DAGLI INSIEMI ALLA LOGICA MATEMATICA

Tentativi di Fondare la Matematica

VOL. II

Giangiacomo Gerla

INDICE

Introduzione

CAPITOLO 1
GLI INSIEMI: CREDERE NELL' INFINITO

1. Il prezzo dell'aritmetizzazione: l'infinito attuale ……..... 1
2. Ma questi insiemi sono poi veramente una novità? .....…..... 5
3. I paradossi dell'infinito .....…..... 8
4. Equipotenza: confrontare le grandezze degli insiemi 12
5. L'assioma della scelta …… 14
6. Una questione complicata: cosa significa essere finito? ……..… 18
7. Insiemi numerabili ed insiemi enumerabili .....…..... 22
8. Tentare di superare il numerabile: esiste un sol tipo di infinito? … 25
9. La grandezza degli intervalli: la lunghezza della mia ombra 31
10. La potenza del continuo: io sono più infinito di te …..... 35
11. Superare la potenza del continuo e poi superare ancora 39

Nota 1: Cantor, l'infinito e la Dottrina Cristiana .....…..... 45
Nota 2: La definizione di Emily di infinito …… 46
Nota 3: Un modo diverso di quozientare una struttura ……..…… 47
Nota 4: Giochi di prestigio con l'insieme vuoto: tutti gli elementi di ∅ sono pari, tutti i suoi elementi sono dispari …..…..... 49

Lettura 1: R. Rucker, *L'albergo di Hilbert* 52
Lettura 2: G. Gerla, *Nel paese del Destino* 54
Lezione 3: *Un esempio di seminario in un liceo* 59

CAPITOLO 2
ALTRI TEOREMI ED ALTRI NUMERI

1. Teorema di Cantor-Bernstein: è tanto scontato che valga? 77
2. Cercarne una dimostrazione …..... 78
3. Trarre altre informazioni dalla dimostrazione ……..... 82
4. Le dimostrazioni di Borel e Kőnig 85
5. Equiscomponibilità e paradosso di Vitali 89
6. Il Paradosso di Banach-Tarski 92
7. Nuovi numeri: i numeri cardinali .....…..... 94
8. Algebra dei cardinali.....…..... 95
9. La nozione di buon ordine ……..…….. 98

10. Alcune somiglianze con le terne di Peano ……..…… 102
11. Nuovi numeri: i numeri ordinali .....…..... 104
12. Algebra degli ordinali .....…..... 106
13. Riassumendo sui possibili numeri …… 111

Divagazione 1: Insiemi ripetitivi, vaghi, rozzi ……..... 113
Divagazione 2: I razionali sono bene ordinabili, i naturali sono non bene ordinabili…….…. 117

CAPITOLO 3
METODO ASSIOMATICO E STRUTTURALISMO

1. Paradossi e crisi della teoria degli insiemi 121
2. Russell, il paradosso del barbiere, Marx e le studentesse 126
3. Affrontare i paradossi: intuizionismo e metodo assiomatico 127
4. Metodo assiomatico e geometria ……..... 132
5. Geometrie e campi …….. 135
6. Metodo assiomatico e numeri reali ……..... 138
7. Assiomi per evitare i paradossi della teoria degli insiemi 142
8. La teoria di Zermelo-Fraenkel 144
9. Assioma della scelta: dimostrarlo o confutarlo 149
10. Ipotesi del continuo 152
11. Categoricità, consistenza, indipendenza, completezza 153
12. Tre diverse ideologie per il metodo assiomatico 156

Divagazioni: Strutturalismo e divisione del lavoro .....…..... 163

CAPITOLO 4
LA LOGICA PER I FONDAMENTI

1. Hilbert contro l'infinito 167
2. L'infinito è solo una parola 170
3. Nuovi oggetti matematici: parole e linguaggi 172
4. Rappresentabilità, definibilità e numerabilità 176
5. Logica del primo ordine: linguaggio ed apparato deduttivo 178
6. Logica del primo ordine: l'interpretazione 184
7. Cosa è la verità 187
8. Teorema di completezza 189
9. Teoremi limitativi …… 191
10. Un po' di storia: la teoria dei sillogismi di Aristotele 195
11. Il contributo degli stoici .....……..... 201
12. Diagrammi di Eulero-Venn, algebre di Boole, sillogismi 202
13. Limiti della logica Aristotelica ……..…….. 207
14. Ma Leibniz aveva le idee chiare ……..…… 208

CAPITOLO 5
TEORIA DELLE CATEGORIE

1. Introduzione 213
2. Globale e locale 217
3. Monomorfismi, epimorfismi, isomorfismi 218
4. Funtori ed isomorfismi tra categorie 220
5. Teoria delle categorie per i fondamenti 222

APPENDICE
CALCOLARE CON OPERATORI

1. Sistemi di chiusura, operatori e punti fissi 225
2. Due teoremi di punto fisso per operatori 227
3. Come generare relazioni di ordine o di equivalenza 231

Indice analitico 235
Bibliografia 229

INTRODUZIONE

Questo è il secondo dei due volumetti in cui raccolgo i miei appunti per i corsi di Matematiche Complementari. Come detto nel sottotitolo, l'attenzione viene concentrata sulla matematica che si è sviluppata in seguito alla nascita della teoria degli insiemi. In accordo con quanto detto nell'introduzione al primo volume, il punto di vista che assumo non è proporre una particolare "fondazione" della matematica ma piuttosto viaggiare all'interno della matematica per evidenziare connessioni fra vari ambiti e, principalmente, mettere in rilievo le difficoltà che nascono quando si tenti di trovare una qualche fondazione. A mio parere questo è l'unico modo per capire almeno un po' la natura misteriosa della matematica.

Salerno 2019

P.S.

Il mio indirizzo è ggerla@unisa.it e ricevo volentieri commenti, segnalazioni di errori o richieste di chiarimenti.

CAPITOLO 1

GLI INSIEMI: CREDERE NELL'INFINITO[1]

Confinato nella sua natura
infinito nei suoi desideri
L'uomo è un Dio caduto
che si ricorda dei cieli
(Lamartine)

1. Il prezzo dell'aritmetizzazione: l'infinito attuale

All fine del primo volume abbiamo mostrato come sia possibile una aritmetizzazione di tutta la matematica che rende possibile svincolare il discorso matematico dall'intuizione del continuo geometrico. Ora per portare avanti questa aritmetizzazione è stato necessario "pagare un prezzo". Questo prezzo è l'accettazione dell'infinito potenziale per potere definire gli interi ed i razionali e l'accettazione dell'infinito attuale per potere definire i reali. Naturalmente l'insieme degli elementi di una terna di Peano è attualmente infinito (anzi l'accettazione dell'esistenza di una terna di Peano equivale all'accettazione di un insieme infinito). Tuttavia i singoli numeri naturali sono oggetti finiti e quando facciamo i nostri calcoli ci serviamo ogni volta di una quantità finita di tali numeri.

Apparentemente la stessa cosa non può essere detta per i numeri relativi e quelli razionali in quanto in entrambi i casi un numero è definito come una classe attualmente infinita di coppie (e quindi ogni numero è un infinito attuale). Ad esempio l'anello Z viene introdotto partendo dal prodotto cartesiano $N_0 \times N_0$, definendo in esso due operazioni + e $\cdot$ e costruendo la struttura alge-

[1] In questo capitolo parleremo della teoria "ingenua" degli insiemi. Questo significa che gli insiemi verranno introdotti in modo completamente intuitivo. In realtà, come vedremo nel prossimo capitolo, esistono molti paradossi della teoria degli insiemi che mostrano come un approccio informale presenti molti problemi e come sia necessario abbandonare la fede indiscriminata verso l'accettazione di insiemi infiniti.

brica ($N_0 \times N_0$, +, ·, **0**, **1**) dove **0** = (0, 0) e **1** = (1, 0). In tale struttura viene poi definita una congruenza ≡ e questo permette di definire Z come quoziente di ($N_0 \times N_0$, +, ·, **0**, **1**) modulo ≡. Gli elementi del quoziente vengono chiamati *numeri relativi* i quali, come abbiamo già detto, vengono ad essere un insieme attualmente infinito. Ad esempio [**0**] è l'insieme attualmente infinito $\{(n, m) : n = m\}$. Un procedimento dello stesso tipo viene utilizzato per i numeri razionali.

Tuttavia l'esperienza scolastica che abbiamo tutti è che i numeri relativi si ottengono "anteponendo" ad un numero naturale i simboli – oppure +. Si definiscono poi le operazioni di addizione e moltiplicazione nel modo che tutti sappiamo. Se ci riferiamo a quest'esperienza appare evidente che gli interi relativi si manipolano all'interno dell'infinito potenziale non differentemente di quello che avviene per i numeri naturali.

Tuttavia esiste un rapporto preciso tra i numeri relativi "ingenui" come vengono intesi nella scuola elementare ed i numeri relativi "colti" come vengono intesi nelle università. Infatti osserviamo che se *n ed m* sono numeri naturali allora

- $(n, m) \equiv (n\text{-}m, 0)$ se $n \geq m$
- $(n, m) \equiv (0, m\text{-}n)$ nel caso in cui $m > n$.

Questo significa che ogni classe si può rappresentare in una delle due forme $[(x, 0)]$ oppure $[(0, x)]$. Se indichiamo con $+x$ la coppia $(x,0)$ e con $-x$ la coppia $(0,x)$ possiamo dire che ogni numero relativo si può rappresentare con uno dei "segni" + e – seguito da un numero naturale. Questo discorso può essere precisato da un punto di vista più formale al modo seguente.[2]

Definizione 1.1. Poniamo

$$Z^* = \{+n : n \in N_0\} \cup \{-m : m \in N_0\}$$

e definiamo la funzione $f : N_0 \times N_0 \to Z^*$ ponendo

- $f((n,m)) = +(n\text{-}m)$ se $n \geq m$,
- $f((n,m)) = -(m\text{-}n)$ se $n < m$.

Allora diciamo che gli elementi di Z^* sono *numeri relativi in forma normale* e che $f((n,m))$ è la *riduzione a forma normale di* (n, m).

E' facile verificare che

[2] Nel seguito si riprende l'argomento della riduzione in forma normale già trattata nel volume 1.

$f((n,m)) = f((n',m')) \Leftrightarrow (n,m) \equiv (n',m') \Leftrightarrow [(n, m)] = [(n', m')]$
cioè che due coppie hanno la stessa forma normale se e solo se sono equivalenti. Questo permettere di "estendere" f al quoziente e quindi di definire f^* ponendo $f^*([(n, m)] = f((n,m))$.
La funzione f^* è ben definita nel senso che il suo valore non dipende dalla scelta dell'elemento rappresentativo (n, m) scelto nella classe $[(n, m)]$.
E' evidente che $f^*([(n,m)])$ è equivalente ad (n, m) ed anche a tutti gli altri elementi della classe $[(n,m)]$. La somma ed il prodotto di due forme normali non è in generale una forma normale ma questo non crea problemi in quanto, dopo avere effettuato la somma, è possibile sempre ridursi alla relativa forma normale tramite f. Ad esempio, alla coppia (3,7) noi associamo la coppia equivalente -4 = (0, 4), alla coppia (7, 3) associamo la coppia equivalente +4 = (4, 0). Dovendo eseguire il calcolo (-8)+(+6) lo interpretiamo come (0, 8)+(6, 0) ottenendo il risultato (6, 8). Riducendo a forma normale avremo (0, 2) e quindi -2.

Teorema 1.2. Indichiamo con $(Z^*, \oplus, \otimes, (0,0), (1,0))$ la struttura il cui dominio è Z^* ed in cui le operazioni $\oplus$ e $\otimes$ sono definite ponendo:

- $x \oplus y$ uguale alla riduzione a forma normale di $x+y$
- $x \otimes y$ uguale alla riduzione a forma normale di $x \cdot y$.

