Cenni di logica e teoria degli insiemi

*

E. Paolini

30 ottobre 2021

INDICE

1 SISTEMI FORMALI

Fin dai tempi di Aristotele si è cercato di individuare e descrivere le leggi che governano la *deduzione*. Si è osservato che combinando tra loro singole informazioni è possibile estrarre da esse nuove infor-

* Puoi scaricare o contribuire a questi appunti su https://github.com/paolini/appunti-vari/

mazioni che in origine non erano disponibili. Ad esempio dalle due informazioni

(P) *in ogni triangolo isoscele gli angoli alla base sono uguali*

(Q) *questo triangolo è isoscele*

si può dedurre

(R) *gli angoli alla base di questo triangolo sono uguali.*

Quello che abbiamo fatto è una *deduzione* (anche detta *derivazione*). Nelle notazioni dei *sistemi formali* P, Q, R si chiamano *formule*. Una volta aggiunta R alle informazioni note, si potranno fare ulteriori derivazioni in cui oltre a P e Q si potrà usare anche R. Questo permette di estendere l'insieme delle conoscenze, a partire da un nucleo iniziale di conoscenze primitive che chiameremo *assiomi*.

sistemi formali

assiomi

Le regole che ci permettono di passare da una o più formule ad una nuova formula, si chiamano *regole di inferenza*. Normalmente le formule sono composte da una sequenza di *simboli* che possono essere scelti tra lettere, cifre o altro. Eventualmente una *grammatica* determinerà come i simboli possono essere utilizzati per comporre le formule (in tal caso le sequenze ammissibili vengono chiamate *formule ben formate*). Le regole di inferenza devono essere le più semplici possibile, di preferenza dovrebbero essere delle regole *meccaniche* in modo che non ci possano essere dubbi su come vadano applicate.

regole di inferenza

simboli

grammatica

formule ben formate

Nell'esempio che abbiamo fatto all'inizio del paragrafo le formule (P), (Q) e (R) sono espresse nel *linguaggio naturale* ovvero nella lingua che siamo abituati ad utilizzare ogni giorno. Formalizzare il linguaggio naturale risulta un compito improbo: sono troppe le ambiguità, i sottointesi, le interpretazioni soggettive, perché si possa pensare di trovare le regole di inferenza di tale linguaggio. Quello che si può fare è costruire un *linguaggio artificiale* che sia sufficientemente semplice da poter essere formalizzato in modo non ambiguo e sufficientemente complesso per ottenere delle derivazioni non banali che possano avere utilità pratica.

linguaggio naturale

linguaggio artificiale

Normalmente il linguaggio artificiale sarà comunque ispirato al linguaggio naturale. E' però possibile costruire dei linguaggi che non abbiano niente a che fare con la lingua naturale, e questo può essere un utile esercizio perché ci mette nella situazione di non poter dare un significato alle formule e di doversi quindi ciecamente e meccanicamente affidare alle regole formali di inferenza. Lo facciamo nel seguente esempio[1].

1 Esempio tratto dal libro *Gödel, Escher, Bach: un'eterna ghirlanda brillante* di Douglas Hofstadter

Esempio 1.1 *(sistema* MIU*).* Prendiamo come simboli le lettere: MIU. Consideriamo ben formate tutte le formule composte da una sequenza di queste lettere. Ad esempio saranno formule ben formate: UMI, MIMMI, IMMUMMMIIUMI. Come regole di inferenza consideriamo le seguenti:

1. $x\mathrm{I} \to x\mathrm{IU}$ (cioé: si può aggiungere una U alla fine delle formule che terminano con I)
2. $\mathrm{M}x \to \mathrm{M}xx$ (cioé: si può raddoppiare la sequenza di simboli dopo una M iniziale)
3. $x\mathrm{III}y \to x\mathrm{U}y$ (cioé: si può rimpiazzare ogni sequenza III con U)
4. $x\mathrm{UU}y \to xy$ (cioé: si può rimuovere la sequenza UU).

Ecco un esempio di derivazione a partire dalla formula MIIMI:

MIIMI (ipotesi)

MIIMIIIMI (regola 2.)
MIIMUMI (regola 3.)
MIIMUMIU (regola 1.)

A partire dalla formula MI è possibile derivare la formula MU?

sistema IVXPU

Esempio 1.2. Si considerino le formule formate dai simboli IVXPU. Si prendano le seguenti regole di inferenza:

1. $x\mathrm{P}y\mathrm{U}z \to x\mathrm{IP}y\mathrm{U}zy$,
2. $x\mathrm{P}y\mathrm{U}z \to x\mathrm{P}y\mathrm{IU}zx$,
3. $x\mathrm{IIIII}y \to x\mathrm{V}y$,
4. $x\mathrm{VV}y \to x\mathrm{X}y$.

Si prenda come assioma: IPIUI. Si riesce ad ottenere la formula VPVUXXV?

Per risolvere la richiesta precedente probabilmente è necessario trovare una *interpretazione* dei simboli utilizzati. Si provi a immaginare che i simboli IVX rappresentino numeri romani... come vanno interpretati i simboli PU per dare un senso comune alle formule del sistema IVXPU?

2 MODELLO, VERITÀ, COMPLETEZZA

Nel sistema formale IVXPU che abbiamo considerato nel paragrafo precedente i simboli possono essere interpretati come operazioni su numeri naturali. Si dice allora che l'insieme dei numeri naturali fornisce un *modello* per questo sistema formale. Il modello associa un valore di *verità* ad ogni formula. Se ogni assioma viene interpretato come un fatto vero, e ogni regola formale mantiene il valore di *verità* delle formule (cioè partendo da una formula vera e applicando una

modello
verità

qualunque regola formale si ottiene un'altra formula vera) allora ogni derivazione del sistema formale produce sicuramente formule vere.

Nel nostro caso l'assioma IPIUI corrisponde alla verità: $1 \cdot 1 = 1$ e la prima regola di inferenza corrisponde alla seguente verità:

$$\text{se } x \cdot y = z \text{ allora } (x+1) \cdot y = z + y.$$

E' dunque chiaro che ogni formula ottenuta con questo sistema formale sarà interpretata come vera. Ci chiediamo: è possibile, in questo sistema, derivare qualunque formula vera? La risposta è negativa in quanto si può osservare che la formula: VIUIIIPII potrebbe essere interpretata come $6 = 3 \cdot 2$ che è vera, ma non può essere dimostrata mediante le regole formali che abbiamo scelto. In questo caso si dice che il sistema è *incompleto* in quanto ci sono formule vere che non possono essere dimostrate.

incompleto

Si potrebbero aggiungere delle regole *grammaticali* per mettere dei vincoli su quali siano le formule ben formate. Si potrebbe ad esempio richiedere che la formula contenga una sola P e una sola U e che la P si trovi sempre prima della U. In questo modo si escludono tutte le formule vere che non posso essere derivate e il sistema si dice *completo*. Il concetto di *completezza* è fondamentale per capire il significato del teorema di Gödel, di cui parleremo brevemente più avanti.

completezza

3 LOGICA DELLE PROPOSIZIONI

Nella *logica delle proposizioni* si aggiunge il concetto di *verità* all'interno del sistema formale. Le formule prendono il nome di *proposizioni* e possono assumere un valore di verità: V=*vero* o F=*falso*. Si introducono quindi i *connettivi logici* ovvero gli operatori $\neg$ (negazione: non), $\wedge$ (congiunzione: e), $\vee$ (disgiunzione: o), $\Rightarrow$ (implicazione: solo se), $\Leftarrow$ (implicazione inversa: se), $\Leftrightarrow$ (doppia implicazione: se e solo se) che applicati ad una (per la negazione) o due proposizioni (per tutti gli altri connettivi) producono una nuova proposizione il cui valore di verità può essere meccanicamente dedotto dal valore di verità delle proposizioni a cui è stato applicato. Essendoci solo un numero finito di combinazioni, possiamo definire le operazioni logiche elencando, in forma di tabella, tutti i valori possibili che possono assumere una coppia di proposizioni P e Q e i corrispondenti valori per le varie operazioni riferite a P e Q:

proposizioni

falso

connettivi logici

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftarrow Q$	$P \Leftrightarrow Q$
V	V	F	V	V	V	V	V
V	F	F	F	V	F	V	F
F	V	V	F	V	V	F	F
F	F	V	F	F	V	V	V

I valori assegnati in questa tabella sono ispirati al significato delle corrispondenti particelle del linguaggio naturale. Si scoprirà, tuttavia, che nel linguaggio naturale le particelle corrispondenti ai connettivi logici hanno una interpretazione che in molti casi dipende dal contesto

e che è quindi molto più complessa e ambigua di quanto non sia il corrispondente connettivo logico. Ma è proprio per evitare le ambiguità e per rendere la verifica di una derivazione un fatto puramente meccanico indipendente dal significato (o *semantica*) delle proposizioni coinvolte, che abbiamo introdotto i linguaggi formali. semantica

Alcuni esempi in cui il linguaggio formale si discosta dall'interpretazione puramente meccanica: "non ho visto niente" (la doppia negazione dovrebbe elidersi), "caffé o cappuccino?" (escludendo la possibilità di scegliere entrambi). L'implicazione logica è probabilmente una delle operazioni che possono sembrare più controverse per quanto riguarda le ultime due righe della tabella che affermano la verità di F⇒V e di F⇒F (da un fatto falso segue qualunque cosa o *ex falso quodlibet*). Per convincerci che in effetti la scelta di questi valori di verità è quella *giusta*, si consideri come esempio la seguente implicazione:

$$n > 5 \Rightarrow n > 3$$

che si può leggere: "se un numero è maggiore di 5 allora è anche maggiore di 3". Siamo convinti che questa implicazione debba essere vera comunque venga scelto il numero n. Scegliendo per n i valori 7, 4 e 2 si ottengono allora le seguenti implicazioni

$$7 > 5 \Rightarrow 7 > 3, \qquad 4 > 5 \Rightarrow 4 > 3, \qquad 2 > 5 \Rightarrow 2 > 3$$

che diventano rispettivamente:

$$\mathrm{V} \Rightarrow \mathrm{V}, \qquad \mathrm{F} \Rightarrow \mathrm{V}, \qquad \mathrm{F} \Rightarrow \mathrm{F}$$

che sono quindi tutte e tre implicazioni vere, coerentemente con quanto riportato nella tabella.

Combinando tra loro più operazioni logiche, si potranno aggiungere altre colonne alla tabella già vista, arrivando facilmente ad ottenere tutte le possibili 16 combinazioni di valori di verità. Ad esempio si potrebbe introdurre la disgiunzione esclusiva (*xor*) con la seguente espressione: $(P \vee Q) \wedge \neg(P \wedge Q)$ (che si interpreta come: P o Q ma non entrambi) la cui colonna di valori di verità risulta essere FVVF. Essendoci solamente un numero finito di possibili valutazioni di una espressione logica, è utile sapere che ogni espressione molto lunga potrà essere certamente semplificata. Le regole più utili che permettono di manipolare le espressioni logiche sono quelle elencate nella Tabella 1. Tutte le righe della tabella possono essere verificate osservando che comunque vengano assegnati dei valori di verità alle proposizioni P, Q ed R si ottiene una proposizione vera (sono, cioè, delle tautologie).

Un esempio di implicazione logica tratta dal linguaggio naturale è la seguente "non aprire se non in caso di pericolo" (si può trovare scritta sul meccanismo manuale di apertura delle porte di un treno). Questa frase ha la struttura $(\neg P) \Leftarrow (\neg Q)$ dove P rappresenta "aprire" e Q rappresenta "in caso di pericolo". Passando alla *contropositiva* la proposizione risulta equivalente a $P \Rightarrow Q$ che se interpretata diventa "se si apre allora è un caso di pericolo". Da notare che l'interpretazione

$\neg\neg P$	$\iff$	P	doppia negazione
$P \wedge Q$	$\iff$	$Q \wedge P$	simmetria
$P \vee Q$	$\iff$	$Q \vee P$	
$\neg(P \wedge Q)$	$\iff$	$(\neg P) \vee (\neg Q)$	formule di De Morgan
$\neg(P \vee Q)$	$\iff$	$(\neg P) \wedge (\neg Q)$	
$(P \wedge Q) \vee R$	$\iff$	$(P \vee R) \wedge (Q \vee R)$	proprietà distributiva
$(P \vee Q) \wedge R$	$\iff$	$(P \wedge R) \vee (Q \wedge R)$	
$(P \Rightarrow Q)$	$\iff$	$(Q \Leftarrow P)$	antisimmetria
$((P \Rightarrow Q) \wedge (Q \Rightarrow P))$	$\iff$	$(P \Leftrightarrow Q)$	doppia implicazione
$\neg(P \Rightarrow Q)$	$\iff$	$P \wedge (\neg Q)$	controesempio
$(P \Rightarrow Q)$	$\iff$	$(\neg Q \Rightarrow \neg P)$	implicazione contropositiva
P	$\implies$	$(Q \Rightarrow P \wedge Q)$	introduzione congiunzione
P	$\implies$	$P \vee Q$	introduzione disgiunzione

Tabella 1: Proprietà degli operatori logici

è corretta, ma non rappresenta un principio di causa-effetto: l'apertura della porta non è la causa del pericolo. Ma visto che la porta va aperta solo in caso di pericolo significa che se la porta viene aperta allora siamo in una situazione di pericolo.

Come si collega il calcolo delle proposizioni ai sistemi formali? Innanzitutto se c'è una formula che corrisponde ad una tautologia essa può essere sempre derivata. Inoltre si può applicare la regola chiamata *modus ponens* ovvero la possibilità di poter dedurre la formula Q se si hanno a disposizione entrambe le formule P e $P \Rightarrow Q$. Le formule della forma $P \Rightarrow Q$ possono essere chiamate *teoremi* e in tal caso P viene chiamata *ipotesi* e Q viene chiamata *tesi*. La derivazione che ci permette di ottenere un teorema viene chiamata *dimostrazione* del teorema.

modus ponens

teoremi

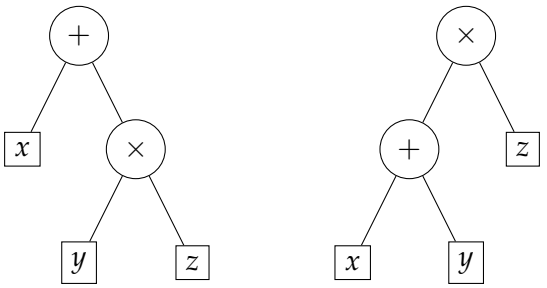
ipotesi

tesi

dimostrazione

4 ALBERO DI VALUTAZIONE

Le formule utilizzate nei linguaggi formali presentano spesso l'uso di operatori *infissi*: il simbolo utilizzato per un operatore binario si trova in mezzo ai due operandi. Questa notazione può presentare ambiguità di lettura, e prevede quindi l'utilizzo di regole di precedenza e di parentesi per determinare la corretta interpretazione della formula. Ad esempio in aritmetica è convenzione che la moltiplicazione abbia precedenza maggiore della somma cosicché la formula $x + y \times z$ viene intesa come $x + (y \times z)$ ed è diversa da $(x + y) \times z$. L'informazione contenuta in una formula sarebbe meglio rappresentata da una struttura ad albero. Ad esempio le due formule $x + (y \times z)$ e $(x + y) \times z$ possono essere rappresentate dai seguenti alberi di valutazione dai quali risulta più chiaro l'ordine di valutazione delle operazioni.



Le regole di interpretazione della precedenza sono convenzionali e possono esserci situazioni in cui non c'è una completa concordanza su come una formula vada interpretata. Quando le formule vengono rappresentate graficamente, inoltre, anche la presentazione tipografica concorre nell'interpretazione dell'ordine delle operazioni. L'uso di spaziature, dimensioni e stili diversi oltre alla posizione spaziale bidimensionale (linee di frazione, incolonnamenti) intendono facilitare l'interpretazione corretta dell'albero di valutazione riducendo la necessità di utilizzare le parentesi.

