$ e $f^{\leftarrow}(f^{\rightarrow}(\mathbb{N})) = \mathbb{N}$.

## 2. Funzioni composte

Supponiamo di voler studiare la pressione di una gas in un recipiente chiuso; abbiamo già richiamato nella sezione precedente che la pressione varia in funzione della temperatura del gas. Ma se a sua volta la temperatura del gas varia al variare del tempo, chiaramente si ottiene che la pressione del gas varia al variare del tempo. Questo esempio introduce il concetto di funzione composta.

DEFINIZIONE 2.1. Siano $f$ e $g$ due funzioni; l'insieme di coppie ordinate

$$\{(a,c) \mid \text{ esiste } b \text{ tale che } (a,b) \in f \text{ e } (b,c) \in g\}$$

si dice *funzione composta di $f$ e $g$* e si indica con $g \circ f$. Se la coppia $(a,c) \in g \circ f$, si scrive $c = g \circ f(a)$ e, evidentemente, $g \circ f(a) = g(f(a))$.

ESEMPI 2.2. Si considerino le funzioni $f = \{(1,5),(3,7),(4,6),(5,5)\}$ e $g = \{(2,3),(5,1),(6,3)\}$; possiamo calcolare le funzioni composte $g \circ f = \{(1,1),(4,3),(5,1)\}$ e $f \circ g = \{(2,7),(5,5),(6,7)\}$.

Sia $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 2x$, e sia $g\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x+5$; allora $g \circ f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 2x+5$ e $f \circ g\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 2(x+5)$.

Come mostra l'esempio precedente, cambiando l'ordine di composizione si ottengono in generale funzioni composte diverse. Si noti inoltre che, date due funzioni $f$ e $g$, affinché la

funzione composta $g \circ f$ sia non vuota, l'intersezione $\mathrm{Im}(f) \cap \mathrm{Def}(g)$ deve essere diversa dall'insieme vuoto. In generale, se $f\colon A \to B$ e $g\colon C \to D$, allora si può assumere come dominio della funzione $g \circ f$ l'insieme $A$, e come codominio l'insieme $D$. Inoltre l'insieme di definizione è $\{x \mid f(x) \in \mathrm{Def}(g)\}$, cioè $\mathrm{Def}(g \circ f) = f^{\leftarrow}(Def(g))$, mentre l'insieme immagine è $\{z \mid z = g(y)$ per qualche $y \in \mathrm{Im}(f)\}$, cioè $\mathrm{Im}(g \circ f) = g^{\rightarrow}(\mathrm{Im}(f))$.

ESEMPI 2.3. Siano $f\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x-2$ e $g\colon \mathbb{Q} \to \mathbb{Q}$, $x \mapsto \frac{1}{x}$; quindi $\mathrm{Def}(f) = \mathbb{Z}$, $\mathrm{Def}(g) = \mathbb{Q} \setminus \{0\}$ e $\mathrm{Def}(g \circ f) = Z \setminus \{2\}$.

Siano $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 2x$ e $g\colon 3\mathbb{N} \to \mathbb{N}$, $x \mapsto \frac{x}{3}$; quindi $\mathrm{Def}(f) = \mathbb{N}$, $\mathrm{Def}(g) = 3\mathbb{N}$ e $\mathrm{Def}(g \circ f) = f^{\leftarrow}(Def(g)) = f^{\leftarrow}(3\mathbb{N}) = 3\mathbb{N}$.

Dall'esempio precedente si osserva come, anche se $f$ e $g$ sono funzioni totali, in generale $g \circ f$ non è una funzione totale. La proposizione seguente analizza il legame tra le proprietà delle funzioni di partenza e quelle della funzione composta.

PROPOSIZIONE 2.4. *Si considerino due funzioni $f\colon A \to B$ e $g\colon C \to D$.*

(1) *La funzione $g \circ f$ è totale se e solo se $f$ è totale e* $\mathrm{Im}(f) \subseteq \mathrm{Def}(g)$*;*
(2) *se $f$ e $g$ sono iniettive, allora $g \circ f$ è iniettiva;*
(3) *se $g$ è suriettiva e* $\mathrm{Def}(g) \subseteq \mathrm{Im}(f)$*, allora $g \circ f$ è suriettiva;*
(4) *se $g$ è iniettiva e $g \circ f$ è suriettiva, allora* $\mathrm{Def}(g) \subseteq \mathrm{Im}(f)$*;*
(5) *se $f$ e $g$ sono biiettive, $g \circ f$ è biiettiva se e solo se* $\mathrm{Im}(f) = \mathrm{Def}(g)$*, cioè se e solo se $B = C$.*

DIMOSTRAZIONE. (1) Supponiamo che $g \circ f$ sia totale; quindi per ogni $x \in A$ esiste $z \in D$ tale che $z = g(f(x))$; in particolare esiste $y \in \mathrm{Im}(f)$ tale che $y = f(x)$ e pertanto $f$ è totale. Si consideri inoltre $y \in \mathrm{Im}(f)$ e sia $x \in A$ tale che $f(x) = y$. Poiché $g \circ f$ è totale, esiste $z \in D$ tale che $z = g(f(x))$; ne segue quindi $y \in \mathrm{Def}(g)$.

Supponiamo invece che $f$ sia totale e che $\mathrm{Im}(f) \subseteq \mathrm{Def}(g)$. Dato $x \in A$, poiché esiste $y \in \mathrm{Im}(f)$ tale che $y = f(x)$ e $y \in \mathrm{Def}(g)$, allora esiste $z \in D$ tale che $z = g(y) = g(f(x))$; ne segue che $g \circ f$ è totale.

(2) Se $g(f(x_1)) = g(f(x_2))$, essendo $g$ iniettiva, segue che $f(x_1) = f(x_2)$. Poiché anche $f$ è iniettiva, si ottiene $x_1 = x_2$.

(3) Supponiamo $\mathrm{Def}(g) \subseteq \mathrm{Im}(f)$ e sia $z \in D$. Poiché $g$ è suriettiva, esiste $y \in \mathrm{Def}(g)$ tale che $z = g(y)$; dato che $y \in \mathrm{Im}(f)$, esiste $x \in A$ tale che $y = f(x)$ e quindi $z = g(f(x))$.

(4) Sia $y \in \mathrm{Def}(g)$; poiché $g \circ f$ è suriettiva, esiste $x \in A$ tale che $g(y) = g(f(x))$. Essendo $g$ iniettiva, segue che $y = f(x)$ e pertanto $\mathrm{Def}(g) \subseteq \mathrm{Im}(f)$.

(5) Segue dalle precedenti. □

## 3. Funzione inversa

Consideriamo la formula che esprime l'area del quadrato in funzione del lato, $A = l^2$; tale funzione ci permette di trovare l'area noto il lato del quadrato. Possiamo però anche considerare il lato come funzione dell'area, secondo la formula $l = \sqrt{A}$. Questo primo esempio introduce il concetto di funzione inversa che studieremo in questa sezione.

In generale, data una funzione $f$, è sempre possibile costruire l'insieme $f^{-1} = \{(y,x) \mid (x,y) \in f\}$; si costruisce cioè l'insieme di coppie ordinate ottenuto scambiando l'ordine dei termini nelle coppie ordinate contenute in $f$. Si osservi che $f^{-1}$ è sicuramente una relazione, ma in generale non è una funzione, dato che potrebbe non godere della proprietà di univocità.

ESEMPI 3.1. Data la funzione $f = \{(1,2),(2,3),(3,2),(4,1)\}$, è immediato verificare che la relazione $f^{-1} = \{(2,1),(3,2),(2,3),(1,4)\}$ non è una funzione. Si osservi che $f$ non è iniettiva. Si consideri invece la funzione $g = \{(1,2),(2,3),(3,4)\}$; si verifica facilmente che la relazione $g^{-1} = \{(2,1),(3,2),(4,3)\}$ è una funzione. Si osservi che $g$ è iniettiva.

Come mostra il precedente esempio, affinché la relazione $f^{-1}$ sia una funzione, $f$ deve essere iniettiva; tale proprietà assicura infatti che $f^{-1}$ sia una relazione univoca.

DEFINIZIONE 3.2. Sia $f$ una funzione iniettiva. La funzione $f^{-1} = \{(y,x) \mid (x,y) \in f\}$ è detta *funzione inversa di $f$*.

Si osservi che se $f\colon A \to B$ e $b = f(a)$, allora $f^{-1}\colon B \to A$ e $a = f^{-1}(b)$. Inoltre, $\mathrm{Def}(f^{-1}) = \mathrm{Im}(f)$ e $\mathrm{Im}(f^{-1}) = \mathrm{Def}(f)$.

ESEMPI 3.3. Sia $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x+2$; la funzione inversa è $f^{-1}\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x-2$.

Si consideri la funzione esponenziale $\mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$, dove $\mathbb{R}_{>0}$ denota l'insieme dei reali strettamente maggiori di 0; la sua funzione inversa è la funzione logaritmica $\mathbb{R}_{>0} \to \mathbb{R}$, $x \mapsto \log x$.

PROPOSIZIONE 3.4. *Sia $f\colon A \to B$ una funzione iniettiva.*

(1) *La funzione inversa $f^{-1}$ è iniettiva;*
(2) *la funzione $f^{-1}$ è totale se e solo se $f$ è suriettiva;*
(3) *la funzione $f^{-1}$ è suriettiva se e solo se $f$ è totale;*
(4) *la funzione $f^{-1}$ è biiettiva se e solo se $f$ è biiettiva.*

DIMOSTRAZIONE. (1) Sia $f^{-1}(y_1) = f^{-1}(y_2) = x$; allora le coppie ordinate $(y_1, x)$ e $(y_2, x)$ appartengono a $f^{-1}$. Quindi le coppie $(x, y_1)$ e $(x, y_2)$ appartengono a $f$. Per la proprietà di univocità si conclude che $y_1 = y_2$.

(2) e (3) Seguono direttamente dal fatto che $\mathrm{Def}(f^{-1}) = \mathrm{Im}(f)$ e $\mathrm{Im}(f^{-1}) = \mathrm{Def}(f)$.

(4) Segue dai punti precedenti. □

ESEMPI 3.5. Si consideri la funzione $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto 2x$; $f$ è iniettiva, totale ma non suriettiva. La sua funzione inversa $f^{-1}\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto \frac{x}{2}$ è iniettiva, suriettiva ma non totale.

Si consideri la funzione biiettiva $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$; la sua inversa $f^{-1}\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^{1/3}$ è ancora biiettiva.

Si osservi inoltre che la funzione inversa della funzione inversa è la funzione di partenza, e componendo una funzione con la sua inversa si ottiene la funzione identica.

PROPOSIZIONE 3.6. *Sia $f$ una funzione iniettiva.*

(1) $(f^{-1})^{-1} = f$;
(2) $f^{-1} \circ f = id_{\mathrm{Def}(f)}$;
(3) $f \circ f^{-1} = id_{\mathrm{Im}(f)}$.

DIMOSTRAZIONE. (1) $(f^{-1})^{-1} = \{(x, y) \mid (y, x) \in f^{-1}\} = \{(x, y) \mid (x, y) \in f\} = f$.

(2) Si consideri $x \in \mathrm{Def}(f)$ e poniamo $y = f(x)$. Poiché, per la definizione di funzione inversa, $f^{-1}(y) = x$, segue che $f^{-1}(f(x)) = f^{-1}(y) = x$ per ogni $x \in \mathrm{Def}(f)$. Quindi $f^{-1} \circ f = id_{\mathrm{Def}(f)}$.

(3) Sia $y \in \mathrm{Im}(f)$; poiché $y = f(x)$ per qualche $x \in \mathrm{Def}(f)$, $f^{-1}(y) = x$ e quindi $f(f^{-1}(y)) = f(x) = y$. Pertanto $f \circ f^{-1} = id_{\mathrm{Im}(f)}$. □

## 4. Funzioni $n$-arie

Le funzioni qui studiate sono dette anche funzioni a una variabile, o funzioni 1-arie dato che esse esprimono matematicamente la situazione in cui una certa quantità varia in funzione di un'altra. Si può generalizzare tale concetto, introducendo le funzioni a $n$ variabili, per descrivere la situazione in cui una certa quantità varia in funzione di altre $n$.

DEFINIZIONE 4.1. Una *funzione $n$-aria*, o *funzione a $n$ variabili*, $f$ è una relazione $n+1$-aria che gode della seguente proprietà: se $(a_1, a_2, \ldots, a_n, b) \in f$ e $(a_1, a_2, \ldots, a_n, c) \in f$, allora $b = c$.

La proprietà che caratterizza le funzione $n$-arie tra le relazioni $n+1$-arie è l'analogo della proprietà di univocità introdotta per la funzioni 1-arie. Si osservi inoltre che una funzione a $n$ variabili può essere vista come una funzione 1-aria $f\colon A \to B$, dove il dominio $A$ è il prodotto di $n$ insiemi, cioè $A = A_1 \times \cdots \times A_n$. In questo modo si possono estendere alle funzioni a $n$ variabili tutti i concetti visti finora.

## ESERCIZI

ESERCIZIO 3.1. Dato l'insieme di coppie ordinate

$$\begin{aligned} g = &\{(x, x^2+2x) \mid x \in \mathbb{N}, x^2-1<10\} \cup \\ &\cup \{(x, 4x+3) \mid x \in \mathbb{N}, 2<x<5\} \cup \\ &\cup \{(x, x-5) \mid x \in \mathbb{N}, x>5\} \cup \{(1,3),(7,2)\}, \end{aligned}$$

motivare perché $g$ è una funzione da $\mathbb{N}$ in $\mathbb{N}$, precisando se è totale, suriettiva, iniettiva o biiettiva, giustificando le risposte. Data poi la funzione $f = \{(0,3),(2,3),(1,5)\}$, scrivere quali sono le funzioni $h = f \circ g$ e $k = g \circ f$. Di esse precisare insieme di definizione e insieme immagine e se sono iniettive.

ESERCIZIO 3.2. Dato l'insieme di coppie ordinate

$$\begin{aligned} g = &\{(x, 5-x) \mid x \in \mathbb{N}, x-1<3\} \cup \\ &\cup \{(x, x^2-2x-1) \mid x \in \mathbb{N}, 7<x^2-1<27\} \cup \\ &\cup \{(x, 2x+3) \mid x \in \mathbb{N}, x>5\} \cup \{(2,3),(6,15)\}, \end{aligned}$$

motivare perché $g$ è una funzione da $\mathbb{N}$ in $\mathbb{N}$, precisando se è totale, suriettiva, iniettiva o biiettiva, giustificando le risposte. Data poi la funzione $f = \{(0,3),(2,6),(1,0)\}$, scrivere quali sono le funzioni $h = f \circ g$ e $k = g \circ f$. Di esse precisare insieme di definizione e insieme immagine e se sono iniettive.

ESERCIZIO 3.3. Dato l'insieme di coppie ordinate

$$\begin{aligned} g = &\{(x, x-x^2) \mid x \in \mathbb{N}, 0<x+1<3\} \cup \\ &\{(x, x-1) \mid x \in \mathbb{N}, 0 \le x^2-1 \le 20\} \cup \\ &\{(x, 2x-7) \mid x \in \mathbb{N}, x>5\} \cup \{(5,4),(3,2)\}, \end{aligned}$$

motivare perché $g$ è una funzione da $\mathbb{N}$ in $\mathbb{N}$, precisando se è totale, suriettiva, iniettiva o biiettiva, giustificando le risposte. Data poi la funzione $f = \{(0,3),(1,5),(3,1)\}$, scrivere quali sono le funzioni $h = f \circ g$ e $k = g \circ f$. Di esse precisare insieme di definizione e insieme immagine e se sono iniettive.

ESERCIZIO 3.4. Si dica se le seguenti relazioni sono funzioni di $\mathbb{R}$ in $\mathbb{R}$:

(a) $\{(x,y) \mid x,y \in \mathbb{R}, x^2+y^2=1\}$;
(b) $\{(x,y) \mid x,y \in \mathbb{R}, y=\sin x\}$;
(c) $\{(x,y) \mid x,y \in \mathbb{R}, x=\sin y\}$.

ESERCIZIO 3.5. La composizione di funzioni suriettive è suriettiva? Si motivi la risposta. In caso di risposta negativa si esibisca un controesempio.

ESERCIZIO 3.6. La composizione di funzioni iniettive è iniettiva? Si motivi la risposta. In caso di risposta negativa si esibisca un controesempio.

ESERCIZIO 3.7. La composizione di funzioni totali è totale? Si motivi la risposta. In caso di risposta negativa si esibisca un controesempio.

ESERCIZIO 3.8. Si può dire che

$$x \mapsto \begin{cases} e^x & \text{se } x \le 0, \\ x-x^2 & \text{se } x \ge 0. \end{cases}$$

definisce una funzione $f$?

Si può dire che

$$x \mapsto \begin{cases} e^x & \text{se } x \le 0, \\ x-x^2+1 & \text{se } x \ge 0. \end{cases}$$

definisce una funzione $g$?

Nel caso la risposta sia affermativa, si dica se $f$ o $g$ sono totali, iniettive o suriettive.

ESERCIZIO 3.9. Si consideri la funzione $f\colon \mathbb{R} \to \mathbb{R}$ definita da $f(x) = x^3 - 4$. Si dimostri che $f$ è biiettiva e si costruisca la funzione inversa $f^{-1}$.

ESERCIZIO 3.10. Sia $\lambda \in \mathbb{R}$ e si ponga, per $x \in \mathbb{R}$, $f(x) = \frac{x^3+\lambda x}{3x+1}$. Esistono valori di $\lambda$ per i quali $f$ definisce una funzione da $\mathbb{R}$ a $\mathbb{R}_{\geq 0}$? Esistono valori di $\lambda$ per i quali $f$ definisce una funzione da $\mathbb{R}_{\geq 0}$ a $\mathbb{R}_{\geq 0}$? (Si ricordi che $\mathbb{R}_{\geq 0}$ indica l'insieme dei reali maggiori o uguali a 0.)

ESERCIZIO 3.11. Dati due insiemi non vuoti $X$ e $Y$ e una funzione $f\colon X \to Y$, definiamo una funzione $f^*\colon P(Y) \to P(X)$ ponendo, per $A \in P(Y)$, $f^*(A) = f^{\leftarrow}(A)$. Si verifichi che: (1) se $f$ è suriettiva, allora $f^*$ è iniettiva; (2) se $f$ è iniettiva, allora $f^*$ è suriettiva.

ESERCIZIO 3.12. Sia $X$ un insieme non vuoto. Sia $A$ un sottoinsieme di $X$ e si consideri la funzione $f\colon P(X) \to P(X)$, $Y \mapsto Y \setminus A$. Per quali sottoinsiemi $A$ la funzione $f$ è iniettiva o suriettiva? Per quali $B \in P(X)$ si ha $f(B) = \emptyset$? Si determini $\mathrm{Im}(f)$.

ESERCIZIO 3.13. Si consideri la funzione $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin x + 2$. $f$ è iniettiva? $f$ è suriettiva? Si determini $\mathrm{Im}(f)$.

ESERCIZIO 3.14. Qual è il massimo sottoinsieme $A \subseteq \mathbb{R}$ su cui $f(x) = \frac{1}{|\log x|}$ definisce una funzione totale $f\colon A \to \mathbb{R}$? Si consideri allora $f\colon A \to \mathbb{R}$ e si calcoli $\mathrm{Im}(f)$. Si ripeta l'esercizio con $f(x) = \frac{1}{\log|x|}$.

ESERCIZIO 3.15. Si determini il più grande sottoinsieme di $\mathbb{R}$ su cui $f(x) = \frac{|x-2|}{|x^2-2x+5|}$ definisce una funzione totale $f\colon S \to [0,1]$? (Si ricordi che $[0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$.)

ESERCIZIO 3.16. Si considerino le funzioni $f\colon \mathbb{R} \to \mathbb{R}$ e $g\colon \mathbb{R} \to \mathbb{R}$ definite da

$$f(x) = \frac{x}{x^2+1}, \qquad g(x) = \begin{cases} 1 & \text{se } x < 0, \\ 0 & \text{se } x = 0, \\ -1 & \text{se } x > 0. \end{cases}$$

Si determini la funzione composta $g \circ f$. Tra le funzioni $f$, $g$ e $g \circ f$, quali sono iniettive, suriettive o biiettive?

ESERCIZIO 3.17. Siano $f\colon A \to B$, $C \subseteq A$ e $D \subseteq B$. Si dimostri che $C \subseteq f^{\leftarrow}(f^{\rightarrow}(C))$ e che $f^{\rightarrow}(f^{\leftarrow}(D)) \subseteq D$. Quando si può concludere che $C = f^{\leftarrow}(f^{\rightarrow}(C))$ per ogni $C \subseteq A$? Quando si può concludere che $D = f^{\rightarrow}(f^{\leftarrow}(D))$ per ogni $D \subseteq B$?

CAPITOLO 4

# Insiemi infiniti

## 1. Introduzione

Finché gli insiemi che si considerano sono finiti (cioè si può contare quanti sono i loro elementi mettendoli in corrispondenza biiettiva con i numeri che precedono un certo numero naturale) la nozione di insieme può fornire un comodo modo di esprimersi, ma non è indispensabile. Di fatto Cantor per primo elaborò la nozione di insieme per risolvere problemi di quantità di elementi in insiemi infiniti (cioè non finiti).