Allora f^* è un isomorfismo dell'anello Z degli interi relativi e $(Z^*, \oplus, \otimes, (0,0), (1,0))$.

La costruzione della struttura $(Z^*, \oplus, \otimes, (0,0), (1,0))$ può sembrare artificiale ma è meno artificiale di quella utilizzata nel volume precedente per definire l'anello degli interi relativi. Infatti è esattamente quella che viene di fatto utilizzata dai bambini quando fanno calcoli con i numeri relativi.

Un discorso analogo può essere fatto per i numeri razionali che, ricordiamo, vengono definiti considerando l'insieme $Z \times (Z - \{0\})$ utilizzando il fatto che ogni classe in Q può essere rappresentata in un solo modo da una coppia (p,q) con p e q primi tra loro e q positivo.

Definizione 1.3. Sia Q^* l'insieme Data un coppia (n, m) di numeri relativi poniamo $f((n,m))$ uguale alla coppia (n',m') equivalente ad (n,m) con $m' > 0$ ed n', m' primi tra loro Denotiamo con Q^*

l'insieme dei valori di tale funzione e chiamiamo *in forma normale* gli elementi di tale insieme.

Ad esempio $f([(6,-10)]) = (-2,5)$ o, se vogliamo, la riduzione a forma normale di (6,-10) è (-2,5).

Proposizione 1.4. Consideriamo la struttura $(Q^*, \oplus, \otimes, (0,1), (1,1))$ in cui,
- $x \oplus y$ è uguale alla riduzione a forma normale di $x+y$
- $x \otimes y$ è uguale alla riduzione a forma normale di $x \cdot y$.

Allora f è un isomorfismo tra tale struttura è il campo dei razionali.

In definitiva quando si maneggiano gli interi relativi o i razionali di fatto è possibile maneggiare solo le forme normali ed inoltre ciascuna forma normale è un oggetto finito.

Invece il passaggio dai razionali ai reali crea un coinvolgimento inevitabile dell'infinito attuale e questo poiché, qualunque sia il modo con cui si sono costruiti i reali,

ogni numero reale è un oggetto infinito.

D'altre parte, se ci riferiamo al metodo delle sezioni ogni ed osserviamo che una sezione è costituita da due insiemi infiniti di razionali. Se invece ci riferiamo al metodo delle successioni di Cauchy, possiamo osservare che una successione di Cauchy è un oggetto infinito e che una classe completa di equivalenza di successioni di Cauchy è un oggetto infinito.[3]

Ora abbiamo già visto come, da Aristotele in poi, fosse netto nel mondo greco il rifiuto dell'infinito attuale. Tale rifiuto fu successivamente condiviso da quasi tutta la cultura occidentale fino alla fine dell'ottocento. Allo stesso tempo l'impetuoso sviluppo dell'analisi matematica dal 1600 in poi aveva fatto sì che l'uso dei metodi infinitari fosse sempre più una cosa inevitabile. L'alternativa che spesso si presentava agli scienziati dell'epoca era tra lo sterile rigore della geometria euclidea e l'uso spregiudicato dei nuovi metodi infinitari del calcolo differenziale ed integrale. A sua volta l'accettazione dei metodi infinitari rendeva l'ambito dell'algebra e della geometria greca troppo ristretto per

[3] Precisamente una successione ha la potenza del numerabile, un numero reale, visto come classe completa di successioni equiconvergenti, ha la potenza del continuo (provare a dimostrare).

la matematica moderna. Infatti, per fare un esempio, è chiaro che l'algebra e la geometria suggerivano e permettevano solo lo studio delle funzioni elementari, cioè quelle definibili geometricamente (come le funzioni trigonometriche), quelle definibili algebricamente (come i polinomi o le funzioni razionali) e quelle ottenibili per composizione da queste. Invece lo sviluppo delle serie trigonometriche determinò un enorme allargamento del campo delle funzioni note. Ci si accorse che, a partire dalle note funzioni trigonometriche, ed operando con somme infinite, era possibile pervenire a nuove funzioni che non erano definibili per via geometrica o algebrica. Era quindi necessario dare una definizione più astratta e generale del concetto di funzione.

La teoria degli insiemi proposta da Cantor alla fine del ottocento fornirà lo strumento adatto allo scopo.

2. Ma questi insiemi sono poi veramente una novità ?

> *Le generazioni seguenti considereranno la teoria degli insiemi come una malattia da cui si è guariti* (*Henri Poincaré,* 1908).

Cantor non è certo stato il primo ad utilizzare concetti come quelli di insieme, classe, collezione, i quali si sono sempre adoperati sia nel discorso scientifico che nel linguaggio comune. In effetti ogni volta che si considera una proprietà appare naturale considerare la collezione di tutti gli oggetti che verificano tale proprietà (la sua estensione). Ad esempio:
- alla proprietà di essere mammifero corrisponde "la classe di tutti i mammiferi",
- alla proprietà di riprodursi tramite uova corrisponde "la classe degli ovipari".

Ma allora se la nozione di classe è sempre esistita:
- *perché si dice che Cantor fu l'inventore della teoria degli insiemi ?*
- *in che cosa consiste la novità della sua proposta ?*
- *può esistere un mondo senza insiemi ?*

Per cercare di capire come vanno le cose, consideriamo alcune frasi del linguaggio comune, ad esempio le frasi:

a) *la rosa che è nel vaso è rossa*;
b) *le rose del vaso sono rosse*;
c) *le rose del vaso sono dodici*.

La prima frase è del tipo usuale, vi è un soggetto (la rosa che è nel vaso) ed un predicato (essere rosso).[4] Le altre due frasi coinvolgono invece collezioni di elementi (di sostanze) come testimonia l'uso del plurale "le rose", ma, a bene osservare, ciò avviene in due modi totalmente diversi. Infatti nella frase *b*) il predicato *"essere rosso"* non si riferisce all'insieme delle rose del fascio: non si è mai visto un insieme rosso. Il predicato si riferisce in realtà ai singoli elementi di tale insieme, cioè a ciascuna rosa nel vaso. La *b*) è in realtà un modo abbreviato per affermare che:

b') *ciascuna rosa che è nel vaso è rossa*.

Volendo utilizzare a tutti i costi gli insiemi, possiamo anche riscrivere la *b*) dicendo che:

b") *l'insieme delle rose del vaso è contenuto nell'insieme delle cose rosse.*

Ma si capisce che comunque in questo modo il coinvolgimento degli insiemi è inessenziale. Di natura completamente differente è invece il coinvolgimento degli insiemi nella frase *c*). Infatti:

non ha senso affermare che ciascuna rosa del vaso è *"dodici"*.

Il predicato *"avere dodici elementi"* si riferisce all'intero insieme delle rose che pertanto viene ad essere il vero soggetto della frase *c*).[5] In tale modo tale insieme viene ad assumere il carattere di sostanza individuale e diviene un nuovo soggetto (al singolare) distinto dagli elementi che lo compongono. Ora, prima di Cantor, tale oggetto non veniva considerato come ente matematico e, conseguentemente, la *c*) non risultava essere una asserzione matematica. Essa esprimeva il risultato di un esperimento (il contare) su di un oggetto e non era diversa da una frase del tipo *"la temperatura del tale corpo è di dodici gradi"*. Dopo Cantor inve-

[4] Ad una struttura della frase di tale tipo corrisponde ad una concezione del mondo secondo cui da un lato vi sono delle "sostanze" e dall'altro delle "proprietà" di cui tali sostanze possono godere o meno. Questo modo di vedere è espresso in netta da Aristotele e gli impedirà di capire il significato e l'importanza delle relazioni binarie.

[5] Nel primo volume abbiamo già osservato che la repulsione per l'infinito attuale portava i matematici greci ad affermare non che i numeri primi sono infiniti ma che "dato un numero primo *p* è possibile trovare un numero primo maggiore di *p*."

ce gli insiemi saranno visti come nuovi enti matematici e la *c*) sarà una asserzione matematica come le altre.[6]

Concludiamo questo paragrafo osservando che, in definitiva, vi sono due modi di coinvolgere una collezione di elementi in un discorso scientifico:
- Il primo si ha quando ci si riferisce a ciascun elemento della collezione stessa.
- Il secondo modo si ha quando si considera tale collezione come ente matematico a cui è possibile attribuire proprietà che non sono riconducibili ai suoi elementi.

Spesso nel primo caso si utilizza il termine "classe" e solo nel secondo caso si usa il termine "insieme" per denotare la collezione. La teoria (per meglio dire il linguaggio) delle classi è sempre esistita e non permette di dire niente di più di quanto permetta il linguaggio comune. La zoologia, la mineralogia l'hanno spesso utilizzata e la parola "classificare" è costantemente presente in tali scienze. Agli oggetti ed alle proprietà si sostituiscono gli elementi e le classi (estensioni di tali proprietà). Alla congiunzione logica "e" ed alla disgiunzione "o" si sostituiscono le operazioni di intersezione e di unione, alla negazione si sostituisce la complementazione, alla implicazione la relazione di inclusione.

La teoria degli insiemi nasce invece con Cantor ed il suo significato si manifesta esclusivamente nell'ambito matematico. Sue caratteristiche peculiari furono l'esame della "grandezza" degli insiemi ed il tentativo di procedere ad una fondazione di tutta la matematica. Quella che molti studenti hanno imparato nelle scuole è solo la teoria delle classi, o, per meglio dire, il linguaggio delle classi. Facciamo invece teoria degli insiemi quando (in generale nelle elementari) si parla di "cardinalità" di un insieme finito tramite il concetto di equipotenza. Ancora si utilizza la teoria degli insiemi quando si costruisce il campo dei

[6] Ricordiamo che già c'era stato un momento dell'evoluzione della matematica in cui questa aveva allargato il proprio ambito creando nuovi enti astratti. Mi riferisco al processo di idealizzazione degli enti geometrici in cui proprietà come "*essere retto*", *"essere circolare"*, *"essere quadrato"* vengono sostituite da enti astratti come *"la retta"*, *"il cerchio"*, *"il quadrato"*.

numeri reali con il metodo delle sezioni o con un qualunque altro metodo.[7]

3. I paradossi dell'infinito

Una delle prime domande che un matematico si pone riguarda la grandezza degli enti matematici che si propone di studiare. Ed infatti la parte centrale degli studi di Cantor sugli insiemi riguarda la loro grandezza, o per meglio dire, la loro cardinalità. Siamo nel 1874 quando appaiono i primi articoli di Cantor in proposito ma già Galileo nel 1638 nel suo *Discorsi e dimostrazioni Matematiche intorno a due nuove scienze* si era posto il problema sulla possibilità di confrontare la grandezza di due insiemi infiniti. La risposta di Galileo a questa domanda fu nettamente negativa, e questo in base ad alcune conseguenze paradossali che si hanno se si accetta tale possibilità.

Il paradosso dei quadrati perfetti. Galileo confrontò l'insieme N degli interi e l'insieme QP dei quadrati perfetti e giunse alla paradossale conclusione che tali insiemi hanno lo stesso numero di elementi. Infatti egli osservò che ad ogni intero n è possibile associare il quadrato perfetto n^2 ottenendo in tale modo la tabella

1 2 3 4 5 6 . . .
1 4 9 16 25 36 . . .