5 CALCOLO DEI PREDICATI, QUANTIFICATORI

predicati

Possiamo pensare ai *predicati* come a proposizioni in cui compaiono delle variabili. Se una proposizione ha un valore di verità ben definito, il predicato ha invece un valore di verità che dipende dal valore assegnato alle sue variabili. Le variabili da cui dipende un predicato vengono chiamate *variabili libere*. Le variabili libere possono venire *chiuse* (rese *mute*) mediante operatori che agiscono (estraendo un dato di sintesi) al variare della variabile su tutti i suoi possibili valori. Per quanto riguarda il calcolo proposizionale la chiusura delle variabili di un predicato può essere fatta tramite i *quantificatori universale* $\forall$ (leggi: "per ogni") ed *esistenziale* $\exists$ (leggi: "esiste"). Ad esempio il predicato $n > 5 \Rightarrow n > m$ ha due variabili libere: n ed m. Possiamo chiudere la variabile n con il quantificatore universale ottenendo:

variabili libere

quantificatori

$$\forall n \colon n > 5 \Rightarrow n > m$$

che è un predicato con una unica variabile libera m. Il predicato può essere letto così: "per ogni n se n è maggiore di 5 allora n è anche maggiore di m." Il valore di verità di questo predicato dipende dal valore assegnato ad m. Più precisamente il predicato è vero se $m \leq 5$ ed è falso altrimenti. La variabile n è invece diventata muta, che significa che non ha più senso assegnare dei valori alla variabile n in quanto la verità di tale predicato non dipende più da n.

Per quanto riguarda l'intepretazione, la proposizione ottenuta mediante un quantificatore universale $\forall x \colon P(x)$ è vera se $P(x)$ è vera per ogni possibile valore assegnato alla variabile x ed è invece falsa se c'è anche un solo valore che assegnato a x rende falsa $P(x)$. Viceversa nella quantificazione esistenziale $\exists x \colon P(x)$ si ottiene il vero nel caso ci sia almeno un valore di x che renda vera $P(x)$ e si ottiene il falso nel caso non ci sia invece nessun valore di x che renda vera $P(x)$.

Valgono in effetti le seguenti regole formali di scambio dei quantificatori con la negazione logica:

$$\neg\forall x\colon P(x) \iff \exists x\colon \neg P(x)$$
$$\neg\exists x\colon P(x) \iff \forall x\colon \neg P(x).$$

Osserviamo che queste relazioni corrispondono alle leggi di De Morgan per lo scambio della negazione con gli operatori logici di congiunzione e disgiunzione. Infatti l'operatore universale $\forall$ corrisponde ad una congiunzione logica $\wedge$ su tutti i possibili valori del predicato, così come l'operatore esistenziale $\exists$ corrisponde ad una disgiunzione logica $\vee$. Dal punto di vista mnemonico osserviamo che i simboli $\forall$ e $\exists$ si ottengono ruotando di 180 gradi le iniziali delle parole *All* ed *Exists*.

Una variante dell'operatore esistenziale è l'operatore di unicità: la proposizione $\exists!x\colon P(x)$ significa che esiste un *unico* valore di x che rende vero il predicato $P(x)$. Formalmente:

$$\exists!x\colon P(x) \iff \exists x\colon P(x) \wedge \neg\exists y\colon (y \neq x) \wedge P(y).$$

Osserviamo che la precedente definizione utilizza il simbolo $\neq$ che è la negazione dell'operatore di uguaglianza $=$ che verrà introdotto nella sezione seguente.

6 TEORIA DEGLI INSIEMI

Fin'ora abbiamo presentato le regole logiche per la manipolazione dei valori di verità dei predicati. Non abbiamo però ancora costruito nessun predicato né tantomeno abbiamo introdotto gli oggetti che i predicati dovrebbero descrivere.

La teoria degli insiemi serve ad introdurre un *universo* all'interno del quale potremo identificare degli oggetti che possano rappresentare gli enti matematici: numeri, funzioni, relazioni, insiemi. Vedremo però che tutti questi enti matematici potranno essere ricondotti al concetto di insieme: sarà dunque questo il concetto fondamentale che vogliamo descrivere.

Quella che segue è la formalizzazione dovuta ai matematici Zermelo e Fraenkel. Tale teoria viene comunemente chiamata ZF.

insiemi

Intuitivamente gli *insiemi* sono collezioni di elementi. Per costruire un sistema formale che descriva gli insiemi sarà sufficiente introdurre un unico predicato che mette in relazione un elemento con l'insieme che lo contiene:

$$x \in A$$

(leggi: "x è un elemento di A"). Indicheremo con $\notin$ la negazione di questa relazione. Dovremo indicare quali sono le regole formali che ci permetteranno di manipolare questo tipo di formule. Sarà utile poter costruire insiemi di insiemi, quindi in realtà nel predicato precedente x potrebbe a sua volta essere un insieme. Dunque, per semplicità, supporremo che tutti gli oggetti siano insiemi.

A partire dalla relazione di *appartenenza* $\in$ potremo definire le altre relazioni tra insiemi: appartenenza

$$\begin{aligned} A \subset B &\iff \forall x\colon (x \in A \Rightarrow x \in B) \\ A \supset B &\iff \forall x\colon (x \in A \Leftarrow x \in B) \\ A = B &\iff A \subset B \wedge B \subset A. \end{aligned}$$

Il simbolo $\subset$ rappresenta l'*inclusione* tra insiemi. Osserviamo che in altri testi potrà essere invece utilizzato il simbolo $\subseteq$ per rappresentare la stessa relazione rendendo esplicito il fatto che non si esclude che i due insiemi siano uguali (inclusione larga). inclusione

La terza delle regole precedenti si chiama *assioma di estensionalità* e definisce il fondamentale concetto di *uguaglianza*. Il nostro sistema formale sarà dotato di opportune regole di inferenza che garantiscano che se due oggetti sono uguali potranno essere liberamente sostituiti uno con l'altro in qualunque altra formula. Questo garantisce la proprietà transitiva dell'uguaglianza. Si definirà la *disuguaglianza* $\neq$ come negazione dell'uguaglianza. uguaglianza disuguaglianza

Vogliamo anche introdurre le usuali operazioni di *intersezione* $A \cap B$, *unione* $A \cup B$ e *differenza* $A \setminus B$ che possono essere codificate dai seguenti assiomi: intersezione differenza

$$\begin{aligned} x \in A \cap B &\iff (x \in A \wedge x \in B) \\ x \in A \cup B &\iff (x \in A \vee x \in B) \\ x \in A \setminus B &\iff x \in A \wedge x \notin B. \end{aligned}$$

Più in generale possiamo richiedere di poter fare l'unione o l'intersezione di una famiglia $\mathcal{F}$ non vuota di insiemi (una *famiglia* di insiemi non è altro che un insieme di insiemi):

$$\begin{aligned} x \in \bigcap \mathcal{F} &\iff \forall A \in \mathcal{F}\colon x \in A \\ x \in \bigcup \mathcal{F} &\iff \exists A \in \mathcal{F}\colon x \in A. \end{aligned}$$

Spesso si usano le seguenti notazioni più espressive:

$$\bigcap \mathcal{F} = \bigcap_{A \in \mathcal{F}} A, \qquad \bigcup \mathcal{F} = \bigcup_{A \in \mathcal{F}} A.$$

Per avere un primo oggetto su cui agire definiamo l'*insieme vuoto*, denotato dal simbolo $\emptyset$, mediante il seguente assioma. insieme vuoto

Assioma 6.1 (insieme vuoto)**.** *Esiste* $\emptyset$ *tale che*

$$\neg\exists x\colon x \in \emptyset.$$

Osserviamo che le operazioni definite in precedenza, se applicate all'insieme vuoto, non ci permettono di ottenere nuovi insiemi. Per avere insiemi con un solo elemento introduciamo l'insieme *singoletto* $\{y\}$ cioè un insieme contenente un unico oggetto y: singoletto

$$x \in \{y\} \iff x = y.$$

A questo punto utilizzando l'unione possiamo già ottenere, per elencazione, insiemi con un numero arbitrario (ma finito) di elementi, ad esempio:

$$\{a, b, c\} = \{a\} \cup \{b\} \cup \{c\}.$$

Con le operazioni che abbiamo introdotto è già possibile descrivere infiniti insiemi tra loro diversi. Ad esempio questi sono quattro insiemi diversi:

$$\emptyset, \quad \{\emptyset\}, \quad \{\{\emptyset\}, \emptyset\}, \quad \{\{\emptyset\}, \{\{\emptyset\}\}\}$$

mentre ognuno dei seguenti coincide con uno (quale?) dei precedenti:

$$\{\emptyset, \emptyset\}, \quad \{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \emptyset\}\}.$$

Possiamo anche definire un insieme mediante una qualunque proprietà che caratterizzi i suoi elementi.

Assioma 6.2 (specificazione)**.** *Se A è un insieme e $P(x)$ un predicato, allora esiste un insieme B denotato con $B = \{x \in A \colon P(x)\}$ tale che si abbia:*

$$b \in B \iff (b \in A) \wedge P(b).$$

Osserviamo che viene richiesto a priori un insieme ambiente A sul quale viene ristretta la caratterizzazione. Questo significa che questo assioma non può generare insiemi più grandi di quelli già esistenti.

Molte delle definizioni precedenti possono essere date mediante l'assioma di specificazione. Ad esempio intersezione e differenza si possono ricondurre all'unione:

$$A \cap B = \{x \in A \cup B \colon x \in A \wedge x \in B\}, A \setminus B \quad = \{x \in A \colon x \notin B\}.$$

7 IL PARADOSSO DI RUSSEL

La formalizzazione ZF che abbiamo esposto ha avuto una storia travagliata. Nel 1902 Frege aveva tentato di assiomatizzare la teoria degli insiemi introducendo l'assioma di specificazione nella forma seguente.

Assioma 7.1 (specificazione ingenua)**.** *Se $P(x)$ è un predicato allora esiste un insieme B denotato con $B = \{x \colon P(x)\}$ tale che*

$$x \in B \iff P(b).$$

Questo assioma è molto più potente di quello introdotto in precedenza perché non vincola la specificazione agli elementi di un insieme già costruito. In realtà Russel (ma prima ancora Zermelo) si accorse che tale assioma è talmente potente da portare ad una contraddizione, che fa cadere l'intera teoria ingenua degli insiemi (chiamiamo così la teoria degli insiemi come era stata introdotta da Cantor e poi formalizzata da Frege[2]).

2 Questo un estratto della lettera di Russel a Frege (16 giugno 1902): "Mi trovo in completo accordo con lei in tutte le parti essenziali, in particolare quando lei rifiuta ogni elemento psicologico dando un grande valore all'ideografia [Begriffsschrift] per il fondamento della matematica e della logica formale [...] c'è solo un punto dove ho incontrato una difficoltà [...]" La risposta di Frege (22 giugno 1902): "La sua scoperta della contraddizione mi ha causato una grandissima sorpresa e, direi, costernazione, perché ha scosso le basi su cui intendevo costruire l'aritmetica."

Paradosso 7.2 (Russel)**.** *Si consideri l'insieme (formalizzato in maniera ingenua)*

$$R = \{x \colon x \notin x\}.$$

Allora $R \in R \iff R \notin R$*. Assurdo.*

Il paradosso di Russel può essere espresso anche nella lingua naturale. Una delle sue accezioni più note si chiama *Paradosso del barbiere* e si enuncia come segue. Il *barbiere* è quella persona che fa la barba alle persone che non se la fanno da se. Il barbiere si fa la barba da se?

Un'altro modo di esprimere il paradosso di Russel nel linguaggio naturale riguarda l'utilizzo degli aggettivi ed è il seguente. Diremo che un aggettivo è *autologico* se esso stesso soddisfa la proprietà che descrive. Ad esempio l'aggettivo *polisillabico* è polisillabico e dunque è autologico. Lo stesso vale per l'aggettivo *sdrucciolo* che è autologico in quanto è una parola con l'accento sulla terz'ultima sillaba. Gli aggettivi che non sono autologici li chiameremo *eterologici*. Ci si può allora chiedere se l'aggettivo *eterologico* è eterologico. Anche in questo caso si arriverà ad un paradosso perché se *eterologico* fosse eterologico allora sarebbe autologico cioè non eterologico. Viceversa se eterologico fosse autologico allora sarebbe eterologico cioè non autologico.

Il paradosso di Russel non si applica alla teoria ZF che abbiamo introdotto in quanto in tale teoria l'assioma di specificazione richiede un insieme ambiente in cui il predicato viene valutato. Se fissiamo un insieme *ambiente* U poossiamo definire il seguente:

$$R = \{x \in U \colon x \notin x\}.$$

In tal caso abbiamo che $R \in R$ se e solo se $(R \in U) \wedge (R \notin R)$. In particolare se fosse $R \in R$ avremmo un assurdo. Ma non è invece assurdo che $R \notin R$, infatti in tal caso potrà essere (anzi, dovrà essere) $R \notin U$. Non abbiamo ottenuto un paradosso, ma abbiamo scoperto che dato un qualunque insieme U esiste un insieme R che non sta in U. Questo significa che non esiste l'insieme *universo*, cioè un insieme che contiene tutti gli insiemi. Osserviamo che l'insieme universo sarebbe il complementare dell'insieme vuoto, e questo è il motivo per cui non è possibile definire il complementare di un insieme ma ci si limita a definire la differenza tra insiemi.

universo

La relazione $x \in x$ potrebbe di per se sembrare contraddittoria. Come è possibile che un insieme contenga se stesso come elemento? Se ad esempio avessimo $x = \{x\}$ si avrebbe $x = \{\{x\}\} = \{\{\{x\}\}\} \dots$ e così via in una discesa infinita che non avrebbe mai termine. La possibilità che esistano insiemi di questo tipo è piuttosto fastidiosa ed è per questo che si pone l'assioma di *fondazione* (o di *regolarità*) che afferma in particolare che non esistono insiemi x tali che $x \in x$. Più in generale l'assioma di fondazione evita che sia possibile costruire una catena discendente infinita di insiemi che siano elemento uno dell'altro:

$$\dots \in x_n \in \dots \in x_2 \in x_1.$$

Osserviamo però che anche assumendo che $x \notin x$ sia sempre vera, il paradosso di Russel rimane valido, in tal caso infatti $R = \{x \colon x \notin x\}$

dovrebbe contenere tutti gli insiemi e quindi dovrebbe essere $R \in R$... che abbiamo escluso.

Un altro modo per dimostrare che è sempre possibile costruire un insieme *più grande* di un insieme dato si ottiene dall'insieme potenza (che vediamo subito) tramite il teorema di Cantor (che vedremo più avanti).

L'assioma dell'insieme potenza, serve a garantire l'esistenza dell'*insieme delle parti*. Se X è un qualunque insieme si può considerare $\mathcal{P}(X)$ come l'insieme dei sottoinsiemi di X: insieme delle parti

$$A \in \mathcal{P}(X) \iff A \subset X.$$

L'insieme $\mathcal{P}(X)$ si chiama anche *insieme potenza* e viene a volte indicato con 2^X in quanto se X ha n elementi allora $\mathcal{P}(X)$ ha 2^n elementi. Ad esempio se $X = \{a, b, c\}$ ha tre elementi, l'insieme delle parti ha otto elementi:

$$\mathcal{P}(X) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Inteso che $\{\} = \emptyset$ osserviamo che l'insieme vuoto è sottoinsieme di qualunque altro insieme (verificarlo tramite la definizione), dunque appartiene sempre all'insieme delle parti. L'insieme delle parti risulta fondamentale per poter esprimere la *logica del secondo ordine* ovvero la possibilità di poter formulare predicati sui sottoinsiemi di un insieme invece che solamente sui suoi elementi.

8 RELAZIONI

Definiamo la *coppia ordinata* (a, b) come un oggetto (un insieme, visto che abbiamo deciso che tutti gli oggetti matematici sono insiemi) con la seguente proprietà: coppia ordinata

$$(a, b) = (c, d) \iff a = c \wedge b = d. \tag{1}$$

In particolare $(a, b) \neq (b, a)$ se $a \neq b$ cioè l'ordine dei due elementi è importante. Formalmente si potrebbe definire $(a, b) = \{\{a\}, \{a, b\}\}$, si provi per esercizio a dimostrare che con questa definizione vale la proprietà (1). Se A e B sono insiemi dati, l'insieme di tutte le coppie di elementi presi il primo da A e il secondo da B si indica con $A \times B$ e si chiama *prodotto cartesiano*: prodotto cartesiano

$$x \in A \times B \iff \exists a \in A, \exists b \in B \colon x = (a, b).$$

Se A ha n elementi e B ha m elementi, il prodotto $A \times B$ ha $n \cdot m$ elementi. Ad esempio se $A = \{a, b, c\}$ ha tre elementi e $B = \{a, b\}$ ha due elementi, il prodotto ha sei elementi:

$$A \times B = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b)\}.$$

Una *relazione* R tra gli elementi di un insieme A e gli elementi di un insieme B non è altro che un sottoinsieme del prodotto cartesiano: $R \subset A \times B$. Scriveremo xRy quando $(x, y) \in R$. Ad esempio su un insieme relazione

di numeri potremmo considerare come R la relazione d'ordine $\leq$ per cui scriveremo $x \leq y$ quando $(x, y) \in R$. Le relazioni da un insieme in sé stesso possono eventualmente avere particolari caratteristiche come essere: *transitive* ($xRy \land yRz \implies xRz$), *simmetriche* ($xRy \implies yRx$), *riflessive* ($xRx$). Come esercizio si provi a pensare alla relazione tra persone xAy definita dalla frase "x ama y". Si consideri il significato delle proprietà transitiva, simmetrica e riflessiva di tale relazione.