DEFINIZIONE. Si dice che due classi *hanno la stessa cardinalità* quando c'è una biiettività tra le due classi. In tal caso si dirà anche che le due classi sono *equinumerose*.

DEFINIZIONE. Si dice che un insieme $A$ è *finito* se esistono un numero naturale $n$ e una biiettività da $A$ sull'insieme dei numeri naturali che precedono $n$; in questo caso diremo che $A$ ha $n$ elementi. Se ciò non succede, si dice che l'insieme è infinito.

Se un insieme $A$ è finito e un altro insieme $B$ è contenuto propriamente (contenuto ma non uguale) in $A$ allora $A$ e $B$ non sono equinumerosi, cioè non c'è alcuna biiettività tra i due.

Questo risultato dipende dal fatto che per nessun numero naturale ci può essere una biiettività tra l'insieme dei numeri che lo precedono e l'insieme di quelli che precedono un diverso numero naturale.

L'ultima affermazione non si estende agli insiemi infiniti; lo giustifichiamo con un controesempio già considerato da Galileo Galilei nel suo *Dialogo sopra i due massimi sistemi del mondo*. I numeri pari sono un sottinsieme proprio dei numeri naturali, ed entrambi gli insiemi non sono finiti; inoltre la funzione che a un numero naturale associa il suo doppio è una biiettività dai numeri naturali sui numeri pari. Così si deve dire che i numeri naturali sono tanti quanti i numeri pari pur costituendo questi un sottinsieme proprio dell'insieme dei naturali.

Per gli insiemi finiti non solo si può dire se hanno lo stesso numero di elementi, ma anche se uno ha più elementi di un altro o meno. A questo scopo ci si rifà alla relazione d'ordine naturale tra i numeri naturali che contano gli elementi di ciascuno dei due insiemi. Per gli insiemi infiniti non si può utilizzare lo stesso metodo. Come decidere allora quando un insieme ha più o meno elementi di un altro?

Ci si potrebbe limitare a dire che un insieme è finito o infinito. Tuttavia l'esperienza di vari insiemi infiniti porta naturalmente a domandarci se si può stabilire una gerarchia simile a quella fra gli insiemi finiti.

Prenderemo a modello le stesse proprietà degli insiemi finiti.

## 2. Cardinalità

DEFINIZIONE 2.1. Siano $A$ e $B$ due insiemi. Diremo che la cardinalità dell'insieme $A$ è minore o uguale a quella dell'insieme $B$, e scriveremo $|A| \leq |B|$ quando esiste una *funzione totale iniettiva* di $A$ in $B$.

Questa relazione fra insiemi non è un ordine, né stretto né largo. Non è stretto perché $|A| \leq |A|$, per motivi ovvi (basta considerare la funzione identità). Non è un ordine largo, perché può accadere che $|A| \leq |B|$ e anche $|B| \leq |A|$, con $A \neq B$. Un esempio è proprio quello in cui $A$ è l'insieme dei numeri naturali e $B$ quello dei numeri naturali pari.

Scopo di queste note è di studiare le proprietà di questa relazione. Attraverso essa potremo arrivare al concetto di "uguale cardinalità", che è ciò che ci interessa.

ESEMPI 2.2. (1) Se $A$ è un insieme e $B \subseteq A$, allora $|B| \leq |A|$.

(2) Se $\mathbb{Z}$ è l'insieme dei numeri interi e $\mathbb{N}$ quello dei numeri naturali, allora $|\mathbb{Z}| \leq |\mathbb{N}|$. Ciò può apparire paradossale, ma vedremo che non lo è.

Consideriamo infatti la seguente funzione:

$$f(x) = \begin{cases} 2x & \text{se } x \geq 0, \\ -2x-1 & \text{se } x < 0. \end{cases}$$

Si può facilmente verificare che $f\colon \mathbb{Z} \to \mathbb{N}$ è non solo iniettiva, ma anche suriettiva.

(3) Se $X$ è un insieme finito e $Y$ è un insieme infinito, allora $|X| \leq |Y|$.

Supponiamo che $X$ abbia $n$ elementi. Faremo induzione su $n$.

Se $n = 0$, la funzione vuota è quella che cerchiamo.

Supponiamo la tesi vera per insiemi con $n$ elementi e supponiamo che $X$ abbia $n+1$ elementi: $X = \{x_1, \ldots, x_n, x_{n+1}\}$. Per ipotesi induttiva esiste una funzione totale iniettiva $f\colon \{x_1, \ldots, x_n\} \to Y$. Siccome $Y$ è infinito, esiste un elemento $y \notin \mathrm{Im}(f)$ (altrimenti $Y$ avrebbe $n$ elementi). Possiamo allora definire una funzione totale iniettiva $g\colon X \to Y$ che estende $f$ ponendo $g(x_{n+1}) = y$.

Diamo subito la definizione che ci interessa maggiormente.

DEFINIZIONE 2.3. Siano $A$ e $B$ due insiemi. Diremo che $A$ e $B$ *hanno la stessa cardinalità*, e scriveremo $|A| = |B|$, quando esiste una funzione biiettiva (totale) di $A$ su $B$.

Non daremo la definizione di cardinalità, per la quale occorrerebbe molta più teoria e che non ci servirà. Sarà più rilevante per noi scoprire le connessioni fra le due relazioni introdotte.

## 3. Proprietà della cardinalità di insiemi infiniti

(C1) Se $A$ è un insieme, allora $|A| = |A|$.
(C2) Se $A$ e $B$ sono insiemi e $|A| = |B|$, allora $|B| = |A|$.
(C3) Se $A$, $B$ e $C$ sono insiemi, $|A| = |B|$ e $|B| = |C|$, allora $|A| = |C|$.

Queste tre proprietà sono quasi ovvie: basta, nel primo caso, considerare la funzione identità; nel secondo si prende la funzione inversa della biiettività $A \to B$; nel terzo si prende la composizione fra la biiettività $A \to B$ e la biiettività $B \to C$.

(M1) Se $A$ è un insieme, allora $|A| \leq |A|$.
(M2) Se $A$, $B$ e $C$ sono insiemi, $|A| \leq |B|$ e $|B| \leq |C|$, allora $|A| \leq |C|$.

La dimostrazione di queste due è facile (esercizio). Notiamo che esse e le precedenti valgono anche per insiemi finiti.

C'è un legame fra le due relazioni? La risposta è sì e sta proprio nella "proprietà antisimmetrica" che sappiamo non valere per $\leq$.

Il risultato che enunceremo ora è uno fra i più importanti della teoria degli insiemi e risale allo stesso Cantor, poi perfezionato da altri studiosi.

TEOREMA 3.1 (Cantor, Schröder, Bernstein). *Siano $A$ e $B$ insiemi tali che $|A| \leq |B|$ e $|B| \leq |A|$, allora*

$$|A| = |B|.$$

DIMOSTRAZIONE. L'ipotesi dice che esistono una funzione $f\colon A \to B$ iniettiva totale e una funzione $g\colon B \to A$ iniettiva totale.

Per completare la dimostrazione dobbiamo trovare una funzione biiettiva $h\colon A \to B$.

Un elemento $a \in A$ ha un *genitore* se esiste un elemento $b \in B$ tale che $g(b) = a$. Analogamente diremo che un elemento $b \in B$ ha un genitore se esiste $a \in A$ tale che $f(a) = b$.

Siccome $f$ e $g$ sono iniettive, il genitore di un elemento, se esiste, è unico.

Dato un elemento $a \in A$ oppure $b \in B$, possiamo avviare una procedura:

(a) poniamo $x_0 = a$ o, rispettivamente $x_0 = b$ e $i = 0$;
(b) se $x_i$ non ha genitore, ci fermiamo;
(c) se $x_i$ ha genitore, lo chiamiamo $x_{i+1}$, aumentiamo di uno il valore di $i$ e torniamo al passo (b).

Partendo da un elemento $a \in A$, possono accadere tre casi:

- la procedura non termina; scriveremo che $a \in A_0$;
- la procedura termina in un elemento di $A$; scriveremo che $a \in A_A$;
- la procedura termina in un elemento di $B$; scriveremo che $a \in A_B$.

Analogamente, partendo da un elemento $b \in B$, possono accadere tre casi:

- la procedura non termina; scriveremo che $b \in B_0$;
- la procedura termina in un elemento di $A$; scriveremo che $b \in B_A$;
- la procedura termina in un elemento di $B$; scriveremo che $b \in B_B$.

Abbiamo diviso ciascuno degli insiemi $A$ e $B$ in tre sottoinsiemi a due a due disgiunti: $A = A_0 \cup A_A \cup A_B$, $B = B_0 \cup B_A \cup B_B$.

Se prendiamo un elemento $a \in A_0$, è evidente che $f(a) \in B_0$, perché, per definizione, $a$ è genitore di $f(a)$. Dunque $f$ induce una funzione $h_0 \colon A_0 \to B_0$, dove $h_0(a) = f(a)$. Questa funzione, essendo una restrizione di $f$, è iniettiva e anche totale. È suriettiva, perché, se $b \in B_0$, esso ha un genitore $a$ che deve appartenere ad $A_0$.

Se prendiamo un elemento $a \in A_A$, allora $f(a) \in B_A$: infatti $a$ è genitore di $f(a)$ e la procedura, a partire da $b = f(a)$ termina in $A$. Dunque $f$ induce una funzione $h_A \colon A_A \to B_A$ che è iniettiva e totale. Essa è anche suriettiva, perché ogni elemento di $B_A$ ha genitore che deve appartenere ad $A_A$.

Analogamente, se partiamo da un elemento $b \in B_B$, allora $g(b) \in A_B$ e $g$ induce una funzione iniettiva e totale $h_B \colon B_B \to A_B$ che è suriettiva, esattamente per lo stesso motivo di prima.

Ci resta da porre $h = h_0 \cup h_A \cup h_B^{-1}$. Allora $h$ è una funzione $h \colon A \to B$ che è totale, iniettiva e suriettiva (lo si verifichi). □

ESEMPIO 3.2. Illustriamo la dimostrazione con la seguente situazione: sia $f \colon \mathbb{N} \to \mathbb{Z}$ la funzione inclusione; consideriamo poi la funzione $g \colon \mathbb{Z} \to \mathbb{N}$

$$g(z) = \begin{cases} 4z & \text{se } z \geq 0, \\ -4z - 2 & \text{se } z < 0. \end{cases}$$

Quali sono gli elementi di $\mathbb{N}$ che hanno un genitore? Esattamente quelli che appartengono all'immagine di $g$, cioè i numeri pari. I numeri dispari, quindi, appartengono a $\mathbb{N}_{\mathbb{N}}$, perché la procedura si ferma a loro stessi.

Consideriamo $x_0 = 2 \in \mathbb{N}$; siccome $g(-1) = 2$, abbiamo $x_1 = -1$; poiché $-1 \notin \mathrm{Im}(f)$, la procedura si ferma e $2 \in \mathbb{N}_{\mathbb{Z}}$.

Consideriamo invece $x_0 = 4 \in \mathbb{N}$; siccome $g(1) = 4$, abbiamo $x_1 = 1$ e possiamo andare avanti, perché $1 = f(1)$, dunque $x_2 = 1 \in \mathbb{N}$. Poiché $1 \notin \mathrm{Im}(g)$, abbiamo che $4 \in \mathbb{N}_{\mathbb{N}}$.

Studiamo ora $x_0 = 16 \in \mathbb{N}$; siccome $g(4) = 16$, abbiamo $x_1 = 4$; siccome $f(4) = 4$, abbiamo $x_2 = 4 \in \mathbb{N}$; siccome $4 = g(1)$, abbiamo $x_3 = 1 \in \mathbb{Z}$; siccome $1 = f(1)$, abbiamo $x_4 = 1 \in \mathbb{N}$. La procedura si ferma qui, dunque $16 \in \mathbb{N}_{\mathbb{N}}$.

Si lascia al lettore l'esame di altri elementi di $\mathbb{N}$ o di $\mathbb{Z}$.

La relazione $\leq$ si può allora vedere non come una relazione d'ordine largo fra insiemi, ma piuttosto come un ordine largo fra le "cardinalità" degli insiemi. Non vogliamo però definire il concetto di cardinalità; ci limiteremo a confrontarle usando le relazioni introdotte.

Il teorema seguente dice, in sostanza, che la cardinalità dell'insieme dei numeri naturali è la più piccola cardinalità infinita.

TEOREMA 3.3. *Sia $A$ un insieme infinito. Allora $|\mathbb{N}| \leq |A|$.*

DIMOSTRAZIONE. Costruiremo un sottoinsieme di $A$ per induzione.

Siccome $A$ è infinito, esso non è vuoto; sia $x_0 \in A$. Evidentemente $\{x_0\} \neq A$, quindi esiste $x_1 \in A \setminus \{x_0\}$. Ancora $\{x_0, x_1\} \neq A$, quindi esiste $x_2 \in A \setminus \{x_0, x_1, x_2\}$.

Proseguiamo allo stesso modo: supponiamo di avere scelto gli elementi $x_0, x_1, \ldots, x_n \in A$, a due a due distinti. Siccome $\{x_0, \ldots, x_n\} \neq A$, esiste

$$x_{n+1} \in A \setminus \{x_0, \ldots, x_n\}.$$

Dunque la procedura associa a ogni numero naturale un elemento di $A$ e la funzione $n \mapsto x_n$ è iniettiva. □

Questo risultato ha una conseguenza immediata.

COROLLARIO 3.4. *Sia $A \subseteq \mathbb{N}$. Allora $A$ è finito oppure $|A| = |\mathbb{N}|$.*

DIMOSTRAZIONE. Se $A$ non è finito, allora è infinito. Per il teorema, $|\mathbb{N}| \leq |A|$. Ma $|A| \leq |\mathbb{N}|$ perché $A \subseteq \mathbb{N}$. Per il teorema di Cantor-Schröder-Bernstein, $|A| = |\mathbb{N}|$. □

Un altro corollario è la caratterizzazione che Dedekind prese come definizione di insieme infinito.

COROLLARIO 3.5. *Un insieme $A$ è infinito se e solo se esiste un sottoinsieme proprio $B \subset A$ tale che $|B| = |A|$.*

DIMOSTRAZIONE. Se $A$ è finito, è evidente che un suo sottoinsieme proprio non può avere tanti elementi quanti $A$.

Supponiamo ora che $A$ sia infinito. Per il corollario precedente, esiste una funzione iniettiva totale $f\colon \mathbb{N} \to A$. Definiamo ora una funzione $g\colon A \to A$ ponendo:

$$g(x) = \begin{cases} f(n+1) & \text{se esiste } n \in \mathbb{N} \text{ tale che } x = f(n), \\ x & \text{se } x \notin \operatorname{Im}(f). \end{cases}$$

La condizione "esiste $n \in \mathbb{N}$ tale che $x = f(n)$" equivale alla condizione "$x \in \operatorname{Im}(f)$".

La funzione $g$ è ben definita, perché $f$ è iniettiva; dunque, se $x = f(n)$ per qualche $n$, questo $n$ è unico. Osserviamo anche che $x \in \operatorname{Im}(f)$ se e solo se $g(x) \in \operatorname{Im}(f)$.

Verifichiamo che $g$ è totale e iniettiva. Il fatto che sia totale è ovvio. Supponiamo che $g(x) = g(y)$.

- Se $x \notin \operatorname{Im}(f)$, allora $g(x) = x$; dunque non può essere $y \in \operatorname{Im}(f)$ e perciò $g(y) = y$, da cui $x = y$.
- Se $x \in \operatorname{Im}(f)$, è $x = f(n)$ per un unico $n \in \mathbb{N}$. Allora $g(x) = f(n+1) \in \operatorname{Im}(f)$. Perciò $g(y) = g(x) = f(n+1) \in \operatorname{Im}(f)$ e quindi, per quanto osservato prima, $y \in \operatorname{Im}(f)$. Ne segue che $y = f(m)$ per un unico $m \in \mathbb{N}$ e $g(y) = f(m+1)$.

  Abbiamo allora $f(n+1) = f(m+1)$ e, siccome $f$ è iniettiva, $n+1 = m+1$; perciò $n = m$ e $x = f(n) = f(m) = y$.

Qual è l'immagine di $g$? È chiaro che $f(0) \notin \operatorname{Im}(g)$. Viceversa, ogni elemento di $A \setminus \{f(0)\}$ appartiene all'immagine di $g$, cioè $\operatorname{Im}(g) = A \setminus \{f(0)\}$. Se allora consideriamo la funzione $g$ come una funzione $g\colon A \to A \setminus \{f(0)\}$, questa è una biiettività.

In definitiva $|A| = |A \setminus \{f(0)\}|$; se poniamo $B = A \setminus \{f(0)\}$, abbiamo il sottoinsieme cercato. □

Notiamo che, nella dimostrazione precedente, $A \setminus B = \{f(0)\}$ è finito. Come esercizio si trovi in modo analogo al precedente un sottoinsieme $C \subset A$ tale che $|C| = |A|$ e $A \setminus C$ sia infinito.

## 4. Insiemi numerabili

Il teorema secondo il quale per ogni insieme infinito $A$ si ha $|\mathbb{N}| \leq |A|$ ci porta ad attribuire un ruolo speciale a $\mathbb{N}$ (più precisamente alla sua cardinalità).

DEFINIZIONE 4.1. Un insieme $A$ si dice *numerabile* se $|A| = |\mathbb{N}|$.

Un sottoinsieme di $\mathbb{N}$ è allora finito o numerabile. Abbiamo già visto in precedenza che anche $\mathbb{Z}$ (insieme dei numeri interi) è numerabile.

Più in generale possiamo enunciare alcune proprietà degli insiemi numerabili.

TEOREMA 4.2. *Se $A$ è finito e $B$ è numerabile, allora $A \cup B$ è numerabile.*

DIMOSTRAZIONE. Se $A \subseteq B$, l'affermazione è ovvia. Siccome

$$A \cup B = (A \setminus B) \cup B$$

possiamo supporre che $A$ e $B$ siano disgiunti, sostituendo $A$ con $A \setminus B$ che è finito.

Possiamo allora scrivere $A = \{a_0, \dots, a_{m-1}\}$ e considerare una biiettività $g\colon \mathbb{N} \to B$. Definiamo una funzione $f\colon \mathbb{N} \to A \cup B$ ponendo

$$f(n) = \begin{cases} a_n & \text{se } 0 \le n < m, \\ g(n-m) & \text{se } n \ge m. \end{cases}$$

È facile verificare che $f$ è una biiettività. □

TEOREMA 4.3. *Se $A$ e $B$ sono numerabili, allora $A \cup B$ è numerabile.*
*Se $A_1$, $A_2$,..., $A_n$ sono insiemi numerabili, allora $A_1 \cup A_2 \cup \cdots \cup A_n$ è un insieme numerabile.*

DIMOSTRAZIONE. La seconda affermazione segue dalla prima per induzione (esercizio).

Vediamo la prima. Supponiamo dapprima che $A \cap B = \emptyset$. Abbiamo due biiettività $f\colon \mathbb{N} \to A$ e $g\colon \mathbb{N} \to B$. Definiamo una funzione $h\colon \mathbb{N} \to A \cup B$ ponendo:

$$h(n) = \begin{cases} f\left(\dfrac{n}{2}\right) & \text{se } n \text{ è pari}, \\ g\left(\dfrac{n-1}{2}\right) & \text{se } n \text{ è dispari}. \end{cases}$$

Si verifichi che $h$ è una biiettività, ciò che dimostra l'asserzione in questo caso particolare.

In generale, possiamo porre

$$A' = A \setminus (A \cap B), \qquad B' = B \setminus (A \cap B)$$

e abbiamo $A \cup B = A' \cup (A \cap B) \cup B'$; questi tre insiemi sono a due a due disgiunti. I casi possibili sono i seguenti:

(1) $A'$, $A \cap B$ e $B'$ sono infiniti;
(2) $A'$ è finito, $A \cap B$ è infinito, $B'$ è infinito;
(3) $A'$ è finito, $A \cap B$ è infinito, $B'$ è finito;
(4) $A'$ è infinito, $A \cap B$ è infinito, $B'$ è finito;
(5) $A'$ è infinito, $A \cap B$ è finito, $B'$ è infinito;
(6) $A'$ è infinito, $A \cap B$ è finito, $B'$ è finito.

Ci basta applicare quanto appena dimostrato e il teorema precedente, dal momento che i tre insiemi $A'$, $A \cap B$ e $B'$ sono a due a due disgiunti. Si concluda con la dimostrazione per induzione della seconda affermazione. □

Il prossimo teorema può essere sorprendente. Un modo breve per enunciarlo è dire: *L'unione di un insieme numerabile di insiemi numerabili è numerabile.*

TEOREMA 4.4. *Per ogni $n \in \mathbb{N}$, sia $A_n$ un insieme numerabile e supponiamo che, per $m \neq n$, $A_m \cap A_n = \emptyset$. Allora*

$$A = \bigcup \{ A_n \mid n \in \mathbb{N} \}$$

*è numerabile.*

DIMOSTRAZIONE. Per questa dimostrazione ci serve sapere che la successione dei numeri primi $p_0 = 2$, $p_1 = 3$, $p_2 = 5$,..., è infinita.