[7] Tale distinzione è importante anche per comprendere il significato che ha l'introduzione (eventuale) della teoria degli insiemi nelle scuole. A volte si definisce il massimo comune divisore tra i numeri n ed m come "l'elemento massimo dell'intersezione tra l'insieme dei divisori di n e l'insieme dei divisori di m". A me sembra un modo inutilmente complicato di dare la definizione! Il linguaggio comune in questo caso è più che sufficiente e non c'è modo più semplice di definire il massimo comune divisore che affermare che è "il massimo dei divisori comuni". Un altro esempio di apparente introduzione della teoria degli insiemi è quando, ad esempio, per illustrare la nozione di intersezione, si dice che la balena è un elemento di intersezione tra l'insieme degli animali acquatici e l'insieme dei mammiferi. Anche in questo caso sembra più semplice dire che la balena è un mammifero che vive nell'acqua senza disturbare l'operazione di intersezione.

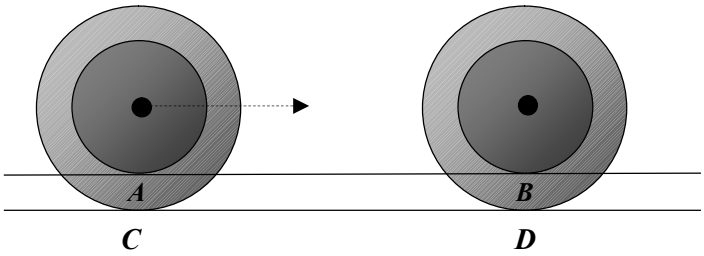
Naturalmente in tale modo a numeri distinti corrispondono quadrati distinti ed ogni quadrato si può ottenere in questo modo (in termini moderni diremmo che la corrispondenza è biettiva) ciò prova che ci sono tanti elementi in N quanti ce ne sono in QP. Ora una tale conclusione non appariva a Galileo soltanto contraria al senso comune (paradossale) ma anche contraddittoria. Precisamente era in contraddizione con l'assioma euclideo "il tutto è maggiore della parte" che Galileo, grande ammiratore di Euclide, non si sognava di mettere in discussione.

Nel paradosso ora descritto abbiamo utilizzato il fatto che la successione $(n^2)_{n\in N}$ è iniettiva e quindi N è equipotente all'insieme dei suoi elementi.

Come vedremo, Cantor, al contrario di Galileo, non esitò a gettare via l'assioma di Euclide accettando tranquillamente la possibilità che esistano insiemi che hanno tanti elementi quanti una loro parte propria.[8]

Problema: Provare che N ha tanti numeri quanti ne ha l'insieme $\{10, 11, 12, \ldots\}$ dei numeri da 10 in poi.

Il Paradosso delle ruote concentriche: Questo paradosso, descritto da Galileo, sembra risalire ad Aristotele. Consideriamo due ruote concentriche incollate una sull'altra, di raggi 0.5 ed 1 e supponiamo di far fare alla più grande un giro completo in modo che rotolando tracci un segmento CD.



Nel frattempo anche la ruota più piccola avrà fatto un giro completo ed avrà tracciato un segmento AB della stessa lunghezza di CD. Ma questo è assurdo perché i due segmenti rappresentando

[8] Questa proprietà diventerà proprio un modo di definire gli insiemi infiniti. Quindi si potrebbe dire che un insieme è infinito se verifica il paradosso di Galileo.

lo "srotolamento" di due circonferenze di lunghezza π e 2π dovrebbero essere uno minore dell'altro. Ecco quello che dice Galileo:

> *"Or come dunque può senza salti scorrere il cerchio minore una linea tanto maggiore della sua circonferenza ?".*

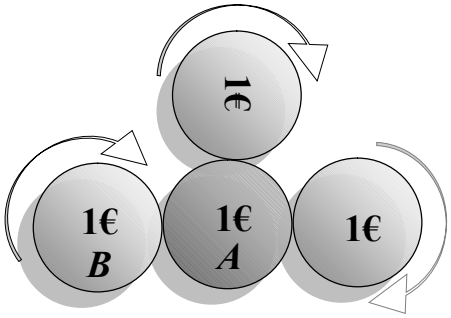
Comunque la conclusione a cui Galileo pervenne fu non tanto che non fosse possibile considerare l'infinito attuale (come affermato dalla tradizione aristotelica) ma che la comprensione dell'infinito attuale forse era al di fuori delle capacità dell'essere umano. Egli infatti asserisce che quando

> *siamo tra gli infiniti e gli indivisibili, quelli sono incomprensibili dal nostro intelletto finito per la loro grandezza, e questi per la loro piccolezza.*

Dove il termine "indivisibile" si riferisce agli infinitesimi che in quel periodo, ad opera del Cavalieri, si andavano utilizzando.

Paradosso delle due monete. Un paradosso simile a quello di Aristotele si ottiene supponendo di porre su di un tavolo due monete uguali *A* e *B* in modo che si tocchino in un punto *P*, di tenere fissa *A* e di fare ruotare di un giro intero *B* mantenendo sempre un punto *P* di contatto. Ci si accorge che alla fine della rotazione *B* non ha percorso tutta la circonferenza di *A* ma solo la metà e che quindi il punto *P* di contatto:

- visto come punto di *A* percorre la lunghezza π
- visto come punto di *B* percorre la lunghezza 2π.



Paradosso delle serie. I paradossi che abbiamo visto fino ad ora sono legati alla nozione di "grandezza". Altri paradossi sono le-

gati alla nozione di "somma infinita". Ne abbiamo già visto uno nel primo volume quando abbiamo parlato del paradosso di Zenone. Un altro, oggetto di discussione agli inizi del settecento, è il seguente. Consideriamo la somma infinita

+1-1+1-1+...

che si ottiene alternando +1 e -1 e cerchiamo di capire quale è il valore di tale somma.[9] Una possibile risposta è che sia uguale a zero. Infatti se raggruppano gli elementi di tali somme nella sequenza

(+1-1)+(+1-1)+...

allora eseguendo le sottrazioni tra parentesi ed effettuando una somma di infiniti zero, si ottiene zero. Ma possiamo ottenere anche 1. Infatti basta isolare il primo 1 e poi raggruppare le coppie di successivi numeri ed ottenere pertanto

1+(-1+1)+(-1+1)+ ... .

Padre Guido Grandi sosteneva che la somma fosse uguale a 0.5. Infatti egli argomentava al modo seguente. Supponiamo che due fratelli ereditino un prezioso gioiello e che, non volendolo vendere o dividere in due, si accordassero che un giorno dovesse essere tenuto dal fratello A e l'altro anno dal fratello B. Allora il tempo di possesso di un fratello risulterebbe uguale a quello dell'altro e quindi uguale a 0.5.[10]

Una argomentazione più convincente, ma sempre a favore del valore 0.5, era data da Leibniz che sosteneva che se si interrompe a caso il calcolo del valore della serie, allora la somma può fornire il valore 0 o 1 e questo con la stessa probabilità. Quindi il valore della somma infinita, dovendosi collocare a metà strada tra 0 ed 1, deve essere uguale a 0.5. In termini attuali diremmo che il valore di aspettazione (o valore medio) della sequenza è 0.5.

---

[9] Se ci si riferisce alla definizione attuale di somma di una serie, tale serie risulta non convergente in quanto la successione delle somme parziali passa alternativamente da 0 ad 1.

[10] Il fatto che fosse possibile fare passare il valore della serie da 0 a 0.5 oppure ad 1 veniva visto da padre Grandi non come una contraddizione ma come prova che Dio, nella sua infinità, potesse creare dal nulla il tutto. Evidentemente la stessa cosa potrebbe essere detta utilizzando la teoria degli insiemi in cui si vede che è possibile aggiungere un elemento ad un insieme infinito senza alterare la grandezza di tale insieme. E' interessante confrontare queste argomentazioni con il paradosso dei pani e dei pesci di cui si parla nel secondo capitolo.

4. Equipotenza: confrontare le grandezze degli insiemi

Nel seguito supporremo come note varie nozioni elementari di teoria degli insiemi come quella di unione, intersezione, complemento, insieme vuoto, relazione, funzione, ed altro. Procederemo ad un livello completamente intuitivo riferendoci ad una idea di insieme che sembrerebbe tutti abbiano nella propria testa. Più in avanti tenteremo di indicare una teoria assiomatica degli insiemi.

Focalizzeremo invece l'attenzione sulla possibilità di confrontare le grandezze di insiemi, possibilità che costituisce la vera caratteristica della teoria degli insiemi.

Definizione 4.1. Diciamo che due insiemi A ed B *sono equipotenti* e scriviamo $A \equiv B$ se esiste una corrispondenza biettiva $f : A \to B$ di A in B. Inoltre si assume che $\varnothing \equiv B$ se e solo se $B = \varnothing$.

In altri termini due insiemi non vuoti A e B sono equipotenti se esiste un procedimento che permette di ottenere, a partire da un elemento di A, uno ed un solo elemento di B in modo che

- ad elementi distinti di A corrispondano elementi distinti di B
- ogni elemento di B si può ottenere in questo modo.

Nel paradosso dei quadrati perfetti tale corrispondenza era ottenuta tramite l'elevazione al quadrato. Ovviamente nel caso di insiemi finiti si ha che due insiemi sono equipotenti se e solo se hanno lo stesso numero di elementi nel senso intuitivo che diamo a questa espressione.

Teorema 4.2. Comunque si considerino gli insiemi A, B e C

1. $A \equiv A$
2. $A \equiv B$ implica $B \equiv A$
3. $A \equiv B$ e $B \equiv C$ implica $A \equiv C$.

Dim. Se $A = \varnothing$ il teorema è ovvio.

1. Sia $A \neq \varnothing$, allora l'applicazione identica $i : A \to A$ è una funzione biettiva di A in A. Quindi A è equipotente ad A.
2. Sia A equipotente a B, allora esiste una corrispondenza biettiva $f : A \to B$. La sua funzione inversa sarà allora una corrispondenza biettiva di B in A e questo prova che B è equipotente ad A.
3. Supponiamo che A abbia potenza uguale B e che B abbia potenza uguale a C, allora esistono due funzioni biettive $f : A \to B$ e

g: $B \to C$. E' evidente che fg è una funzione biettiva di A in C e quindi che A e C sono equipotenti. □

Si potrebbero sintetizzare le tre proprietà ora dimostrate dicendo che la relazione di equipotenza è una relazione di equivalenza. Purtroppo ciò non sarebbe completamente corretto. Infatti tale relazione dovrebbe essere definita nella classe di tutti gli insiemi e tale classe, come vedremo nel prossimo capitolo, crea problemi poiché è fonte di paradossi. Insomma le cose sono sempre più complicate di come si pensa.

Definizione 4.3. Diciamo che *la potenza di A è minore o uguale della potenza di B* e scriviamo $A \leqq B$ se esiste una corrispondenza iniettiva di A in B. Inoltre si assume che $\varnothing \leqq B$ per ogni B.

A volte, invece di usare la parola *"potenza"* si usa la parola *"cardinalità"*.

Teorema 4.4. La relazione $\leqq$ è un preordine, cioè, dati gli insiemi A, B e C, sono verificate le seguenti proprietà:

i) $A \leqq A$ (riflessiva)

ii) se $A \leqq B$ e $B \leqq C$ allora $A \leqq C$ (transitiva).

Dim. Si procede allo stesso modo che nei punti 2 e 3 del Teorema 4.2. □

Proprietà della relazione $\leqq$ che sono un po' più difficili da provare sono le seguenti e saranno provate nel seguito.

Teorema 4.5. Dati due insiemi A e B risulta che:

i) $A \leqq B$ e $B \leqq A$ implica $A \equiv B$ (Teorema di Cantor-Bernstein)

ii) o $A \leqq B$ oppure $B \leqq A$ (Teorema di Hartogs o dell'ordine totale).

Il teorema di Cantor-Bernstein mostra che l'equivalenza associata al preordine $\leqq$ è l'equipotenza. Il teorema di Hartogs ci dice che il preordine $\leqq$ è una relazione totale.