Possiamo pensare ad una coppia (a, b) come ad una freccia che parte da a e arriva in b: $a \mapsto b$. Potremmo scrivere più espressivamente $(a, b) \in R$ come $a \overset{R}{\mapsto} b$. In questo modo una relazione su $A \times B$ risulta essere un insieme di frecce che partono da elementi di A ed arrivano su elementi di B. La rappresentazione che si ottiene prende anche il nome di *grafo orientato*. Si provi ad interpretare *graficamente* le proprietà transitiva, simmetrica e riflessiva di un grafo.

relazione inversa

Ogni relazione può essere *invertita* semplicemente scambiando il ruolo dei due insiemi A e B. Se R è una relazione e vale xRy per la relazione inversa R' si avrà $yR'x$. Pensando ad una relazione R come un insieme di frecce $x \overset{R}{\mapsto} y$, la relazione inversa R' risulta essere lo stesso insieme di frecce ma con la direzione opposta $y \overset{R'}{\mapsto} x$.

Nel seguito saremo interessati ad identificare alcune tipologie di relazioni.

Definizione 8.1 (relazione di equivalenza)**.** *Una relazione $\sim$ su un insieme A si dice essere una* relazione di equivalenza *se verifica le seguenti proprietà per ogni $a, b, c \in A$:*

relazione di equivalenza

1. $a \sim a$ *(proprietà riflessiva);*
2. $(a \sim b) \implies (b \sim a)$ *(proprietà simmetrica);*
3. $((a \sim b) \land (b \sim c)) \implies (a \sim c)$ *(proprietà transitiva).*

Definizione 8.2 (relazione d'ordine)**.** *Una relazione $\leq$ definita su un insieme A si dice essere una* relazione d'ordine *verifica le seguenti proprietà per ogni $a, b, c \in A$:*

relazione d'ordine

1. $a \leq a$ *(proprietà riflessiva);*
2. $((a \leq b) \land (b \leq a)) \implies (a = b)$ *(proprietà antisimmetrica);*
3. $((a \leq b) \land (b \leq c)) \implies (a \leq c)$ *(proprietà transitiva).*

Se inoltre vale la seguente per ogni $a, b \in A$:

4. $(a \leq b) \lor (b \leq a)$

diremo che l'ordinamento è totale*.*

9 FUNZIONI

funzioni

Le *funzioni* sono le relazioni *univoche* cioè quelle relazioni f in $A \times B$ che mandando (nel senso delle frecce) ogni elemento $a \in A$ in uno ed un solo elemento $b \in B$:

$$\forall a \in A \colon \exists! b \in B \colon a \overset{f}{\mapsto} b.$$

Tale unico elemento $b \in B$ associato all'elemento $a \in A$ viene chiamato *immagine* di a tramite f e viene indicato con $b = f(a)$. Una funzione definita da A in B si indica con $f\colon A \to B$. L'insieme A viene chiamato *dominio* e l'insieme B *codominio*. dominio

Le funzioni vengono spesso utilizzate per rappresentare delle trasformazioni. Possiamo pensare ad una funzione come ad una scatola nera (un macinino) a cui possiamo dare in pasto elementi dell'insieme A (*input*) e otteniamo come risposta elementi dell'insieme B (*output*). codominio

Se l'output (codominio) di una funzione f coincide con l'input (dominio) di una funzione g, cioè se $f\colon A \to B$ e $g\colon B \to C$ possiamo comporre le due funzioni per ottenere una funzione $g \circ f\colon A \to C$: *funzione composta*

$$(g \circ f)(x) = g(f(x)) \qquad x \overset{f}{\mapsto} f(x) \overset{g}{\mapsto} g(f(x)).$$

Vedremo come la composizione ci permette di costruire innumerevoli funzioni componendo tra loro poche funzioni elementari, così come si può costruire un edificio utilizzando semplici mattoni. Ovviamente sarà importante conoscere a fondo tutte le caratteristiche dei mattoni (proprietà delle funzioni elementari) e sarà pure importante capire come tali proprietà si combinano quando mettiamo insieme i diversi blocchi.

Uno dei problemi più importanti a cui si può probabilmente ricondurre qualunque problema matematico è quello dell'invertibilità di una funzione: data $f\colon A \to B$ trovare una funzione $g\colon B \to A$ tale che se $x \overset{f}{\mapsto} y$ allora $y \overset{g}{\mapsto} x$. Se ad esempio io so qual è la traiettoria di un proiettile in funzione dell'angolo di tiro, mi chiedo quale angolo devo scegliere per centrare un determinato bersaglio. Oppure (altro esempio) data la funzione $f(x) = x^2$ (definita su un qualche insieme numerico) dire se è possibile trovare x tale che $f(x) = 2$ (definizione della radice quadrata). Oppure ancora: se xAy è la relazione "x ama y" e se io sono y sarei interessato a trovare gli x tali che xAy.

Per poter invertire una funzione $f\colon A \to B$ abbiamo la necessità di verificare due differenti proprietà: che per ogni $b \in B$ esista un elemento $a \in A$ tale che $f(a) = b$ (surgettività) e che tale elemento a sia unico (iniettività). Più precisamente diremo che $f\colon A \to B$ è *surgettiva* se surgettiva

$$\forall b \in B\colon \exists a \in A\colon f(a) = b$$

ed è *iniettiva* se iniettiva

$$\forall a \in A, \forall a' \in A\colon (f(a) = f(a') \implies a = a').$$

Se una funzione $f\colon A \to B$ è iniettiva e surgettiva allora si dice che f è *bigettiva* o *invertibile*. La funzione $g\colon B \to A$ che ad ogni $b \in B$ associa l'unico $a \in A$ tale che $f(a) = b$ si chiama *funzione inversa* di f. Tale funzione g si indica anche con il simbolo f^{-1} ed ha le proprietà bigettiva

$$\forall x \in A\colon g(f(x)) = x, \qquad \forall y \in B\colon f(g(y)).$$

La funzione inversa di f è quindi anch'essa invertibile e l'inversa dell'inversa è f stessa: $(f^{-1})^{-1} = g^{-1} = f$.

L'insieme di tutte le funzioni $f\colon A \to B$ viene denotato con B^A. L'insieme di tutte le funzioni $f\colon A \to A$ potrà essere denotato con $A!$ o (più comunemente) con $S(A)$ (si veda l'esercizio 12.6 per avere una motivazione di tali notazioni).

Se $f\colon X \to Y$ è una funzione e se $A \subset X$ si definisce l'insieme $f(A)$, chiamato *immagine* di A tramite f come: immagine

$$f(A) = \{f(x)\colon x \in A\}$$

se invece $B \subset Y$ si definisce l'insieme $f^{-1}(B)$, chiamato *controimmagine* di B tramite f come: controimmagine

$$f(B) = \{x \in A\colon f(x) \in B\}.$$

Notiamo innanzitutto che la prima definizione non rientra esattamente nell'assioma di specificazione ma è un modo più immediato per intendere la seguente definizione che è invece perfettamente valida:

$$f(A) = \{y \in B\colon \exists x \in A\colon f(x) = y\}.$$

Notiamo inoltre che questa definizione rappresenta un *abuso di notazione*. Infatti avevamo già dato una definizione per il simbolo $f(x)$. Questa notazione va quindi utilizzata solo se il contesto rende chiaro il fatto che A va inteso come un sottoinsieme del dominio di f e non come un elemento di tale dominio.

Se $A = X$ è l'intero dominio della funzione l'insieme $f(X)$ si chiama *immagine di* f. Possiamo allora osservare che una funzione $f\colon X \to Y$ risulta essere surgettiva se e solo se $f(X) = Y$. Se prendiamo un qualunque $y \in Y$ possiamo considerare l'insieme $f^{-1}(\{y\})$ che è sempre definito, anche se f non fosse invertibile. Se tale insieme ha sempre almeno un elemento significa che la funzione è surgettiva. Se tale insieme ha sempre non più di un elemento significa che la funzione è iniettiva. Se tale insieme ha sempre esattamente un elemento allora la funzione è invertibile e si ha $f^{-1}(\{y\}) = \{f^{-1}(y)\}$.

Questo abuso di notazione (inserire un insieme dove dovrebbe starci un singolo elemento) potrà essere utilizzato anche con gli operatori infissi. Una operazione, rappresentata ad esempio dal simbolo $+$, può essere pensata come ad una funzione che agisce su una coppia di valori: $+\colon X \times Y \to Z$. La notazione $x + y$ serve quindi ad abbreviare la notazione $+(x, y)$. Anche in questo caso potrà capitare che al posto di x o di y o di entrambi, si inserisca un insieme di valori:

$$\begin{aligned} A + y &= \{x + y\colon x \in A\}, \\ x + B &= \{x + y\colon y \in B\}, \\ A + B &= \{x + y\colon x \in A, y \in B\}. \end{aligned}$$

In tutti questi casi il risultato è un insieme di valori, invece che un singolo valore.

In maniera simile, questo abuso viene attuato anche con le relazioni. Se ad esempio abbiamo una relazione $x \leq y$, e A, B sono insiemi, si potrà intendere che valgano le seguenti notazioni:

$$\begin{aligned} x \leq B &\iff (\forall y \in B \colon x \leq y), \\ A \leq y &\iff (\forall x \in A \colon x \leq y), \\ A \leq B &\iff (\forall x \in A, \forall y \in B \colon x \leq y). \end{aligned}$$

Esercizio 9.1. Se R è una relazione tra A e B si dia una definizione di $R(C) \subset B$ quando $C \subset A$ in modo che tale definizione coincida con la definizione di *immagine* se R è una funzione. Si osservi che con tale definizione la controimmagine di un insieme tramite una funzione f non è altro che l'immagine tramite la relazione inversa f^{-1} (ricordando che ogni funzione essendo una relazione ha una relazione inversa).

10 I NUMERI NATURALI

Teorema 10.1 (assiomi di Peano)**.** *L'insieme $\mathbb{N}$ dei numeri naturali è un insieme su cui è data una funzione $\sigma \colon \mathbb{N} \to \mathbb{N}$ e un elemento $0 \in \mathbb{N}$ (chiamato* zero*) che soddisfano le seguenti proprietà.* *zero*

1. *σ è iniettiva;*
2. *non esiste $n \in \mathbb{N}$ tale che $\sigma(n) = 0$;*
3. *(assioma di induzione) per ogni $A \subset \mathbb{N}$ se*
   a) *$0 \in A$;*
   b) *$\forall n \in \mathbb{N} \colon n \in A \implies \sigma(n) \in A$;*

   allora $A = \mathbb{N}$.

I numeri naturali sono i numeri utilizzati per *contare*. La funzione $\sigma \colon \mathbb{N} \to \mathbb{N}$ rappresenta il successore di un numero naturale, quindi quando avremo definito la somma vedremo che sarà $\sigma(n) = n + 1$. Il fatto che σ sia iniettiva serve a esprimere il fatto che durante un conteggio non si torna mai ad un numero già utilizzato. Lo zero è inoltre particolare perché esso non è il successore di nessun altro numero naturale (questo viene espresso dal secondo assioma). L'ultimo assioma serve a garantire che partendo da zero e cominciando a considerare il suo successore (che si chiama $1 = \sigma(0)$) e poi il successore del successore (chiamato $2 = \sigma(1)$) e così via, si ottengono tutti i numeri naturali. Vedremo, ad esempio, che l'insieme $\mathbb{Q}^+$ dei numeri razionali non negativi soddisfa i primi due assiomi di Peano se si pone $\sigma(q) = q + 1$ ma non soddisfa il terzo assioma in quanto la frazione $1/2$ non viene mai raggiunta partendo da 0 e sommando 1.

L'esistenza di un insieme che soddisfa gli assiomi di Peano non è garantita dagli assiomi visti finora. Sarà necessario un assioma apposito. Tale assioma si chiama *assioma di infinito* in quanto, come vedremo nel Teorema 13.3, è equivalente a supporre l'esistenza di un qualunque insieme infinito.

Assioma 10.2 (di infinito)**.** *Esiste un insieme* $\mathbb{N}$ *che soddisfa gli assiomi di Peano.*

La proprietà induttiva dei numeri naturali permette di definire le funzioni su $\mathbb{N}$ utilizzando le *definizioni per induzione*, come nel seguente.

Teorema 10.3 (definizione per induzione)**.** *Sia* A *un insieme,* $\alpha \in A$ *e* $g\colon \mathbb{N} \times A \to A$*. Allora esiste un unica funzione* $f\colon \mathbb{N} \to A$ *tale che*

$$\begin{cases} f(0) = \alpha, \\ \forall n \in \mathbb{N}\colon f(\sigma(n)) = g(n, f(n)). \end{cases} \tag{2}$$

(La parentesi graffa serve ad indicare che entrambe le condizioni devono essere soddisfatte contemporaneamente).

Intuitivamente dopo aver definito $f(0) = \alpha$ si potrà definire $f(1) = g(0, \alpha)$, $f(2) = g(1, f(1))$, $f(3) = g(2, f(2))$ etc. Per la proprietà induttiva dei numeri naturali la funzione f risulterà definita univocamente su tutti i numeri naturali. Riportiamo di seguito una dimostrazione più formale, che ci permette di osservare come viene utilizzata in pratica la definizione di funzione.

Dimostrazione. L'idea della dimostrazione è di definire f come la "più piccola" relazione che soddisfa le condizioni (2). Si prenderà poi l'insieme su cui f è definita univocamente e si dimostrerà che è tutto $\mathbb{N}$ concludendo quindi che è una funzione $f\colon \mathbb{N} \to A$.

Consideriamo l'insieme di tutte le relazioni tra N e A che soddisfano (2):

$$\mathcal{F} = \{R \subset \mathbb{N} \times A\colon (0, \alpha) \in R, \\ (n, a) \in R \implies (\sigma(n), g(n, a)) \in R\}$$

e definiamo

$$f = \bigcap \mathcal{F}.$$

Chiaramente $f \subset \mathbb{N} \times A$ è una relazione. E' anche facile verificare che $f \in \mathcal{F}$ (si ragioni sulla definizione di intersezione). Posto

$$D = \{n \in \mathbb{N}\colon \exists! a \in A\colon (n, a) \in f\}$$

vogliamo dimostrare che $D = \mathbb{N}$. Lo possiamo fare utilizzando l'assioma di induzione. Visto che $f \in \mathcal{F}$ sappiamo che $(0, \alpha) \in f$. Se esistesse $a \neq \alpha$ tale che $(0, a) \in f$ allora potrei considerare la relazione $R = f \setminus \{(0, a)\}$ e osservare che $R \in \mathcal{F}$ (visto che $a \neq \alpha$ questo non inficia la condizione $(0, \alpha) \in R$ e visto che $\sigma(n) \neq 0$ non viene inficiata neanche la condizione $(n, a) \in R \implies (\sigma(n), g(n, a)) \in R$. Siccome $R \in \mathcal{F}$ e $R \subset f$ otteniamo una contraddizione in quanto essendo $f = \bigcap \mathcal{F}$ si dovrebbe avere $f \subset R$ e quindi $f = R$, cosa che non è. Abbiamo quindi mostrato che $0 \in D$ che è la prima condizione nell'assioma di induzione.

Supponiamo ora di sapere che $n \in D$: dobbiamo allora dimostrare che anche $\sigma(n) \in D$. Ma se $n \in D$ significa che esiste un

unico $a \in A$ tale che $(n, a) \in f$. Essendo $f \in \mathcal{F}$ questo implica che $(\sigma(n), g(n, a)) \in R$ e quindi esiste $b = g(n, a)$ tale che $(\sigma(n), b) \in R$. Dobbiamo mostrare che tale y è unico. Se ci fosse $c \neq b$ tale che $(\sigma(n), c) \in f$ potrei definire (analogamente a come abbiamo fatto nel passo precedente) $R = f \setminus \{(\sigma(n), c)\}$. Anche in questo caso possiamo dimostrare che $R \in \mathcal{F}$. Certamente $(0, a) \in f$ ed essendo $\sigma(n) \neq 0$ possiamo affermare che $(0, a) \in R$. Inoltre se $(k, d) \in R$ allora certamente $(k, d) \in f$ (in quanto $R \subset f$) e quindi $(\sigma(k), g(k, d)) \in f$ dunque basta escludere che sia $(\sigma(k), g(k, d)) = (\sigma(n), c)$. Questo succede in quanto se fosse $\sigma(k) = \sigma(n)$ avremmo $k = n$ e quindi $d = a$ in quanto $n \in D$. Ma allora si avrebbe $g(k, d) = g(n, a) = b \neq c$.