Sia, per ogni $n \in \mathbb{N}$, $g_n\colon A_n \to \mathbb{N} \setminus \{0\}$ una funzione biiettiva. Se $x \in A$, esiste un unico $n \in \mathbb{N}$ tale che $x \in A_n$; poniamo $j(x) = n$. Definiamo allora

$$f(x) = p_{j(x)}^{g_{j(x)}(x)}.$$

Per esempio, se $x \in A_2$, sarà $f(x) = 5^{g_2(x)}$. La funzione $f\colon A \to \mathbb{N}$ è iniettiva; quindi $|A| \le |\mathbb{N}|$. Ma $A_0 \subseteq A$ e quindi

$$|\mathbb{N}| = |A_0| \le |A| \le |\mathbb{N}|.$$

Per il teorema di Cantor-Schröder-Bernstein, $|A| = |\mathbb{N}|$. □

Il succo della dimostrazione si può riassumere così: possiamo considerare, per ogni numero primo $p_n$, l'insieme

$$X_n = \{p_n, p_n^2, p_n^3, \ldots\}$$

e questi insiemi sono a due a due disgiunti e numerabili. Una volta che consideriamo una funzione biiettiva $f_n\colon A_n \to X_n$, per ogni $n \in \mathbb{N}$, possiamo metterle insieme per ottenere una funzione totale iniettiva $f\colon \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N}$.

Il teorema si può estendere anche al caso in cui gli insiemi $A_n$ non sono a due a due disgiunti. Si provi a delinearne una dimostrazione, usando ancora le funzioni biiettive $f_n\colon A_n \to X_n$ per definire una funzione iniettiva $f\colon \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N}$; l'unico punto complicato è garantire l'univocità.

Questo teorema ha una conseguenza sorprendente.

TEOREMA 4.5. *L'insieme $\mathbb{N}\times\mathbb{N}$ è numerabile.*

DIMOSTRAZIONE. Poniamo $A_n = \{(m,n) \mid m \in \mathbb{N}\}$. Gli insiemi $A_n$ sono a due a due disgiunti e ciascuno è numerabile. È evidente che $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}\times\mathbb{N}$. □

Ancora più sorprendente è forse quest'altro fatto.

TEOREMA 4.6. *L'insieme $\mathbb{Q}$ dei numeri razionali è numerabile.*

DIMOSTRAZIONE. Un numero razionale positivo si scrive in uno e un solo modo come $m/n$, con $m, n \in \mathbb{N}$ primi fra loro (cioè aventi massimo comune divisore uguale a 1). Ne segue che l'insieme $\mathbb{Q}'$ dei numeri razionali positivi è numerabile, perché a $m/n$ (con $m$ e $n$ primi fra loro) possiamo associare la coppia $(m,n) \in \mathbb{N}\times\mathbb{N}$ e la funzione così ottenuta è iniettiva. Dunque

$$|\mathbb{N}| \le |\mathbb{Q}'| \le |\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|.$$

L'insieme $\mathbb{Q}''$ dei numeri razionali negativi è numerabile, perché la funzione $f\colon \mathbb{Q}' \to \mathbb{Q}''$ definita da $f(x) = -x$ è chiaramente biiettiva. Per concludere, possiamo applicare altri teoremi precedenti, tenendo conto che

$$\mathbb{Q} = \mathbb{Q}' \cup \{0\} \cup \mathbb{Q}''.$$ □

C'è un altro modo per convincersi che $\mathbb{Q}'$ è numerabile, illustrato nella figura 1. Si immagina una griglia dove segniamo tutte le coppie con coordinate intere positive. Possiamo percorrere tutta la griglia secondo il percorso indicato e associare in questo modo a ogni numero naturale un numero razionale, incontrandoli tutti. Trascuriamo naturalmente i punti in cui il quoziente fra ascissa e ordinata è un numero razionale già incontrato precedentemente (per esempio, nella prima diagonale si trascura il punto $(2,2)$ che corrisponderebbe al numero razionale $2/2 = 1$, già incontrato come $1/1$; nella terza diagonale si trascurano $(2,4)$, $(3,3)$ e $(4,2)$).

## 5. Esistenza di cardinalità

A questo punto sorge naturale la domanda se ci sono insiemi infiniti di un'infinità diversa da quella dei numeri naturali. Non ci siamo riusciti nemmeno considerando l'insieme dei razionali che, intuitivamente, dovrebbe avere più elementi dei numeri naturali.

C'è una costruzione che produce cardinalità maggiori. Prima però definiamo con precisione ciò che intendiamo.

DEFINIZIONE 5.1. Se $A$ e $B$ sono insiemi, diciamo che *$A$ ha cardinalità minore della cardinalità di $B$*, e scriviamo $|A| < |B|$, se $|A| \le |B|$, ma non è vero che $|A| = |B|$.

Il modo corretto per verificare che $|A| < |B|$ è questo:

- *esiste* una funzione totale iniettiva di $A$ in $B$;
- *non esiste* una biiettività di $A$ su $B$.

Notiamo che non basta verificare che una funzione iniettiva totale di $A$ in $B$ non è suriettiva. Per esempio, esiste certamente una funzione totale iniettiva di $\mathbb{N}$ in $\mathbb{Q}$ che non è suriettiva; tuttavia, come abbiamo visto, $|\mathbb{N}| = |\mathbb{Q}|$. Un altro esempio: l'insieme $\mathbb{N}\cup\{-2\}$ è numerabile, anche se la funzione di inclusione $\mathbb{N} \to \mathbb{N}\cup\{-2\}$ non è suriettiva. Infatti la funzione $f\colon \mathbb{N} \to \mathbb{N}\cup\{-2\}$ definita da $f(0) = -2$ e $f(n) = n-1$ per $n > 0$ è una biiettività.

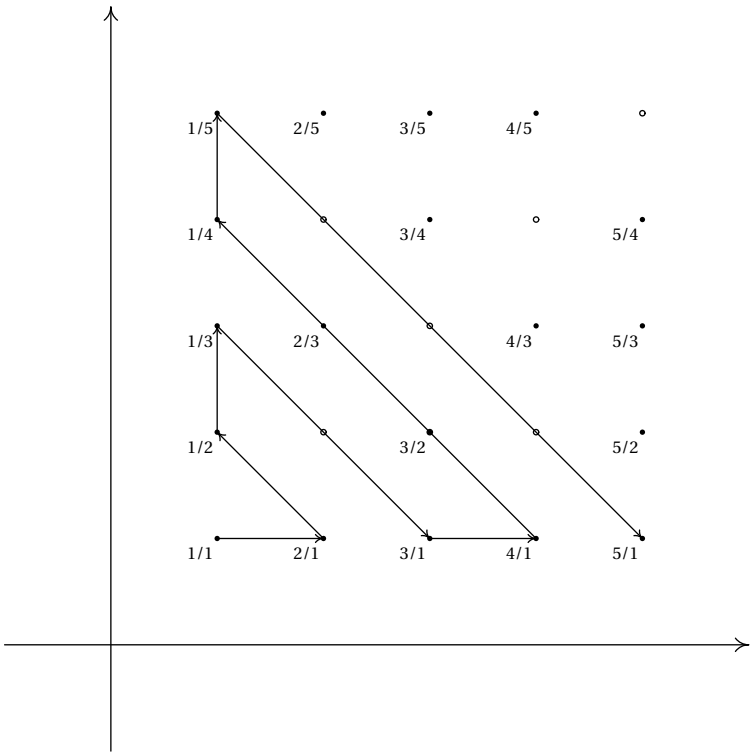


FIGURA 1. Enumerazione dei razionali positivi

L'idea per trovare un insieme di cardinalità maggiore partendo da un insieme $X$ è dovuta a Cantor.

TEOREMA 5.2 (Cantor). *Se $X$ è un insieme, allora $|X| < |P(X)|$.*

DIMOSTRAZIONE. Dimostriamo che esiste una funzione totale iniettiva $X \to P(X)$; essa è, per esempio,

$$\{(x, \{x\}) \mid x \in X\}$$

cioè la funzione che all'elemento $x \in X$ associa il sottoinsieme $\{x\} \in P(X)$.

Dobbiamo ora dimostrare che non esistono funzioni biiettive di $X$ su $P(X)$. Lo faremo per assurdo, supponendo che $g\colon X \to P(X)$ sia biiettiva. Consideriamo

$$C = \{x \in X \mid x \notin g(x)\}.$$

La definizione di $C$ ha senso, perché $g(x)$ è un sottoinsieme di $X$, dunque si hanno sempre due casi: $x \in g(x)$ oppure $x \notin g(x)$.

Siccome, per ipotesi, $g$ è suriettiva, deve esistere un elemento $c \in X$ tale che $C = g(c)$.

Dunque si ha $c \in C$ oppure $c \notin C$.

Supponiamo $c \in C$; allora $c \in g(c)$ e quindi, per definizione di $C$, $c \notin C$: questo è assurdo.

Supponiamo $c \notin C$; allora $c \notin g(c)$ e quindi, per definizione di $C$, $c \in C$: assurdo.

Ne concludiamo che l'ipotesi che $g$ sia suriettiva porta a una contraddizione. Perciò nessuna funzione di $X$ in $P(X)$ è suriettiva. □

## 6. La cardinalità dell'insieme dei numeri reali

Con il teorema di Cantor a disposizione, si può affrontare il problema di determinare la cardinalità dei numeri reali.

Intanto dimostriamo un risultato preliminare; consideriamo l'intervallo aperto

$$I = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

e dimostriamo che $|I| = |\mathbb{R}|$. Consideriamo la funzione $f\colon \mathbb{R} \to \mathbb{R}$,

$$f(x) = \frac{x}{2(\sqrt{1+x^2}+1)} + \frac{1}{2}$$

Un facile studio di funzione mostra che $f$ è iniettiva e che $\mathrm{Im}(f) = I$.

Allo stesso risultato si arriva considerando la funzione

$$g(x) = \frac{1}{2} + \frac{1}{\pi}\arctan x.$$

La considerazione di $I$ ci permetterà di semplificare i ragionamenti.

Sappiamo che ogni numero reale in $I$ si può scrivere come allineamento decimale:

$$\frac{1}{2} = 0{,}500000000000\ldots$$
$$\frac{1}{3} = 0{,}333333333333\ldots$$
$$\frac{1}{7} = 0{,}142857142857\ldots$$
$$\frac{\sqrt{2}}{2} = 0{,}707106781187\ldots$$
$$\frac{\pi}{4} = 0{,}785398163397\ldots$$

dove i puntini indicano altre cifre decimali. Prevedibili in base a uno schema periodico nei primi tre casi, non così negli ultimi due che sono numeri irrazionali.

Il numero dieci non ha nulla di particolare. Si può allo stesso modo sviluppare un numero reale come allineamento binario. Gli stessi numeri, scritti a destra dell'uguale come allineamenti binari, sono:

$$\frac{1}{2} = 0{,}10000000000000000000000000000\ldots$$
$$\frac{1}{3} = 0{,}01010101010101010101010101010\ldots$$
$$\frac{1}{7} = 0{,}00100100100100100100100100100\ldots$$
$$\frac{\sqrt{2}}{2} = 0{,}10110101000001001111001100 1\ldots$$
$$\frac{\pi}{4} = 0{,}11001001000011111101101010 1\ldots$$

e le cifre si ripetono ancora periodicamente nei primi tre casi. La regola della frazione generatrice continua a valere:

$$0{,}\overline{01}_2 = \frac{1_2}{11_2} = \frac{1}{3},$$

(al numeratore il periodo e al denominatore tanti 1, cioè uno meno della base, quante le cifre del periodo).

In generale un numero $r \in I$ si scrive come

$$r = 0{,}r_0 r_1 r_2\ldots,$$

dove $r_i = 0$ oppure $r_i = 1$; in modo unico, se escludiamo tutte le successioni che, da un certo momento in poi, valgono 1. Questo è analogo ai numeri di periodo 9 nel caso decimale.

Dunque abbiamo in modo naturale una funzione $f\colon I \to P(\mathbb{N})$:

$$f(r) = \{\, n \in \mathbb{N} \mid r_n = 1 \,\}$$

dove $r_0, r_1, \ldots$ sono le cifre dello sviluppo binario di $r$.

La funzione $f$ è totale (ovvio) e iniettiva (esercizio), quindi concludiamo che $|I| \le |P(\mathbb{N})|$.

Vogliamo ora definire una funzione $g\colon P(\mathbb{N}) \to I$. Prendiamo $A \in P(\mathbb{N})$; la tentazione sarebbe di definire $g(A)$ come quel numero reale il cui sviluppo binario è

$$0{,}a_0 a_1 \ldots a_n \ldots$$

ponendo

$$a_n = \begin{cases} 0 & \text{se } n \notin A, \\ 1 & \text{se } n \in A. \end{cases}$$

Questo non funziona, perché, se per esempio l'insieme $A$ è $\mathbb{N}$, avremmo, secondo quella regola, $a_n = 1$ per ogni $n \in \mathbb{N}$, ma il numero

$$0{,}111111\ldots = 1 \notin I.$$

Se anche escludessimo questo insieme, avremmo comunque il problema del "periodo 1". Dunque agiamo in un altro modo. All'insieme $A$ associamo il numero reale il cui sviluppo binario è

$$g(A) = 0{,}a_0 a_1 a_2 a_3 \ldots$$

dove

$$a_n = \begin{cases} 0 & \text{se } n \text{ è dispari}, \\ 0 & \text{se } n \text{ è pari e } n/2 \notin A, \\ 1 & \text{se } n \text{ è pari e } n/2 \in A, \end{cases}$$

cioè con la regola precedente, ma intercalando uno zero fra ogni termine. È evidente che, se $A, B \in P(\mathbb{N})$ e $A \neq B$, allora $g(A) \neq g(B)$, dunque $g$ è iniettiva e totale.

Siccome abbiamo definito $f\colon I \to P(\mathbb{N})$ e $g\colon P(\mathbb{N}) \to I$ entrambe totali e iniettive, il teorema di Cantor-Schröder-Bernstein termina la dimostrazione del risultato seguente.

TEOREMA 6.1 (Cantor). $|\mathbb{R}| = |P(\mathbb{N})|$.

Occorre commentare questo risultato. Per dimostrarlo abbiamo usato il teorema di Cantor-Schröder-Bernstein, quindi non abbiamo potuto scrivere esplicitamente una biiettività di $\mathbb{R}$ su $P(\mathbb{N})$. Ma non è questo il punto più importante. La conseguenza più rilevante del teorema è che non è possibile descrivere *ogni* numero reale, perché, come vedremo in seguito, i numeri reali che possono essere espressi con una formula sono un insieme numerabile.

## 7. Il paradiso di Cantor

Un'altra applicazione del teorema di Cantor porta alla costruzione del cosiddetto "paradiso di Cantor". Questa espressione vuole indicare l'esistenza di una successione di cardinalità infinite ciascuna strettamente maggiore della precedente. Allo scopo basta iterare il passaggio all'insieme dei sottinsiemi, per esempio a partire dall'insieme dei numeri naturali, per ottenere una successione di insiemi la cui cardinalità, per il teorema di Cantor, continua a crescere strettamente:

$$|\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < |P(P(P(\mathbb{N})))| < \cdots < |P(\cdots P(P(P(\mathbb{N})))\cdots)| < \cdots$$

Si potrebbe ancora andare avanti; definiamo, per induzione,

$$P^0(X) = X, \qquad P^{n+1}(X) = P(P^n(X)).$$

Allora possiamo considerare l'insieme

$$Y_1 = \bigcup_{n \in \mathbb{N}} P^n(\mathbb{N}),$$

e si può dimostrare che $|P^n(\mathbb{N})| < |Y_1|$, per ogni $n \in \mathbb{N}$. Dunque abbiamo trovato una cardinalità ancora maggiore di tutte quelle trovate in precedenza e il gioco può continuare: consideriamo

$$Y_2 = \bigcup_{n \in \mathbb{N}} P^n(Y_1)$$

e ancora $|P^n(Y_1)| < |Y_2|$. E così via, costruendo una gerarchia infinita di cardinalità sempre maggiori.

Oltre a interrogarci sul prolungarsi della successione delle cardinalità infinite sempre maggiori, è del tutto naturale domandarsi se tra $|\mathbb{N}|$ e $|P(\mathbb{N})|$ c'è o no una cardinalità strettamente compresa tra le due. Più in generale, ci si può chiedere se, dato un insieme infinito $X$, esiste un insieme $Y$ tale che $|X| < |Y| < |P(X)|$.

Cantor ipotizzò che non ci siano insiemi $Z$ tali che $|\mathbb{N}| < |Z| < |P(\mathbb{N})|$, e questa ipotesi ha preso il nome di *ipotesi del continuo*. Non è questo il luogo dove discutere questa questione, risolta brillantemente da P. J. Cohen nel 1963: *l'ipotesi del continuo è indecidibile* rispetto agli assiomi della teoria degli insiemi, nel senso che è altrettanto coerente prenderla come vera che prenderla come falsa. Non si tratta di argomenti semplici, tanto che per i suoi studi Cohen fu insignito della *Fields Medal* che, per i matematici, è l'analogo del Premio Nobel.

## ESERCIZI

Si ricordi che $k\mathbb{N}$ indica l'insieme dei numeri naturali multipli di $k$, $\mathbb{N}_{\geq k}$ l'insieme dei numeri naturali maggiori o uguali a $k$, e $\mathbb{N}_{>k}$ l'insieme dei numeri naturali strettamente maggiori di $k$.

ESERCIZIO 4.1. Si dica, motivando la risposta, se gli insiemi $3\mathbb{N} \cup \{2,5\}$ e $2\mathbb{N} \setminus \{10,8\}$ hanno la stessa cardinalità.

ESERCIZIO 4.2. Si costruisca una funzione biiettiva tra gli insiemi $4\mathbb{N} \cup \{\frac{3}{2}, 7, \sqrt{2}\}$ e $\mathbb{N}_{>9}$.

ESERCIZIO 4.3. Si dimostri che per ogni insieme finito $X$, se $f\colon X \to X$ è totale e iniettiva, allora è biiettiva. Si dia un esempio di un insieme infinito in cui l'analoga proprietà non sussiste.

ESERCIZIO 4.4. Si dimostri che per ogni insieme finito $X$, se $f\colon X \to X$ è totale e suriettiva, allora è biiettiva. Si dia un esempio di un insieme infinito in cui l'analoga proprietà non sussiste.

ESERCIZIO 4.5. Si costruisca una funzione biiettiva tra gli insiemi $\mathbb{Z} \cup \{\frac{3}{2}, \sqrt[3]{2}\}$ e $3\mathbb{N}$.

ESERCIZIO 4.6. Si dica, motivando la risposta, se gli insiemi $(5\mathbb{N} \setminus \{5,15\}) \cup \{\sqrt{3}, \frac{5}{2}\}$ e $2\mathbb{N} \cup \{11,17\}$ hanno la stessa cardinalità.

ESERCIZIO 4.7. Si dica, motivando la risposta, se gli insiemi $\mathbb{N}_{\geq 50} \cup 5\mathbb{N}$ e $3\mathbb{N} \cap 2\mathbb{N}$ hanno la stessa cardinalità.

ESERCIZIO 4.8. Sia $A$ un insieme numerabile e sia $a \notin A$. Si costruisca una biiezione tra gli insiemi $A$ e $A \cup \{a\}$.

ESERCIZIO 4.9. Sia $A$ un insieme numerabile e sia $a \in A$. Si costruisca una biiezione tra gli insiemi $A$ e $A \setminus \{a\}$.

ESERCIZIO 4.10. Sia $\Pi$ l'insieme dei numeri reali irrazionali. L'insieme $\Pi$ è numerabile?

ESERCIZIO 4.11. L'insieme di tutte le funzioni da $\mathbb{Q}$ all'insieme $\{0,1,2,3\}$ è numerabile?

ESERCIZIO 4.12. Sia $P = \{I \mid I \subseteq \mathbb{N} \text{ e } I \text{ è un insieme finito}\}$ l'insieme delle *parti finite* di $\mathbb{N}$. Qual è la cardinalità di $P$?

ESERCIZIO 4.13. Si dica, motivando la risposta, se l'insieme $P(3\mathbb{N})$ è numerabile.

CAPITOLO 5

# Induzione e numeri naturali

## 1. Il principio di induzione

Il principio di induzione è una tecnica di dimostrazione molto usata in matematica. Lo scopo di questa sezione è di enunciare tale principio e di mostrare con vari esempi come esso possa essere applicato.