Problema. Indichiamo con R l'insieme dei numeri reali e con R_+ l'insieme dei reali maggiori o uguali a zero, allora la funzione f:

$R_+ \to R$ che associa ad ogni numero x il suo quadrato non è suriettiva in quanto il valore -1 non può essere assunto da f. Si può affermare che R_+ ed R non sono equipotenti? (attenti al significato del quantificatore esistenziale).

Problema. Dimostrare che a Salerno esistono due persone che hanno esattamente lo stesso numero di capelli. Nella dimostrazione si devono utilizzare i due fatti seguenti:

- un essere umano non ha mai più di 130.000 capelli.
- a Salerno vivono più di 200.000 persone.

5. L'assioma della scelta

Molti importanti teoremi si possono provare solo se si accetta che la classe degli insiemi verifica un particolare assioma che è noto sotto il nome di *"assioma della scelta"*. Per poterlo enunciare premettiamo la seguente definizione.

Definizione 5.1. Sia S un insieme e Σ una classe non vuota di sottoinsiemi non vuoti di S. Si chiama *funzione di scelta* su Σ ogni funzione $f: \Sigma \to \cup_{X \in \Sigma} X$ tale che $f(X) \in X$ per ogni $X \in \Sigma$.

La funzione di scelta viene chiamata in questo modo poiché permette di *"scegliere"* in ogni insieme $X \in \Sigma$ un suo elemento $f(X)$.

(**Assioma della scelta)**. Ogni classe Σ di insiemi non vuoti ammette una funzione di scelta.

In realtà, poiché solo più in avanti tratteremo la teoria degli insiemi in modo assiomatico, non dovremmo ancora parlare di assioma ma di asserzione valida nell'universo degli insiemi. Per capire il significato di tale assioma possiamo ricorrere al seguente esempio suggerito da Bertrand Russell.

Scarpe e calzini. Supponiamo preliminarmente di avere una famiglia infinita $(S_i)_{i \in I}$ di paia di scarpe (possiamo visualizzare S_i come una scatola su cui è attaccata una etichetta i per distinguerla dalle altre) e di voler individuare una "funzione di scelta" che permetta di scegliere in ogni S_i una scarpa $f(i) \in S_i$ particolare. In questo caso non ci sono difficoltà, possiamo scegliere in ogni

paio, ad esempio, la scarpa destra. Supponiamo invece di disporre una famiglia infinita $(C_i)_{i\in I}$ di paia di calzini. Allora poiché i due calzini di un dato paio non sono distinguibili, non sarà semplice definire una funzione di scelta che consenta di scegliere in ogni paio C_i un particolare calzino. L'assioma della scelta afferma che una tale funzione di scelta esiste e questo indipendentemente dal fatto che si sia capaci di descriverla.

In effetti è difficile capire perché si debba assumere come assioma una cosa tanto evidente ed intuitiva. Il fatto è che la nostra intuizione si basa su esperienze di collezioni finite di oggetti ma non è detto che tale intuizione rimanga valida quando vengono coinvolti insiemi infiniti.

Un modo leggermente diverso di riformulare l'assioma della scelta è utilizzare la nozione di *famiglia di insiemi* invece che quella di classe di insiemi. Infatti, data una famiglia $(A_i)_{i\in I}$ di insiemi non vuoti possiamo chiamare *funzione di scelta* ogni funzione $f: I \to \cup_{i\in I} A_i$ tale che $f(i)\in A_i$.

Assioma della scelta. Per ogni famiglia $(A_i)_{i\in I}$ di insiemi non vuoti esiste una funzione di scelta.[11]

Con questa formulazione è possibile dimostrare il seguente teorema che mostra come in molti casi diamo per scontato fatti per la cui dimostrazione è invece necessario l'assioma della scelta.

Teorema 5.2. Accettiamo l'assioma della scelta. Allora il prodotto cartesiano di insiemi non vuoti è non vuoto. In altri termini, data una qualunque famiglia di insiemi non vuoti $(A_i)_{i\in I}$:

[11] Alessandro Andretta nei suoi appunti di teoria degli insiemi (reperibili in rete e che suggerisco di scaricare) osserva che l'uso di lettere indicizzate può nascondere alcuni aspetti delicati. Ad esempio, supponiamo di avere una famiglia $(A_i)_{i\in I}$ di insiemi con $I \neq \emptyset$ ed $A_i \neq \emptyset$ per ogni $i\in I$. Possiamo allora scrivere che $\forall i\in I(\exists x\in A_i)$. Viene allora naturale riformulare la condizione $\exists x\in A_i$ come "esiste $a_i \in A_i$". Tuttavia la scrittura "a_i" sottintende l'esistenza di una funzione f che ad $i\in I$ associa $f(i) = a_i \in A_i$. In altre parole, siamo passati dall'ipotesi originale "$\forall i\in I\ \exists x\in A_i$" a "$\exists f\ \forall i\in I(f(i)\in A_i)$" scambiando in un certo senso l'ordine dei quantificatori. L'assioma di scelta asserisce che questo scambio è lecito.

$$A_i \neq \emptyset \ \forall i \in I \Rightarrow \ \times_{i\in I} A_i \neq \emptyset.$$

Dim. Basta osservare che la definizione di prodotto cartesiano di una famiglia di insiemi (si veda l'appendice) è proprio che $\times_{i\in I} A_i$ coincide con l'insieme di tutte le funzioni di scelta per la famiglia $(A_i)_{i\in I}$. □

Un altro esempio di proprietà elementare per la cui dimostrazione si rende necessario l'assioma della scelta è il seguente. E' evidente che se un mucchio A di oggetti viene ripartito in più mucchietti, allora il numero di mucchietti è inferiore al numero di elementi di A. Detto in linguaggio insiemistico, se A è un insieme finito e Σ una partizione di A allora Σ ha un numero di elementi minore o uguale a quello di A. Per estendere una proprietà tanto semplice agli insiemi infiniti abbiamo bisogno dell'assioma della scelta.

Teorema 5.3. Accettiamo l'assioma della scelta, allora dato un insieme non vuoto A ogni partizione di A ha potenza minore o uguale ad A.

Dim. Se Σ è una partizione di A allora esiste una funzione $f : \Sigma \to A$ che associa ad ogni elemento di $Z \in \Sigma$ un elemento $f(Z) \in Z$. La funzione f è iniettiva perché se $f(Z) = f(Z') = c$ allora Z e Z' hanno l'elemento c in comune e quindi coincidono. Questo mostra che la potenza di Σ è minore di quella di A. □

Se si tiene conto del legame stretto che intercorrre tra la nozione di partizione e quella di quoziente modulo una equivalenza, è possibile riformulare tale proposizione al modo seguente.

Proposizione 5.4. Supponiamo che valga l'assioma della scelta. Allora dato un insieme non vuoto A ed una relazione di equivalenza $\equiv$ in A, il quoziente $A/\equiv$ ha potenza minore o uguale ad A.

Ne segue il seguente corollario dove si ricorda che il nucleo di una funzione f è l'insieme $\{(x, y) : f(x) = f(y)\}$ cioè la relazione di equivalenza definita dall'essere $x \equiv y$ se e solo se $f(x) = f(y)$.

Proposizione 5.5. Sia $f : A \to B$ suriettiva e $\equiv$ il nucleo di f, allora B è equipotente a $A/\equiv$ e quindi ha potenza minore o uguale ad A.

Dim. Consideriamo la funzione $g : A/\equiv \to B$ definita ponendo $g([x]) = f(x)$. Tale funzione è ben definita perché il suo valore non dipende dall'elemento rappresentativo in $[x]$. Inoltre, poiché

$$g([x]) = g([y]) \Rightarrow f(x) = f(y) \Rightarrow x \equiv y \Rightarrow [x] = [y],$$

g è iniettiva. Questo prova che $A/\equiv$ è equipotente a B. □

Una proprietà che risulta essere equivalente all'assioma della scelta è utilizzata spesso dai matematici. Essa è espressa dal seguente teorema di cui omettiamo la dimostrazione.

Teorema 5.6. (Lemma di Zorn). Sia $(S,\leq)$ un insieme ordinato e supponiamo che ogni catena abbia un maggiorante, allora $(S,\leq)$ ha un elemento massimale.

Questo lemma permette di *"costruire"* oggetti matematici. Ecco un esempio di sua utilizzazione.

Teorema 5.7. (Teorema di Hartogs o dell'ordine totale). Per ogni coppia di insiemi A e B risulta che $A \leqq B$ oppure $B \leqq A$

Dim. Se $A = \varnothing$ oppure se $B = \varnothing$ la proposizione è dimostrata poiché abbiamo assunto che l'insieme vuoto ha la cardinalità minore di quella di ogni altro insieme. Se A e B sono entrambi non vuoti, ci proponiamo di trovare una funzione iniettiva parziale $f : A \to B$ tale che
- o $dom(f) = A$
- oppure $cod(f) = B$.

Infatti nel primo caso risulterebbe $A \leqq B$ essendo f una funzione totale iniettiva di A in B. Nel secondo caso risulterebbe che $B \leqq A$ essendo f^{-1} una funzione totale ed iniettiva in B in A. Tentiamo di trovare tale funzione nel caso in cui A e B siano finiti. Procedendo in modo intuitivo, detto a_1 un elemento di A possiamo scegliere un elemento b_1 in B come immagine di a_1 e quindi considerare l'insieme $f_1 = \{(a_1,b_1)\}$ che interpretiamo come funzione parziale con $dom(f_1) = \{a_1\}$ e $cod(f_1) = \{b_1\}$. Se $dom(f_1) = A$ o $cod(f_1) = B$ possiamo porre $f = f_1$. In caso contrario, cioè nel caso in cui $A - \{a_1\} \neq \varnothing$ e $B - \{b_1\} \neq \varnothing$, prendiamo in A un elemento

$a_2 \neq a_1$ ed in B un elemento $b_2 \neq b_1$ ottenendo la funzione parziale iniettiva $f_2 = \{(a_1,b_1), (a_2,b_2)\}$ con $dom(f_2) = \{a_1, a_2\}$ e $cod(f_2) = \{b_1, b_2\}$. Se $dom(f_2) = A$ o $cod(f_2) = B$ poniamo $f = f_2$, in caso contrario esiste a_3 in A con $a_3 \neq a_1$ e $a_3 \neq a_2$, e b_3 in B con $b_3 \neq b_1$ e $b_3 \neq b_2$ e quindi è possibile considerare la funzione parziale iniettiva $f_3 = \{(a_1,b_1), (a_2,b_2), (a_3, b_3)\}$. .. Procedendo in questo modo, stante la finitezza di A e di B, si crea una catena finita $f_1 \subsetneq f_2 \subsetneq \ldots \subsetneq f_n$ di funzioni iniettive con $dom(f_n) = A$ oppure $cod(f_n) = B$ e quindi basta porre $f = f_n$.

Naturalmente nel caso infinito questo modo di procedere non funziona più. Inoltre utilizza in modo intuitivo la nozione di insieme finito che tratteremo solo nel prossimo paragrafo. Per trovare una dimostrazione più adeguata del teorema, consideriamo l'insieme ordinato $(Par(A,B), \subseteq)$ dove $Par(A,B)$ è l'insieme delle funzioni parziali iniettive di A in B e $\subseteq$ l'usuale inclusione. Allora data una catena C di elementi di $(Par(A,B), \subseteq)$ la relazione ottenuta effettuando l'unione di tutte le funzioni parziali in C (viste come relazioni binarie) è una funzione parziale iniettiva. Per il Lemma di Zorn ciò comporta che esiste in $Par(A, B)$ un elemento massimale h. Sostengo che o $dom(h) = A$ oppure $cod(h) = B$. Infatti in caso contrario esisterebbero $a \in A\text{-}dom(h)$ e $b \in B\text{-}cod(h)$ e la funzione h si estenderebbe nella funzione $h \cup \{(a,b)\}$ in contrasto con la massimalità di h. □

6. Una questione complicata: cosa significa essere finito?

Fino ad ora abbiamo parlato di insiemi finiti ed infiniti basandoci su una idea intuitiva di cosa significano queste parole. Si pone il problema di come si possano dare precise definizioni del loro significato. Naturalmente è sufficiente dare una definizione di insieme finito e poi dire che un insieme è infinito se non è finito (o viceversa).