L'assioma di induzione può dunque essere applicato e ci permette di concludere che $D = \mathbb{N}$. Significa che f è univocamente definita su tutto $\mathbb{N}$ e quindi è una funzione $f \colon \mathbb{N} \to A$ che soddisfa (2) in quanto $f \in \mathcal{F}$. □

Con questo tipo di definizioni è possibile definire per induzione l'operazione $+$ (addizione) facendo in modo che valga la seguente proprietà:

$$\begin{cases} n + 0 = n \\ n + \sigma(m) = \sigma(n + m). \end{cases}$$

In particolare si ottiene $\sigma(n) = n + 1$ e quindi d'ora in avanti non useremo più la funzione σ ma useremo sempre l'addizione. Analogamente sarà possibile definire la moltiplicazione $\cdot$ in modo che valga

$$\begin{cases} n \cdot 0 = 0 \\ n \cdot \sigma(m) = n \cdot m + n. \end{cases}$$

Si potrà poi verificare (cosa elementare ma non semplice) che le operazioni così definite soddisfano le ben note proprietà:

1. $n + 0 = n$, $n \cdot 1 = n$ (esistenza degli elementi neutri);
2. $n + m = m + n$, $n \cdot m = m \cdot n$ (proprietà commutativa);
3. $n \cdot (a + b) = n \cdot a + n \cdot b$ (proprietà associativa).

Si potrà anche definire una relazione d'ordine $\leq$ tramite la condizione

$$n \leq m \iff \exists k \in \mathbb{N} \colon m = n + k.$$

La relazione $\geq$ si definisce come la relazione inversa di $\leq$. La relazione $<$ si definisce richiedendo che sia $x \leq y \wedge x \neq y$ e la relazione $>$ è definita come l'inversa di $<$.

Come esempio di applicazione della definizione per induzione definiamo il *fattoriale* $n! = 1 \cdot 2 \dots n$ (il prodotto dei numeri naturali da 1 a n). Per definire tale funzione $\mathbb{N} \to \mathbb{N}$ in maniera rigorosa osserviamo che il prodotto dei numeri da 1 a $n + 1$ può essere definito come il

prodotto dei numeri da 1 a n moltiplicato per $n+1$. Imponendo poi che[3] $0! = 1$, si ottiene una caratterizzazione univoca:

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n! \end{cases}$$

Si tratta di applicare il Teorema 10.3 con $A = \mathbb{N}$, $\alpha = 1$, $g(n, a) = (n+1) \cdot a$ per garantire che esiste una unica funzione $\mathbb{N} \to \mathbb{N}$, $n \mapsto n!$, che soddisfa queste proprietà.

In maniera simile si potrà definire per ogni $n, m \in \mathbb{N}$ l'elevamento a potenza n^m in modo che valga[4]

$$\begin{cases} n^0 = 1 \\ n^{m+1} = n \cdot n^m. \end{cases}$$

La proprietà induttiva dei numeri naturali è equivalente al seguente.

Teorema 10.4 (principio di induzione)**.** *Sia $P(n)$ un predicato sui numeri naturali $n \in \mathbb{N}$. Se valgono le seguenti condizioni*

1. *$P(0)$ è vera*
2. *$P(n) \implies P(n+1)$*

allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Si consideri l'insieme $A = \{n \in \mathbb{N} \colon P(n) \text{ è vera}\}$ e si applichi il terzo assioma di Peano per verificare che $A = \mathbb{N}$. □

Esercizio 10.5. La somma $S(n) = 1 + 2 + \cdots + n$ dei naturali da 1 fino a n può essere definita come quella unica funzione che soddisfa le proprietà

$$\begin{cases} S(0) = 0 \\ S(n+1) = S(n) + (n+1). \end{cases}$$

Dimostrare che $S(n) = n \cdot (n+1)/2$.

Esercizio 10.6. Dimostrare che per la somma $Q(n) = 1^2 + 2^2 + \cdots + n^2$ (somma dei quadrati dei naturali da 1 a n) vale la formula $Q(n) = n \cdot (n+1) \cdot (2n+1)/6$.

Potrà risultare utile utilizzare le seguenti varianti del principio di induzione

3 E' chiaro che deve essere $1! = 1$ e di conseguenza se vale $(n+1)! = (n+1) \cdot n!$ dovrà essere $0! = 1$. D'altra parte è naturale che il prodotto di un insieme vuoto di numeri sia l'elemento neutro del prodotto, così come la somma di zero numeri è l'elemento neutro della somma.

4 Si noti che stiamo definendo $0^0 = 1$. Alcuni testi lasciano indefinita questa operazione ma in realtà la formula è giustificata dal fatto che 0^0 è un prodotto di 0 fattori e quindi, come $0!$, deve valere 1. Questo viene confermato dal fatto che n^m è il numero di funzioni da un insieme con m elementi in un insieme con n elementi e su un dominio vuoto è definita una unica funzione (la funzione vuota) qualunque sia il codomonio.

Teorema 10.7 (principio di induzione (variante))**.** *Sia $P(n)$ un predicato definito sui numeri naturali n non inferiori a $n_0 \in \mathbb{N}$. Se*

1. *$P(n_0)$ è vero*
2. *$P(n) \implies P(n+1)$ per ogni $n \geq n_0$*

allora $P(n)$ è vero per ogni $n \geq n_0$.

Teorema 10.8 (principio di induzione forte)**.** *Sia $P(n)$ un predicato definito sui numeri naturali $n \in \mathbb{N}$. Se*

1. *$P(0)$ è vero*
2. *$(\forall k \leq n \colon P(k)) \implies P(n+1)$*

Allora $P(n)$ è vero per ogni $n \in \mathbb{N}$.

Definizione 10.9 (massimo/minimo)**.** *Se $\leq$ è una relazione d'ordine definita su un insieme X e $A \subset X$ diremo che a è un* massimo *di A e scriveremo*

$$a = \max A$$

se $a \in A$ e $A \leq a$ (cioè $x \leq a$ per ogni $x \in A$). Diremo che a è un minimo *di A e scriveremo*

$$a = \min A$$

se $a \in A$ e $a \leq A$ (cioè $a \leq x$ per ogni $x \in A$).

E' facile dimostrare che se prendiamo $I_n = \{k \in \mathbb{N} \colon k < n\}$ ogni sottoinsieme non vuoto A di I_n ha sia massimo che minimo (lo si dimostri per induzione su n). Su tutto $\mathbb{N}$ esistono però degli insiemi non vuoti che non hanno massimo. Ad esempio l'insieme dei numeri pari: $2 \cdot \mathbb{N} = \{2k \colon k \in \mathbb{N}\}$ non ha massimo perchè se n è pari anche $n+2$ è pari ed è strettamente maggiore di n.

Teorema 10.10 (buon ordinamento di $\mathbb{N}$)**.** *Se A è un sottoinsieme non vuoto di $\mathbb{N}$ allora A ha minimo.*

Dimostrazione. Supponiamo per assurdo che A non abbia minimo e consideriamo l'insieme $B = \{b \in \mathbb{N} \colon b \leq A\}$. Vogliamo dimostrare per induzione che per ogni $n \in \mathbb{N}$ si ha $n \in B$. Chiaramente $0 \in B$ in quanto $0 \leq \mathbb{N}$. Dato ora qualunque $n \in B$ si ha $n \leq A$ e non può essere $n \in A$ altrimenti n sarebbe il minimo di A. Dunque $n < A$ e quindi $n+1 \leq A$. Dunque, per il principio di induzione, $B = \mathbb{N}$. Ma se A è non vuoto deve esistere almeno un $a \in A$ e certamente $a+1 \notin B$... abbiamo quindi un assurdo. □

11 IL TEOREMA DI INCOMPLETEZZA DI GÖDEL (CENNI)

Il teorema di incompletezza di Gödel afferma, in parole povere, che ogni sistema formale in grado di formalizzare l'aritmetica dei numeri naturali o è incoerente oppure è incompleto. Incoerente significa che è possibile dimostrare proposizioni false (e quindi è possibile dimostrare qualunque proposizione, visto che *ex falso quodlibet*). Incompleto

significa che esistono proposizioni che pur essendo vere non possono essere dimostrate. L'idea del teorema di Gödel è quella di formalizzare la proposizione: "questa proposizione non può essere dimostrata." Risulta infatti chiaro che se tale proposizione potesse essere dimostrata allora sarebbe falsa (e quindi il sistema sarebbe incoerente) se invece tale proposizione non potesse essere dimostrata sarebbe vera (e quindi il sistema sarebbe incompleto).

La dimostrazione del teorema di Gödel è molto complessa, cercheremo di seguito solamente di dare una vaga idea di come può essere attuata.

Abbiamo detto che le regole di inferenza di un sistema formale devono essere regole meccaniche che anche un *calcolatore* deve essere in grado di fare. Per formalizzare questa idea si può introdurre il concetto di *macchina di Turing*. Una macchina di Turing è formata da un nastro infinito (che ne rappresenta la memoria) su cui la macchina può leggere e scrivere dei simboli (ad esempio le lettere utilizzate per rappresentare le formule del sistema formale). La macchina può essere programmata: ad ogni passo viene eseguita una istruzione che può leggere il simbolo nella posizione corrente, in base al valore del simbolo può scrivere un nuovo simbolo, spostarsi a destra o sinistra sul nastro e quindi passare ad una istruzione successiva.

Formalmente l'intero nastro (infinito) di una macchina di Turing può essere memorizzato con un singolo numero naturale n (nastro) Infatti ogni simbolo può essere codificato con una sequenza di cifre e l'intero nastro può essere rappresentato giustaponendo le cifre una di seguito all'altra. La posizione sul nastro è anch'essa un numero naturale p (posizione). E ogni istruzione dell'algoritmo può essere numerata e quindi rappresentata da un terzo naturale s (stato). In un sistema formale abbastanza potente (Gödel dimostra che è sufficiente avere una logica dei predicati su un sistema formale che contiene i simboli per rappresentare i numeri naturali con somma e prodotto. un qualunque programma può quindi essere codificato tramite un predicato $P(n, p, s, n', p', s')$ che significa: "se la macchina ha il nastro n in posizione p e si trova nello stato s, nel passo seguente il nastro diventerà n' la posizione sarà p' e il nuovo stato sarà s'". Grazie al predicato P si potrà definire una successione per ricorrenza (n_k, p_k, s_k) che rappresenta lo stato della macchina dopo che è stata eseguita la k-esima istruzione. Un qualunque sistema formale potrebbe quindi essere definito da una macchina di Turing provvista di un programma che è in grado di verificare se una data formula scritta sul nastro è un teorema del sistema. Codificando questo programma con una formula aritmetica possiamo quindi trovare un predicato $T(n)$ che afferma: "la formula rappresentata dal numero naturale n può essere dimostrata nel sistema formale".

A questo punto serve un metodo per scrivere una formula autoreferenziale. Se $P(n)$ è un qualunque predicato dipendente da una variabile libera "n", è possibile programmare una macchina di Turing in modo che prenda in input il predicato e un numero naturale n e sostituisce ogni occorrenza della variabile libera n all'interno del predicato con la costante che rappresenta il numero intero k. Esiste

quindi una formula aritmetica $Q(p, n, q)$ che afferma: "q è la codifica del predicato che si ottiene dal predicato codificato dal numero p sostituendo ogni occorrenza della variabile "n" con il numero naturale n.

Possiamo finalmente considerare il predicato $G(n)$ che afferma: "la proposizione che si ottiene sostituendo il numero naturale n alla variabile libera "n" nel predicato codificato dal numero n, non è dimostrabile". Ora il predicato G sarà codificato da un numero naturale g. Se al posto di n in G sostituiamo il numero naturale g otteniamo una proposizione $G(n = g)$ che afferma: "la proposizione che si ottiene sostituendo il numero naturale g alla variabile libera "n" nel predicato codificato dal numero nel predicato codificato dal numero g, non è dimostrabile". Ma chi è il predicato a cui si riferisce $G(n = g)$? E' proprio $G(n = g)$ stesso! Quindi $G(n = g)$ sta affermando: "questa proposizione non è dimostrabile".

12 CARDINALITÀ

La teoria degli insiemi è nata con l'intento di formalizzare l'utilizzo degli insiemi con infiniti elementi. Infatti finché gli insiemi hanno un numero finito di elementi non ci sono dubbi sulle loro proprietà. L'utilizzo di insiemi con infiniti elementi, invece, ci pone di fronte a questioni che possono sembrare paradossali.

Per confrontare gli insiemi finiti è sufficiente contare il numero degli elementi. Diremo che un insieme è *più grande* se ha un numero di elementi maggiore. Ma se gli insiemi sono infiniti, non siamo in grado di effettuare un conteggio degli elementi. Possiamo però osservare che non è necessario contare il numero di elementi per poter dire che due insiemi hanno la stessa numerosità. Ad esempio in un parcheggio pieno posso dire che il numero di automobili è uguale al numero di posti, senza dover contare né l'uno né l'altro ma semplicemente osservando che c'è una corrispondenza biunivoca tra i posti e le auto. Faremo lo stesso per confrontare insiemi infiniti.

Diciamo che due insiemi A e B sono equipotenti e scriveremo $\#A = \#B$ se esiste una funzione bigettiva $f\colon A \to B$. Il simbolo $\#A$ si chiama *cardinalità* di A e quindi due insiemi sono equipotenti se hanno la stessa cardinalità. In tal caso la funzione f è invertibile e l'inversa è anch'essa bigettiva, quindi se $\#A = \#B$ risulta anche $\#B = \#A$. Tramite la composizione è inoltre facile verificare che se $\#A = \#B$ e $\#B = \#C$ allora $\#A = \#C$. Nel caso degli insiemi finiti vedremo che la cardinalità coincide con il numero di elementi dell'insieme, ma ci potranno essere anche cardinalità *infinite*.

cardinalità

La relazione di equipotenza definisce il concetto di cardinalità, specificando quali sono gli insiemi che hanno la stessa cardinalità. Possiamo anche mettere un ordinamento tra gli insiemi, specificando che un insieme A ha cardinalità minore o uguale a quella di B, $\#A \leq \#B$, se esiste una funzione iniettiva $f\colon A \to B$. Scriveremo $\#A < \#B$ per indicare che $\#A \leq \#B$ ma non $\#A = \#B$ (dunque esistono funzioni iniettive da A in B ma nessuna di queste risulta essere surgettiva).

Non è difficile verificare che se esiste una funzione iniettiva $f\colon A \to B$ allora esiste anche una funzione surgettiva $g\colon B \to A$ (basta osservare che una funzione iniettiva f è invertibile sulla propria immagine $f\colon A \to f(A)$ e la funzione inversa può essere estesa a tutto B in maniera arbitraria). Più delicato mostrare il viceversa cioè che se esiste una funzione surgettiva $g\colon B \to A$ allora esiste una funzione iniettiva $f\colon A \to B$. Intuitivamente si tratta di scegliere, per ogni elemento $b \in B$, un elemento $a \in g^{-1}(\{b\})$. Visto che f è suriettiva l'insieme su cui scegliere non può essere vuoto e quindi viene definita una funzione $f\colon A \to B$ che necessariamente sarà iniettiva.

Questa dimostrazione intuitiva non può essere formalizzata con gli assiomi che abbiamo introdotto finora ma richiede un assioma aggiuntivo chiamato *assioma della scelta* (AC).

assioma della scelta

Un'altra dimostrazione che richiede l'assioma della scelta (e che non faremo) garantisce che dati due insiemi A e B possiamo confrontarne la cardinalità:

$$(\#A \leq \#B) \vee (\#B \leq \#A).$$

Significa cioè che se non esiste una funzione iniettiva da A in B allora deve esistere una funzione iniettiva da B in A.

Assioma 12.1 (assioma della scelta)**.** *Se A è un insieme i cui elementi sono tutti insiemi non vuoti allora esiste una funzione $f\colon A \to \bigcup A$ tale che*

$$f(X) \in X$$

(cioè la funzione manda ogni insieme elemento di A in un suo elemento).