PRINCIPIO DI INDUZIONE 1.1. *Sia $\{\mathscr{P}(i)\}_{i\in\mathbb{N}}$ un insieme di proposizioni tali che:*

(1) *$\mathscr{P}(0)$ è vera;*
(2) *per ogni $n\in\mathbb{N}$, se $\mathscr{P}(n)$ è vera, allora $\mathscr{P}(n+1)$ è vera.*

*Allora $\mathscr{P}(i)$ è vera per ogni $i\in\mathbb{N}$.*

Il principio di induzione afferma che per dimostrare la veridicità di una data proprietà per ogni numero naturale, è sufficiente verificare: (1) che essa è vera in zero; (2) che se si suppone essere vera per un numero naturale arbitrario $n$, allora essa è vera anche per il naturale successivo $n+1$. La prima verifica viene detta *passo base* dell'induzione, la seconda *passo induttivo*.

ESEMPIO 1.2. *Si dimostri che ogni insieme con $i$ elementi ha $2^i$ sottoinsiemi.*

Possiamo considerare l'affermazione come un insieme di proposizioni $\{\mathscr{P}(i)\}_{i\in\mathbb{N}}$; per poter applicare il principio di induzione dobbiamo verificare i due punti seguenti:

(1) $\mathscr{P}(0)$ è vera, cioè ogni insieme con 0 elementi ha $2^0$ sottoinsiemi; questo è chiaro, dato che l'unico sottoinsieme di $\emptyset$ è $\emptyset$.
(2) se $\mathscr{P}(n)$ è vera, allora $\mathscr{P}(n+1)$ è vera. Questo punto si traduce nella seguente verifica: supponiamo di sapere che ogni insieme con $n$ elementi ha $2^n$ sottoinsiemi e verifichiamo che ogni insieme con $n+1$ elementi ha $2^{n+1}$ sottoinsiemi. A tal fine, sia $X$ un insieme con $n+1$ elementi, e sia $a\in X$; allora $X = X'\cup\{a\}$, dove $X'$ è un insieme di $n$ elementi e $a\notin X'$. Osserviamo che, dato un generico sottoinsieme $Y\subseteq X$, o $a\in Y$ oppure $a\notin Y$; nel primo caso $Y\subseteq X'$, nel secondo caso è $Y = Y'\cup\{a\}$, dove $Y'\subseteq X'$. Poiché si sta supponendo che i possibili sottoinsiemi di $X'$ siano $2^n$, i sottoinsiemi di $X$ sono $2^n+2^n = 2^{n+1}$.

Avendo verificato i punti (1) e (2), in base al principio di induzione possiamo concludere che $\mathscr{P}(i)$ è vera per ogni $i\in\mathbb{N}$, cioè che ogni insieme con $i$ elementi ha $2^i$ sottoinsiemi, per ogni $i\in\mathbb{N}$.

ESEMPIO 1.3. *Si dimostri che, per ogni $i\in\mathbb{N}$, la somma dei primi $i$ numeri naturali pari è $i^2+i$.*

Dobbiamo dimostrare che per ogni $i\in\mathbb{N}$ vale la seguente formula:

$$\sum_{k=0}^{i} 2k = i^2+i.$$

In base al principio di induzione è sufficiente verificare i due punti seguenti:

(1) $\sum_{k=0}^{0} 2k = 0^2+0$, uguaglianza chiaramente vera;
(2) supponendo $\sum_{k=0}^{n} 2k = n^2+n$, allora $\sum_{k=0}^{n+1} 2k = (n+1)^2+n+1$; per verificare questa uguaglianza, osserviamo che

$$\sum_{k=0}^{n+1} 2k = \sum_{k=0}^{n} 2k + 2(n+1).$$

Quindi, dall'ipotesi segue che

$$\sum_{k=0}^{n+1} 2k = n^2 + n + 2(n+1) = (n+1)^2 + (n+1).$$

Avendo verificato sia il passo base che il passo induttivo, possiamo concludere che la formula $\sum_{k=0}^{i} 2k = i^2 + i$ vale per ogni $i \in \mathbb{N}$.

ESEMPIO 1.4. *Si dimostri che* $(1+x)^n \geq 1 + nx$ *per ogni* $n \in \mathbb{N}$ *e per ogni* $x \in \mathbb{R}$ *con* $x > -1$.

Dimostriamo l'enunciato per induzione su $n$. Poiché $(1+x)^0 = 1$, il passo base è facilmente verificato. Supponendo che $(1+x)^n \geq 1 + nx$, si ha

$$(1+x)^{(n+1)} = (1+x)(1+x)^n \geq (1+x)(1+nx) = 1 + nx + x + nx^2 = 1 + (n+1)x + nx^2.$$

Poiché $nx^2 \geq 0$, $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$. Si conclude quindi $(1+x)^{(n+1)} \geq 1 + (n+1)x$; pertanto abbiamo verificato anche il passo induttivo.

Una variante del principio di induzione permette di considerare come passo base un naturale qualsiasi.

VARIANTE DEL PRINCIPIO DI INDUZIONE 1.5. *Sia* $\{\mathscr{P}(i)\}_{i\in\mathbb{N}}$ *un insieme di proposizioni e sia* $l \in \mathbb{N}$ *tali che:*

(1) $\mathscr{P}(l)$ *è vera;*
(2) *se* $\mathscr{P}(n)$ *è vera per ogni* $n \geq l$*, allora* $\mathscr{P}(n+1)$ *è vera.*

*Allora* $\mathscr{P}(i)$ *è vera per ogni* $i \geq l$.

ESEMPIO 1.6. *Si dimostri che per ogni* $i \geq 1$*, vale la seguente formula:*

$$\sum_{k=1}^{i} k \cdot k! = (i+1)! - 1.$$

Poiché si deve dimostrare la veridicità della formula per $i \geq 1$, si applica la variante del principio di induzione considerando come passo base $l = 1$. Pertanto si deve verificare:

(1) $\sum_{k=1}^{1} 1 \cdot 1! = (2)! - 1$, uguaglianza chiaramente vera;
(2) se $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$, allora $\sum_{k=1}^{n+1} k \cdot k! = (n+2)! - 1$. Poiché $\sum_{k=1}^{n+1} k \cdot k! = \sum_{k=1}^{n} k \cdot k! + (n+1) \cdot (n+1)!$, per ipotesi induttiva segue $\sum_{k=1}^{n+1} k \cdot k! = (n+1)! - 1 + (n+1) \cdot (n+1)! = (n+1)!(n+2) - 1$.

Si noti che il principio di induzione, se applicato erroneamente, può portare a conclusioni assurde, come mostra il seguente esempio.

ESEMPIO 1.7. *Per ogni* $k \in \mathbb{N}$*,* $k \geq 2$*, dati* $k$ *punti del piano, essi sono allineati.*

Per applicare il principio di induzione, verifichiamo innanzitutto il passo base, partendo da $k = 2$: dati due punti del piano, esso sono certamente allineati. Verifichiamo ora il passo induttivo: supponiamo che dati $n$ punti essi siano allineati, e concludiamo che anche $n+1$ punti sono allineati. A tal fine, siano dati $n+1$ punti del piano $\{X_1, \ldots, X_n, X_{n+1}\}$. Per ipotesi induttiva, esiste una retta $r$ che passa per i punti $X_1, \ldots, X_n$; inoltre esiste una retta $t$ che passa per i punti $X_2, \ldots, X_{n+1}$. Pertanto l'intersezione tra le rette $r$ e $t$ contiene i punti $X_2, \ldots, X_n$. Osserviamo che, date due rette del piano, o la loro intersezione è vuota, o consiste di un unico punto, oppure le due rette sono coincidenti. Nel nostro caso $\{X_2, \ldots, X_n\} \subseteq r \cap t$, e quindi concludiamo che $r = t$; da ciò segue che gli $n+1$ punti sono allineati. In base al principio di induzione possiamo pertanto concludere che dati $k$ punti del piano, essi sono allineati.

Poiché l'affermazione dimostrata è chiaramente assurda, abbiamo commesso un errore nell'applicare il principio di induzione. L'errore consiste nella verifica del passo induttivo: per esempio, mentre è ovviamente vero che due punti del piano sono sempre allineati, non è vero che lo sono anche tre punti. Per esercizio lo studente individui l'errore commesso.

Concludiamo questa sezione osservando come l'argomento che sta alla base del principio di induzione può essere applicato non solo per dimostrare proprietà, ma anche per dare definizioni. Si consideri per esempio la definizione di potenza con esponente naturale di una data

base $a \in \mathbb{R}$. Tale definizione si può enunciare nel modo seguente: $a^0 = 1$ e $a^{n+1} = a \cdot a^n$, per ogni $n \in \mathbb{N}$; in altre parole, si costruisce $a^0$ e poi, supponendo di conoscere $a^n$, si costruisce $a^{n+1}$. In tal modo si costruisce qualsiasi potenza naturale di $a$. Queste definizioni si dicono *definizioni per ricorrenza.*

ESEMPIO 1.8. Si definisca $0! = 1$ e, per ogni $n \in \mathbb{N}$, sia $(n+1)! = (n+1)n!$. In questo modo si definisce per ricorrenza il prodotto fattoriale $n!$ per ogni $n \in \mathbb{N}$.

Dunque avremo $1! = 1 \cdot 0! = 1$, $2! = 2 \cdot 1! = 2$, $3! = 3 \cdot 2! = 6$ e così via.

## 2. Il principio di induzione: dimostrazione

Nel sezione precedente abbiamo visto come si enuncia e come si applica il principio di induzione. In questa sezione vogliamo invece capire *perché* vale tale principio. La dimostrazione della validità del principio di induzione si basa essenzialmente sulla proprietà di buon ordinamento dei numeri naturali, sul fatto cioè che ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette elemento minimo (vedi Esempio 4.6, Capitolo 2).

TEOREMA 2.1. *Sia $\{\mathscr{P}(i)\}_{i\in\mathbb{N}}$ un insieme di proposizioni tali che:*

(1) *$\mathscr{P}(0)$ è vera;*
(2) *se $\mathscr{P}(n)$ è vera, allora $\mathscr{P}(n+1)$ è vera.*

*Allora $\mathscr{P}(i)$ è vera per ogni $i \in \mathbb{N}$.*

DIMOSTRAZIONE. Sia $M = \{m \in \mathbb{N} \mid \mathscr{P}(m) \text{ è falsa}\}$. Supponiamo che l'insieme $M$ sia non vuoto; allora $M$, in quanto sottoinsieme dei numeri naturali, ammette elemento minimo $\overline{m}$. Dal punto (1) segue che $\overline{m} \neq 0$, e pertanto $\overline{m} \geq 1$. Inoltre, poiché $\overline{m} - 1 \notin M$, la proposizione $\mathscr{P}(\overline{m}-1)$ è vera; dal punto (2) segue pertanto che $\mathscr{P}(\overline{m})$ è vera, contrariamente all'ipotesi $\overline{m} \in M$. □

Dal buon ordinamento di $\mathbb{N}$, segue anche un'utile variante del principio di induzione.

TEOREMA 2.2 (Seconda forma del principio di induzione). *Sia $\{\mathscr{P}(i)\}_{i\in\mathbb{N}}$ un insieme di proposizioni e sia $l \in \mathbb{N}$ tali che:*

(1) *$\mathscr{P}(l)$ è vera;*
(2) *se $\mathscr{P}(k)$ è vera per ogni $l \leq k < n$ , allora $\mathscr{P}(n)$ è vera.*

*Allora $\mathscr{P}(i)$ è vera per ogni $i \geq l$.*

DIMOSTRAZIONE. Sia $M = \{m \in \mathbb{N} \mid m \geq l \text{ e } \mathscr{P}(m) \text{ è falsa}\}$. Supponiamo che l'insieme $M$ sia non vuoto; allora $M$, in quanto sottoinsieme dei numeri naturali, ammette elemento minimo $\overline{m}$. Dal punto (1) segue che $\overline{m} > l$; inoltre, per la minimalità di $\overline{m}$, le proposizioni $\mathscr{P}(l)$, $\mathscr{P}(l+1)$,..., $\mathscr{P}(\overline{m}-1)$ sono vere; dal punto (2) segue pertanto che $\mathscr{P}(\overline{m})$ è vera, contrariamente all'ipotesi $\overline{m} \in M$. □

ESEMPIO 2.3. *Si dimostri che ogni numero naturale maggiore o uguale a 2 o è primo o è prodotto di primi.*

Dimostriamo l'enunciato applicando la seconda forma del principio di induzione, assumendo come passo base $n = 2$.

(1) Passo base: per $n = 2$ l'enunciato è vero, dato che 2 è primo.

(2) Passo induttivo: sia $n > 2$ e supponiamo che per ogni $2 \leq k < n$, $k$ è primo o è prodotto di primi; dobbiamo concludere che $n$ è primo o prodotto di primi. Se $n$ è primo, allora si conclude. Se $n$ non è primo, allora esistono due numeri naturali $r$ e $s$ tali che $r < n$, $s < n$ e $n = rs$. Per ipotesi induttiva, $r$ e $s$ o sono primi o sono prodotto di numeri primi; pertanto $n$ è prodotto di numeri primi.

## 3. I numeri naturali

Nel dimostrare il principio di induzione a partire dal buon ordinamento di $\mathbb{N}$, si è assunta nota la struttura e la costruzione dell'insieme dei numeri naturali. È tuttavia importante cercare di dare una definizione formale di $\mathbb{N}$, da cui derivino tutte le proprietà comunemente note di tale insieme. Concludiamo questo capitolo con un cenno all'approccio assiomatico a tale problema introdotto da Peano.

ASSIOMI DI PEANO. Sia $(\mathcal{N}, 0, s)$ una terna dove $\mathcal{N}$ è un insieme, 0 un elemento di $\mathcal{N}$ e $s\colon \mathcal{N} \to \mathcal{N}$ una funzione, tali che valgano le seguenti proprietà:

P1. la funzione $s$ è iniettiva;
P2. l'elemento 0 non appartiene all'immagine di $s$;
P3. Se $\mathcal{M} \subseteq \mathcal{N}$ ha la proprietà che $0 \in \mathcal{M}$ e $s(x) \in \mathcal{M}$ per ogni $x \in \mathcal{M}$, allora $\mathcal{M} = \mathcal{N}$.

Si dimostra che la terna $(\mathcal{N}, 0, s)$ costruita con le proprietà P1, P2 e P3 è essenzialmente unica, nel senso che se $(\mathcal{N}', 0', s')$ è un'altra terna soddisfacente le stesse proprietà, allora esiste una funzione biiettiva $\varphi\colon \mathcal{N} \to \mathcal{N}'$ tale che $\varphi(s(x)) = s'(\varphi(x))$ per ogni $x \in \mathcal{N}$. Una volta dimostrata l'unicità della terna $(\mathcal{N}, 0, s)$, definiamo l'insieme dei numeri naturali come l'insieme $\mathcal{N}$. Si osservi che, per ogni $x \in \mathcal{N}$, il ruolo di $s(x)$ è quello del "successore" di $x$, cioè del numero naturale $x+1$.

A partire da questa definizione assiomatica dell'insieme dei numeri naturali, possiamo dare una definizione rigorosa delle usuali operazioni di addizione e moltiplicazione. Si consideri infatti la funzione $F\colon \mathcal{N} \times \mathcal{N} \to \mathcal{N}$ tale che $F(x,0) = x$ e $F(x, s(y)) = s(F(x,y))$ per ogni $x, y \in \mathcal{N}$. Si può dimostrare che tale funzione esiste ed è unica; poiché $F$ corrisponde all'usuale addizione, si denota comunemente con $+$. Analogamente si consideri la funzione $G\colon \mathcal{N} \times \mathcal{N} \to \mathcal{N}$ tale che $G(x,0) = 0$ e $G(x, s(y)) = G(x,y) + x$. Si può dimostrare che tale funzione esiste ed è unica: poiché $G$ corrisponde all'usuale moltiplicazione, si denota comunemente con $\times$. Applicando gli assiomi $P1$, $P2$ e $P3$ si dimostra che le operazioni $+$ e $\times$ godono di ben note proprietà, come ad esempio la proprietà commutativa, associativa o distributiva. A titolo di esempio, dimostriamo esplicitamente come l'operazione $+$ sia associativa.

PROPOSIZIONE 3.1. *Per ogni $a, b, c \in \mathcal{N}$, $F(a, F(b,c)) = F(F(a,b), c)$.*

DIMOSTRAZIONE. Siano $a$ e $b$ due arbitrari elementi di $\mathcal{N}$, e si consideri l'insieme $\mathcal{M} = \{c \in \mathcal{N} \mid F(a, F(b,c)) = F(F(a,b),c)\}$. Vogliamo dimostrare che $\mathcal{M} = \mathcal{N}$. A tal fine, in base all'assioma $P3$, basta verificare che $0 \in \mathcal{M}$ e che $s(x) \in \mathcal{M}$ per ogni $x \in \mathcal{M}$. Il fatto che $0 \in \mathcal{M}$ segue dalla prima proprietà di $F$, dato che $F(a, F(b,0)) = F(a,b) = F(F(a,b),0)$. Sia quindi $c \in \mathcal{M}$; dobbiamo verificare l'uguaglianza $F(a, F(b, s(c))) = F(F(a,b), s(c))$. Dalla seconda proprietà di $F$ segue $F(a, F(b, s(c))) = F(a, s(F(b,c)) = s(F(a, F(b,c))$; inoltre, poiché $c \in \mathcal{M}$, si ha $s(F(a, F(b,c)) = s(F(F(a,b),c) = F(F(a,b), s(c))$. Si conclude pertanto $F(a, F(b, s(c))) = F(F(a,b), s(c))$, cioè $s(c) \in \mathcal{M}$. □

Dopo aver introdotto l'operazione $+$, possiamo definire in modo rigoroso anche l'usuale relazione d'ordine $<$, procedendo nel modo seguente. Sia $R = \{(x,y) \mid x, y \in \mathcal{N}$ ed esiste $k \in \mathcal{N}, k \neq 0$, tale che $y = x + k\}$; si dimostra che $R$ è una relazione d'ordine stretto su $\mathcal{N}$. Applicando gli assiomi P1, P2 e P3, si dimostra che $R$ gode delle ben note proprietà di $<$, come ad esempio la tricotomia o il buon ordinamento.

OSSERVAZIONE 3.2. Si osservi che l'assioma $P3$ è equivalente al principio di induzione; in altre parole nell'approccio assiomatico di Peano il principio di induzione è implicitamente assunto come assioma, da cui segue anche il buon ordinamento di $\mathbb{N}$. Si noti la differenza tra questo approccio e quello seguito nella sezione 2, dove il principio di induzione è stato ottenuto come conseguenza del principio del minimo.

## ESERCIZI

ESERCIZIO 5.1. Si dimostri che $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

ESERCIZIO 5.2. Si dimostri che, per ogni $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{2^i} = \frac{2^n - 1}{2^n}$

ESERCIZIO 5.3. Ricordando che $\mathrm{D}(fg) = \mathrm{D}(f)g + f\,\mathrm{D}(g)$ e che $\mathrm{D}(x) = 1$, si dimostri che $\mathrm{D}(x^n) = nx^{n-1}$.

ESERCIZIO 5.4. Si dimostri che, per ogni $n \geq 1$, $2^3 + 4^3 + \cdots + (2n)^3 = 2n^2(n+1)^2$.

ESERCIZIO 5.5. Si dimostri che, per ogni $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \frac{1}{6} n(n+1)(2n+1).$$

ESERCIZIO 5.6. Si dimostri per induzione che $n! > n2^n$ per $n > 5$.

ESERCIZIO 5.7. Si dimostri che, per ogni $n > 3$, $n! > 2^n + n$

ESERCIZIO 5.8. Si dimostri per induzione che per ogni intero $n \geq 1$ risulta

$$\sum_{i=1}^{n} i\left(i + \frac{1}{3}\right) = \frac{n(n+1)^2}{3}.$$

ESERCIZIO 5.9. Si dimostri per induzione che, per ogni $a, b, c \in \mathbb{N}$, $a \times (b+c) = (a \times b) + (a \times c)$. (Si supponga di aver già dimostrato la proprietà associativa della somma.)

CAPITOLO 6

# Elementi di logica

## 1. L'esigenza di studiare un linguaggio formale

La matematica ha bisogno di un modo di esprimersi che eviti le ambiguità linguistiche. Consideriamo qualche esempio.

- *Questa frase è falsa* è una frase vera o falsa?
- *Ogni cempo è fristo; un dunco è un cempo; quindi un dunco è fristo.*
- *Mus syllaba est. Mus autem caseum rodit. Ergo syllaba caseum rodit.*
- *Mus syllaba est. Syllaba autem caseum non rodit. Ergo mus caseum non rodit.*
- Ogni insieme non vuoto di numeri naturali ha minimo. È evidente che esiste almeno un numero naturale che non sia definibile con meno di venti parole. *Sia n il minimo numero naturale non definibile con meno di venti parole.* Abbiamo appena definito questo numero $n$ con meno di venti parole.

Il primo esempio è noto come *paradosso del mentitore* e ha una storia lunghissima.

Il secondo esempio è un *sillogismo*. Nella sua struttura questo è simile al famoso *Ogni uomo è mortale; Socrate è un uomo; dunque Socrate è mortale* che riconosciamo come vero. Ma che dire del nostro esempio?