La questione è un po' più complessa di come sembra. Il modo più naturale sembra essere quello basato sul contare.

Un insieme è infinito se non posso mai finire di contarne gli elementi, finito altrimenti.

E' possibile precisare tale modo di procedere definendo i *segmenti iniziali* di N per ricorsione:

- indichiamo con $\{1\}$ l'insieme con unico elemento 1
- poniamo $\{1,...,n+1\} = \{1,...,n\} \cup \{n+1\}$.

Detto in parole povere, $\{1,\ldots,n\}$ è l'insieme dei primi n numeri di N.

Definizione 6.1. Un insieme non vuoto si dice *SI-finito* se è equipotente ad un segmento iniziale di numeri naturali. Si dice *SI-infinito* se non è *SI*-infinito (il prefisso *SI* ricorda '*segmento iniziale'*).

In altre parole, si considerano i segmenti iniziali come prototipi degli insiemi finiti e si chiama finito un insieme che è equipotente ad uno di tali prototipi. Da notare che una tale definizione ci permette di descrivere un qualunque insieme *SI*-finito con la notazione $\{a_1,...,a_n\}$ in quanto il mettere gli indici 1, …,*n* ai suoi elementi equivale appunto a fissare una funzione biettiva tra un segmento iniziale e gli elementi dell'insieme.

Un modo differente di procedere punta invece a considerare l'insieme *N* dei naturali positivi come prototipo di insieme infinito ed a chiamare infiniti gli insiemi che siano più grandi di *N*.

Definizione 6.2. Un insieme non vuoto si dice *N-infinito* se ha potenza maggiore o uguale ad *N*, si dice *N-finito* altrimenti (il prefisso *N* ricorda i numeri naturali).

Tuttavia entrambe le definizioni hanno il difetto di dare per noti i numeri naturali mentre con la teoria degli insiemi si vorrebbe costruire l'intero edificio matematico, compreso *N*.

Una definizione che invece evita questo riferimento prende spunto dal paradosso di Galileo. Infatti in un certo senso viene chiamato infinito un insieme per cui si possa riprodurre tale paradosso.

Definizione 6.3. Un insieme non vuoto si dice *D-infinito* se è equipotente ad una sua parte propria, si dice *D-finito* altrimenti (il prefisso *D* ricorda il matematico Dedekind che ha proposto tale definizione).

Tale definizione pur non essendo molto naturale è quella attualmente più utilizzata da chi vuole fondare l'intera matematica su nozioni insiemistiche. Infatti, come abbiamo visto nel primo volume, se si postula l'esistenza di un insieme infinito allora è possibile definire una terna di Peano-Dedekind e poi procedere alla costruzione dei numeri reali e così via. Questo impedisce di utilizzare i naturali per definire gli insiemi infiniti.

Si pone il problema se tali definizioni siano equivalenti. Per potere rispondere abbiamo bisogno dei seguenti lemmi.

Lemma 6.4. La nozione di *D*-infinito è compatibile con la relazione di equipotenza. In altri termini, se $S' \equiv S$ S ed S è *D*-infinito e allora S' è *D*-infinito.

Dim. Sia f una funzione iniettiva di S in una parte propria di S e $g : S \to S'$ è una funzione biettiva di S in S', allora ponendo

$$f'(x) = g(f(g^{-1}(x)))$$

si ottiene una funzione di S' in una parte propria di S'. Infatti se $c \in S\text{-}f(S)$, allora $g(c) \in S'\text{-}f'(S')$. □

Teorema 6.5. Un insieme è *N*-infinito se e solo se è *D*-infinito e quindi è *N*-finito se e solo se è *D*-finito.

Dim. Sia S un insieme *N*-infinito, allora esiste una funzione iniettiva $f : N \to S$ di N in S. Consideriamo la funzione $g : S \to S$ definita ponendo $g(x) = x$ se $x \notin f(N)$ e $g(f(n)) = f(n+1)$ altrimenti. In altri termini tale funzione sposta di un passo gli elementi della successione $f(n)$ e lascia immutati gli altri elementi di S. Poiché g non può assumere il valore $f(1)$, g è una funzione biettiva di S nella sua parte propria $S\text{-}\{f(1)\}$. Ciò prova che S è *D*-infinito.

Viceversa, sia S un insieme *D*-infinito, allora nel primo volume abbiamo già visto che all'interno di S è possibile definire una terna di Peano. Pertanto, essendo tutte le terne di Peano isomorfe e quindi equipotenti tra loro, S ha potenza maggiore o uguale ad N. Possiamo provare la stessa cosa in maniera più esplicita al modo seguente. Supponiamo che h sia una funzione iniettiva di S in se che non sia suriettiva e sia $c \in S\text{-}h(S)$. Allora possiamo considerare la funzione $f : N \to S$ definita ponendo $f(n) = h^n(c)$. Tale funzione non è suriettiva poiché c, non potendo essere uno dei valori di h non può essere nemmeno uno dei valori assunti da f. Inoltre f è iniettiva poiché altrimenti, detti m, n due naturali tali $m \neq n$ e $f(n) = f(m)$ risulta che $h^m(c) = h^n(c)$. Supposto ad esempio che $m > n$, avremmo allora che $h^{m-n}(c) = h^{n-n}(c) = c$. Ma ciò è in contrasto con il fatto che $c \notin h(S)$. □

La questione se la nozione di *SI*-infinito coincida con le altre due nozioni di infinito è invece più problematica. Infatti per provare che ciò è vero siamo costretti ad utilizzare l'assioma del-

la scelta.[12] Anche in questo caso abbiamo bisogno di un paio di lemmi.

Lemma 6.6. Supponiamo che S sia D-infinito e fissiamo un qualunque $a \in S$, allora esiste una funzione iniettiva $h : S \to S$ tale che $a \notin h(S)$.

Dim. Per ipotesi esiste $f : S \to S$ iniettiva ma non suriettiva e quindi esiste $\underline{a} \in S\text{-}f(S)$. Sia $f_{a \rightleftarrows \underline{a}}$ la funzione che scambia i due elementi a ed $\underline{a}$. Allora la funzione h definita ponendo $h(x) = f_{a \rightleftarrows \underline{a}}((f(x))$ è iniettiva. Se esistesse x tale che $h(x) = f_{a \rightleftarrows \underline{a}}(f(x)) = a$ avremmo che

$$f(x) = f_{a \rightleftarrows \underline{a}}(f_{a \rightleftarrows \underline{a}}((f(x))) = f_{a \rightleftarrows \underline{a}}(h(x)) = f_{a \rightleftarrows \underline{a}}(a) = \underline{a}$$

in contrasto con l'ipotesi per cui $\underline{a} \notin f(S)$. □

Da notare che la definizione di insieme D-infinito è

esiste $h : S \to S$ iniettiva per cui esiste $s \in S$ ed tali che $s \notin h(S)$.

Il lemma 6.6. dice qualcosa di più:

per ogni $s \in S$ esiste $h : S \to S$ iniettiva tali che $s \notin h(S)$.

In altre parole dice che s lo possiamo fissare noi a piacere.

Il secondo lemma viene anche chiamato "principio dei cassetti" poiché afferma che se $m > n$ allora è impossibile mettere m oggetti in n cassetti se non infilando due oggetti nello stesso cassetto.

Lemma 6.7. (Principio dei cassetti). Nessun segmento iniziale $\{1,\ldots,m\}$ può essere equipotente ad una sua parte propria.

Dim. Supponiamo per assurdo che $\{1,\ldots,m\}$ sia equipotente ad una sua parte propria, non è restrittivo supporre che m sia il più piccolo dei naturali per cui ciò avviene. Allora per il lemma 7.6 esiste $h : \{1,\ldots,m\} \to \{1,\ldots,m\}$ iniettiva con $m \notin h(\{1,\ldots,m\})$. Quindi h è in realtà un'applicazione iniettiva di $\{1,\ldots,m\}$ in $\{1,\ldots,m\text{-}1\}$. La restrizione di h a $\{1,\ldots,m\text{-}1\}$ continua ad essere iniettiva. Pertanto $\{1,\ldots,m\text{-}1\}$ è equipotente ad una sua parte propria in contrasto con l'ipotesi di minimalità per m. □

[12] Si veda anche il bel libro di Gabriele Lolli "Guida alla teoria degli insiemi", libro che consiglio per il rigore e la semplicità.

Teorema 6.8. Accettiamo l'assioma della scelta. Allora un insieme è *SI*-infinito se e solo se è *N*-infinito. Pertanto le tre definizione di infinito coincidono.

Dim. Supponiamo che *S* sia *SI*-infinito cioè che sia non vuoto e non sia equipotente ad un segmento iniziale $\{1,\ldots,n\}$. Vogliamo definire una funzione iniettiva di *N* in *S.* A tale scopo fissato un elemento *a* di *S*, possiamo definire, per induzione su *n*, la funzione $f: N \to S$ ponendo

$f(1) = a$

$f(n+1)$ è uguale ad un elemento scelto[13] in $S-\{f(1),\ldots,f(n)\}$.

Quest'ultimo insieme infatti è non vuoto poiché essendo *S* un insieme *SI*-infinito non può essere equipotente ad un segmento iniziale. E' evidente che *f* è una funzione iniettiva di *N* in *S* e che quindi *S* è *N*-infinito.

Assumiamo che *S* sia *N*-infinito e quindi, per il teorema 6.5, che sia *D*-infinito e supponiamo per assurdo che *S* non sia *SI*-infinito. Allora esiste una funzione biettiva *f* tra un segmento iniziale $\{1,\ldots,n\}$ ed *S* e quindi, per il Lemma 6.4 avremmo che anche tale segmento è *D*-infinito in contrasto con il principio dei cassetti. □

Poiché i matematici usualmente lavorano utilizzando l'assioma della scelta, nel seguito userò solo le parole *"finito"* ed *"infinito"* senza le distinzioni fatte in questo paragrafo.

7. Insiemi numerabili ed insiemi enumerabili

N è il primo esempio di insieme infinito che abbiamo incontrato. Allora è naturale confrontare la grandezza degli altri insiemi con quella di *N*.

Definizione 7.1. Gli insiemi equipotenti ad *N* vengono detti *numerabili*, gli insiemi che hanno potenza minore od uguale ad *N* vengono chiamati *enumerabili.*[14]

---

[13] E' qui che si utilizza l'assioma della scelta. E' stato dimostrato che l'uso di tale assioma è essenziale.

[14] La nozione di insieme enumerabile non sembra essere usata molto nei libri italiani di matematica. Nei libri in lingua inglese di matematica invece viene considerata e si parla di *countable set*. Invece in informatica teorica si parla di *effettivamente enumerabile* (in inglese *effectively*

Pertanto un insieme A
- è numerabile se esiste una funzione $f : A \to N$ biettiva,
- è enumerabile se esiste una funzione $f : A \to N$ iniettiva.

L'insieme vuoto si considera enumerabile. La parola "enumerabile" si giustifica con la *c*) della seguente proposizione

In termini intuitivi un insieme non vuoto è enumerabile se si possono *"numerare"* tutti gli elementi di A uno dopo l'altro in una successione dicendo che

$f(1)$ è il primo elemento
$f(2)$ è il secondo elemento
. . .

ed in tale numerazione nessun elemento di A deve sfuggire (f è suriettiva). Se in tale enumerazione non esistono ripetizioni, essendo f anche iniettiva, A risulta essere numerabile. In proposito si consiglia di leggere l'esempio di lezione di teoria degli insiemi per un liceo che ho riportato alla fine del capitolo.