Tale assioma serve a garantire che data una famiglia arbitraria di insiemi non vuoti esiste un insieme formato da un elemento per ognuno degli insiemi della famiglia. Per quanto possa sembrare strano tale assioma risulta indipendente dai precedenti. Risulta inoltre che tale assioma abbia delle conseguenze controintuitive come mostrato, per esempio, dal *paradosso di Banach-Tarski*[5].

paradosso di Banach-Tarski

Teorema 12.2 (Cantor-Bernstein)**.** *Se $\#A \leq \#B$ e $\#B \leq \#A$ allora $\#A = \#B$.*

Dimostrazione. Per prima cosa al posto dell'ipotesi $\#B \leq \#A$ prendiamo l'ipotesi apparentemente più forte $B \subset A$. Vedremo alla fine che questa ipotesi non ci fa perdere di generalità.

Essendo per ipotesi $\#A \leq \#B$ esiste $f\colon A \to B$ iniettiva. Intuitivamente l'idea è quella di definire l'insieme

$$D = (A \setminus B) \cup f(A \setminus B) \cup f^2(A \setminus B) \cup \dots$$

e di definire la biezione $\phi\colon A \to B$ mandando ogni "buccia" $f^n(A \setminus B)$ in $f^{n+1}(A \setminus B)$ e lasciando fisso il resto di B.

Per farlo in maniera rigorosa consideriamo allora la famiglia di insiemi $\mathcal{F} = \{X \subset A\colon X \supset A \setminus B, f(X) \subset X\}$ e definiamo $D = \bigcap \mathcal{F}$. Osserviamo che $A \in \mathcal{F}$ quindi $\mathcal{F} \neq \emptyset$.

5 Si veda ad esempio http://pagine.dm.unipi.it/paolini/diletto/banach-tarski/banach-tarski.pdf

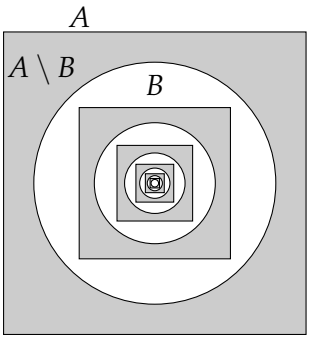


Figura 1: Nella dimostrazione del teorema di Cantor-Bernstein A è rappresentato da un quadrato e B da un cerchio contenuto in A. L'immagine di A in B è rappresentata da un quadrato contenuto in B e così via. La parte ombreggiata è l'insieme D.

E' facile verificare che $f(D) \subset D$ infatti dato $x \in D$ per ogni $X \in \mathcal{F}$ deve essere $x \in X$ ma allora $f(x) \in X$ (per come è definito $\mathcal{F}$), dunque $f(x) \in D$. In modo analogo si dimostra che $D \supset A \setminus B$ e dunque concludiamo che $D \in \mathcal{F}$.

Verifichiamo ora che $f(D) = D \cap B$. Da un lato se $x \in D$ allora $f(x) \in f(D) \subset D$ e $f(x) \subset f(A) \subset B$ da cui $f(x) \in D \cap B$. Dall'altro lato se $y \in D \cap B$ e non fosse $y \in f(D)$ allora potremmo considerare l'insieme $X = D \setminus \{y\}$ e osservare che $X \in \mathcal{F}$. Infatti in primo luogo $X \supset A \setminus B$ in quanto D ha questa proprietà e $y \in B$. Inoltre dato qualunque $x \in X$ visto che $X \subset D$ allora $f(x) \in f(D)$ e, per ipotesi, $y \notin f(D)$ dunque $f(x) \neq y$ da cui $f(x) \in X$. Dunque $X \in \mathcal{F}$ ma allora dovrebbe essere $D \subset X$ mentre per costruzione abbiamo $y \in D$ ma non in X.

Possiamo allora definire $\phi \colon A \to B$

$$\phi(x) = \begin{cases} f(x) & \text{se } x \in D, \\ x & \text{altrimenti.} \end{cases}$$

Chiaramente ϕ è iniettiva in quanto f è iniettiva e manda D in D e l'identità è iniettiva e manda $A \setminus D$ in $A \setminus D$.

Per dimostrare che ϕ è suriettiva consideriamo qualunque $y \in B$. Se $y \notin D$ allora $\phi(y) = y$. Se invece $y \in D$ essendo $y \in D \cap B = f(D)$ esisterà $x \in D$ tale che $\phi(x) = f(x) = y$.

Abbiamo dimostrato il teorema nel caso $B \subset A$. Nel caso generale sappiamo che esiste $f \colon A \to B$ iniettiva ed esiste $g \colon B \to A$ iniettiva. Definiamo $\tilde{B} = g(B)$ e definiamo $\tilde{f} \colon A \to \tilde{B}$ tramite $\tilde{f}(x) = g(f(x))$. Chiaramente $\tilde{B} \subset A$ e $\tilde{f}$ è iniettiva. Dunque ci siamo ricondotti alle ipotesi particolari e sappiamo che esiste $\tilde{\phi} \colon A \to \tilde{B}$ biettiva. Ma allora possiamo definire $\phi \colon A \to B$ come $\phi(x) = g^{-1}(\tilde{\phi}(x))$. Essendo $\tilde{\phi}(A) = \tilde{B}$ ed essendo $g \colon B \to \tilde{B}$ invertibile, risulta che anche ϕ sia biettiva. □

Il seguente teorema è rilevante in quanto ci dice che gli insiemi infiniti non sono sempre tra loro equipotenti, ma ci sono infiniti più grandi e più piccoli. Osserviamo inoltre che il paradosso di Russel ricalca la dimostrazione di questo teorema.

Teorema 12.3 (Cantor). *Per qualunque insieme X si ha $\#X < \#\mathcal{P}(X)$.*

Dimostrazione. Che sia $\#X \leq \#\mathcal{P}(X)$ è facile, basta prendere la funzione $f\colon X \to \mathcal{P}(X)$ definita da $f(x) = \{x\}$ e verificarne l'iniettività.

Per mostrare che $\#X \neq \#P(X)$ consideriamo $f\colon X \to \mathcal{P}(X)$ una qualunque funzione e definiamo l'insieme

$$C = \{x \in X\colon x \notin f(x)\}.$$

Vogliamo ora mostrare che non esiste un $c \in X$ tale che $f(c) = C$. Infatti se tale c esistesse, si avrebbe che la proposizione $c \in C$ risulterebbe equivalente a $c \notin C$ il che è impossibile. Dunque la funzione f non può essere surgettiva e questo significa che non è $\#X \leq \#P(X)$. □

Definizione 12.4. *Dato $n \in \mathbb{N}$ definiamo $I_n = \{k \in \mathbb{N}\colon k < n\}$ (ad esempio $I_3 = \{0, 1, 2\}$ è un insieme formato da 3 elementi). Se A è un insieme diremo che $\#A = n$ se $\#A = \#I_n$. Diremo in tal caso che A ha n elementi.*

Se vogliamo che la definizione precedente abbia senso, dobbiamo assicurarci che $\#I_m = \#I_n$ se e solo se $m = n$. Questo fatto apparentemente ovvio richiede una dimostrazione un poco articolata. Cominciamo con il seguente.

Lemma 12.5. *Se $\#I_m \leq \#I_n$ allora $m \leq n$.*

Dimostrazione. Dimostreremo per induzione su n la seguente proprietà:

$$P(n)\colon \forall m \in \mathbb{N}\colon\ (\#I_m \leq \#I_n) \implies m \leq n.$$

Verifichiamo se $P(0)$ è vera. Se $\#I_m \leq \#I_0$ significa che esiste una funzione iniettiva $f\colon I_m \to I_0 = \emptyset$. Ma non esistono funzioni a valori nell'insieme vuoto, a meno che anche il dominio non sia vuoto. Dunque $I_m = \emptyset$ e $m = 0$ da cui segue ovviamente $m \leq n$. Dunque $P(0)$ è vera.

Supponiamo per ipotesi induttiva che $P(n)$ sia vera e consideriamo $P(n+1)$. Sia dunque $f\colon I_m \to I_{n+1}$ una funzione iniettiva.

Come primo passo vogliamo dimostrare che esiste una funzione iniettiva $g\colon I_m \to I_{n+1}$ tale che $g(m-1) = n$. Per fare ciò consideriamo due casi a seconda che $n \in f(I_m)$ oppure $n \notin f(I_m)$. Il secondo caso è più facile perché se $n \notin f(I_m)$ basterà definire

$$g(k) = \begin{cases} f(k) & \text{se } k < m-1 \\ n & \text{se } k = m-1. \end{cases}$$

La funzione g così definita è certamente iniettiva in quanto f lo è e il valore n non era già stato utilizzato da f. Nel primo caso si avrà invece $f(j) = n$ per qualche $j < m$. Se $j = m-1$ abbiamo finito perché $f(m-1) = n$ e basterà quindi scegliere $g = f$. Se invece $j \neq m-1$ basterà scambiare i valori di f nei punti j e $m-1$:

$$g(k) = \begin{cases} f(k) & \text{se } k \neq j \text{ e } k \neq m-1; \\ f(m-1) & \text{se } k = j; \\ n & \text{se } k = m-1. \end{cases}$$

E' chiaro che g rimane iniettiva se f lo era.

Abbiamo quindi una funzione $g\colon I_m \to I_{n+1}$ iniettiva e tale che $g(m-1) = n$. Significa che la restrizione $h = g_{|I_{m-1}}$ è una funzione $h\colon I_{m-1} \to I_n$ in quanto il valore n non viene mai assunto da h. Ma allora ad h si applica l'ipotesi induttiva e possiamo quindi affermare che $m-1 \leq n$ da cui si ottiene immediatamente $m \leq n+1$ come volevamo dimostrare. □

Dal lemma segue che se $\#I_m = \#I_n$ allora $m \leq n$ e $n \leq m$ e quindi $m = n$. Viceversa è chiaro che se $m = n$ allora $\#I_n = \#I_m$ in quanto in tal caso $I_m = I_n$.

Esercizio 12.6. Utilizzando il principio di induzione dimostrare che se $\#A = n$ allora:

1. $\#\mathcal{P}(A) = 2^n$;
2. $\#(A!) = \#\{f\colon A \to A\colon f \text{ biettiva}\} = n!$ (le funzioni biettive di un insieme in sé si chiamano anche *permutazioni*);
3. se $\#B = m$ allora $\#B^A = \#\{f\colon A \to B\} = m^n$.

Teorema 12.7 (unicità di $\mathbb{N}$)**.** *Se $\mathbb{N}$ e $\mathbb{N}'$ sono due insiemi che soddisfano gli assiomi di Peano con $0 \in \mathbb{N}$, $0' \in \mathbb{N}'$ e $\sigma\colon \mathbb{N} \to \mathbb{N}$ e $\sigma'\colon \mathbb{N}' \to \mathbb{N}'$ allora esiste una bigezione $\phi\colon \mathbb{N} \to \mathbb{N}'$ tale che*

$$0' = \phi(0), \qquad \sigma'(\phi(n)) = \phi(\sigma(n)).$$

Potremmo quindi dire che $\mathbb{N}'$ è una copia isomorfa *di $\mathbb{N}$. In particolare $\#\mathbb{N}' = \#\mathbb{N}$: gli insiemi che soddisfano gli assiomi di Peano hanno tutti la stessa cardinalità.*

Dimostrazione. Possiamo definire $\phi\colon \mathbb{N} \to \mathbb{N}'$ per induzione:

$$\begin{cases} \phi(0) = 0', \\ \phi(\sigma(n)) = \sigma'(\phi(n)) \end{cases}$$

e allo stesso modo possiamo definire $\psi\colon \mathbb{N}' \to \mathbb{N}$:

$$\begin{cases} \psi(0') = 0, \\ \phi(\sigma'(n)) = \sigma(\psi(n)). \end{cases}$$

A questo punto è facile verificare per induzione che $\psi(\phi(n)) = n$ per ogni $n \in \mathbb{N}$. Invertendo i ruoli di ϕ e ψ si dimostra allo stesso modo che $\phi(\psi(n)) = n$ per ogni $n \in \mathbb{N}'$. Significa che ψ è l'inversa di ϕ e che quindi ϕ è bigettiva. □

13 INSIEMI FINITI/INFINITI

L'insieme dei numeri naturali è, per certi versi, paradossale, come si può capire dalla seguente storiella.

Esercizio 13.1 *(Hotel Hilbert).* Nell'hotel Hilbert, come in tutti gli hotel, ogni stanza ha associato univocamente un numero naturale: il numero della stanza. Però a differenza degli altri hotel nell'hotel Hilbert c'è una stanza per ogni numero naturale, quindi le stanze e i numeri naturali sono in corrispondenza biunivoca (diremo quindi che ci sono *infinite* stanze).

Un bel giorno arriva un cliente all'hotel e chiede all'addetto alla *reception* di avere una stanza. Purtroppo l'hotel è pieno e quindi l'addetto informa il cliente che non è possibile avere una stanza. Il cliente insiste e fa chiamare il direttore che risolve la questione in maniera assolutamente brillante. Il direttore chiede gentilmente ad ogni ospite dell'hotel di spostarsi dalla sua stanza a quella seguente. Cioè: l'ospite nella stanza n si deve spostare nella stanza $n+1$. In tal modo si libera la stanza numero 0 che quindi può essere utilizzata dal nuovo arrivato.

Il giorno seguente arriva all'albergo una corriera che porta infinite persone, una per ogni numero naturale, come per l'albergo. Ma l'albergo è già pieno. Come farà il direttore a fare spazio per tutte queste persone?

In realtà non c'è niente di paradossale nella storiella precedente, se non il fatto che vogliamo ragionare con insiemi infiniti. L'esistenza della funzione σ può anzi essere presa come definizione di insieme infinito.

Definizione 13.2. *Diremo che un insieme A è* finito *se esiste $n \in \mathbb{N}$ tale che $\#A = n$. Diremo che un insieme A è* infinito *(più precisamente si direbbe* Dedekind infinito*) se esiste una funzione $\sigma\colon A \to A$ iniettiva ma non suriettiva.*

finito
infinito

Chiaramente $\mathbb{N}$ (se esiste) è un esempio di insieme infinito in quanto la funzione successore $\sigma(n) = n+1$ è iniettiva ma non suriettiva su $\mathbb{N}$. E' anche facile verificare che se $\#A \geq \#\mathbb{N}$ allora A è infinito (lo si provi per esercizio).

Viceversa si ha il seguente teorema che afferma, sostanzialmente, che ogni insieme infinito contiene una copia di $\mathbb{N}$ e dunque $\mathbb{N}$ è, in un certo senso, il più piccolo insieme infinito.

Teorema 13.3. *Se A è un insieme infinito allora esiste un insieme $N \subset A$ che soddisfa gli assiomi di Peano e quindi $\#A \geq \#\mathbb{N}$.*

Dimostrazione. Sia $\sigma\colon A \to A$ una funzione iniettiva ma non suriettiva. Scegliamo un punto $0 \in A \setminus \sigma(A)$ e definiamo

$$\mathcal{F} = \{X \subset A\colon 0 \in X, x \in X \implies \sigma(x) \in X\}.$$

Sostanzialmente $\mathcal{F}$ è l'insieme dei sottoinsiemi di A che soddisfano l'assioma di induzione di Peano. Definiamo quindi

$$N = \bigcap \mathcal{F}.$$

Chiaramente $N \in \mathcal{F}$ (verificare!) e quindi N soddisfa tutti gli assiomi di Peano scelto $0 \in N$ come zero e $\sigma_{|N}\colon N \to N$ come funzione successore. □

Per quanto riguarda gli insiemi finiti abbiamo il seguente risultato che ci assicura, in particolare, che gli insiemi finiti non sono infiniti.

Teorema 13.4. *Se A è finito e $f\colon A \to A$ è una funzione allora risultano equivalenti*

1. *f è iniettiva;*
2. *f è surgettiva;*
3. *f è bigettiva.*

Dimostrazione. Se A è finito significa che esiste $n \in \mathbb{N}$ tale che A è in corrispondenza biunivoca con I_n. Potremo quindi supporre, senza perdere di generalità, che sia $A = I_n$.