Anche il terzo e quarto esempio sono sillogismi. Occorre dirli in latino (è una citazione da Seneca, *Lettere a Lucilio*); 'mus' è 'topo', 'syllaba' è 'sillaba', 'caseum' è 'formaggio', 'rodit' è 'rosicchia'; 'autem' e 'ergo' sono avverbi irrilevanti che si possono tradurre 'del resto' e 'dunque'. È facile confutare il terzo, perché da un'affermazione particolare si deduce una conclusione generale, come in *Ogni uomo è bipede; una gallina è bipede; dunque una gallina è un uomo*. Il quarto esempio invece non è così facilmente confutabile: dove sta il problema?

Il quinto esempio è noto come *paradosso di Richard*. Lo possiamo confutare osservando che non è per niente chiaro che cosa significhi 'definibile' né che cosa sia 'parola'. Sono note le seguenti 'parole' pronunciate dall'americano alla corte di re Artù nel famoso romanzo di Mark Twain:

> Constantinopolitanischerdudelsackspfeifenmachersgesellschafft
>
> Nihilistendynamittheaterkästchensprengungsattentatversuchungen
>
> Transvaaltruppentropentransporttrampelthiertreibertrauungsthränentragödie
>
> Mekkamuselmannenmassenmenschenmördermohrenmuttermarmormonumentenmacher

che non significano nulla, ma sono costruite secondo le regole della lingua tedesca e apparentemente sono una sola parola. In tedesco è comune creare parole uniche componendone altre. Che cos'è una parola? In quale lingua la dobbiamo interpretare? Se in un contesto inglese leggiamo la parola 'dice', non la interpretiamo certo come verbo, perché significa 'dadi'; ma se la vedessimo priva di contesto, come dovremmo interpretarla? Come verbo italiano o come sostantivo inglese? O forse in un'altra lingua ancora?

Come possiamo allora evitare le ambiguità? Come possiamo essere certi che un'affermazione matematica o una dimostrazione siano corrette?

Facciamo altri esempi. Se consideriamo l'equazione $4x^2 = 9$, quante soluzioni ha? La domanda è mal posta, sebbene siamo abituati a domande del genere.

L'equazione non ha soluzioni nell'insieme dei numeri interi, ma ne ha due nell'insieme dei numeri razionali. La domanda, di per sé, è ambigua. Torneremo su questo problema.

Un altro campo nel quale il problema del linguaggio è molto rilevante è quello dell'informatica. Non possiamo certo 'parlare' a un calcolatore usando il linguaggio naturale, ma solo con linguaggi codificati e precisi. Il linguaggio naturale è ambiguo, non esisterebbe la poesia, altrimenti. Invece per scrivere un programma da inserire in un calcolatore dobbiamo precisare le istruzioni in modo che abbiano un significato univoco.

## 2. Strutture

Cercheremo dunque di costruire un linguaggio artificiale che sia adatto a discutere le questioni matematiche. Un tale linguaggio avrà le sue espressioni, che saranno successioni finite di simboli precedentemente introdotti. Dovrà anche essere possibile riconoscere in modo effettivo quali espressioni abbiano significato e quali no.

Un tale linguaggio formale sarà usato per descrivere una certa situazione matematica, per esempio i numeri naturali.

DEFINIZIONE 2.1. Una *struttura* $\mathfrak{A}$ consiste di

- un insieme non vuoto $A$, detto *universo* della struttura;
- un insieme non vuoto di relazioni su $A$;
- un insieme di funzioni su $A$;
- un insieme di elementi di $A$ che saranno chiamati *costanti*.

Chiariamo subito che le relazioni che consideriamo non sono necessariamente binarie, ma possono essere anche ternarie, quaternarie, eccetera. Una relazione $n$-aria su $A$ è un sottoinsieme di $A^n = A \times A \times \cdots \times A$ ($n$ volte).

Anche le funzioni su $A$ possono essere unarie, binarie, eccetera. Una funzione $n$-aria su $A$ è una funzione totale di $A^n$ in $A$, cioè

$$\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}} \to A$$

Per evitare altri dubbi, chiariamo che tutte le funzioni considerate in queste note saranno *totali*.

Come esempio, che ci guiderà in tutta la trattazione, considereremo la struttura dei numeri naturali $\mathfrak{N}$ dove

- l'universo è l'insieme $\mathbb{N}$ dei numeri naturali;
- le relazioni che consideriamo sono l'identità (binaria) e l'essere minore (binaria);
- le funzioni che consideriamo sono l'addizione (binaria), la moltiplicazione (binaria) e il successore (unaria);
- le costanti che consideriamo sono il numero zero e il numero uno.

L'altro esempio che considereremo sarà quello della geometria del piano $\mathfrak{P}$ dove

- l'universo è l'insieme $P$ dei punti e delle rette del piano;
- le relazioni che consideriamo sono l'identità (binaria), essere un punto (unaria), essere una retta (unaria), appartenere (binaria)
- non consideriamo funzioni;
- non consideriamo costanti.

Si potrebbe economizzare nella descrizione di ciò che costituisce una struttura, perché una funzione è una particolare relazione e un elemento è una particolare funzione; tuttavia non si guadagna in chiarezza economizzando così e quindi non lo faremo.

## 3. Il linguaggio

Data una struttura $\mathfrak{A}$, vogliamo un linguaggio adatto a descriverla. Introdurremo i simboli un po' alla volta, intanto uno per ciascun costituente specifico della struttura:

- un *simbolo di relazione* (o *predicato*) per ogni relazione;
- un *simbolo di funzione* per ogni funzione;
- un *simbolo di costante* per ogni costante.

Di ogni simbolo di relazione o funzione si sa che si riferisce a una relazione o funzione $n$-aria.

Per esempio, il linguaggio adatto alla struttura dei numeri naturali $\mathfrak{N}$ avrà i seguenti simboli:

- $=$ per l'identità;
- $<$ per 'essere minore';
- $+$ per l'addizione;
- $\times$ per la moltiplicazione;
- $\mathbf{s}$ per la funzione successore;
- $\mathbf{0}$ per il numero zero;
- $\mathbf{1}$ per il numero uno.

Un linguaggio può essere adatto a più strutture. Per esempio, considereremo anche la struttura $\mathfrak{R}$ dei numeri reali in cui prenderemo la relazione di identità, quella di 'essere minore', l'addizione, la moltiplicazione, la funzione 'aggiungere uno', il numero zero e il numero uno nell'insieme dei numeri reali $\mathbb{R}$. O anche la struttura $\mathfrak{Z}$ dei numeri interi, con analoghi costituenti. Va notato che la relazione di 'essere minore' nei numeri reali o nei numeri naturali sono diverse e così per tutti gli altri costituenti.

DEFINIZIONE 3.1. Sia $\mathfrak{A}$ una struttura e $\mathscr{L}$ un linguaggio adatto a essa. L'interpretazione di un simbolo di relazione, funzione o costante $\mathbf{S}$ è $\mathbf{S}^{\mathfrak{A}}$, la relazione, funzione o costante a esso associata.

Per esempio, $+^{\mathfrak{N}}$ è la funzione binaria addizione nei numeri naturali, $\mathbf{0}^{\mathfrak{N}}$ è il numero naturale zero.

## 4. Termini e loro interpretazione

Cominciamo a introdurre alcune espressioni del linguaggio. I termini saranno espressioni che intuitivamente indicano un elemento dell'universo; più precisamente sono 'nomi' per tali elementi. Ricordiamo che un'espressione del linguaggio è una successione finita di simboli del linguaggio.

DEFINIZIONE 4.1 (provvisoria). Un *termine* è una successione finita di simboli del linguaggio costruita mediante le seguenti regole:

(T1) ogni simbolo di costante è un termine;
(T2) se $t_1, t_2, \ldots, t_n$ sono termini e $\mathbf{f}$ è un simbolo di funzione $n$-aria, allora $\mathbf{f}\,t_1\,t_2\ldots t_n$ è un termine.

Una definizione del genere richiede parecchi commenti. Apparentemente, infatti, il concetto di termine è definito mediante sé stesso, in un circolo vizioso. Non è così, naturalmente. La definizione va letta come una procedura per stabilire se una certa successione di simboli è un termine oppure no. Un altro aspetto da tenere presente: con $t_i$ rappresentiamo un'intera successione di simboli, non necessariamente un solo simbolo.

Vediamo allora qual è la procedura da seguire. Un solo simbolo è un termine se e solo se è un simbolo di costante. Una successione di più di un simbolo è un termine se e solo se:

- il primo simbolo (da sinistra) è un simbolo di funzione;
- cancellando questo simbolo, ciò che resta è una successione di $n$ termini (quando il simbolo è di funzione $n$-aria).

ESEMPIO 4.2. Nel linguaggio dei numeri naturali, le seguenti espressioni sono termini:

$$\mathbf{0}\quad \mathbf{1}\quad +\mathbf{01}\quad \times\mathbf{11}\quad +\,+\mathbf{111}\quad \times\,+\mathbf{11}+\mathbf{01}$$

Siamo in realtà più abituati a scrivere queste espressioni in un altro modo; per esempio la terza sarebbe più familiare nella forma $0+1$. Tuttavia è più comodo impiegare la notazione che abbiamo introdotto, perché rende più facili le regole per stabilire se un'espressione è un termine.

Analizziamo l'ultima; comincia con un simbolo di funzione binaria $\times$. Se lo cancelliamo, vediamo che ciò che resta sono due termini: $+\mathbf{11}$ e $+\mathbf{01}$. Per riconoscere questi due come termini, dobbiamo applicare ancora una volta la regola (T2).

Per chiarire meglio, abbiamo in questo caso $\times$ come simbolo di funzione binaria, dove $t_1$ e $t_2$ sono rispettivamente $+\mathbf{11}$ e $+\mathbf{01}$. Ciascuno di questi due termini è a sua volta costruito da termini secondo la regola (T2).

Il concetto di termine sarà esteso in seguito. Ora vogliamo introdurre quello di *interpretazione di un termine*.

DEFINIZIONE 4.3 (provvisoria). Sia $\mathfrak{A}$ una struttura e sia $\mathscr{L}$ un linguaggio adatto a essa.

(IT1) L'interpretazione $\mathbf{c}^{\mathfrak{A}}$ di un simbolo di costante $\mathbf{c}$ è la costante associata al simbolo.

(IT2) Se $\mathbf{f}\,t_1\,t_2\ldots t_n$ è un termine secondo la regola (T2), la sua interpretazione è

$$(\mathbf{f}\,t_1\,t_2\ldots t_n)^{\mathfrak{A}} = \mathbf{f}^{\mathfrak{A}}(t_1^{\mathfrak{A}}, t_2^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}}).$$

ESEMPIO 4.4. Calcoliamo l'interpretazione del termine $\times+\mathbf{11}+\mathbf{01}$ del linguaggio dei numeri naturali nella struttura dei numeri naturali:

$$\begin{aligned}(\times+\mathbf{11}+\mathbf{01})^{\mathfrak{N}} &= \times^{\mathfrak{N}}((+\mathbf{11})^{\mathfrak{N}}, (+\mathbf{01})^{\mathfrak{N}})\\ &= \times^{\mathfrak{N}}(+^{\mathfrak{N}}(\mathbf{1}^{\mathfrak{N}}, \mathbf{1}^{\mathfrak{N}}), +^{\mathfrak{N}}(\mathbf{0}^{\mathfrak{N}}, \mathbf{1}^{\mathfrak{N}}))\\ &= \times^{\mathfrak{N}}(+^{\mathfrak{N}}(1,1), +^{\mathfrak{N}}(0,1))\\ &= \times^{\mathfrak{N}}(2,1) = 2.\end{aligned}$$

Invece l'interpretazione del termine $++++\mathbf{11111}$ è il numero cinque. Anche $(\mathbf{s}+++\mathbf{1111})^{\mathfrak{N}}$ è il numero cinque, come è facile vedere e pure il termine $\mathbf{sssss0}$ ha come interpretazione il numero cinque.

Come nella definizione di termine, anche il calcolo dell'interpretazione avviene ricorsivamente, da sinistra verso destra, scomponendo un termine via via.

## 5. Formule atomiche

I termini sono 'nomi per elementi'; ora vogliamo introdurre ciò che ci serve per dire qualcosa di questi 'elementi'.

DEFINIZIONE 5.1. Se $\mathbf{P}$ è un simbolo di relazione $n$-aria e $t_1$, $t_2$,..., $t_n$ sono termini, allora

$$\mathbf{P}\,t_1\,t_2\ldots t_n$$

è una formula atomica.

Dunque una formula atomica si riconosce in modo analogo a un termine: è un'espressione che comincia con un simbolo di relazione che deve essere seguito dal numero corretto di termini.

ESEMPIO 5.2. Nel linguaggio dei numeri naturali, le seguenti espressioni sono formule atomiche:

$$=\mathbf{00}\quad =\mathbf{01}\quad <\mathbf{10}\quad <\mathbf{s0}+\mathbf{11}$$

L'interpretazione di una formula atomica non è un elemento dell'universo; del resto una formula deve dirci un fatto che riguarda certi elementi dell'universo. Per parlare di interpretazione di una formula atomica, introdurremo due simboli ai quali non attribuiamo alcun significato formale: **V** e **F**.

Per essere onesti, la forma assegnata a questi simboli dovrebbe ricordarci 'vero' e 'falso'. Tuttavia non è necessario assumere questi significati, anche se è opportuno tenerli presente.

DEFINIZIONE 5.3. L'interpretazione della formula atomica $\mathbf{P}\,t_1\,t_2\ldots t_n$ è

$$(\mathbf{P}\,t_1\,t_2\ldots t_n)^{\mathfrak{A}} = \begin{cases}\mathbf{V} & \text{se } (t_1^{\mathfrak{A}}, t_2^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}}) \in \mathbf{P}^{\mathfrak{A}}\\ \mathbf{F} & \text{se } (t_1^{\mathfrak{A}}, t_2^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}}) \notin \mathbf{P}^{\mathfrak{A}}\end{cases}$$

Se ci pensiamo, questa è una definizione ragionevole: l'interpretazione di $\mathbf{P}$ è una relazione $n$-aria su $A$ e perciò ha senso domandarsi se una certa $n$-pla di elementi appartiene o no a $\mathbf{P}^{\mathfrak{A}}$. La $n$-pla di elementi è fornita dalle interpretazioni degli $n$ termini che compaiono nella formula atomica.

ESEMPIO 5.4. Calcoliamo le interpretazioni delle formule precedenti:

$$(\mathbf{=00})^{\mathfrak{N}} = \mathbf{V}$$
$$(\mathbf{=01})^{\mathfrak{N}} = \mathbf{F}$$
$$(\mathbf{<10})^{\mathfrak{N}} = \mathbf{F}$$
$$(\mathbf{<s0+11})^{\mathfrak{N}} = \mathbf{V}$$

Infatti $(0,0) \in =^{\mathfrak{N}}$, $(0,1) \notin =^{\mathfrak{N}}$, $(1,0) \notin <^{\mathfrak{N}}$, $(1,2) \in <^{\mathfrak{N}}$.

## 6. Connettivi

Con gli strumenti che abbiamo a disposizione, siamo in grado di esprimere ben poco. Prendiamo il caso dei numeri naturali: possiamo nominare ogni numero (con un termine opportuno, per esempio '$\mathbf{s}\ldots\mathbf{s0}$'); se $t_1$ e $t_2$ sono termini, possiamo esprimere la loro uguaglianza (con la formula '$\mathbf{=}\,t_1\,t_2$') o se uno è minore dell'altro (con la formula '$\mathbf{<}\,t_1\,t_2$').

Non possiamo però esprimere molte altre cose interessanti, per esempio che un termine rappresenti un numero "minore o uguale" a un altro, oppure che un numero sia divisore di un altro. Eppure questi concetti sono ovviamente esprimibili usando la relazione di minore, quella di uguaglianza e la funzione moltiplicazione. Il problema è che occorre "mettere insieme" più formule.

Cominciamo in astratto, perché il nostro scopo è di evitare di assegnare significati intuitivi a ciò che facciamo: il nostro linguaggio deve essere non ambiguo. Vogliamo studiare le funzioni $\{\mathbf{V},\mathbf{F}\} \to \{\mathbf{V},\mathbf{F}\}$ e le funzioni $\{\mathbf{V},\mathbf{F}\}^2 \to \{\mathbf{V},\mathbf{F}\}$. Possiamo sintetizzarle in due tabelle:

| | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| **V** | **V** | **V** | **F** | **F** |
| **F** | **V** | **F** | **V** | **F** |

per le funzioni di $\{\mathbf{V},\mathbf{F}\}$ in $\{\mathbf{V},\mathbf{F}\}$ e

| | $g_1$ | $g_2$ | $g_3$ | $g_4$ | $g_5$ | $g_6$ | $g_7$ | $g_8$ | $g_9$ | $g_{10}$ | $g_{11}$ | $g_{12}$ | $g_{13}$ | $g_{14}$ | $g_{15}$ | $g_{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **(V,V)** | **V** | **V** | **V** | **V** | **V** | **V** | **V** | **V** | **F** | **F** | **F** | **F** | **F** | **F** | **F** | **F** |
| **(V,F)** | **V** | **V** | **V** | **V** | **F** | **F** | **F** | **F** | **V** | **V** | **V** | **V** | **F** | **F** | **F** | **F** |
| **(F,V)** | **V** | **V** | **F** | **F** | **V** | **V** | **F** | **F** | **V** | **V** | **F** | **F** | **V** | **V** | **F** | **F** |
| **(F,F)** | **V** | **F** | **V** | **F** | **V** | **F** | **V** | **F** | **V** | **F** | **V** | **F** | **V** | **F** | **V** | **F** |

per le funzioni di $\{\mathbf{V},\mathbf{F}\}^2$ in $\{\mathbf{V},\mathbf{F}\}$.

Fra le funzioni della prima tabella ce n'è una che ha un certo interesse ed è la $f_3$: quella che "scambia i valori di verità". Nella seconda tabella ce ne sono varie che ci possono interessare, già dalla $g_2$ che corrisponde alla nostra idea di "oppure", così come la $g_8$ corrisponde alla nostra idea di "e".

È interessante notare come tutte le funzioni della tabella possono essere espresse con composizioni delle funzioni $f_3$ e $g_2$. Per esempio, si consideri la $g_5$; dati comunque $x_1, x_2 \in \{\mathbf{V},\mathbf{F}\}$, vogliamo verificare che

$$g_5(x_1,x_2) = g_2(f_3(x_1),x_2).$$

Si dovrebbero esaminare i quattro casi possibili per i valori di $x_1$ e $x_2$; il tutto può essere riassunto con la seguente tabella:

| $g_2\,(\,f_3\,(\,x_1\,),\,x_2\,)$ | | | |
|---|---|---|---|
| **V** | **F** | **V** | **V** |
| **F** | **F** | **V** | **F** |
| **V** | **V** | **F** | **V** |
| **V** | **V** | **F** | **F** |

Si vede come sotto a $x_1$ e $x_2$ sono stati posti tutti i possibili valori; sotto al simbolo delle funzioni si scrive il valore assunto in dipendenza dai vari valori delle variabili. Quindi, per esempio, $g_2(f_3(\mathbf{F}),\mathbf{V})$ si legge sotto il simbolo $g_3$ sulla terza riga.

In modo analogo si può verificare che, per ogni $x_1, x_2 \in \{\mathbf{V},\mathbf{F}\}$,

$$g_8(x_1,x_2) = f_3(g_2(f_3(x_1),f_3(x_2))).$$

Scriviamo ancora la tabella:

| $f_3(g_2(f_3(x_1), f_3(x_2)))$ | | | | | |
|---|---|---|---|---|---|
| **V** | **F** | **F** | **V** | **F** | **V** |
| **F** | **V** | **F** | **V** | **V** | **F** |
| **F** | **V** | **V** | **F** | **F** | **V** |
| **F** | **V** | **V** | **F** | **V** | **F** |

e leggiamo sotto all'ultima funzione applicata il valore associato alla coppia in esame. Siccome i valori coincidono con quelli delle funzioni $g_5$ e $g_8$, abbiamo dimostrato la tesi. Si provi a ottenere anche le altre funzioni come composizione di $f_3$ e $g_2$.

Forse le tabelle precedenti sono più chiare se indichiamo quelle funzioni con simboli più consueti: useremo $\neg$ per $f_3$, $\vee$ per $g_2$, $\wedge$ per $g_8$, $\to$ per $g_5$ e $\leftrightarrow$ per $g_7$.

ESEMPIO 6.1. Dimostriamo che la $g_7 = \leftrightarrow$ si può esprimere come composizione di $\to$ e $\wedge$: calcoliamo infatti la tabella corrispondente a $\wedge(\to(x_1, x_2), \to(x_2, x_1))$:

| $\wedge(\to(x_1, x_2), \to(x_2, x_1))$ | | | | | | |
|---|---|---|---|---|---|---|
| **V** | **V** | **V** | **V** | **V** | **V** | **V** |
| **F** | **F** | **V** | **F** | **V** | **F** | **V** |
| **F** | **V** | **F** | **V** | **F** | **V** | **F** |
| **V** | **V** | **F** | **F** | **V** | **F** | **F** |

Così come $\to$ traduce l'idea intuitiva di "implicazione" ("se … allora …"), $\leftrightarrow$ traduce quella di "se e solo se".