Proposizione 7.3. L'unione di due insiemi enumerabili è un insieme enumerabile.

Dim. Siano A e B due insiemi enumerabili e siano $f : N \to A$ e $g : N \to B$ due funzioni enumeranti A e B. Intuitivamente il processo di enumerazione di $A \cup B$ consiste nell'alternare la numerazione di A e di B, cioè nel considerare la seguente successione

$f(1), g(1), f(2), g(2), \ldots$

Più precisamente, possiamo considerare la funzione $h : N \to A \cup B$ definita ponendo

$$h(n) = \begin{cases} f((n+1)/2) & \text{se } n \text{ è dispari} \\ g(n/2) & \text{se } n \text{ è pari.} \end{cases}$$

Poiché h è suriettiva, h è una funzione enumerante $A \cup B$.[15] □

enumerable) per indicare un insieme A per cui esiste una funzione suriettiva $f : N \to A$ che sia effettivamente computabile.

[15] Si noti che se A e B hanno elementi in comune la funzione h non è iniettiva.

Proposizione 7.4. L'unione di un insieme numerabile ed uno finito è un insieme numerabile. L'unione di due insiemi numerabili è un insieme numerabile.[16]

Dim. Sia S numerabile ed A finito. Supponiamo che $A = \{a_1,...,a_p\}$ e che $f : N \to S$ sia una funzione biettiva enumerante S. In tale caso una numerazione di $A \cup S$ sia ottiene al modo seguente:

$a_1, a_2,..., a_p, f(1), f(2), ...$

In altri termini si cominciano ad elencare tutti gli elementi di A e poi si elencano quelli di S. Volendo formalizzare un tale modo di procedere definiamo la funzione $k : N \to A \cup S$ ponendo

$k(1) = a_1$,
$k(2) = a_2$,
...
$k(p) = a_p$,
$k(p+1) = f(1)$,
...
$k(p+m) = f(m)$,
...

E' evidente che k è una funzione suriettiva di N in $A \cup S$. Ora se A è disgiunto da S è evidente che k è anche iniettiva. Invece nel caso esista uno elemento a_i che appartiene ad S allora $ah(i)$ sarebbe uguale ad un opportuno $f(j) \in S$ con $j > i$ e quindi $h(i) = h(j)$ con $i \neq j$.

Siano A ed S entrambi numerabili, allora, essendo A ed S disgiunti la funzione h definita nella dimostrazione della proposizione 7.3 è biettiva.

Nel caso $A \cap B \neq \varnothing$ è sufficiente riferirsi alla coppia B e A-B di insiemi disgiunti ed osservare che per quanto ora dimostrato $A \cup (A-B) = A \cup B$ è numerabile. □

Esempio. Sia $A = \{5,3,7\}$ e sia QP l'insieme infinito dei quadrati perfetti. Allora possiamo enumerare al modo seguente gli elementi di $A \cup QP$:

5, 3, 7, 1, 4, 9, . . .

[16] Alla fine di questo capitolo tale teorema viene illustrato tramite il raccontino degli "alberghi di Hilbert".

Più precisamente sappiamo che la funzione $f(n) = n^2$ è una biezione di N in QP, cioè è una funzione enumerante QP. Possiamo allora definire una funzione $h : N \to A \cup QP$ enumerante $A \cup QP$ ponendo:

$h(1) = 5$
$h(2) = 3$
$h(3) = 7$
$h(4) = f(1) = 1$
$h(5) = f(2) = 4$
...
$h(n) = f(n\text{-}3)$.

Proposizione 7.5. L'insieme Z degli interi relativi è numerabile.

Dim. L'insieme Z è unione dell'insieme degli interi positivi Z^+ (compreso lo zero) e dell'insieme degli interi negativi Z^-. Poiché entrambi questi due insiemi sono numerabili, Z è numerabile. □

Un modo esplicito di enumerare gli elementi di Z si ottiene alternando i numeri positivi ai numeri negativi modo seguente

0, -1, +1, -2, +2, +3, -3 . . .

cioè tramite la funzione $h : N \to Z$ definita ponendo $h(n) = -n/2$ se n è pari e $h(n) = (n\text{-}1)/2$ se n è dispari.

Problema. Trovare una funzione capace di enumerare l'insieme $Z \cup \{-\infty, +\infty\}$ che si ottiene aggiungendo a Z i simboli $-\infty$ e $+\infty$.

8. Tentare di superare il numerabile: esiste solo un tipo di infinito?

(Da una disputa tra Il Dio del Sud ed Il Dio del Nord prima dello scontro delle civiltà del 2022).

- Io sono Dio perché sono infinito!
- Ed io sono più infinito di te!
- No! più infinito di me non esiste niente.
- Guarda che io contengo tutto l'universo !
- Ed io contengo tutte le parti dell'universo che sono di più dell'universo, tiè!
- Allora contieni anche queste due pallottole nella pancia: bam!, bam!

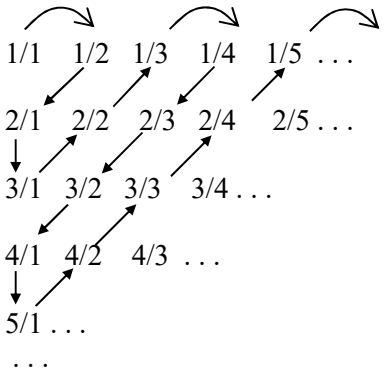
- Haaaaa, Verme infinitesimo, mi hai ucciso ma poiché io ti contengo morrai con me!
- Haaaaaaa, non ci avevo pensato
- Bambini, finite di giocare a *"facciamo finta di essere due dei"* perché è ora di fare i compiti e la maestra ha detto che non sapete ancora le tabelline! (la mamma dalla cucina).

Fino ad ora abbiamo parlato di insiemi finiti ed insiemi numerabili. Si pone il problema se sia possibile trovare insiemi che siano più grandi del numerabile e quindi se esistano almeno due tipi di infinito. Ovviamente la prima cosa che viene in mente è quella di confrontare N con l'insieme Q dei razionali che sembrerebbe molto più grande. Infatti se tra due interi successivi non esiste nessun intero, tra due razionali esiste sempre un razionale. A dispetto di ciò, Cantor provò che:

anche Q, che appare tanto più grande di N, ha tanti elementi quanti ne ha N !

Proposizione 8.1. Q è numerabile.

Dim. Proviamo prima che l'insieme Q^+ dei razionali positivi è numerabile. Una dimostrazione intuitiva si ottiene disponendo i suoi elementi nella seguente matrice infinita in cui, dato un razionale n/m, il numeratore n individua la riga di appartenenza ed il denominatore m la posizione all'interno della riga.



Ovviamente in una tale matrice un razionale compare più volte. Il problema è trovare una strategia che consenta di *leggere* i razionali in questa tabella uno dopo l'altro in modo che:

- nessun razionale sia escluso (la corrispondenza deve essere suriettiva)
- nessun razionale sia letto due volte (la corrispondenza deve essere iniettiva).

Ad esempio è possibile seguire la strategia indicata dalle frecce avendo cura di *saltare* i numeri razionali che già si sono incontrati. Per precisare una tale strategia osserviamo che:

- si è cominciato a "contare" gli elementi di $Q_2 = \{1/1\}$,
- poi si sono contati gli elementi di $Q_3 = \{1/2, 2/1\}$,
- poi gli elementi di $Q_4 = \{3/1, 2/2, 1/3\}$

...

Ciascuno di tali insiemi si può caratterizzare dal fatto che la somma del numeratore e del denominatore è rispettivamente 2, 3, 4, ... Indichiamo allora con Q_n l'insieme dei razionali del tipo p/q con p e q interi positivi primi tra loro e $p+q = n$. Pertanto,

$Q_2 = \{1/1\} = \{1\}$,
$Q_3 = \{1/2, 2/1\}$,
$Q_4 = \{1/3, 3/1\}$,
$Q_5 = \{1/4, 4/1, 2/3, 3/2\}$
. . .

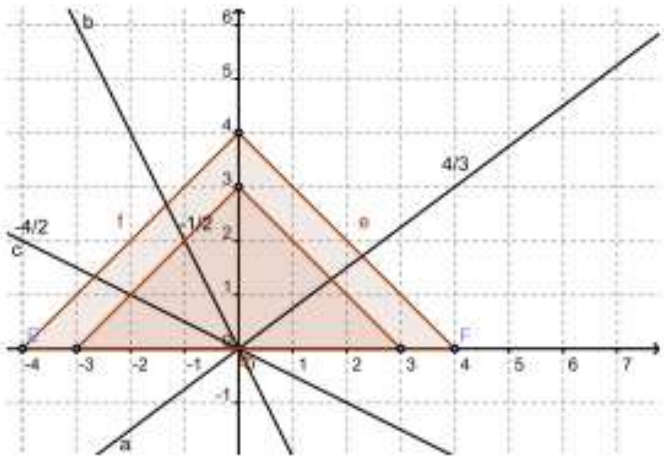
E' evidente che ciascun Q_n è finito e che $Q^+ = \cup_{n \in N-\{1\}} Q_n$. Una numerazione degli elementi di Q^+ si può ottenere pertanto enumerando prima gli elementi di Q_2, poi quelli di Q_3 e così via. In tale modo si ottiene la numerazione:

0, 1, 1/2, 2/1, 1/3, 3/1, 1/4, 4/1, 2/3, 3/2, ...

Una volta che si è visto che Q^+ è numerabile risulta evidente che anche Q^- è numerabile in quanto equipotente a Q^+ tramite la funzione che ad ogni $x \in Q^+$ associa $-x \in Q^-$. Quindi $Q = Q^+ \cup Q^- \cup \{0\}$ è numerabile in quanto unione di un numero finito di insiemi finiti o numerabili. □

Quella che abbiamo riportata ora è la dimostrazione che si trova nella maggior parte dei libri di testo. Tuttavia non è difficile sbizzarrirsi a trovare altre dimostrazioni più intuitive e di carattere

geometrico. Basta associare ad ogni punto del piano cartesiano le cui coordinate sono (n,m), con $m \neq 0$, il corrispondente numero razionale n/m. Ovviamente tale corrispondenza non è iniettiva ma punti a cui corrispondono lo stesso razionale si dispongono su di una retta passante per l'origine. I razionali positivi si collocano nel primo quadrante, quelli negativi nel quarto. Nella dimostrazione fatta per enumerare Q^+ abbiamo di fatto considerato una successione di triangoli rettangoli con un vertice nell'origine e gli altri due nei punti $(n,0)$ e $(0,n)$.



Abbiamo poi contato i razionali corrispondenti a punti all'interno del primo triangolo, poi quelli all'interno del secondo triangolo e così via. Tutto ciò ovviamente con la precauzione di non contare due volte lo stesso razionale. Con una piccola variazione possiamo enumerare l'insieme di tutti i razionali. Basta considerare la la successione di triangoli di vertici $(-n,0)$, $(0,n)$, $(n,0)$. Avremmo anche potuto considerare successioni di altre figure geometriche limitate, ad esempio la successione di cerchi di centro l'origine e raggio l'intero n.