Supponiamo per assurdo che esista una funzione iniettiva ma non suriettiva $f\colon I_n \to I_n$. Se fosse $n \notin f(I_n)$ si avrebbe $f\colon I_n \to I_{n-1}$ iniettiva, da cui, per il Lemma 12.5 avremmo $n \leq n-1$ assurdo. Ma se anche fosse $n = f(k)$ per qualche $k \in I_n$ dovrebbe allora esistere $x \in I_n \setminus f(I_n)$ e sarebbe $x \neq n$. Allora potrei definire $g\colon I_n \to I_{n-1}$ che redireziona in x il punto che prima andava in n:

$$g(j) = \begin{cases} f(j) & \text{se } j \neq k, \\ x & \text{se } j = k. \end{cases}$$

Chiaramente $g\colon I_n \to I_{n-1}$ sarebbe iniettiva e di nuovo otterremmo un assurdo.

Abbiamo mostrato che se f è iniettiva allora f è anche suriettiva e dunque anche bigettiva.

Viceversa consideriamo una funzione surgettiva $f\colon I_n \to I_n$. Possiamo allora definire $g\colon I_n \to I_n$

$$g(n) = \min f^{-1}(n).$$

Visto che f è surgettiva, $f^{-1}(\{n\})$ non è mai vuoto e quindi g è ben definita su tutto I_n. Risulta inoltre che g è iniettiva in quanto $f^{-1}(\{n\}) \cap f^{-1}(\{m\}) = \emptyset$ se $m \neq n$. Per quanto visto prima g deve però essere anche surgettiva e questo significa che $f^{-1}(\{n\})$ contiene un unico elemento. Ma allora f era anche iniettiva. Abbiamo quindi mostrato che se f è surgettiva allora è anche iniettiva e quindi anche bigettiva. □

Teorema 13.5. *Se A è finito e $B \subset A$ allora anche B è finito.*

Teorema 13.6. *Dimostriamo per induzione su n che se $\#A = n$ allora ogni $B \subset A$ è finito. Per $n = 0$ si nota che $\#A = 0$ implica $A = \emptyset$ e quindi $B = \emptyset$ è certamente finito. Supponiamo ora che sia $\#A = n+1$ e consideriamo $B \subset A$. Se $B = A$ allora ovviamente $\#B = \#A = n+1$ e quindi B è finito. Altrimenti esiste $x \in A \setminus B$. E' facile verificare che $\#(A \setminus \{x\}) = n$ ed essendo $B \subset A \setminus \{x\}$ applicando l'ipotesi induttiva si ottiene che B è finito.*

Viceversa si può dimostrare il seguente risultato.

Teorema 13.7. *Un insieme è finito oppure infinito.*

Dimostrazione. Se $\#A \geq \#\mathbb{N}$ allora esiste una funzione iniettiva $f\colon \mathbb{N} \to A$ e sappiamo esistere una funzione iniettiva ma non surittiva $\sigma\colon \mathbb{N} \to \mathbb{N}$. Posto $B = f(\mathbb{N})$ si ha dunque che $f\colon \mathbb{N} \to B \subset A$ è bigettiva. Dunque possiamo definire $g\colon A \to A$ come

$$g(a) = \begin{cases} a & \text{se } a \notin B \\ f(\sigma(f^{-1}(a))) & \text{se } a \in B. \end{cases}$$

Non è difficile verificare che g è iniettiva ma non suriettiva in quanto l'elemento $f(0)$ non viene mai raggiunto da g. Dunque se $\#A \geq \#\mathbb{N}$ certamente A è infinito.

Ora mediante l'assioma della scelta si potrebbe dimostrare che se non è $\#A \geq \#\mathbb{N}$ allora necessariamente si ha $\#A < \#\mathbb{N}$ (non lo dimostriamo perché richiederebbe diverse nuovi nozioni). Ma se $\#A < \#\mathbb{N}$ allora esiste una funzione iniettiva $f\colon A \to \mathbb{N}$. Poniamo $B = f(A)$ cosicché $f\colon A \to B$ è bigettiva. Per dimostrare che A è finito basterà allora dimostrare che $B \subset \mathbb{N}$ è finito.

Se esiste $n \in \mathbb{N}$ tale che $B \subset I_n$ allora si avrebbe $\#A \leq \#I_n$ e dunque A sarebbe finito perché in corrispondenza biunivoca con un sottoinsieme di un insieme finito. Supponiamo allora che per ogni $n \in \mathbb{N}$ si abbia $B \setminus I_n \neq \emptyset$. Costruiamo allora una funzione $f\colon \mathbb{N} \to B$ tramite la seguente definizione ricorsiva:

$$\begin{cases} f(0) = \min B \\ f(n+1) = \min(B \setminus I_{f(n)+1}). \end{cases}$$

La funzione è ben definita perché B e $B \setminus I_m$ non sono mai vuoti e il buon ordinamento di $\mathbb{N}$ garantisce l'esistenza del minimo. E' chiaro che $f(n+1) > f(n)$ e dunque (lo si potrebbe dimostrare per induzione) la funzione f è iniettiva. Significa dunque che $\mathbb{N} \leq A$ contro l'ipotesi $\#A < \#\mathbb{N}$.

□

14 ENNUPLE E SUCCESSIONI

Abbiamo denotato con B^A l'insieme delle funzioni $f\colon A \to B$ e abbiamo denotato con $I_n = \{1, 2, \ldots, n-1\} = \{k \in \mathbb{N}\colon k < n\}$. Se A è un insieme qualunque e $n \in \mathbb{N}$ definiamo allora:

$$A^n = A^{I_n} = \{\boldsymbol{a}\colon \{1, 2, \ldots, n-1\} \to A\}.$$

Gli elementi $\boldsymbol{a} \in A^n$ vengono chiamate n-uple (ennuple) perché sono identificate dagli n valori che assumono sugli n numeri $0, 1, \ldots, n-1$. Normalmente si utilizza la notazione $a_k = \boldsymbol{a}(k)$ per denotare il k-esimo valore assunto dalla funzione $\boldsymbol{a}$ e si scriverà:

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}).$$

Gli elementi (di solito saranno numeri) a_0, a_1, …, a_{n-1} vengono chiamati componenti della ennupla $\boldsymbol{a}$. I pedici $0, 1, \ldots, n-1$ vengono chiamati *indici*.

Noi utilizzeremo la convenzione di usare simboli in *grassetto* per denotare le ennuple. Nella scrittura a mano (dove il grassetto è impraticabile) si scriverà $\underline{a}$ al posto di $\boldsymbol{a}$. Un'altra alternativa (meno comoda) è $\vec{a}$. La notazione è quella utilizzata in fisica per denotare i *vettori* perché, in effetti, se mettiamo una base in uno spazio vettoriale di dimensione finita ogni vettore può essere identificato dalla ennupla delle sue componenti rispetto alla base.

Ad esempio l'ennupla $\boldsymbol{a} = (3,5,3)$ è elemento di $\mathbb{N}^3$. Sarà $\boldsymbol{a} = (a_0, a_1, a_2)$ con $a_0 = 3$, $a_1 = 5$, $a_2 = 3$. Formalmente $\boldsymbol{a}$ è definita come una funzione: $\boldsymbol{a} = \{0 \mapsto 3, 1 \mapsto 5, 2 \mapsto 3\}$ ma in pratica non è importante quale sia la definizione (altri testi potrebbero dare definizioni diverse ma equivalenti) ma solo quali siano le sue proprietà. E' anche consuetudine utilizzare gli indici a partire da 1 invece che da 0 e quindi spesso si troverà scritto $\boldsymbol{a} = (a_1, a_2, a_3)$.

Osserviamo che se $n = 2$ la notazione utilizzata per le ennuple A^2 è la stessa notazione utilizzata per le coppie $A \times A$. L'ambiguità è giustificata dal fatto che si potrebbe in effetti identificare A^2 con $A \times A$ in quanto gli elementi di A^2 soddisfano la proprietà caratterizzante le coppie:

$$(x, y) = (x', y') \iff (x = x') \wedge (y = y').$$

Osserviamo che formalmente $(A \times A) \times A \neq A^3$ in quanto gli elementi del primo insieme sono coppie del tipo $((x, y), z)$ mentre gli elementi del secondo insieme sono 3-uple (triple) della forma (x, y, z). E' chiaro quindi che pur essendo oggetti diversi possono essere messi in corrispondenza tra loro.

In maniera analoga chiameremo *successioni* a valori in A gli elementi dell'insieme

$$A^{\mathbb{N}} = \{\boldsymbol{a} \colon \mathbb{N} \to A\}.$$

Di nuovo useremo la notazione $a_k = \boldsymbol{a}(k)$ per denotare i valori della successione $\boldsymbol{a}$ e scriveremo, in maniera espressiva:

$$\boldsymbol{a} = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Gli elementi $a_0, a_1, \dots$ vengono chiamati *termini* o *valori* della successione. I pedici $0, 1, \dots$ vengono chiamati *indici* come per le ennuple.

Per scrivere una successione a partire dai suoi termini si può usare la notazione $\boldsymbol{a} = (a_n)_{n \in \mathbb{N}}$ o $\boldsymbol{a} = (a_n \colon n \in \mathbb{N})$ o anche $\boldsymbol{a} = (a_n)_{n=0}^{+\infty}$. In queste notazioni la variabile n è muta. Spesso tali notazioni si abbreviano in una notazione (formalmente impropria) $\boldsymbol{a} = (a_n)$ o anche $\boldsymbol{a} = a_n$.

Per esempio la funzione $\boldsymbol{a}(n) = n^2$ definisce la successione dei quadrati:

$$\boldsymbol{a} = (0,\ 1,\ 4,\ 9,\ 16,\ \dots, n^2,\ \dots).$$

Ma più spesso si dirà: consideriamo la successione $a_n = n^2$ indicando il termine generico invece dell'intera successione.

Deve essere chiaro che la successione $(a_n)_{n \in \mathbb{N}}$ è cosa diversa dall'insieme dei suoi valori $\{a_n \colon n \in \mathbb{N}\}$. Ad esempio le successioni con termini

$$a_k = \begin{cases} 1 & \text{se } k = 0 \\ 0 & \text{se } k > 0 \end{cases}, \qquad b_k = \begin{cases} 0 & \text{se } k = 0 \\ 1 & \text{se } k > 0 \end{cases},$$

sono successioni diverse ma hanno lo stesso insieme di valori

$$\{a_k \colon k \in \mathbb{N}\} = \{b_k \colon k \in \mathbb{N}\} = \{0, 1\}.$$

La differenza sta nel fatto che in un insieme gli elementi non sono ordinati e non contano le ripetizioni, nelle succesioni invece (come nelle coppie e nelle ennuple) conta l'ordine e contano eventuali ripetizioni.

Ennuple e successioni potrebbero essere entrambe racchiuse dal termine *sequenze*. Una ennupla sarebbe una sequenza finita, una successione una sequenza infinita.

15 I NUMERI INTERI

Dati due numeri naturali $n, m \in \mathbb{N}$ vogliamo definire il *percorso* (o traslazione) $m \mapsto n$ necessario per andare da m a n. Se $n \geq m$ significa che n si può ottenere da m sommando un certo numero naturale k: $n = m + k$. Il numero k viene chiamato *differenza* tra n ed m. Se invece $n < m$ il percorso $m \mapsto n$ è il percorso *opposto* di $n \mapsto m$ e la differenza è, in un senso da precisare, l'opposto del numero k tale che $m = n + k$. A posteriori vedremo che il percorso $m \mapsto n$ rappresenta il numero intero $n - m$.

differenza

Diremo che due percorsi $m \mapsto n$ e $m' \mapsto n'$ sono *equivalenti* se la differenza è la stessa, ovvero se:

$$m + n' = m' + n.$$

Se, ad esempio, $m' = m + k$ e $n' = n + k$ è chiaro che $m' \mapsto n'$ risulta equivalente a $m \mapsto n$. Ricordando che $m \mapsto n$ può essere rappresentato come una coppia $(m, n) \in \mathbb{N} \times \mathbb{N}$ definiamo quindi la seguente relazione $\sim$ su $\mathbb{N} \times \mathbb{N}$:

$$(m, n) \sim (m', n') \iff m + n' = m' + n.$$

E' facile verificare che la relazione $\sim$ appena introdotta è una relazione di equivalenza in base alla seguente definizione.

Definizione 15.1 (relazione di equivalenza)**.** *Una relazione $\sim$ su un insieme A si dice essere una* relazione di equivalenza *se è una relazione riflessiva (cioé $x \sim x$), simmetrica (cioé $x \sim y \iff y \sim x$) e transitiva (cioé $(x \sim y) \wedge (y \sim z) \implies x \sim z$).*

relazione di equivalenza

Le relazioni di equivalenza permettono di definire un insieme chiamato *quoziente*.

Definizione 15.2 (insieme quoziente)**.** *Sia $\sim$ una relazione di equivalenza su un insieme A. Dato $a \in A$ definiamo la* classe di equivalenza di a *come l'insieme di tutti gli elementi di A che sono in relazione con a:*

classe di equivalenza di a

$$[a] = \{x \in A \colon x \sim a\}.$$

L'insieme di tutte le classi di equivalenza viene chiamato insieme quoziente*:*

insieme quoziente

$$A/\sim = \{[x] \colon x \in A\}.$$

Dunque se $\alpha \in A/\sim$ deve esistere $a \in A$ tale che $\alpha = [a]$. In tal caso si dirà che a è un rappresentante *di α.*

rappresentante

L'insieme quoziente serve a identificare come uguali tutti gli elementi che sono tra loro equivalenti: se $\sim$ è una relazione di equivalenza allora si ha

$$x \sim y \iff [x] = [y].$$

Infatti se $x \sim y$ e se $z \in [x]$ si ha $z \sim x \sim y$ e quindi $z \in [y]$. Dunque se $x \sim y$ si ha $[x] \subset [y]$ ma, scambiando i ruoli di x e y si avrà anche $[y] \subset [x]$ e quindi $[x] = [y]$. D'altra parte se $[x] = [y]$ essendo $x \sim x$ si ha $x \in [x] = [y]$ e quindi $x \sim y$.

Tornando alla relazione di equivalenza $\sim$ definita su $\mathbb{N} \times \mathbb{N}$ andremo quindi a definire:

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim .$$

Ogni elemento di $\mathbb{Z}$ è dunque una classe di equivalenza di percorsi $m \mapsto n$ tutti con la stessa direzione e lunghezza.

I percorsi possono essere sommati per *concatenazione*. Se concateniamo il percorso $m \mapsto n$ con $n \mapsto h$ otteniamo il percorso $m \mapsto h$. In generale se vogliamo sommare $m \mapsto n$ con $m' \mapsto n'$ dobbiamo spostare uno dei due percorsi in modo che il suo punto di partenza coincida con il punto di arrivo dell'altro. Se, ad esempio, si ha $m' \geq n$ troveremo $k \in \mathbb{N}$ tale che $m' = n + k$ e dunque $(m, n) \sim (m + k, n + k) = (m + k, m')$ da cui

$$(m + k, m') + (m', n') = (m + k, n')$$

e sommando n alle due componenti del risultato si ottiene $(m + k + n, n' + n) = (m + m, n + n')$. In generale si può quindi verificare che la somma di due classi di equivalenza di percorsi è sempre ben definita nel modo seguente:

$$[(m, n)] + [(m', n')] = [(m + m', n + n')].$$

Si osserva che se al posto di (m, n) mettiamo $(m + k, n + k)$ si ottiene

$$[(m+k, n+k)] + [(m', n')] = [(m+m'+k, n+n'+k)] = [(m+m', n+n')]$$

cioè il risultato non cambia (se così non fosse la definizione non sarebbe ben posta perché dipenderebbe dal rappresentante scelto).

E' facile verificare che l'addizione così definita gode delle proprietà: associativa e commutativa.