DEFINIZIONE 6.2. I *connettivi* $\mathsf{V}$ e $\neg$ sono simboli del linguaggio. Li leggiamo "o" e "non" rispettivamente.

Avendo introdotto nuovi simboli nel linguaggio, vogliamo usarli per estendere il concetto di formula.

DEFINIZIONE 6.3 (provvisoria). In ogni linguaggio valgono le seguenti regole:

(F1) ogni formula atomica è una formula;
(F2) se $\varphi$ è una formula, allora $\neg\varphi$ è una formula;
(F3) se $\varphi$ e $\psi$ sono formule, allora $\mathsf{V}\varphi\psi$ è una formula.

ESEMPIO 6.4. Abbiamo già visto che $\mathbf{=00}$, $\mathbf{=01}$, $\mathbf{<10}$ e $\mathbf{<s0+11}$ sono formule atomiche nel linguaggio dei numeri naturali. Perciò

$$\neg\mathbf{=01}$$
$$\neg\mathbf{<10}$$
$$\mathsf{V}\mathbf{<10<s0+11}$$

sono formule del linguaggio.

Osserviamo di nuovo che le regole appena stabilite sono ricorsive; per verificare che un'espressione del linguaggio è una formula occorre "smontarla":

- un'espressione è una formula solo se comincia con un simbolo di relazione, con $\neg$ oppure con $\mathsf{V}$;
- nel primo caso deve essere una formula atomica;
- nel secondo caso ciò che rimane cancellando $\neg$ deve essere una formula;
- nel terzo caso ciò che rimane devono essere due formule.

La verifica, se l'espressione non è una formula atomica, riduce sempre il numero di simboli, quindi termina: data un'espressione, siamo in grado di dire se è una formula oppure no.

Ora che abbiamo esteso il concetto di formula, dobbiamo anche dire come le interpretiamo in una certa struttura $\mathfrak{A}$.

DEFINIZIONE 6.5 (provvisoria). Sia $\mathfrak{A}$ una struttura e sia $\mathscr{L}$ un linguaggio adatto a essa.

(IF1) L'interpretazione di una formula atomica è come già definita.

(IF2) L'interpretazione di una formula del tipo $\neg\varphi$ è

$$(\neg\varphi)^{\mathfrak{A}} = \neg(\varphi^{\mathfrak{A}}).$$

(IF3) L'interpretazione di una formula del tipo $\mathsf{V}\varphi\psi$ è

$$(\mathsf{V}\varphi\psi)^{\mathfrak{A}} = \vee(\varphi^{\mathfrak{A}}, \psi^{\mathfrak{A}}).$$

Per essere del tutto rigorosi, non dovremmo usare lo stesso simbolo per indicare i connettivi e le funzioni mediante le quali calcoliamo le interpretazioni. Tuttavia la pignoleria a volte non aiuta la chiarezza e basterà un minimo di attenzione per capire con quale significato usiamo i simboli. In effetti, guardando attentamente, possiamo vedere che in queste note si usa un peso diverso dei caratteri: i simboli usati per denotare quelli del linguaggio sono più marcati.

ESEMPIO 6.6. Vogliamo calcolare l'interpretazione della formula

$$\mathsf{V}\neg\mathbf{<10<s0+11}$$

e, per evitare troppi simboli, identifichiamo le formule atomiche e le abbreviamo: scriviamo $\varphi$ per $\mathbf{<10}$ e $\psi$ per $\mathbf{<s0+11}$. La formula da esaminare diventa allora

$$\mathsf{V}\neg\varphi\psi$$

e le interpretazioni delle formule atomiche sono:

$$(\varphi)^{\mathfrak{N}} = \mathbf{F},$$

perché $(1,0) \notin \mathbf{<}^{\mathfrak{N}}$;

$$(\psi)^{\mathfrak{N}} = \mathbf{V}$$

perché $(1,2) \in \mathbf{<}^{\mathfrak{N}}$. Ora la regola per l'interpretazione delle formule dice:

$$(\mathsf{V}\neg\varphi\psi)^{\mathfrak{N}} = \vee((\neg\varphi)^{\mathfrak{N}}, (\psi)^{\mathfrak{N}}) = \vee(\neg((\varphi)^{\mathfrak{N}}), (\psi)^{\mathfrak{N}}) = \vee(\neg(\mathbf{F}), \mathbf{V}) = \vee(\mathbf{V}, \mathbf{V}) = \mathbf{V}.$$

Intuitivamente la formula dice che "non è $1 < 0$ oppure è $1 < 2$" e l'interpretazione è "vero", come ci aspettiamo.

Useremo anche altri connettivi come abbreviazioni di formule che compaiono spesso; non saranno strettamente simboli del linguaggio, ma è comodo usarli per maggiore espressività.

DEFINIZIONE 6.7. Se $\varphi$ e $\psi$ sono formule, allora

$$\begin{array}{lll} \mathsf{A}\varphi\psi & \text{sta per} & \neg\mathsf{V}\neg\varphi\neg\psi, \\ \mathsf{C}\varphi\psi & \text{sta per} & \mathsf{V}\neg\varphi\psi, \\ \mathsf{E}\varphi\psi & \text{sta per} & \mathsf{A}\mathsf{C}\varphi\psi\mathsf{C}\psi\varphi. \end{array}$$

Leggeremo i simboli $\mathsf{A}$ e $\mathsf{C}$ come "e" e "implica" rispettivamente.

Per come abbiamo definito le cose, se $\varphi$ e $\psi$ sono formule, allora anche $\mathsf{A}\varphi\psi$ e $\mathsf{C}\varphi\psi$ sono formule e possiamo usare regole analoghe alla (F3) per smontare espressioni in cui compaiono questi simboli, perché sappiamo che queste espressioni vanno in realtà sostituite con altre che sono formule.

L'interpretazione di una formula abbreviata è facile da calcolare:

$$\begin{aligned}(\mathsf{A}\varphi\psi)^{\mathfrak{A}} = (\neg\mathsf{V}\neg\varphi\neg\psi)^{\mathfrak{A}} &= \neg((\mathsf{V}\neg\varphi\neg\psi)^{\mathfrak{A}}) = \neg(\vee((\neg\varphi)^{\mathfrak{A}}, (\neg\psi)^{\mathfrak{A}})) \\ &= \neg(\vee(\neg(\varphi^{\mathfrak{A}}), \neg(\psi^{\mathfrak{A}}))) = \wedge(\varphi^{\mathfrak{A}}, \psi^{\mathfrak{A}})\end{aligned}$$

per quanto visto quando abbiamo dimostrato che $g_8 = \wedge$ si può esprimere come composizione di $f_3 = \neg$ e di $g_2 = \vee$. Analogamente, come abbiamo visto che $g_5 = \rightarrow$ si può esprimere come composizione di $\neg$ e $\vee$, abbiamo

$$(\mathsf{C}\varphi\psi)^{\mathfrak{A}} = (\mathsf{V}\neg\varphi\psi)^{\mathfrak{A}} = \vee((\neg\varphi)^{\mathfrak{A}}, \psi^{\mathfrak{A}}) = \vee(\neg(\varphi^{\mathfrak{A}}), \psi^{\mathfrak{A}}) = \rightarrow(\varphi^{\mathfrak{A}}, \psi^{\mathfrak{A}}).$$

In altre parole, per calcolare le interpretazioni di formule abbreviate, possiamo usare le funzioni corrispondenti, esattamente come si fa per i connettivi $\neg$ e $\mathsf{V}$. Allo stesso modo si opera per $\mathsf{E}$.

## 7. Variabili

Nel linguaggio formale che stiamo via via definendo possiamo esprimere già alcune cose. Ci manca però un ingrediente fondamentale, il modo di indicare un oggetto "arbitrario". Inoltre possiamo osservare che abbiamo un problema: se nella struttura considerata non ci sono costanti (e quindi non abbiamo simboli di costanti nel linguaggio), non abbiamo nemmeno formule! Infatti la definizione di termine, sulla quale poggia quella di formula atomica e di seguito quella di formula, richiede che termini esistano; ma se non ci sono simboli di costante, la definizione precedente non ce ne fornisce.

DEFINIZIONE 7.1. In ogni linguaggio ammettiamo una infinità numerabile di simboli, detti *variabili*, che indicheremo con $\mathbf{v}_0$, $\mathbf{v}_1$,..., $\mathbf{v}_n$,..., uno per ogni numero naturale.

Ogni variabile sarà un termine. Perciò amplieremo la definizione precedente e questa sarà la versione definitiva. Ci occuperemo in seguito dell'interpretazione.

DEFINIZIONE 7.2. Un *termine* è un'espressione del linguaggio costruita secondo le seguenti regole:

(T1) ogni simbolo di costante è un termine;
(T2) ogni variabile è un termine;
(T3) se $\mathbf{f}$ è un simbolo di funzione $n$-aria e $t_1$, $t_2$,..., $t_n$ sono termini, allora $\mathbf{f}\,t_1\,t_2\ldots t_n$ è un termine;
(T4) nessun'altra espressione del linguaggio è un termine.

ESEMPIO 7.3. Nel linguaggio dei numeri naturali, le seguenti espressioni sono termini:

$$\mathbf{+\,v}_0\,\mathbf{v}_1 \qquad \mathbf{\times\,v}_1\,\mathbf{v}_3 \qquad \mathbf{\times\,s\,1\,v}_6 \qquad \mathbf{s\,v}_1$$

La definizione di formula (che amplieremo più avanti) va ovviamente estesa tenendo conto dei nuovi termini introdotti; ma le regole (F1), (F2) e (F3) rimangono esattamente le stesse.

ESEMPIO 7.4. Nel linguaggio dei numeri naturali, le seguenti espressioni sono formule:

$$\mathbf{=\,v}_1\,\mathbf{v}_2 \qquad \mathbf{<\,1\,v}_0 \qquad \mathbf{=\,+\,v}_0\,\mathbf{v}_1\,\mathbf{+\,v}_1\,\mathbf{v}_0$$

L'ultima formula dovrebbe ricordare la proprietà commutativa dell'addizione nei numeri naturali: scritta in forma più usuale potrebbe essere infatti $v_0 + v_1 = v_1 + v_0$.

## 8. Realizzazioni

Intuitivamente una variabile sta a indicare un elemento "qualunque". Per interpretare una formula atomica, però, dobbiamo valutare se una certa $n$-pla appartiene alla relazione associata, nella struttura, al simbolo di relazione che compare nella formula. Che valore di verità potremmo dare alla formula $\mathbf{=\,v}_0\,\mathbf{0}$?

La soluzione a questo problema richiede un nuovo concetto; lo scopo successivo sarà di riuscire a farne a meno.

DEFINIZIONE 8.1. Sia data la struttura $\mathfrak{A}$ con universo $A$. Una funzione $\mathsf{a}\colon \mathbb{N} \to A$ si chiama *assegnazione di valori alle variabili* (abbrevieremo con AVV).

Una *realizzazione* della struttura $\mathfrak{A}$ è una coppia ordinata $\sigma = (\mathfrak{A}, \mathsf{a})$ dove $\mathsf{a}$ è una AVV.

Diremo ora come interpretare un termine in una realizzazione. Prima di tutto però ci accordiamo che l'interpretazione di ogni simbolo di relazione o di funzione nella realizzazione è la stessa che nella struttura: se $\mathbf{S}$ è un simbolo di relazione o di funzione,

$$\mathbf{S}^{\sigma} = \mathbf{S}^{\mathfrak{A}}.$$

DEFINIZIONE 8.2. Sia $\sigma = (\mathfrak{A}, \mathsf{a})$ una realizzazione. L'interpretazione di un termine nella realizzazione $\sigma$ è calcolata secondo le regole seguenti:

(IT1) se $\mathbf{c}$ è un simbolo di costante, allora $\mathbf{c}^{\sigma} = \mathbf{c}^{\mathfrak{A}}$;
(IT2) $(\mathbf{v}_n)^{\sigma} = \mathsf{a}(n)$;

(IT3) se $\mathbf{f}$ è un simbolo di funzione $n$-aria e $t_1$, $t_2$,..., $t_n$ sono termini, allora

$$(\mathbf{f}\, t_1\, t_2 \ldots t_n)^\sigma = \mathbf{f}^\sigma(t_1^\sigma, t_2^\sigma, \ldots, t_n^\sigma).$$

In altre parole, alla variabile $\mathbf{v}_n$ sostituiamo il valore della funzione $\mathsf{a}$ in $n$. Naturalmente, l'interpretazione di un termine può cambiare cambiando la realizzazione (cioè la funzione di assegnazione di valori alle variabili).

ESEMPIO 8.3. Sia $\mathsf{a}$ la funzione così definita: $\mathsf{a}(0) = 1$, $\mathsf{a}(1) = 1$, $\mathsf{a}(2) = 4$, $\mathsf{a}(n) = n$ per $n > 2$.
Sia $\mathsf{b}$ la funzione così definita: $\mathsf{b}(0) = 3$, $\mathsf{b}(1) = 0$, $\mathsf{b}(2) = 1$, $\mathsf{b}(n) = 2$ per $n > 2$.
Consideriamo le realizzazioni $\sigma = (\mathfrak{N}, \mathsf{a})$ e $\tau = (\mathfrak{N}, \mathsf{b})$.
Vogliamo calcolare l'interpretazione in $\sigma$ e $\tau$ della formula

$$\bigvee \mathbf{<}\, \mathbf{v}_1\, \mathbf{1}\, \mathbf{=}\, \mathbf{v}_3\, \mathbf{v}_4$$

e, prima di tutto, identifichiamo le formule atomiche che vi compaiono: scriviamo $\varphi$ per $\mathbf{<}\, \mathbf{v}_1\, \mathbf{1}$ e $\psi$ per $\mathbf{=}\, \mathbf{v}_3\, \mathbf{v}_4$. Abbiamo

$$\varphi^\sigma = \mathbf{F} \qquad \text{e} \qquad \psi^\sigma = \mathbf{F}$$

perché $(\mathsf{a}(1), \mathbf{1}^{\mathfrak{N}}) = (1,1) \notin \mathbf{<}^{\mathfrak{N}}$ e $(\mathsf{a}(3), \mathsf{a}(4)) = (3,4) \notin \mathbf{=}^{\mathfrak{N}}$. Dunque

$$(\bigvee \varphi\, \psi)^\sigma = \bigvee(\varphi^\sigma, \psi^\sigma) = \bigvee(\mathbf{F}, \mathbf{F}) = \mathbf{F}.$$

Abbiamo poi

$$\varphi^\tau = \mathbf{F} \qquad \text{e} \qquad \psi^\tau = \mathbf{V}$$

perché $(\mathsf{b}(1), \mathbf{1}^{\mathfrak{N}}) = (3,1) \notin \mathbf{<}^{\mathfrak{N}}$ e $(\mathsf{b}(3), \mathsf{b}(4)) = (2,2) \in \mathbf{=}^{\mathfrak{N}}$. Dunque

$$(\bigvee \varphi\, \psi)^\tau = \bigvee(\varphi^\tau, \psi^\tau) = \bigvee(\mathbf{F}, \mathbf{V}) = \mathbf{V}.$$

Come vediamo, l'interpretazione della formula dipende dalla AVV.

## 9. Quantificatori

Consideriamo le seguenti formule nel linguaggio dei numeri naturali:

$$(1) \quad \mathbf{=}\, \mathbf{v}_0\, \mathbf{v}_0 \qquad\qquad (2) \quad \mathbf{=}\, \mathbf{v}_0\, \mathbf{v}_1$$

e calcoliamone l'interpretazione in una realizzazione $\sigma = (\mathfrak{N}, \mathsf{a})$. Dobbiamo allora considerare le due coppie $((\mathbf{v}_0)^\sigma, (\mathbf{v}_0)^\sigma) = (\mathsf{a}(0), \mathsf{a}(0))$ e $((\mathbf{v}_0)^\sigma, (\mathbf{v}_1)^\sigma) = (\mathsf{a}(0), \mathsf{a}(1))$. Si vede che la prima coppia appartiene a $\mathbf{=}^\sigma$ indipendentemente dalla funzione $\mathsf{a}$, mentre la seconda può appartenere alla relazione di identità oppure no.

Un esempio meno banale è dato dalla formula

$$\mathbf{<}\, \mathbf{0}\, \mathbf{+}\, \mathbf{v}_0\, \mathbf{1}$$

che, scritta in forma usuale, sarebbe "$0 < v_0 + 1$". Riconosciamo facilmente che l'interpretazione di questa formula è vera in ogni realizzazione della struttura dei numeri naturali. Tuttavia ciò non accade in almeno una realizzazione della struttura dei numeri interi: se $\mathsf{a}(0) = -2 \in \mathbb{Z}$ e $\sigma = (\mathfrak{Z}, \mathsf{a})$, abbiamo che

$$(\mathbf{<}\, \mathbf{0}\, \mathbf{+}\, \mathbf{v}_0\, \mathbf{1})^\sigma = \mathbf{F}$$

perché

$$(\mathbf{0}^\sigma, (\mathbf{+}\, \mathbf{v}_0\, \mathbf{1})^\sigma) = (0, \mathsf{a}(0) + 1) = (0, -2 + 1) = (0, -1) \notin \mathbf{<}^{\mathfrak{Z}}.$$

Non dovrebbe sorprenderci: il linguaggio dei numeri naturali è adatto sia alla struttura $\mathfrak{N}$ che alla struttura $\mathfrak{Z}$; siccome queste strutture sono diverse, può accadere che una formula sia interpretata come vera in ogni realizzazione della prima e non in ogni realizzazione della seconda.

È il momento di aggiungere l'ultimo simbolo al linguaggio. Questo simbolo si chiama *quantificatore universale* e si denota con $\mathbf{\forall}$. Con questo simbolo si possono costruire nuove formule e siamo pronti per dare la regola definitiva per le formule.

DEFINIZIONE 9.1. Una *formula* è un'espressione del linguaggio costruita secondo le seguenti regole:

(F1) ogni formula atomica è una formula;
(F2) se $\varphi$ è una formula, allora $\neg\varphi$ è una formula;

(F3) se $\varphi$ e $\psi$ sono formule, allora $\mathsf{V}\varphi\psi$ è una formula;
(F4) se $\varphi$ è una formula e $v$ è una variabile, allora $\forall v\,\varphi$ è una formula;
(F5) niente altro è una formula.

Abbiamo aggiunto alla definizione provvisoria precedente una regola riguardante il quantificatore universale. Oltre ai casi precedentemente visti, una formula può cominciare con il quantificatore universale, purché questo sia seguito da una variabile e il resto dell'espressione sia una formula.

ESEMPIO 9.2. Le seguenti sono formule nel linguaggio dei numeri naturali:

$$\forall \mathbf{v}_0 = \mathbf{v}_0\,\mathbf{v}_0$$
$$\forall \mathbf{v}_0\,\forall \mathbf{v}_1 \to = \mathbf{v}_0\,\mathbf{v}_1 = \mathbf{v}_1\,\mathbf{v}_0$$

Che proprietà esprimono queste formule?

Vogliamo ora definire l'interpretazione di una formula che comincia con il quantificatore universale. Le altre regole per l'interpretazione delle formule rimangono invariate, le ripetiamo qui per completezza.

Abbiamo bisogno prima di una definizione supplementare.

DEFINIZIONE 9.3. Sia $\mathfrak{A}$ una struttura con universo $A$ e sia $\mathsf{a}\colon \mathbb{N} \to A$ una assegnazioni di valori alle variabili. Consideriamo la realizzazione $\sigma = (\mathfrak{A}, \mathsf{a})$. Dati $k \in \mathbb{N}$ e un elemento $b \in A$, indichiamo con $\mathsf{a}[\mathbf{v}_k / b]$ la funzione $\mathbb{N} \to A$ così definita:

$$\mathsf{a}[\mathbf{v}_k / b](n) = \begin{cases} \mathsf{a}(n) & \text{se } n \neq k, \\ b & \text{se } n = k. \end{cases}$$

La realizzazione $\sigma[\mathbf{v}_k / b]$ è

$$\sigma[\mathbf{v}_k / b] = (\mathfrak{A}, \mathsf{a}[\mathbf{v}_k / b]).$$

In altre parole $\sigma[\mathbf{v}_k / b]$ è la realizzazione $\sigma$ in cui, però, alla variabile $\mathbf{v}_k$ viene sostituito $b$ invece di $\mathsf{a}(k)$.

DEFINIZIONE 9.4. Sia $\mathfrak{A}$ una struttura con universo $A$, sia $\mathscr{L}$ un linguaggio adatto a essa e sia $\mathsf{a}\colon \mathbb{N} \to A$ una assegnazione di valori alle variabili. Consideriamo la realizzazione $\sigma = (\mathfrak{A}, \mathsf{a})$.