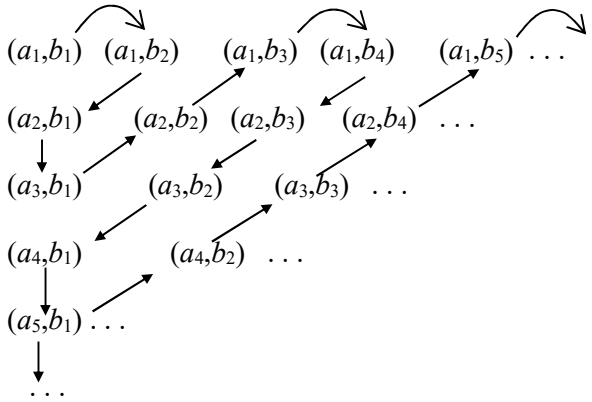
Proposizione 8.2. Il prodotto cartesiano $N \times N$ è numerabile. Più in generale il prodotto di un numero finito di insiemi numerabili è un insieme numerabile.

Dim. Possiamo enumerare $N \times N$ allo stesso modo della con cui abbiamo enumerato i razionali positivi ponendo al posto delle frazioni n/m le coppie (n,m). Un modo più elegante consiste nel

considerare la funzione $k : N\times N \to N$ definita ponendo $k(i,j) = 2^i\cdot(2\cdot j+1)$. Tale funzione è biettiva perché un numero n può essere scomposto in uno ed un solo modo come prodotto del tipo $2^i\cdot(2\cdot j+1)$. D'altra parte è facile calcolare la funzione inversa di k. Infatti, se indichiamo con h: $N\to N\times N$ tale funzione, allora $h(n) = (i,j)$ dove:

- i è tale che 2^i è la massima potenza di 2 che divide n
- $j = (n/2^i -1)/2$.

Proviamo la seconda parte della proposizione per induzione sul numero $n \geq 2$ di insiemi numerabili. Sia $n = 2$ potremmo osservare che se A e B sono numerabili allora, avendo dimostrato che $N\times N$ è numerabile, per il principio di compatibilità rispetto all'equivalenza è ovvio che $A\times B$ è numerabile. Non volendo utilizzare tale principio, ordiniamo gli elementi di A e di B in due successioni $(a_n)_{n\in N}$ e $(b_n)_{n\in N}$. Essendo allora ogni elemento di $A\times B$ del tipo (a_n,b_m), potremo disporre gli elementi di $A\times B$ in una matrice infinita e "contarli" alla stessa maniera di Q.

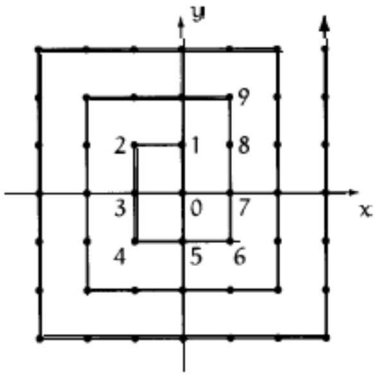


Un modo più esplicito di enumerare $A\times B$ si ottiene tramite la funzione $f : N\to A\times B$ definita ponendo, per ogni $n\in N$, $f(n) = (a_i,b_j)$ dove $h(n) = (i, j)$ sono tali che $n = 2^i\cdot(2\cdot j+1)$.

Supponiamo che la proposizione sia vera per $n\geq 2$ insiemi $A_1,...,A_n$ cioè che $A_1\times...\times A_n$ sia numerabile, allora per ogni insieme numerabile A_{n+1} risulta che $(A_1\times...\times A_n)\times A_{n+1}$ è numerabile e

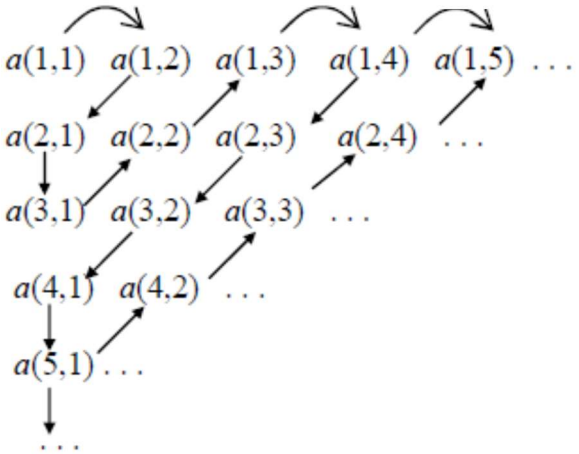
quindi la proposizione è vera per $n+1$ insiemi numerabili. In conclusione la proposizione è vera per ogni $n \geq 2$. [17] □

Esempio. E' possibile utilizzare la seguente spirale per enumerare gli elementi di $Z \times Z$



Proposizione 8.3. L'unione di una successione di insiemi numerabili è ancora un insieme numerabile.

Dim. La tecnica è la stessa di



quella della numerazione dei razionali. Sia $(A_n)_{n \in N}$ una successione di insiemi numerabili ed indichiamo con $a(i,j)$ l'elemento di A_i che occupa il posto j in una enumerazione di A_i.[18] Si definisce così una matrice infinita i cui elementi possono essere enumerati con la solita strategia. □

[17] Una dimostrazione che ricorra alla visualizzazione geometrica è ancora possibile per $n = 3$ poiché è possibile disporre le terne nello spazio a tre dimensioni e "contare" i punti corrispondenti. Ovviamente, per $n>3$ si deve perdere la speranza di una possibile visualizzazione.

[18] In questo punto si nasconde l'assioma della scelta poiché per definire $a(i,j)$ dobbiamo scegliere in ogni A_i una delle enumerazione di A_i.

9. La grandezza degli intervalli: la lunghezza della mia ombra
Rispetto alla questione dell'esistenza di due tipi di infinito sembra di essere ad un punto morto. Abbiamo considerato l'insieme *QP* dei quadrati perfetti ed abbiamo visto che ha lo stesso numero di elementi di *N*, poi abbiamo esaminato *Z*, Q^+ e *Q* ed ancora abbiamo visto che sono numerabili. Abbiamo tentato di trovare insiemi più grandi del numerabile tramite unioni e prodotti cartesiani e non ci siamo riusciti. Si pone allora l' interrogativo:

e se tutti gli insiemi infiniti fossero numerabili?

In tale caso una teoria che si occupa delle grandezze degli insiemi si ridurrebbe a ben poca cosa perché avremmo da un lato gli insiemi finiti, di diverse grandezze, e dall'altra tutti i rimanenti insiemi tutti della stessa grandezza infinita. D'altra parte è questa l'opinione di Galileo quando afferma.

> *Io non veggo che ad altra decisione si possa pervenire, che a dire, infiniti essere tutti i numeri, infiniti i quadrati, infinite le lor radici, ne' la moltitudine dei quadrati essere minore di quella di tutti i numeri, ne' questa maggiore di quella, ed in ultima conclusione, gli attributi di eguale, maggiore e minore non aver luogo negli infiniti, ma solo nelle quantità terminate.*

Ma il merito di Cantor non fu solo di avere avuto il coraggio di negare validità all'assioma euclideo "il tutto è maggiore della parte" e di accettare l'esistenza dell'infinito attuale. Egli riuscì anche a trovare due insiemi infiniti di grandezza diversa; precisamente riuscì a provare che l'insieme *R* dei numeri reali ha potenza maggiore di quella di *N* e che quindi esistono almeno due ordini di infinito.

Cominciamo con mostrare la non numerabilità dell'intervallo aperto (0,1). Una prima dimostrazione di questo fatto è stata fatta da Cantor nel 1873.

Teorema 9.1. (**Dimostrazione topologica**). L'insieme (0,1) di reali ha potenza strettamente maggiore del numerabile.

Dim. Ricordiamo che in *R* si chiama *compatto* un sottoinsieme che sia chiuso e limitato. Una proprietà importante degli insiemi compatti è che l'intersezione di una successione decrescente di compatti è non vuota. Supponiamo per assurdo che esista una

funzione biettiva $f : N \to (0,1)$, allora possiamo definire una successione $(I_n)_{n\in N}$ di intervalli chiusi contenuti in (0,1) tale che

- $I_1 \subseteq (0,1)$ è scelto in modo che non contenga $f(1)$
- $I_2 \subseteq I_1$ è scelto in modo che non contenga $f(2)$
- ...
- $I_{n+1} \subseteq I_n$ è scelto in modo che non contenga $f(n+1)$
- ...

Poiché in R ogni successione decrescente di compatti non vuoti ha intersezione non vuota, abbiamo che $\bigcap_{n\in N} I_n \neq \varnothing$. Sia r un numero reale in $\bigcap_{n\in N} I_n$, allora comunque si fissi n, poichè $r \in I_n$ ed $f(n) \notin I_n$, r risulta essere diverso da $f(n)$. Ciò è in contrasto con l'ipotesi di suriettività per f. L'assurdo a cui siamo pervenuti prova che (0,1) non è numerabile. □

Il fatto che questa bella dimostrazione sia di natura squisitamente topologica non deve sorprendere se si pensa che Cantor ha sviluppato le proprie idee nell'ambito delle sue ricerche di analisi matematica. Da un punto di vista fondazionale e didattico il suo difetto è il ricorrere alla nozione di compattezza che non è semplice e che può essere data solo dopo avere sviluppato un po' di analisi matematica. Fortunatamente Cantor nel 1891 propone una dimostrazione diversa che richiede solo la conoscenza della rappresentazione decimale dei numeri reali.

Teorema 9.2. (Dimostrazione per diagonalizzazione) L'insieme (0,1) di reali ha potenza strettamente maggiore del numerabile.

Dim. Come nella dimostrazione precedente supponiamo per assurdo che esista una funzione biettiva $f : N \to (0,1)$. Come è noto ogni numero $f(n)$ della successione $f(1)$, $f(2)$, ... può essere rappresentato con una espansione decimale e ciò consente di costruire una tabella del tipo

$f(1) = 0.\ \mathbf{r(1,1)}\ r(1,2)\ r(1,3) \ldots$
$f(2) = 0.\ r(2,1)\ \mathbf{r(2,2)}\ r(2,3) \ldots$
$f(3) = 0.\ r(3,1)\ r(3,2)\ \mathbf{r(3,3)} \ldots$
$\ldots$
$f(n) = 0.\ r(n,1)\ r(n,2)\ r(n,3) \ldots \mathbf{r(n,n)} \ldots$
$\ldots$

dove $r(n,i)$ rappresenta la cifra di posto i-esimo della espansione decimale di $f(n)$. Si noti che, stante il significato del periodo 9 nella rappresentazione decimale di un numero, uno stesso numero può essere indicato con espansioni diverse, ad esempio 0.2999... coincide con il numero 0.3000... . Supporremo di rappresentare i numeri sempre senza il periodo nove in modo che espansioni diverse rappresentino sempre numeri diversi.[19] Ci proponiamo ora di costruire un numero reale $r = 0.c_1c_2c_3...$ appartenente a (0,1) che sia diverso da tutti gli elementi della successione $f(1), f(2), ...$. A tale scopo basta prendere c_1 diverso da $r(1,1)$, c_2 diverso da $r(2,2)$ e, più in generale, c_n diverso da $r(n,n)$. Ad esempio possiamo porre

$$c_n = \begin{cases} 1 & \text{se } r(n,n) \neq 1 \\ 2 & \text{se } r(n,n) = 1. \end{cases}$$

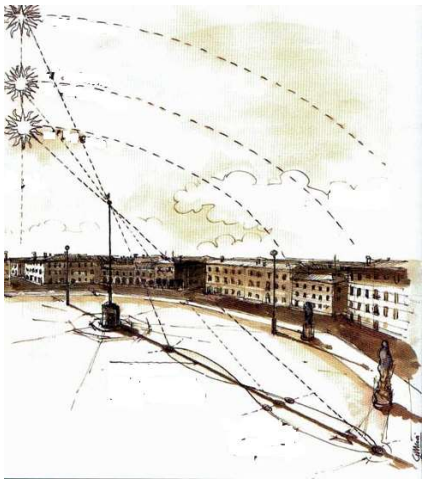
Allora, per come è stato costruito, il numero r non può coincidere con nessun numero $f(n)$, in contrasto con l'ipotesi per cui f è suriettiva. L'assurdo a cui siamo pervenuti prova che (0,1) non può essere numerabile. □