Similmente vorremmo dire che il percorso $m \mapsto n$ è maggiore-o-uguale del percorso $m \mapsto n'$ quando $n \geq n'$. Se due percorsi non partono dallo stesso punto posso sempre spostarne uno dei due mantenendo l'equivalenza e riconducendosi al caso in cui entrambi partono dallo stesso punto. Procedendo in maniera analoga a quello che abbiamo fatto per la somma si ottiene la segunte definizione per la relazione d'ordine $\leq$:

$$[(m, n)] \leq [(m', n')] \iff n + m' \geq n' + m.$$

E' facile verificare che la relazione d'ordine così definita gode della proprietà invariantiva:

$$i \geq j \iff i + k \geq j + k, \qquad \forall i, j, k \in \mathbb{Z}$$

e più in generale è compatibile con la somma:

$$(i \geq j) \wedge (i' \geq j') \implies i + i' \geq j + j'.$$

Se due percorsi sono equivalenti anche i percorsi opposti lo sono. Questo ci permette di definire anche l'operazione di opposto (denotato con l'operatore unario $-$) sulle classi di equivalenza:

$$-[(m, n)] = [(n, m)].$$

Si osservi che sommando un percorso con l'opposto si ottiene la classe di equivalenza del percorso nullo:

$$[(m, n)] + [(n, m)] = [(m + n, n + m)] = [(0, 0)]$$

e l'opposto dell'opposto è il percorso originario:

$$-(-[(m, n)]) = -[(n, m)] = [(m, n)].$$

Un percorso $m \mapsto n$ può essere di tre tipi: *positivo* se $n > m$, *negativo* se $n < m$ e *nullo* se $m = n$. Ogni percorso positivo $m \mapsto n$ è equivalente ad un percorso del tipo $0 \mapsto k$ dove k è la differenza tra n ed m ovvero $n = m + k$. I percorsi *positivi* sono quindi rappresentati dalla coppia $(0, k)$ con $k \in \mathbb{N}$, $k \neq 0$. Il percorso nullo è equivalente al percorso $0 \mapsto 0$ e può quindi essere rappresentato, come i percorsi positivi ponendo $k = 0$, dalla coppia $(0, 0)$. I percorsi *negativi* sono della forma $m \mapsto n$ con $n < m$. In tal caso esiste $k \in \mathbb{N}$ tale che $m = n + k$ e il percorso può essere rappresentato dal suo equivalente $k \mapsto 0$ ovvero dalla coppia $(k, 0)$ con $k \in \mathbb{N}$, $k \neq 0$.

Se chiamiamo $\mathbb{N}' \subset \mathbb{Z}$ l'insieme delle classi di equivalenza dei percorsi positivi o nulli potremo scrivere:

$$\mathbb{N}' = \{[(0, k)] \colon k \in \mathbb{N}\}.$$

Si osserva allora che l'addizione ristretta a $\mathbb{N}'$ si esegue banalmente sommando la seconda componente su $\mathbb{N}$:

$$[(0, k)] + [(0, j)] = [(0, k + j)]$$

e l'ordinamento su $\mathbb{N}'$ corrisponde all'ordinamento su $\mathbb{N}$:

$$[(0, k)] \geq [(0, j)] \iff k \geq j.$$

Significa che $\mathbb{N}'$ è *isomorfo* ad $\mathbb{N}$ tramite la bigezione $\mathbb{N} \mapsto \mathbb{N}'$ dato da $k \mapsto [(0, k)]$. Tale bigezione preserva l'addizione e l'ordinamento e in questo senso diciamo che è un isomorfismo. Il numero naturale $0 \in \mathbb{N}$ corrisponde in tale isomorfismo al percorso nullo $[(0, 0)] \in \mathbb{N}'$.

In questo senso possiamo pensare che $\mathbb{Z}$ sia una estensione di $\mathbb{N}$. D'ora in poi chiameremo *numeri interi* gli elementi di $\mathbb{Z}$ e penseremo ai numeri naturali come al sottoinsieme $\mathbb{N}'$ dei numeri interi. Si ha infatti:

$$\mathbb{Z} = \mathbb{N}' \cup (-(\mathbb{N}' \setminus \{0\}))$$

dove $\mathbb{N}'$ sono dunque i numeri interi positivi o nulli, $\mathbb{N}' \setminus \{0\}$ sono i numeri interi positivi $-(\mathbb{N}' \setminus \{0\})$ sono i numeri interi negativi.

Visto che $\mathbb{N}$ era un qualunque insieme soddisfacente gli assiomi di Peano e visto che anche $\mathbb{N}'$ come $\mathbb{N}$ soddisfa gli assiomi di Peano, potremo d'ora in poi dimenticare il vecchio $\mathbb{N}$ e utilizzare $\mathbb{N}'$ al suo posto chiamandolo, d'ora in poi $\mathbb{N}$. Supporremo dunque che sia $\mathbb{N} \subset \mathbb{Z}$.

Dunque abbiamo $0, 1, 2, \cdots \in \mathbb{Z}$ ma anche $-1, -2, -3, \cdots \in \mathbb{Z}$. Dalle definizioni precedenti è facile osservare che $-0 = 0$.

Oltre all'addizione e all'ordinamento che abbiamo estesi da $\mathbb{N}$ a $\mathbb{Z}$, su $\mathbb{Z}$ possiamo definire l'operazione di *sottrazione* (denotata con l'operatore binario $-$) come segue:

$$a - b = a + (-b).$$

Osserviamo inoltre che l'opposto $-a$ di un intero $a \in \mathbb{Z}$ è l'unico intero tale che

$$a + (-a) = 0$$

e dunque in generale $a - a = 0$.

Su $\mathbb{N}$ avevamo definito anche l'operazione di moltiplicazione e vogliamo estendere anch'essa a tutto $\mathbb{Z}$. Avendo identificato $\mathbb{N}$ con $\mathbb{N}'$ ora scriveremo $n - m$ al posto di $[(m, n)]$. Se vogliamo mantenere la proprietà distributiva del prodotto rispetto alla somma dovrà essere, per ogni $n \in \mathbb{N}$:

$$0 = 0 \cdot n = (1 + (-1)) \cdot n = 1 \cdot n + (-1) \cdot n = n + (-1) \cdot n$$

da cui si ottiene che $(-1) \cdot n$ è l'opposto di n, ovvero:

$$-n = (-1) \cdot n.$$

Analogamente dovrà essere $n \cdot (-1) = -n$.

Allora se $n, m \in \mathbb{N}$ e se vogliamo mantenere la proprietà associativa della moltiplicazione dovremo avere:

$$n \cdot (-m) = n \cdot (-1) \cdot m = (-n) \cdot m = (-1) \cdot (n \cdot m) = -(n \cdot m)$$

(più per meno: meno) e

$$(-n) \cdot (-m) = (-1) \cdot n \cdot (-1) \cdot m = (-1)(-n) \cdot m = (-(-n)) \cdot m = n \cdot m$$

(meno per meno: più). Sulle classi di equivalenza potremo quindi definire la moltiplicazione come segue:

$$[(m, n)] \cdot [(m', n')] = [(n \cdot n' + m \cdot m', n \cdot m' + n' \cdot m)].$$

Si potrà quindi verificare che cambiando i rappresentanti scelti per le classi (ad esempio sostituendo (m, n) con $(m + k, n + k)$) il risultato non cambia (si utilizzerà la proprietà distributiva su $\mathbb{N}$). Si potrà quindi verificare che la moltiplicazione così definita su $\mathbb{Z}$ estende la moltiplicazione di $\mathbb{N}$ e continua a mantenere le proprietà associativa, commutativa e distributiva.

Chiaramente su $\mathbb{Z}$ come avevamo fatto su $\mathbb{N}$ oltre alla relazione d'ordine $\geq$ si definiscono conseguentemente le relazioni d'ordine stretto $>$ e le relazioni inverse $\leq$ e $<$. Risulta che gli interi positivi

sono gli $n \in \mathbb{Z}$ tali che $n > 0$ e gli interi negativi sono gli $n \in \mathbb{Z}$ tali che $n < 0$.

Su $\mathbb{Z}$ definiamo anche la funzione *valore assoluto*

$$|n| = \begin{cases} n & \text{se } n \geq 0 \\ -n & \text{se } n < 0 \end{cases}.$$

L'immagine di tale funzione definita su $\mathbb{Z}$ è $\mathbb{N}$.

16 DIVISIBILITÀ E NUMERI PRIMI

Se $n, m \in \mathbb{Z}$ e se esiste $k \in \mathbb{Z}$ tale che $m = k \cdot m$ diremo che n *divide* m, che m è un *divisore* di n e scriveremo $n \mid m$. Ad esempio se $2 \mid n$ diremo che n è *pari*, altrimenti diremo che n è *dispari*. Visto che $n = 1 \cdot n$ è chiaro che 1 e n sono sempre divisori di n (e anche -1 e $-n$ lo sono).

divide
divisore
pari
dispari

Definiamo il *massimo comun divisore* di due numeri n, m come

$$MCD(n, m) = \max\{k \in \mathbb{N} \colon (k \mid n) \wedge (k \mid m)\}.$$

Tale massimo esiste perché l'insieme preso in considerazione è non vuoto (contiene sempre il numero 1) ed è finito perchè

Se $n = k \cdot m$ con $k \neq \pm 1$ (cioè $k \neq 1$ e $k \neq -1$) diremo che n è *riducibile*. In caso contrario diremo che n è *irriducibile*.

Teorema 16.1 (teorema fondamentale dell'aritmetica)**.** *Ogni $n \in \mathbb{N}$, $n \geq 2$, può essere scritto nella forma:*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_N \tag{3}$$

dove tutti i p_k sono irriducibili e $2 \leq p_1 \leq p_2 \leq \cdots \leq p_N$. Inoltre i p_k sono univocamente determinati (la decomposizione (3) è unica).

L'espressione (3) viene chiamata fattorizzazione *di n (in quanto gli operandi della moltiplicazione si chiamano* fattori*).*

fattorizzazione

Dimostrazione. Dimostriamo per induzione su m il seguente $P(m)$: "ogni naturale $n < m$, $n \geq 2$ ammette una unica decomposizione nella forma (3)".

L'enunciato è banalmente vero per $m = 3$ in quanto l'unico n in questione è $n = 2$ e se $k, j \geq 2$ allora $k \cdot j \geq 4$ e quindi $n = 2$ non può essere scritto come prodotto di due naturali non inferiori a 2. Significa che 2 è irriducibile e può essere scritto in modo unico come $2 = 2$ (prodotto di un unico irriducibile).

Supponiamo ora di sapere che vale $P(m)$ e dimostriamo $P(m+1)$. E' sufficiente dimostrare che $n = m$ può essere scritto in modo unico nella forma (3) (in quanto se $n < m$ il risultato è garantito dall'ipotesi induttiva $P(m)$). Sia $p_1 = \min\{p \geq 2 \colon p|n\}$. Tale minimo esiste certamente perché l'insieme non è vuoto visto che contiene quantomeno il numero n. Inoltre p_1 è certamente irriducibile perché se p_1 avesse a sua volta un divisore p allora anche p sarebbe un divisore di n e sarebbe $p < p_1$ contro l'ipotesi che p_1 fosse il minimo. Visto che $p_1 \mid n$ esiste n' tale che $n = p_1 \cdot n'$. Visto che $p_1 > 1$ certamente è

$n' < n = m$ e dunque applicando $P(m)$ sappiamo che n' ammette una unica decomposizione che possiamo scrivere nella forma:

$$n' = p_2 \cdot p_3 \dots p_N$$

(abbiamo utilizzato gli indici a partire da 2 invece che da 1 perché p_1 è già stato utilizzato). Dunque avremo che

$$n = p_1 \cdot n' = p_1 \cdot p_2 \dots p_N$$

come volevamo dimostrare. L'unica cosa che rimane da verificare è che sia $p_1 \leq p_2$. Ma visto che $p_2 \mid n'$ e $n' \mid n$ scopriamo che $p_2 \mid n$ e quindi essendo p_1 il minimo divisore di n deve essere $p_1 \leq p_2$. □

Un numero p si dice essere *primo* se ogni volta che p divide un prodotto esso divide almeno uno dei due fattori cioè se per ogni $n, m \in \mathbb{Z}$ si ha: primo

$$p \mid m \cdot n \implies (p \mid m) \vee (p \mid n).$$

Il prossimo teorema ci dice che sui numeri interi *primo* e *irriducibile* sono sinonimi (e spesso la definizione di numero primo viene espressa mediante irriducibilità) ma in contesti più generali si possono distinguere i due concetti.

Teorema 16.2. *Un numero $p \in \mathbb{Z}$ è primo se e solo se è irriducibile.*

Dimostrazione. Supponiamo che p sia primo e che si possa scrivere $p = n \cdot m$ con $n, m \in \mathbb{Z}$. Allora chiaramente $p \mid n \cdot m$ e quindi p divide almeno uno tra n e m. Senza perdita di generalità possiamo supporre $p \mid n$ da cui $p = p \cdot m$. Significa quindi che $m = 1$ e quindi p non è riducibile.

Viceversa supponiamo che p sia irriducibile e supponiamo che $p \mid n \cdot m$. Per il teorema fondamentale dell'aritmetica n e m hanno una unica fattorizzazione e il prodotto delle fattorizzazioni mi dà una fattorizzazione di $n \cdot m$. D'altra parte la fattorizzazione di p è p stesso in quanto p è irriducibile. Dunque se $p \mid n \cdot m$ necessariamente p è uno dei termini della fattorizzazione di $n \cdot m$ ma visto che tale fattorizzazione si ottiene moltiplicando tra loro le fattorizzazioni di n e di m, si deduce che p è in una delle due fattorizzazioni e quindi divide uno tra n e m. □

17 I NUMERI RAZIONALI

In maniera simile a come abbiamo ottenuto gli interi estendendo i naturali in modo da poter invertire l'operazione di addizione, vogliamo estendere gli inter in modo da poter invertire l'operazione di moltiplicazione. Dati due interi p, q con $q \neq 0$, consideriamo la *dilatazione* $q \mapsto p$ che lascia fisso lo 0, manda q in p e manda ogni multiplo di q ovvero ogni intero n della forma $n = kq$ in kp. Chiamiamo *frazione* la coppia $q \mapsto p$ che denoteremo più espressivamente nella forma $\frac{p}{q}$. Nella frazione $\frac{p}{q}$ il numero p viene chiamato *numeratore* e il frazione numeratore

numero q *denominatore*. Sulle frazioni possiamo mettere una relazione di equivalenza. In effetti se $p' = kp$ e $q' = kq$ con $k \in \mathbb{Z}$, $k \neq 0$, le dilatazioni $q \mapsto p$ e $q' \mapsto p'$ agiscono nello stesso modo sui multipli di q'. Infatti se $n = jq' = kjq$ la dilatazione $q \mapsto p$ lo manda in kjp e la dilatazione $q' \mapsto p'$ lo manda in $jp' = kjp$. Se $q' = kq$ e $p' = kp$ allora equivalentemente si ha $pq' = p'q$. Definiamo quindi la relazione di equivalenza tra frazioni:

denominatore

$$\frac{p}{q} \sim \frac{p'}{q'} \iff pq' = p'q$$

e definiamo i numeri razionali come il quoziente (ricordando che $\frac{p}{q}$ è stato definito come la coppia $(q, p) = (q \mapsto p)$ con $q \neq 0$):

$$\mathbb{Q} = ((\mathbb{Z} \setminus \{0\}) \times \mathbb{Z})/\sim.$$

Data una frazione $\frac{p}{q}$ possiamo considerare $k = MCD(p, q)$. Essendo $k \mid p$ e $k \mid q$ si avrà $p = kp'$ e $q = kq'$ e quindi la frazione $\frac{p}{q}$ risulta equivalente alla frazione (ridotta) $\frac{p'}{q'}$. A questo punto si avrà $MCD(p', q') = 1$ e quindi la frazione ottenuta non può essere ulteriormente ridotta. Se $MCD(p, q) = 1$ si dirà che la frazione $\frac{p}{q}$ è ridotta ai minimi termini. Se $q < 0$ si potrà inoltre cambiare segno sia a p che a q in quanto $\frac{-p}{-q}$ è equivalente a $\frac{p}{q}$. Data una qualunque frazione si potrà dunque trovare una frazione equivalente, ridotta ai minimi termini, con denominatore positivo. Tale frazione è unica ed è quindi un naturale rappresentante della classe di equivalenza.

Le frazioni possono essere moltiplicate e sommate tra loro con le ben note regole:

$$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}, \qquad \frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}$$

e possono essere ordinate con il criterio:

$$\frac{p}{q} \geq \frac{p'}{q'} \iff pq' \geq p'q.$$

L'opposto di una frazione si ottiene prendendo l'opposto del numeratore (o, sarebbe lo stesso, del denominatore).