(IF1) L'interpretazione in $\sigma$ della formula atomica $\mathbf{P}\,t_1\,t_2 \ldots t_n$ è

$$(\mathbf{P}\,t_1\,t_2 \ldots t_n)^\sigma = \begin{cases} \mathbf{V} & \text{se } (t_1^\sigma, t_2^\sigma, \ldots, t_n^\sigma) \in \mathbf{P}^\sigma \\ \mathbf{F} & \text{se } (t_1^\sigma, t_2^\sigma, \ldots, t_n^\sigma) \notin \mathbf{P}^\sigma \end{cases}$$

(IF2) L'interpretazione in $\sigma$ di una formula del tipo $\neg\varphi$ è

$$(\neg\varphi)^\sigma = \neg(\varphi^\sigma).$$

(IF3) L'interpretazione in $\sigma$ di una formula del tipo $\mathsf{V}\varphi\psi$ è

$$(\mathsf{V}\varphi\psi)^\sigma = \mathsf{V}(\varphi^\sigma, \psi^\sigma).$$

(IF4) L'interpretazione in $\sigma$ di una formula del tipo $\forall \mathbf{v}_k\,\varphi$ si calcola nel modo seguente:

$$(\forall \mathbf{v}_k\,\varphi)^\sigma = \mathbf{V} \text{ se e solo se } \varphi^{\sigma[\mathbf{v}_k / b]} = \mathbf{V}, \text{ per ogni } b \in A;$$

Altrimenti $(\forall \mathbf{v}_k\,\varphi)^\sigma = \mathbf{F}$.

In altre parole, la formula $\forall \mathbf{v}_k\,\varphi$ è interpretata come vera nella realizzazione $\sigma$ se l'interpretazione della formula $\varphi$ è vera in ogni realizzazione che differisca da $\sigma$ solo per il valore assegnato alla variabile $\mathbf{v}_k$.

ESEMPIO 9.5. Se $\sigma = (\mathfrak{N}, \mathsf{a})$ è una realizzazione della struttura dei numeri naturali, l'interpretazione in $\sigma$ della formula

$$\forall \mathbf{v}_0\,\neg = \mathbf{v}_0\,\mathbf{s}\,\mathbf{v}_0$$

è vera. Prendiamo infatti $b \in \mathbb{N}$ e calcoliamo

$$(\neg = \mathbf{v}_0\,\mathbf{s}\,\mathbf{v}_0)^{\sigma[\mathbf{v}_0 / b]} = \neg((= \mathbf{v}_0\,\mathbf{s}\,\mathbf{v}_0)^{\sigma[\mathbf{v}_0 / b]}).$$

Ora dobbiamo considerare la coppia

$$(\mathsf{a}[\mathbf{v}_0/b](0), \mathbf{s}^{\mathfrak{N}}(\mathsf{a}[\mathbf{v}_0/b](0)) = (b, b+1) \notin =^{\mathfrak{N}}.$$

Dunque $(=\mathbf{v}_0\,\mathbf{s}\,\mathbf{v}_0)^{\sigma[\mathbf{v}_0/b]} = \mathbf{F}$ e quindi abbiamo la tesi.

ESEMPIO 9.6. Se $\sigma = (\mathfrak{N}, \mathsf{a})$ è una realizzazione della struttura dei numeri naturali, l'interpretazione in $\sigma$ della formula

$$\forall\,\mathbf{v}_0\,\neg =\times\,\mathbf{s}\,\mathbf{1}\,\mathbf{s}\,\mathbf{1}\times\,\mathbf{v}_0\,\mathbf{v}_0$$

è falsa. Se traduciamo in parole usuali la formula, questa direbbe che, per ogni $n$, $4 \neq n^2$. E in effetti, se consideriamo la realizzazione $\sigma[\mathbf{v}_0/2]$, abbiamo che

$$(\neg =\times\,\mathbf{s}\,\mathbf{1}\,\mathbf{s}\,\mathbf{1}\times\,\mathbf{v}_0\,\mathbf{v}_0)^{\sigma[\mathbf{v}_0/2]} = \mathbf{F}$$

perché $(4,4) \in =^{\mathfrak{N}}$.

Come abbiamo visto nell'ultimo esempio, affinché l'interpretazione di una formula con quantificatore universale sia falsa, basta che esista un elemento dell'universo che non renda vera la sottoformula nella realizzazione "modificata".

È interessante notare quando l'interpretazione di una formula che comincia con un quantificatore universale è falsa (e quindi la sua negazione è interpretata come vera). Meglio ancora, cerchiamo di capire quando l'interpretazione della formula $\forall\,\mathbf{v}_k\,\neg\varphi$ è falsa. Abbiamo già visto nell'esempio che ciò equivale all'esistenza di un elemento $b \in A$ tale che

$$(\neg\varphi)^{\sigma[\mathbf{v}_k/b]} = \mathbf{F}$$

cioè

$$\varphi^{\sigma[\mathbf{v}_k/b]} = \mathbf{V}.$$

Dunque

$$\boxed{\begin{array}{c}(\neg\,\forall\,\mathbf{v}_k\,\neg\varphi)^{\sigma} = \mathbf{V}\\ \text{se e solo se}\\ \text{esiste } b \in A \text{ tale che } \varphi^{\sigma[\mathbf{v}_k/b]} = \mathbf{V}.\end{array}}$$

Abbiamo dunque trovato il modo di esprimere il concetto di "esistenza" attraverso il quantificatore universale. Possiamo allora introdurre una nuova abbreviazione:

$$\exists\,\mathbf{v}_k\varphi \quad \text{sta per} \quad \neg\,\forall\,\mathbf{v}_k\,\neg\varphi$$

e chiameremo $\exists$ *quantificatore esistenziale*.

ESEMPIO 9.7. Vogliamo scrivere una formula nel linguaggio dei numeri naturali che esprima il fatto che *un numero è divisibile per un altro*.

Avremo bisogno di due variabili, $\mathbf{v}_0$ e $\mathbf{v}_1$, per indicare il numero dato e il divisore. Osserviamo che, affinché $a$ sia divisibile per $b$, deve esistere un numero $c$ tale che $a = bc$. La formula cercata sarà allora

$$\exists\,\mathbf{v}_2 = \mathbf{v}_0 \times \mathbf{v}_1\,\mathbf{v}_2.$$

Vediamo qui uno dei motivi per i quali abbiamo scelto di introdurre nel linguaggio infinite variabili: possiamo sempre trovarne una diversa da quelle che abbiamo già impiegato.

ESEMPIO 9.8. Cerchiamo ora di esprimere la relazione di "essere minore" usando solo l'addizione e la relazione di identità. Un numero $a$ è minore del numero $b$ se e solo se esiste un terzo numero $c$, diverso da zero, tale che $b = a + c$. Dunque la formula sarà:

$$\exists\,\mathbf{v}_2 \wedge \neg =\mathbf{v}_2\,\mathbf{0} = \mathbf{v}_1 + \mathbf{v}_0\,\mathbf{v}_2.$$

Il lettore verifichi che la formula

$$\forall\,\mathbf{v}_0\,\forall\,\mathbf{v}_1 \leftrightarrow <\mathbf{v}_0\,\mathbf{v}_1\,\exists\,\mathbf{v}_2 \wedge \neg =\mathbf{v}_2\,\mathbf{0} = \mathbf{v}_1 + \mathbf{v}_0\,\mathbf{v}_2$$

è vera in ogni realizzazione della struttura dei numeri naturali $\mathfrak{N}$. Vale lo stesso per ogni realizzazione della struttura dei numeri interi $\mathfrak{Z}$?

Consideriamo la formula $\forall \mathbf{v}_0 = + \mathbf{v}_0 \mathbf{1} + \mathbf{1} \mathbf{v}_0$; non è difficile verificare che questa è vera in ogni realizzazione della struttura dei numeri naturali (scritta in termini usuali dice che, per ogni $n$, $n+1 = 1+n$). Viceversa, la formula $\exists \mathbf{v}_2 = \mathbf{v}_0 \times \mathbf{v}_1 \mathbf{v}_2$ è vera in certe realizzazioni e falsa in altre.

Per esempio, se $\mathsf{a}(0) = 6$, $\mathsf{a}(1) = 3$, $\mathsf{a}(2) = 5$, mentre $\mathsf{b}(0) = 7$, $\mathsf{b}(1) = 4$, $\mathsf{b}(2) = 9$, ponendo $\sigma = (\mathfrak{N}, \mathsf{a})$ e $\tau = (\mathfrak{N}, \mathsf{b})$, possiamo facilmente vedere che (chiamando $\varphi$ la formula in esame):

$$\varphi^\sigma = \mathbf{V}, \qquad \varphi^\tau = \mathbf{F}.$$

Infatti $\mathsf{a}(0) = 6$ è divisibile per $\mathsf{a}(1) = 3$, mentre $\mathsf{b}(0) = 7$ non è divisibile per $\mathsf{a}(1) = 4$. Come si vede, nel calcolo dell'interpretazione in $\sigma$ o in $\tau$ non ha alcuna rilevanza il valore delle AVV in 2 o nei numeri maggiori di due. Il valore assegnato alle variabili che non compaiono è irrilevante e non ci sono particolari motivi che non ce lo facessero supporre già da prima.

ESEMPIO 9.9. Analizziamo per semplicità una formula ancora più breve:

$$\forall \mathbf{v}_0 < \mathbf{v}_0 \mathbf{s} \mathbf{v}_0.$$

In forma usuale questa dice che, per ogni $n$, $n < n+1$. È facile verificare che l'interpretazione di questa formula non dipende da alcuno dei valori assegnati alle variabili nella realizzazione: infatti, quando vogliamo "togliere il quantificatore", dobbiamo sostituire $\sigma$ con $\sigma[\mathbf{v}_0/b]$, per ogni valore di $b \in \mathbb{N}$; dunque fissiamo il valore in 0 della AVV e gli altri valori non contano perché l'unica variabile che compare è $\mathbf{v}_0$. Ora, se $b \in \mathbb{N}$,

$$(b, b+1) \in <^{\mathfrak{N}}$$

quindi

$$(< \mathbf{v}_0 \mathbf{s} \mathbf{v}_0)^{\sigma[\mathbf{v}_0/b]} = \mathbf{V}$$

e questo non dipende dalla scelta di $b$. Dunque

$$(\forall \mathbf{v}_0 < \mathbf{v}_0 \mathbf{s} \mathbf{v}_0)^\sigma = \mathbf{V}.$$

Quando parliamo in modo informale, ci accorgiamo che certe "variabili" hanno un nome che può essere cambiato. Per fare un esempio concreto, quando diciamo che

Per ogni $n \in \mathbb{N}$ la somma dei numeri naturali da 0 a $n$ è $n(n+1)/2$,

è evidente che la lettera $n$ può essere sostituita con qualunque altra. Non è la stessa cosa quando diciamo che

Esiste un numero naturale $n$ tale che $n > 2$ e $n$ divide $m$,

dove ancora la lettera $n$ può essere sostituita, ma la lettera $m$ no.

Dove sta il motivo della differenza? Sembra evidente che risiede nel fatto che su $n$ "agisce un quantificatore".

DEFINIZIONE 9.10. Quando una formula è costruita usando la regola (F4) e $v$ è la variabile che vi compare, questa variabile si dice *vincolata*.

Nella formula $\forall \mathbf{v}_1 \bigvee < \mathbf{v}_0 \mathbf{v}_1 = \mathbf{v}_0 \mathbf{v}_1$, la variabile $\mathbf{v}_1$ è vincolata, la variabile $\mathbf{v}_0$ no.

Naturalmente, quando si usa il quantificatore esistenziale, vale la stessa regola, visto che si tratta solo di un'abbreviazione. Per esempio, nella formula

$$\bigwedge \bigwedge \neg = \mathbf{v}_0 \mathbf{0} \neg = \mathbf{v}_0 \mathbf{1} \exists \mathbf{v}_1 \exists \mathbf{v}_2 \bigwedge \bigwedge < \mathbf{1} \mathbf{v}_1 < \mathbf{1} \mathbf{v}_2 = \mathbf{v}_0 \times \mathbf{v}_1 \mathbf{v}_2$$

la variabile $\mathbf{v}_0$ non è vincolata, mentre lo sono le variabili $\mathbf{v}_1$ e $\mathbf{v}_2$. (Si scopra che cosa voglia dire questa formula, trovando in quali realizzazioni del linguaggio dei numeri naturali è vera.)

Ci sono inconvenienti quando si mettono insieme più formule, perché in esse una variabile potrebbe apparire vincolata oppure non vincolata. Per esempio questo accade nella formula

$$\bigvee = \mathbf{v}_0 \mathbf{0} \forall \mathbf{v}_0 = \mathbf{v}_0 \mathbf{v}_0$$

che probabilmente è stata costruita in modo non attento. Di fatto, quando vogliamo costruire una formula che asserisca una condizione significativa, ci preoccupiamo di non usare le variabili a sproposito. Ma se qualcuno non è così attento, non tutto è perduto.

TEOREMA 9.11. *Se $\mathbf{v}_n$ è una variabile che non compare nella formula $\varphi$ e chiamiamo $\varphi'$ la formula che si ottiene sostituendo ogni occorrenza della variabile vincolata $\mathbf{v}_k$ in $\varphi$ con $\mathbf{v}_n$, allora le formule $\varphi$ e $\varphi'$ sono interpretate allo stesso modo in tutte le realizzazioni.*

Non daremo la dimostrazione di questo teorema, del resto non difficile (si fa per induzione sul numero di connettivi della formula $\varphi$). Quello che ci interessa è notare che, quando abbiamo una formula "scritta male", la possiamo sostituire con una che sia "scritta bene". Una formula è "scritta bene" quando nessuna variabile che compare in essa è sia vincolata che non vincolata. D'ora in poi supporremo che tutte le formule siano "scritte bene"; la cosa ci è permessa dal teorema.

In una formula "scritta bene", diremo che una variabile non vincolata è *libera*.

DEFINIZIONE 9.12. Una formula si dice un *enunciato* se non ha variabili libere.

Prima di dire a che serve distinguere gli enunciati tra le formule, vediamo che cosa accade quando una formula ha variabili libere.

Per fare un esempio facile, la formula $\neg = \mathbf{v}_0 \mathbf{0}$ è vera in tutte le realizzazioni del linguaggio dei numeri naturali nelle quali alla variabile $\mathbf{v}_0$ è assegnato un valore diverso da zero. Dunque abbiamo una condizione che la realizzazione deve soddisfare affinché la formula sia vera.

In generale, data una formula $\varphi$, scriveremo $\varphi(\mathbf{v}_0, \ldots, \mathbf{v}_n)$ per dire che in $\varphi$ compaiono come libere solo variabili fra quelle indicate. Se $\mathfrak{A}$ è una struttura e $a_0$, $a_1$,..., $a_n$ sono elementi del suo universo, scriveremo

$$\mathfrak{A} \models \varphi(\mathbf{v}_0, \ldots, \mathbf{v}_n)[a_0, \ldots, a_n]$$

per indicare che la formula $\varphi$ è vera in ogni realizzazione in cui la AVV assegni alla variabile $\mathbf{v}_i$ il valore $a_i$ ($i = 0, 1, \ldots, n$).

ESEMPIO 9.13. Scrivere una formula $\varphi$ con la variabile libera $\mathbf{v}_0$ tale che

$$\mathfrak{N} \models \varphi(\mathbf{v}_0)[a_0]$$

se e solo se $a_0$ è un numero primo.

La costruiremo un pezzo alla volta. Intanto dobbiamo dire che il numero dato non è né 0 né 1. Poi dovremo dire che un divisore di questo numero è necessariamente 1 o il numero stesso. I primi due pezzi sono allora

$$\neg = \mathbf{v}_0 \mathbf{0}, \qquad \neg = \mathbf{v}_0 \mathbf{1}.$$

Il pezzo più complicato si può costruire dicendo che, quando si ha un prodotto di due numeri maggiori di 1, questo non è il numero di cui si asserisce che è primo:

$$\forall \mathbf{v}_1 \forall \mathbf{v}_2 \rightarrow \wedge < \mathbf{1} \mathbf{v}_1 < \mathbf{1} \mathbf{v}_2 \neg = \mathbf{v}_0 \times \mathbf{v}_1 \mathbf{v}_2.$$

Dunque la nostra formula sarà:

$$\wedge \wedge \neg = \mathbf{v}_0 \mathbf{0} \neg = \mathbf{v}_0 \mathbf{1} \forall \mathbf{v}_1 \forall \mathbf{v}_2 \rightarrow \wedge < \mathbf{1} \mathbf{v}_1 < \mathbf{1} \mathbf{v}_2 \neg = \mathbf{v}_0 \times \mathbf{v}_1 \mathbf{v}_2.$$

Se ne trovino altre.

Un enunciato, invece, è una formula della quale siamo sicuri che l'interpretazione non dipende dalla realizzazione, ma solo dalla struttura.

TEOREMA 9.14. *Sia $\varphi$ una formula. Se $\sigma = (\mathfrak{A}, \mathsf{a})$ e $\tau = (\mathfrak{A}, \mathsf{b})$ sono realizzazioni le cui* AVV *coincidono sulle variabili libere di $\varphi$, allora*

$$\varphi^\sigma = \varphi^\tau.$$

DIMOSTRAZIONE. Faremo induzione sul numero $k$ di connettivi e quantificatori nella formula $\varphi$.

(Passo base) Se $k = 0$, la formula è atomica. L'interpretazione della formula dipende allora solo dal valore assegnato alle variabili che effettivamente compaiono.

(Passo induttivo) Supponiamo la tesi vera per formule in cui il numero di connettivi e quantificatori è minore di $n$.

Primo caso: $\varphi$ è della forma $\neg\alpha$. Per ipotesi induttiva l'interpretazione di $\alpha$ è la stessa in $\sigma$ e in $\tau$.

Secondo caso: $\varphi$ è della forma $\bigvee \alpha\,\beta$. Per ipotesi induttiva l'interpretazione di $\alpha$ e $\beta$ è la stessa in $\sigma$ e in $\tau$.

Terzo caso: $\varphi$ è della forma $\forall \mathbf{v}_k\,\alpha$ e possiamo supporre che la variabile $\mathbf{v}_k$ non compaia fra le variabili libere in $\varphi$. Sia $b$ un elemento dell'universo; dobbiamo verificare che

$$\alpha^{\sigma[\mathbf{v}_k/b]} \qquad \text{e} \qquad \alpha^{\tau[\mathbf{v}_k/b]}$$

sono uguali. Ma le AVV delle realizzazioni $\sigma[\mathbf{v}_k/b]$ e $\tau[\mathbf{v}_k/b]$ coincidono sia sulle variabili libere di $\varphi$ che su $\mathbf{v}_k$; dunque coincidono sulle variabili libere di $\alpha$ che ha un quantificatore in meno rispetto a $\varphi$. Per ipotesi induttiva le due interpretazioni considerate di $\alpha$ sono uguali. □

COROLLARIO 9.15. *L'interpretazione di un enunciato è la stessa in tutte le realizzazioni di una data struttura.*

Abbiamo finalmente tolto di mezzo le realizzazioni! Non del tutto, perché sono necessarie per calcolare le interpretazioni.

Osserviamo che il corollario non dice che l'interpretazione di un enunciato è indipendente dalla struttura, ma solo da una sua realizzazione. Se un linguaggio è adeguato a più strutture, un suo enunciato può essere interpretato diversamente in esse.

ESEMPIO 9.16. Consideriamo l'enunciato nel linguaggio dei numeri naturali

$$\forall \mathbf{v}_0\,\forall \mathbf{v}_1 \rightarrow < \mathbf{v}_0\,\mathbf{v}_1\,\exists \mathbf{v}_2 \bigwedge < \mathbf{v}_0\,\mathbf{v}_2 < \mathbf{v}_2\,\mathbf{v}_1$$

che dice, intuitivamente: fra due elementi distinti ce n'è un terzo.

Questo enunciato è falso nella struttura $\mathfrak{N}$ dei numeri naturali; è invece vero nella struttura $\mathfrak{R}$ dei numeri reali.

## 10. Teorema di deduzione semantica

Vogliamo ora analizzare più in profondità quanto abbiamo studiato fin qui. In particolare vogliamo vedere che l'usuale modo di ragionare ha un corrispettivo nell'analisi dell'interpretazione delle formule.

Fisseremo una struttura $\mathfrak{A}$ e un linguaggio $\mathscr{L}$ a essa adeguato.

DEFINIZIONE 10.1. Una formula $\varphi$ nel linguaggio $\mathscr{L}$ si dice *valida* in $\mathfrak{A}$ se l'interpretazione di $\varphi$ è vera in ogni realizzazione di $\mathfrak{A}$ e scriveremo, in tal caso

$$\models_{\mathfrak{A}} \varphi$$

o, più semplicemente, quando è chiaro a quale struttura ci riferiamo, $\models \varphi$.

Possiamo dare una definizione più generale.

DEFINIZIONE 10.2. Una formula $\varphi$ si dice *conseguenza logica* di un insieme di formule $\Phi$ se l'interpretazione di $\varphi$ è vera in ogni realizzazione di $\mathfrak{A}$ in cui ogni formula dell'insieme $\Phi$ è vera; scriveremo, in tal caso

$$\Phi \models_{\mathfrak{A}} \varphi$$

o, se la struttura di cui si parla è chiara, $\Phi \models \varphi$.

La seconda definizione è più generale perché una formula è valida se e solo se è conseguenza logica dell'insieme vuoto di formule.