E' facile verificare che somma, prodotto, opposto e ordinamento non dipendono dalla classe di equivalenza quindi tali operazioni sono ben definite anche su $\mathbb{Q}$. Si verifica inoltre che tali operazioni mantengono tutte le proprietà che avevamo già ottenuto per le stesse operazioni in $\mathbb{Z}$. Osserviamo che la funzione $\phi\colon \mathbb{Z} \to \mathbb{Q}$ definita da $\phi(n) = \frac{n}{1}$ è un *isomorfismo* di $\mathbb{Z}$ in $\mathbb{Z}' = \phi(\mathbb{Z}) \subset \mathbb{Q}$ nel senso che $\phi\colon \mathbb{Z} \to \mathbb{Z}'$ è bigettiva e trasforma le operazioni di addizione, moltiplicazione, opposto e ordinamento definite in $\mathbb{Z}$ nelle corrispondenti operazioni definite in $\mathbb{Q}$. In particolare le classi di equivalenza delle frazioni $\frac{0}{1}$ e $\frac{1}{1}$ corrispondono a 0 e 1 di $\mathbb{Z}$ Ad esempio:

$$\phi(n + m) = \frac{n + m}{1} = \frac{n}{1} + \frac{m}{1} = \phi(n) + \phi(m).$$

Visto che di $\mathbb{Z}$ non ci interessa sapere come è stato costruito ma ci interessano solamente le sue proprietà, d'ora in poi potremmo rimpiazzare $\mathbb{Z}$ con $\mathbb{Z}'$ supponendo quindi che $\mathbb{Z} \subset \mathbb{Q}$. All'interno di $\mathbb{Z}$ manteniamo pure i numeri naturali $\mathbb{N}$ cosicché avremo $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Ogni numero razionale $r \in \mathbb{Q}$, $r \neq 0$ ha ora un *reciproco* (inverso moltiplicativo) che denotiamo con r^{-1} o con $\frac{1}{r}$ e che ha la proprietà:

$$r \cdot r^{-1} = 1.$$

Questo perché se $p \neq 0$ e $q \neq 0$ il prodotto delle frazioni $\frac{p}{q}$ e $\frac{q}{p}$ è pari a 1. Questo ci permette di definire l'operazione di divisione tra numeri razionali quando il secondo operando non è nullo:

$$r/s = r \cdot s^{-1} \qquad \text{se } r, s \in \mathbb{Q},\ s \neq 0.$$

Osserviamo che se $r, s \in \mathbb{Q} \cap \mathbb{Z}$ sono interi, allora si ha

$$r/s = \frac{r}{1} \cdot \frac{1}{s} = \frac{r}{s}.$$

Questa uguaglianza giustifica l'uso della notazione $\frac{r}{s}$ per denotare r/s anche quando r ed s non sono interi. Anche in tal caso diremo (forse impropriamente?) che r è il numeratore ed s il denominatore. Il risultato di una divisione si chiama *rapporto* e può quindi essere rappresentato con le seguenti notazioni: rapporto

$$r/s = \frac{r}{s} = r \cdot s^{-1}.$$

Le proprietà delle operazioni che abbiamo ottenuto sull'insieme numerico $\mathbb{Q}$ sono notevoli e, in base alla seguente definizione, ci permettono di dire che $\mathbb{Q}$ è un *campo*.

Definizione 17.1 (campo)**.** *Sia K un insieme su cui sono definite due operazioni $+$ e $\cdot$ e siano $0, 1 \in K$ tali che:*

1. *sia $+$ che $\cdot$ sono operazioni associative e commutative;*
2. *vale la proprietà distributiva: $(x + y) \cdot z = x \cdot z + y \cdot z$;*
3. *0 e 1 sono rispettivamente gli elementi neutri delle operazioni $+$ e $\cdot$;*
4. *ogni elemento ha l'opposto, ovvero per ogni $x \in K$ esiste $-x \in K$ tale che $x + (-x) = 0$; ogni elemento di K tranne 0 ha il reciproco ovvero per ogni $x \in K \setminus \{0\}$ esiste $x^{-1} \in K$ tale che $x \cdot x^{-1} = 1$.*

Di più, $\mathbb{Q}$ è un *campo ordinato* secondo la seguente definizione

Definizione 17.2 (campo ordinato)**.** *Sia K un campo su cui è definita una relazione d'ordine totale $\leq$. Diremo che K è un* campo ordinato *se vale le seguenti proprietà di compatibilità dell'ordinamento con la struttura di campo:* *campo ordinato*

$$x \leq y \iff x + z \leq y + z \qquad x \geq 0,\ y \geq 0 \implies x \cdot y \geq 0.$$

18 I NUMERI REALI

La costruzione degli insiemi numerici è motivata dalla necessità di misurare. Con i numeri naturali possiamo misurare (diremmo: contare) gli oggetti discreti: sassi, pecore, monete. Con i numeri interi possiamo considerare i fenomeni di aumento e diminuzione di queste quantità discrete (differenze tra numeri naturali). Con i numeri razionali possiamo suddividere l'unità di misura per misurare lunghezze, aree, tempi, con precisione arbitraria.

Non siamo però completamente soddisfatti di come i numeri razionali possono misurare (ad esempio) le lunghezze. Per il teorema di Pitagora sappiamo, ad esempio, che la diagonale di un quadrato unitario dovrebbe essere un numero x tale che $x^2 = 2$. Possiamo facilmente dimostrare che non esiste un numero razionale con tale proprietà.

Teorema 18.1 (Pitagora)**.** *Non esiste $x \in \mathbb{Q}$ tale che $x^2 = 2$.*

Dimostrazione. Supponiamo per assurdo che tale x esista. Allora si potrebbe scrivere $x = \frac{p}{q}$ con $p, q \in \mathbb{Z}$, $q > 0$. Possiamo anche supporre che la frazione sia ridotta ai minimi termini e quindi che p e q non abbiano fattori comuni. Per assurdo stiamo supponendo che sia

$$2 = x^2 = \frac{p^2}{q^2}$$

da cui

$$p^2 = 2q^2.$$

Significa che p^2 è pari cioè $2 \mid p \cdot p$. Essendo 2 primo significa che $2 \mid p$ e quindi si può scrivere $p = 2p'$ con $p' \in \mathbb{Z}$. Allora abbiamo

$$(2 \cdot p)^2 = 2q^2$$

che è equivalente a

$$2p^2 = q^2.$$

Ma allora, per lo stesso ragionamento di prima, anche q è divisibile per 2. Ma questo è assurdo perché abbiamo assunto che p e q non avessero divisori comuni. □

Lo stesso fenomeno (anche se molto più complicato da dimostrare) avviene quando cerchiamo di misurare il rapporto tra la lunghezza di una circonferenza e il suo diametro. Tale rapporto π può essere approssimato con precisione arbitraria tramite numeri razionali, ma non può essere espresso mediante frazione. Quando il rapporto tra due misure non è razionale si dice che le due misure sono *incommensurabili*.

Definizione 18.2 (ordinamento completo)**.** *Sia $\leq$ una relazione d'ordine su un insieme X. Diremo che l'ordinamento $\leq$ su X è* completo *(o Dedekind completo) e diremo che X è* continuo *se data una qualunque coppia (A, B) di sottoinsiemi non vuoti di X se*

completo

$$A \leq B \implies \exists x \in X \colon A \leq x \leq B.$$

Ricordiamo che $A \leq B$ significa che per ogni $a \in A$ e $b \in B$ si ha $a \leq b$ mentre $A \leq x \leq B$ significa $a \leq x \leq b$ per ogni $a \in A$ e ogni $b \in B$. Il punto x verrà chiamato elemento di separazione *dei due insiemi A e B.*

elemento di separazione

Intuitivamente le misure fisiche (ad esempio la misura di lunghezza di un segmento) dovrebbero essere un insieme continuo. La misura della circonferenza di un cerchio di diametro unitario può essere infatti approssimata per difetto dalla misura dei poligoni regolari inscritti nel cerchio e per eccesso dalla misura dei poligoni regolari circoscritti al cerchio. Questi perimetri, a loro volta, possono essere approssimati per difetto e per eccesso tramite numeri razionali. Dunque è possibile trovare una coppia di insiemi di misure (A, B) dove A sono tutte le approssimazioni per difetto e B sono tutte le approssimazioni per eccesso e si può verificare che le approssimazioni per difetto possono essere prese arbitrariamente vicine alle approssimazioni per eccesso in quanto se i poligoni regolari hanno un numero di lati abbastanza grande, la differenza dei perimetri diventa arbitrariamente piccola.

Possiamo verificare che $\mathbb{Q}$ non è continuo. Infatti consideriamo i seguenti insiemi:

$$\begin{aligned} A &= \{x \in \mathbb{Q} \colon (x^2 < 2) \vee (x \leq 0)\}, \\ B &= \{x \in \mathbb{Q} \colon (x^2 > 2) \wedge (x \geq 0)\}. \end{aligned} \tag{4}$$

Questi insiemi non sono vuoti perché, ad esempio, $1 \in A$ e $2 \in B$. Verifichiamo che $A \leq B$: siano $a \in A$ e $b \in B$. Per definizione di B si ha $b \geq 0$. Se $a \leq 0$ risulta quindi $a \leq b$. Se invece $a \geq 0$ dovrà essere $a^2 \leq 2 \leq b^2$. Dunque $a^2 - b^2 \leq 0$ ovvero $(a-b) \cdot (a+b) \leq 0$. Visto che $a + b \geq 0$ dovrà essere $a - b \leq 0$ cioè $a \leq b$ che è quanto volevamo dimostrare. Supponiamo ora (per assurdo) che esista un elemento di separazione cioè un $x \in \mathbb{Q}$ tale che $A \leq x \leq B$. Visto che $0 \in A \leq x$ dovrà essere $x \geq 0$. Vogliamo mostrare che $x^2 = 2$. Certamente sappiamo che $1 \leq x \leq 2$ in quanto $1 \in A$ e $2 \in B$. Se fosse $x^2 < 2$ poniamo $\delta = 2 - x^2$. Visto che $x \geq 1$ sarà $\delta < 1$. Se poniamo $y = x + \delta/8$ si trova

$$y^2 = \left(x + \frac{\delta}{8}\right)^2 = x^2 + x \cdot \frac{\delta}{4} + \frac{\delta^2}{64} \leq x^2 + \frac{\delta}{2} + \frac{\delta}{64} < x^2 + \delta = 2.$$

Dunque $x < y$ e $y \in A$ che significa che non è $A \leq x$. Se fosse $x^2 > 2$ poniamo $\delta = x^2 - 2$. Visto che $x \leq 2$ sarà $\delta < 1$. Se poniamo $y = x - \delta/4$ si trova

$$y^2 = \left(x - \frac{\delta}{4}\right)^2 = x^2 - x \cdot \frac{\delta}{2} + \frac{\delta^2}{16} > x^2 - \delta + 0 = 2.$$

Dunque $x > y$ e $y \in B$ che significa che non è $x \leq B$. Abbiamo quindi concluso che dovrebbe essere $x^2 = 2$ ma questo è impossibile se $x \in \mathbb{Q}$. Dunque $\mathbb{Q}$ non è continuo.

Vogliamo allora estendere $\mathbb{Q}$ per ottenere un campo continuo. Se $A \subset \mathbb{Q}$ diremo che A è una *sezione di Dedekind* se:

sezione di Dedekind

1. $A \neq \emptyset$, $A \neq \mathbb{Q}$;

2. se $a \in A$, $x \in \mathbb{Q}$ e $x \leq a$ allora $x \in A$;

3. se $a \in A$ esiste $x \in A$ tale che $x > a$.

Potremo allora definire l'insieme dei numeri reali $\mathbb{R}$ come: $\mathbb{R}$

$$\mathbb{R} = \{A \in \mathcal{P}(\mathbb{Q}) \colon A \text{ è una sezione di Dedekind}\}.$$

Per ogni $q \in \mathbb{Q}$ possiamo considerare l'insieme $A_q = \{a \in \mathbb{Q} \colon a < q\}$. E' facile verificare che $A_q \in \mathbb{R}$ (cioè che A_q è una sezione di Dedekind). Anche l'insieme $A = \{a \in \mathbb{Q} \colon (a < 0) \vee a^2 < 2\}$ risulta essere una sezione di Dedekind che non corrisponde a nessun A_q con $q \in \mathbb{Q}$. Dunque $\mathbb{R}$ contiene al suo interno un rappresentante di ogni numero razionale ma non solo, ha degli elementi in più.

Su $\mathbb{R}$ definiamo $\leq_{\mathbb{R}}$ tramite l'inclusione:

$$A, B \in \mathbb{R} : A \leq_{\mathbb{R}} B \iff A \subset B.$$

E' chiaro che $\leq_{\mathbb{R}}$ è una relazione d'ordine (perché $\subset$ lo è in generale). Vogliamo dimostrare che è un ordine totale cioè che se A, B sono due sezioni di Dedekind allora o $A \subset B$ oppure $B \subset A$. Supponiamo per assurdo che ciò non succeda: significa che esistono $a \in A \setminus B$ e $b \in B \setminus A$. Ma dovrà essere $a \leq b$ oppure $b \leq a$ (perché su $\mathbb{Q}$ l'ordine è totale). Se $a \leq b$ visto che $b \in B$ dovrà essere anche $a \in B$: assurdo. Viceversa se fosse $b \leq a$ visto che $a \in A$ dovrebbe essere anche $b \in A$: di nuovo assurdo. Dunque $\leq_{\mathbb{R}}$ è un ordinamento totale di $\mathbb{R}$.

Possiamo facilmente definire l'operazione di addizione $+_{\mathbb{R}}$ su $\mathbb{R}$:

$$A +_{\mathbb{R}} B = A + B = \{a + b \colon a \in A, b \in B\}.$$

Bisogna innanzitutto verificare che $A + B$ è una sezione di Dedekind se A e B lo sono. Certamente se A e B sono non vuoti anche $A + B$ è non vuoto. Se A e B sono diversi da $\mathbb{Q}$ sappiamo che esiste $x \in \mathbb{Q} \setminus A$ ed esiste $y \in \mathbb{Q} \setminus B$. Se chiamiamo z il più grande tra x e y si ha $z \notin A$ e $z \notin B$ perchè se z fosse un elemento della sezione allora anche x e y lo sarebbero. Dunque ogni $a \in A$ e ogni $b \in B$ sono più piccoli di z e di conseguenza $a + b \leq 2z$. Significa che $2z \notin A + B$ e quindi $A + B$ è non vuoto. Vogliamo ora mostrare che se $x \in A + B$ e $y \leq x$ allora anche $y \in A + B$. Sarà $x = a + b$ con $a \in A$ e $b \in B$. Se $y \leq x$ allora $y - b \leq x - b = a \in A$ e dunque $y - b \in A$ e $y = (y - b) + b \in A + B$. Ultima proprietà: dobbiamo mostrare che se $x \in A + B$ esiste $y > x$ con $y \in A + B$. Sarà $x = a + b$ con $a \in A$ e $b \in B$. Ma allora esistono $a' \in A$ e $b' \in B$ tali che $a' > a$ e $b' > b$ e dunque si avrà $a + b < a' + b' \in A + B$. Questo conclude la dimostrazione che $A + B$ è una sezione di Dedekind.

19 IL COEFFICIENTE BINOMIALE

*** **Definizione 19.1** (coefficiente binomiale)**.** *Definiamo per ogni $n \in \mathbb{N}$ e per ogni $k \in \mathbb{Z}$ il* coefficiente binomiale *coefficiente binomiale*

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{se } 0 \leq k \leq n \\ 0 & \text{altrimenti.} \end{cases}$$

* **Teorema 19.2** (triangolo di Tartaglia)**.** *Per ogni $n \in \mathbb{N}$ e $k \in \mathbb{Z}$ si ha*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Dimostrazione.

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\ &= \frac{k \cdot n! + (n-k+1) \cdot n!}{k!(n-k+1)!} \\ &= \frac{(n+1) \cdot n!}{k!(n+1-k)!} = \binom{n+1}{k}.\end{aligned}$$

□

*** **Teorema 19.3** (sviluppo binomiale)**.** *Se $a, b \in \mathbb{R}$ e $n \in \mathbb{N}$ si ha:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}.$$

Dimostrazione. Lo dimostriamo per induzione su n. Per $n = 0$ l'uguaglianza è soddisfatta per verifica diretta (ambo i membri sono uguali ad 1).

Supponendo valida l'uguaglianza per un certo $n \in \mathbb{N}$ proviamo a verificarla per $n+1$:

$$\begin{aligned}(a+b)^{n+1} = (a+b) \cdot (a+b)^n &= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} \cdot b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k+1} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \cdot b^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k+1} \\ &= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k \cdot b^{n+1-k}.\end{aligned}$$

Nell'ultimo passaggio abbiamo sfruttato il fatto che per $k < 0$ e per $k > n$ il coefficiente binomiale è nullo. Sfruttando la relazione del triangolo di Tartaglia si ottiene infine, come volevamo dimostrare

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k \cdot b^{n+1-k}.$$

□

Esercizio 19.4 *(interpretazione combinatoria del coefficiente binomiale).* Il numero di sottoinsiemi di k elementi di un insieme con n elementi è $\binom{n}{k}$.

Esercizio 19.5. Provare che

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

20 CONTRIBUTI

Hanno segnalato errori e correzioni: niccolo-p, Antoine Venturini.