Usualmente l'insieme di formule $\Phi$ è dato dagli *assiomi* di una teoria (quelli di Peano per i numeri naturali o quelli di Euclide per la geometria piana). Il nostro scopo è di scoprire quali siano gli enunciati che valgono in tutte le strutture nei quali gli assiomi siano soddisfatti.

Prendiamo una tipica situazione. Quando vogliamo dimostrare una proposizione del tipo "se $A$ allora $B$", il ragionamento usuale è: supponiamo che valga $A$ (oltre agli assiomi) e da questa ipotesi supplementare ricaviamo $B$.

Non vogliamo qui analizzare il concetto di dimostrazione, che richiederebbe molto più tempo. Ci limiteremo a una descrizione "semantica" della situazione, cioè legata al concetto di interpretazione. Nel corso di Logica Matematica verrà invece mostrato che i concetti di "conseguenza logica" e "dimostrabilità" sono intimamente collegati.

TEOREMA 10.3 (Teorema di deduzione semantica). *Siano $\varphi$ e $\psi$ due formule e sia $\Phi$ un insieme di formule. Allora*

$$\Phi \models \to \psi\, \varphi \qquad \textit{se e solo se} \qquad \Phi \cup \{\psi\} \models \varphi.$$

DIMOSTRAZIONE. La dimostrazione va divisa in due parti.

*Supponiamo che* $\Phi \models \to \psi\, \varphi$. Vogliamo dunque verificare che $\Phi \cup \{\psi\} \models \varphi$. Perciò prendiamo una realizzazione $\sigma$ in cui l'interpretazione di tutte le formule di $\Phi \cup \{\psi\}$ sia vera.

Siccome l'interpretazione di ogni formula di $\Phi$ è vera, possiamo dire, per ipotesi, che

$$(\to \psi\, \varphi)^\sigma = \mathbf{V}.$$

Dunque

$$\mathbf{V} = (\to \psi\, \varphi)^\sigma = \to(\psi^\sigma, \varphi^\sigma) = \to(\mathbf{V}, \varphi^\sigma)$$

e perciò $\varphi^\sigma = \mathbf{V}$ per come è definita la funzione $\to$.

*Supponiamo che* $\Phi \cup \{\psi\} \models \varphi$. Vogliamo verificare che $\Phi \models \to \psi\, \varphi$. Perciò prendiamo una realizzazione $\sigma$ in cui l'interpretazione di tutte le formule di $\Phi$ sia vera.

Abbiamo due casi: (1) $\psi^\sigma = \mathbf{F}$ oppure (2) $\psi^\sigma = \mathbf{V}$. Nel caso (1) si ha

$$(\to \psi\, \varphi)^\sigma = \to(\psi^\sigma, \varphi^\sigma) = \to(\mathbf{F}, \varphi^\sigma) = \mathbf{V},$$

per come è definita $\to$.

Nel caso (2) abbiamo che l'interpretazione in $\sigma$ di tutte le formule di $\Phi \cup \{\psi\}$ è vera. Per ipotesi, allora $\varphi^\sigma = \mathbf{V}$. Dunque

$$(\to \psi\, \varphi)^\sigma = \to(\psi^\sigma, \varphi^\sigma) = \to(\mathbf{V}, \mathbf{V}) = \mathbf{V}.$$

Perciò, in entrambi i casi, $(\to \psi\, \varphi)^\sigma = \mathbf{V}$ e dunque $\Phi \models \to \psi\, \varphi$. □

Un altro modo comune di condurre un ragionamento matematico è la *reductio ad absurdum*, cioè assumere come ipotesi la negazione di ciò che si vuole dimostrare e dedurre da essa una contraddizione. Ricordiamo che l'intepretazione di una formula in una realizzazione è vera o falsa e che esistono formule la cui interpretazione è vera e altre (le loro negazioni) la cui interpretazione è falsa.

DEFINIZIONE 10.4. Un insieme di formule $\Phi$ del linguaggio $\mathscr{L}$ si dice *soddisfacibile* se esiste una realizzazione $\sigma = (\mathfrak{A}, \mathsf{a})$ in cui l'interpretazione di tutte le formule di $\Phi$ sia vera. Diremo anche che $\sigma$ soddisfa $\Phi$.

L'insieme $\Phi$ si dirà *non soddisfacibile* in caso contrario.

Abbiamo allora un teorema analogo al precedente.

TEOREMA 10.5. *Sia $\Phi$ un insieme di formule e sia $\varphi$ una formula del linguaggio $\mathscr{L}$. Allora*

$$\Phi \models \varphi \qquad \textit{se e solo se} \qquad \Phi \cup \{\neg\varphi\} \textit{ è non soddisfacibile.}$$

DIMOSTRAZIONE. Dobbiamo ancora dividere la dimostrazione in due parti.

*Supponiamo che* $\Phi \models \varphi$. Vogliamo verificare che $\Phi \cup \{\neg\varphi\}$ non è soddisfacibile.

Sia $\sigma = (\mathfrak{A}, \mathsf{a})$ una realizzazione, dove $\mathfrak{A}$ è una struttura adeguata al linguaggio $\mathscr{L}$ e supponiamo che l'interpretazione di ogni formula di $\Phi$ in $\sigma$ sia vera: se $\sigma$ soddisfa $\Phi \cup \{\neg\varphi\}$ allora necessariamente deve soddisfare $\Phi$. Ma, per ipotesi, $\varphi^\sigma = \mathbf{V}$ e dunque $(\neg\varphi)^\sigma = \mathbf{F}$. Dunque $\sigma$ non soddisfa $\Phi \cup \{\neg\varphi\}$.

*Supponiamo che* $\Phi \cup \{\neg\varphi\}$ *non sia soddisfacibile*. Vogliamo verificare che $\Phi \models \varphi$.

Sia $\sigma$ una realizzazione in cui l'interpretazione di tutte le formule di $\Phi$ è vera. Siccome $\Phi \cup \{\neg\varphi\}$ non è soddisfacibile, l'unica possibilità è che $(\neg\varphi)^\sigma = \mathbf{F}$, da cui $\varphi^\sigma = \mathbf{V}$, come desiderato. □

Un facile esempio di insieme non soddisfacibile è $\{\varphi, \neg\varphi\}$, perché in nessuna realizzazione entrambe le formule possono essere vere.

ESEMPIO 10.6. Consideriamo due formule $\varphi$ e $\psi$ e dimostriamo, usando il teorema di deduzione semantica, che

$$\models \to \psi \to \varphi \psi$$

cioè che la formula $\to \psi \to \varphi \psi$ è valida. Se la scriviamo in modo più tradizionale, essa è $\psi \to (\varphi \to \psi)$ e ne intuiamo chiaramente la natura: se sappiamo $\psi$, allora sappiamo che qualunque cosa implica $\psi$. Ricordiamo che il concetto di implicazione che stiamo usando prescinde da qualunque collegamento di tipo causa-effetto fra le formule.

La dimostrazione è del tutto formale:

$$\models \to \psi \to \varphi \psi \quad \text{se e solo se} \quad \{\psi\} \models \to \varphi \psi \quad \text{se e solo se} \quad \{\psi, \varphi\} \models \psi$$

e l'ultima asserzione è ovvia. Infatti in qualunque realizzazione in cui l'interpretazione delle formule $\varphi$ e $\psi$ sia vera, l'interpretazione di $\psi$ è vera!

## 11. Calcolo proposizionale

L'ultimo esempio della sezione precedente ammette un altro tipo di trattazione. Si può notare che la formula $\to \psi \to \varphi \psi$ è valida *indipendentemente* da quali sono le formule $\varphi$ e $\psi$; queste possono essere vere o false in una data realizzazione, senza che ciò influisca sull'intepretazione di $\to \psi \to \varphi \psi$.

Fissiamo allora un linguaggio $\mathscr{L}$; chiameremo *formule elementari* le formule atomiche o quelle che cominciano con un quantificatore.

DEFINIZIONE 11.1. Una *valutazione* (*proposizionale*) *elementare* è una funzione totale $\mathcal{V}$ dall'insieme delle formule elementari in $\mathscr{L}$ all'insieme $\{\mathbf{V}, \mathbf{F}\}$.

Il primo passo è quello di estendere una valutazione elementare all'insieme di tutte le formule. Ora una formula non elementare è sempre della forma

$$\neg \varphi \qquad \text{oppure} \qquad \bigvee \varphi \psi$$

e quindi possiamo immaginare, per induzione, di aver già definito l'estensione alle formule più corte; porremo quindi

$$\widehat{\mathcal{V}}(\neg \varphi) = \neg(\widehat{\mathcal{V}}(\varphi)) \qquad \text{e} \qquad \widehat{\mathcal{V}}(\bigvee \varphi \psi) = \bigvee(\widehat{\mathcal{V}}(\varphi), \widehat{\mathcal{V}}(\psi)).$$

Nel calcolo di $\widehat{\mathcal{V}}(\varphi)$ ovviamente possiamo usare anche le altre funzioni ($\bigwedge$ e $\to$), come abbiamo già fatto per le intepretazioni.

DEFINIZIONE 11.2. Una formula $\varphi$ si dice *proposizionalmente valida* se, per ogni valutazione elementare $\mathcal{V}$, si ha

$$\widehat{\mathcal{V}}(\varphi) = \mathbf{V}.$$

ESEMPIO 11.3. La formula $\to \psi \to \varphi \psi$ è proposizionalmente valida. Infatti, sia $\mathcal{V}$ una valutazione elementare. Allora

$$\widehat{\mathcal{V}}(\to \psi \to \varphi \psi) = \to(\widehat{\mathcal{V}}(\psi), \widehat{\mathcal{V}}(\to \varphi \psi)) = \to(\widehat{\mathcal{V}}(\psi), \to(\widehat{\mathcal{V}}(\varphi), \widehat{\mathcal{V}}(\psi))) = x.$$

Abbiamo usato $x$ per indicare il valore da calcolare. Se ora consideriamo i quattro casi possibili, otteniamo la tesi.

$$\begin{aligned}
&\text{Se } \widehat{\mathcal{V}}(\varphi) = \mathbf{V} \text{ e } \widehat{\mathcal{V}}(\psi) = \mathbf{V}, && x = \to(\mathbf{V}, \to(\mathbf{V}, \mathbf{V})) = \to(\mathbf{V}, \mathbf{V}) = \mathbf{V} \\
&\text{Se } \widehat{\mathcal{V}}(\varphi) = \mathbf{V} \text{ e } \widehat{\mathcal{V}}(\psi) = \mathbf{F}, && x = \to(\mathbf{F}, \to(\mathbf{V}, \mathbf{F})) = \to(\mathbf{F}, \mathbf{F}) = \mathbf{V} \\
&\text{Se } \widehat{\mathcal{V}}(\varphi) = \mathbf{F} \text{ e } \widehat{\mathcal{V}}(\psi) = \mathbf{V}, && x = \to(\mathbf{V}, \to(\mathbf{F}, \mathbf{V})) = \to(\mathbf{V}, \mathbf{V}) = \mathbf{V} \\
&\text{Se } \widehat{\mathcal{V}}(\varphi) = \mathbf{F} \text{ e } \widehat{\mathcal{V}}(\psi) = \mathbf{F}, && x = \to(\mathbf{F}, \to(\mathbf{F}, \mathbf{F})) = \to(\mathbf{F}, \mathbf{V}) = \mathbf{V}
\end{aligned}$$

e in ogni caso, $\widehat{\mathcal{V}}(\to \psi \to \varphi \psi) = \mathbf{V}$.

Si riconosce chiaramente che un modo per verificare se una formula è proposizionalmente valida è di impiegare le tavole di verità. Questo mostra che per certe formule esiste una procedura "meccanica" per verificarne la validità: è infatti ovvio che una formula proposizionalente valida è valida.

Il fatto importante è che questo non accade per tutte le formule. Si può anzi dimostrare che, in generale, non esiste alcun procedimento meccanico per verificare se una formula è valida o quanto meno conseguenza logica di un insieme di formule. Per questo l'attività di dimostrazione è essenziale: una macchina può "scoprire teoremi" (cioè enunciati che sono conseguenza logica degli assiomi), ma non si può essere certi che li abbia dimostrati tutti.

## ESERCIZI

### Termini e formule

ESERCIZIO 6.1. In un linguaggio in cui c'è un simbolo di relazione binaria $\mathbf{P}$ e un simbolo di funzione binaria $\mathbf{f}$, dire quali delle seguenti successioni di simboli sono formule, quali termini, e quali nulla; in quest'ultimo caso motivare la risposta.

$\forall \mathbf{v}_0 \neg \vee \mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0$ $\quad$ $\mathbf{f}\mathbf{v}_1\mathbf{f}\mathbf{v}_1\mathbf{v}_2$

$\mathbf{f}\mathbf{v}_1\mathbf{f}\mathbf{v}_2$ $\quad$ $\vee\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0\mathbf{v}_3\neg\mathbf{P}\mathbf{v}_0\mathbf{v}_1\mathbf{v}_2$

$\vee\forall \mathbf{v}_0\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0\mathbf{v}_3\neg\mathbf{P}\mathbf{v}_0\mathbf{f}\mathbf{v}_1\mathbf{v}_2$ $\quad$ $\vee\vee\mathbf{f}\mathbf{v}_1\mathbf{v}_2\neg\mathbf{P}\mathbf{v}_3\mathbf{v}_0\neg\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$

$\vee\vee\mathbf{P}\mathbf{v}_1\mathbf{v}_2\neg\mathbf{P}\mathbf{v}_3\mathbf{f}\mathbf{v}_0\mathbf{v}_4\neg\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$

ESERCIZIO 6.2. In un linguaggio in cui c'è un simbolo di relazione binaria $\mathbf{P}$ e un simbolo di funzione unaria $\mathbf{f}$, dire quali delle seguenti successioni di simboli sono formule, quali termini, e quali nulla; in quest'ultimo caso motivare la risposta.

$\forall \mathbf{v}_0 \neg \vee \mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0$ $\quad$ $\mathbf{f}\mathbf{v}_1\mathbf{f}\mathbf{v}_2$

$\vee\forall \mathbf{v}_1\mathbf{P}\mathbf{v}_1\mathbf{v}_0\neg\mathbf{P}\mathbf{f}\mathbf{v}_0\mathbf{f}\mathbf{v}_1$ $\quad$ $\vee\forall \mathbf{v}_0\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0\neg\mathbf{P}\mathbf{v}_0\mathbf{f}\mathbf{v}_1\mathbf{v}_2$

$\vee\vee\mathbf{v}_1\neg\mathbf{P}\mathbf{v}_3\mathbf{f}\mathbf{v}_0\neg\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$ $\quad$ $\vee\vee\mathbf{P}\mathbf{v}_1\mathbf{f}\mathbf{v}_2\neg\mathbf{P}\mathbf{v}_3\mathbf{v}_4\neg\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_3$

$\mathbf{f}\mathbf{f}\mathbf{f}\mathbf{f}\mathbf{v}_0$

ESERCIZIO 6.3. In un linguaggio in cui c'è un simbolo di relazione unaria $\mathbf{P}$ e un simbolo di funzione unaria $\mathbf{f}$, dire quali delle seguenti successioni di simboli sono formule, quali termini, e quali nulla; in quest'ultimo caso motivare la risposta.

$\forall \mathbf{v}_0 \neg \wedge \mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0$ $\quad$ $\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_2$

$\wedge\forall \mathbf{v}_2\mathbf{P}\mathbf{v}_1\neg\mathbf{P}\mathbf{f}\mathbf{v}_0\mathbf{v}_1$ $\quad$ $\wedge\forall \mathbf{v}_0\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_0\neg\mathbf{P}\mathbf{v}_0\mathbf{f}\mathbf{v}_1\mathbf{v}_2$

$\wedge\wedge\mathbf{f}\mathbf{v}_1\mathbf{v}_0\neg\mathbf{P}\mathbf{v}_4\neg\forall \mathbf{v}_0\mathbf{P}\mathbf{f}\mathbf{v}_0\mathbf{v}_2$ $\quad$ $\wedge\wedge\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_2\neg\mathbf{P}\mathbf{v}_3\neg\forall \mathbf{v}_1\mathbf{P}\mathbf{f}\mathbf{v}_1\mathbf{v}_3$

$\mathbf{f}\mathbf{f}\mathbf{v}_0\mathbf{v}_1\mathbf{v}_2$

### Formule con variabili libere

In questi esercizi, si consideri la struttura $\mathfrak{N} = (\mathbb{N}, \{=, <\}, \{+, \times\}, \{0, 1\})$, dove $\mathbb{N}$ denota l'insieme dei numeri naturali, $=$ la relazione binaria di essere lo stesso numero, $<$, $+$ e $\times$ rispettivamente l'ordine, l'addizione e la moltiplicazione tra numeri naturali, 0 e 1 i numeri zero e uno.

Sia $\mathscr{L}$ un linguaggio adatto alla struttura i cui simboli propri siano i predicati $=$, $<$; i simboli per funzione $+$ e $\times$; i simboli per costante $\mathbf{0}$ e $\mathbf{1}$.

ESERCIZIO 6.4. Nel linguaggio $\mathscr{L}$ si scriva una formula $\varphi(\mathbf{v}_0, \mathbf{v}_1)$ con le sole variabili libere indicate tale che $\mathfrak{N} \models \varphi(\mathbf{v}_0, \mathbf{v}_1)[a, b]$ se e solo se: $b - 2a > 0$ e $a$ è divisibile per 2 e per 5.

ESERCIZIO 6.5. Nel linguaggio $\mathscr{L}$ si scriva una formula $\varphi(\mathbf{v}_0, \mathbf{v}_1)$ con le sole variabili libere indicate tale che $\mathfrak{N} \models \varphi(\mathbf{v}_0, \mathbf{v}_1)[a, b]$ se e solo se: $ab \geq 0$ e se $a > 3$, allora $ab > 6$.

ESERCIZIO 6.6. Nel linguaggio $\mathscr{L}$ si scriva una formula $\varphi(\mathbf{v}_0, \mathbf{v}_1)$ con le sole variabili libere indicate tale che $\mathfrak{N} \models \varphi(\mathbf{v}_0, \mathbf{v}_1)[a, b]$ se e solo se: $a - b > 0$ e $a$ è pari se e solo se $b$ è dispari.

ESERCIZIO 6.7. Nel linguaggio $\mathscr{L}$ si scriva una formula $\varphi(\mathbf{v}_0)$ con la sola variabile libera indicata tale che $\mathfrak{N} \models \varphi(\mathbf{v}_0)[a]$ se e solo se: $a$ è multiplo di 2 e $a$ non è multiplo di 3.

ESERCIZIO 6.8. Nel linguaggio $\mathscr{L}$ si scriva una formula $\varphi(\mathbf{v}_0, \mathbf{v}_1)$ con le sole variabili libere indicate tale che $\mathfrak{N} \models \varphi(\mathbf{v}_0, \mathbf{v}_1)[a, b]$ se e solo se: $b \geq 2$, $a > 3$ e $ab$ divide 4.

**Enunciati**

Negli esercizi seguenti il linguaggio ha come simbolo proprio solo quello di una relazione binaria $\mathbf{=}$ la cui interpretazione nella struttura è la relazione di identità.

ESERCIZIO 6.9. Si dica in quali strutture è vero il seguente enunciato

$$\forall \mathbf{v}_0 \exists \mathbf{v}_2 \neg = \mathbf{v}_2 \mathbf{v}_0.$$

ESERCIZIO 6.10. Si dica in quali strutture è vero il seguente enunciato

$$\forall \mathbf{v}_0 \forall \mathbf{v}_1 \neg = \mathbf{v}_1 \mathbf{v}_0.$$

ESERCIZIO 6.11. Si dica in quali strutture è vero il seguente enunciato

$$\forall \mathbf{v}_0 \forall \mathbf{v}_1 = \mathbf{v}_1 \mathbf{v}_0.$$

ESERCIZIO 6.12. Si dica in quali strutture è vero il seguente enunciato

$$\exists \mathbf{v}_0 \forall \mathbf{v}_1 \neg = \mathbf{v}_1 \mathbf{v}_0.$$

ESERCIZIO 6.13. Si dica in quali strutture è vero il seguente enunciato

$$\forall \mathbf{v}_0 \forall \mathbf{v}_1 \exists \mathbf{v}_2 \wedge = \mathbf{v}_1 \mathbf{v}_2 = \mathbf{v}_2 \mathbf{v}_0.$$

ESERCIZIO 6.14. Si dica in quali strutture è vero il seguente enunciato

$$\forall \mathbf{v}_0 \forall \mathbf{v}_1 \exists \mathbf{v}_2 \vee = \mathbf{v}_0 \mathbf{v}_2 \neg = \mathbf{v}_1 \mathbf{v}_0.$$

**Teorema di deduzione**

ESERCIZIO 6.15. Date due formule $\varphi$ e $\psi$, dimostrare che

$$\models \rightarrow \wedge \psi \rightarrow \psi \varphi \varphi.$$

ESERCIZIO 6.16. Date due formule $\varphi$ e $\psi$, dimostrare che

$$\models \rightarrow \neg \varphi \rightarrow \rightarrow \psi \varphi \neg \psi.$$