Tale dimostrazione è quella riportata usualmente nei testi delle scuole o delle università poiché considerata più semplice. Tutta-

[19] Molti miei studenti agli esami espongono correttamente il teorema ma dicono una frase del tipo "escludiamo i numeri di periodo nove". In tale caso alla fine della dimostrazione io chiedo: "ma allora il teorema non è stato dimostrato per tutto l'intervallo (0,1) ma solo per l'insieme dei numeri di tale intervallo che non hanno periodo nove". A volte gli studenti se la cavano lo stesso osservando che se un sottoinsieme di (0,1) non è numerabile allora, a maggior ragione, (0,1) non è numerabile. Tuttavia questo modo di dire nasconde la difficoltà di distinguere un numero reale (che, riferendoci alla costruzione dei reali tramite le successioni di Cauchy, è una classe) dalla sua rappresentazione (che è un particolare elemento della classe). Ripetendo quanto detto nel primo volume, la scrittura decimale rappresenta uno dei tanti modo di rappresentare un numero reale tramite una successione di Cauchy. Tale successione è quella corrispondente ad una serie di potenze di base 10. Se vogliamo che la rappresentazione sia univoca, dobbiamo decidere di escludere il periodo 9 ma tale esclusione non comporta l'esclusione di un qualche numero reale. Riassumendo, suggerisco ai miei studenti di dire "decidiamo di rappresentare i numeri reali senza utilizzare l'espansione decimale di periodo nove" e non "escludiamo i numeri reali di periodo nove".

via non è solo più semplice ma mostra un metodo di dimostrazione, quello per diagonalizzazione, che si dimostra importante in vari campi della logica e dell'informatica.

Se invece di prendere l'intervallo (0,1) ne prendo un molto più grande o molto più piccolo che cosa succede ? Ad esempio l'intervallo (0,10.000) ha più elementi dell'intervallo (0,1) ? Detto in termini geometrici questa domanda equivale a chiedersi se due segmenti hanno sempre lo stesso numero di punti. Una risposta intuitiva potrebbe essere suggerita dall'ombra che una persona (preferibilmente magra poiché deve rappresentare un segmento) o dall'ombra che un'asta lascia sulla strada quando il sole sorge o è al tramonto. Infatti, dato un istante del giorno, ogni raggio che parte dal sole colpendo un punto dell'asta-segmento lascia un punto-ombra sul pavimento. Allora esistono tanti punti nel segmento asta quanti ne esistono nel segmento-ombra. Questo mostra che i due insiemi sono equipotenti. Al variare dell'istante del giorno l'ombra cresce da zero all0infinito. Quindi l'asta è equipotente ad ogni segmento che esso sia corto o lungo. Da ciò segue che tutti i segmenti sono equipotenti tra loro.



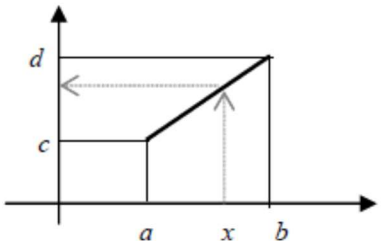
Una trattazione meno romantica della questione è fornita dalla seguente proposizione.

Proposizione 9.3. Tutti gli intervalli chiusi sono equipotenti tra loro. Tutti gli intervalli aperti sono equipotenti tra loro.

Dim. Dati gli intervalli chiusi $[a,b]$ e $[c,d]$, consideriamo la retta passante per il punto di coordinate (a,c) e (b,d). Tale retta è il grafico della funzione:

$$f(x) = \frac{d-c}{b-a}(x-a)+c$$

E' immediato che tale funzione, ristretta all'intervallo $[a, b]$, è una corrispondenza biettiva tra $[a,b]$ e $[c,d]$. La stessa funzione f ristretta all'intervallo aperto (a, b) può essere vista come una corrispondenza biettiva tra gli intervalli aperti (a, b) e (c, d) e questo prova che anche due intervalli aperti sono equipotenti tra loro. □



Problema. Trovare l'espressione analitica di una funzione che esprima l'equipotenza tra l'intervallo [1,2] e l'intervallo [3,7].

10. La potenza del continuo: io sono più infinito di te

Dobbiamo ora confrontare la grandezza di un intervallo aperto con quella di un intervallo chiuso. A tale scopo abbiamo bisogno della seguente proposizione che mostra che aggiungendo ad un insieme infinito una quantità finita o numerabile di elementi non aumenta la sua cardinalità.

Proposizione 10.1. Se S è infinito ed A è finito o numerabile allora S ed $S \cup A$ sono equipotenti.[20]

Dim. Abbiamo già dimostrato un teorema analogo nel caso in cui S sia numerabile. Con un piccolo adattamento la stessa dimostrazione può essere estesa al caso di un qualunque insieme infinito S. Supponiamo che i due insiemi S ed A siano disgiunti. Essendo S infinito la potenza di S è maggiore o uguale al numerabile e quindi esiste una funzione iniettiva $f : N \to S$. Se A è finito allora A è equipotente ad un segmento iniziale $\{1,...,n\}$ e quindi potremo indicare i suoi elementi tramite una sequenza finita $a_1,...,a_n$. Definitamo $h : S \cup A \to S$ ponendo

$h(a_1) = f(1)$

[20] Possiamo visualizzare la dimostrazione riferendoci agli "alberghi di Hilbert" esposti alla fine del capitolo. Infatti se S è infinito allora ha abbastanza spazio da poter contenere un albergo di Hilbert. Ma in tale albergo anche se pieno, possiamo sempre inserire gli elementi di un insieme finito o numerabile A.

$h(a_2) = f(2)$
...,
$h(a_n) = f(n)$
$h(f(1)) = f(1+n)$
...
$h(f(i)) = f(i+n)$
…
$h(x) = x$ se $x \notin f(N)$ e $x \notin \{a_1,...,a_n\}$.[21]

E' immediato che h è iniettiva e suriettiva e che quindi $S \cup A$ è equipotente ad S.

Nel caso A numerabile, supponiamo che $g : N \to A$ sia una funzione enumerante A. Allora possiamo definire h al modo seguente:

$h(g(n)) = f(2 \cdot n)$
$h(f(n)) = f(2 \cdot n+1)$
$h(x) = x$ se x non appartiene né ad $f(N)$ né a $g(N)$.

Anche in questo caso h risulta essere biettiva.[22]

Nel caso S non fosse disgiunto da A possiamo applicare quanto dimostrato alla coppia S e $S-A$ e quindi giungere alla conclusione che $S \cup (S-A) = S \cup A$ è equipotente ad S. □

Esercizio. Dare un esempio di funzione biettiva tra l'insieme R dei numeri reali e l'insieme $\{a,b,c\} \cup R$.

Corollario 10.2. Tutti gli intervalli sono equipotenti tra loro (che siano aperti o chiusi).

Dim. Ogni intervallo aperto (a,b) e' infinito, pertanto poiché $[a,b] = (a,b) \cup \{a,b\}$, per la proposizione precedente (a,b) è equipotente a $[a,b]$. □

---

[21] In altri termini si *"spostano in avanti di n passi"* gli elementi della successione $f(n)$ e nei posti che si sono liberati *"si collocano"* gli elementi di A.

[22] In altri termini:

- si sposta ciascun elemento $f(n)$ in $f(2 \cdot n+1)$ e si liberano gli elementi di posto pari della successione $f(n)$.
- si utilizzano i posti liberati per inserire gli elementi della successione $g(n)$, cioè gli elementi di A
- si lasciano immutati tutti gli altri elementi.

Esempio: Supponiamo di volere definire esplicitamente una funzione biettiva f di [0,1] su (0,1). Allora basta
- fissare una qualunque funzione iniettiva $h : N \to (0,1)$ ad esempio la funzione $h(n) = 1/(n+1)$
- definire $f : [0,1] \to (0,1)$ ponendo
  $f(0) = h(1) = 1/2$
  $f(1) = h(2) = 1/3$
  $f(1/(n+1)) = h(n+2) = 1/(n+3)$
  $f(x) = x$ se $x \neq 1/n$ per ogni n.

Problema. Esibire una funzione biettiva di [0,5] in (0,5).

Abbiamo visto che gli intervalli, che possono essere interpretati come segmenti, sono tutti equipotenti tra di loro ed hanno tutti potenza maggiore del numerabile. Se vogliamo cercare insiemi che hanno potenza più grande possiamo, per esempio, prendere in esame l'intero insieme dei numeri reali o, se si vuole, l'insieme dei punti di una retta. Infatti il fatto che tale insieme non sia limitato potrebbe far pensare che contenga più elementi di un intervallo. Vale però il seguente teorema.

Teorema 10.3. Ogni intervallo è equipotente all'insieme R dei numeri reali.

Dim. L' intervallo (-1,+1) è equipotente ad R. Infatti la funzione $f(x) = x/(x^2-1)$ risulta essere biettiva. Poiché ogni intervallo è equipotente a (-1,+1) possiamo concludere che ogni intervallo è equipotente ad R. □

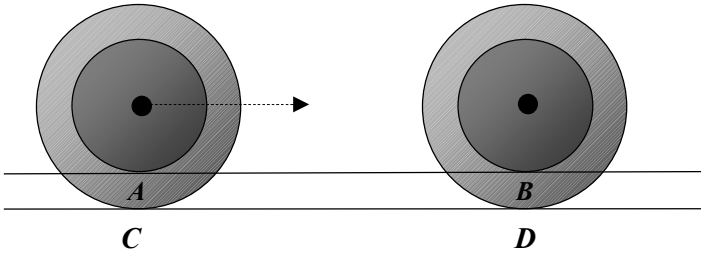
Definizione 10.4. Diciamo che un insieme ha la *potenza del continuo* se è equipotente ad R.

Abbiamo visto che tutti gli intervalli, che siano aperti o chiusi, hanno la potenza del continuo.

Problema. Dimostrare che tutte le circonferenze hanno la potenza del continuo.

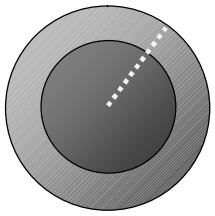
NOTA. I paradossi delle ruote concentriche e delle monete. Torniamo al paradosso delle ruote concentriche in cui sono coin-

volte le linee *r* ed *s* su cui scorrono i punti *A* e *C* delle due circonferenze.



Una possibile soluzione può essere trovata proprio con la nozione di equipotenza. Basta dire che il paradosso prova solo che in una circonferenza piccola ci sono tanti punti quanti ce ne sono in una circonferenza grande e non che la lunghezza della circonferenza piccola è uguale a quella della circonferenza grande. Questo non è affatto paradossale in quanto abbiamo visto che tutte le circonferenze sono tra loro equipotenti.

Possiamo esaminare il fenomeno più da vicino. Possiamo considerare la corrispondenza biettiva che, durante la rotazione completa della ruota grande, associa ad ogni punto della circonferenza della ruota piccola il punto del segmento *AB* che viene toccato in un dato istante. Tale corrispondenza è iniettiva perché due punti diversi della ruota toccheranno in istanti diversi due punti diversi del segmento. E' anche suriettiva in quanto ogni punto del segmento sarà toccato in un dato istante. Tuttavia l'esistenza di tale corrispondenza mostra che la circonferenza piccola è equipotente al segmento *AB* e non che ha la sua stessa lunghezza di tale segmento.



D'altra parte che le due circonferenze siano equipotenti tra loro è dimostrato dalla corrispondenza che ad ogni punto *P* della circonferenza piccola associa la sua proiezione dal centro su quella grande.

In modo analogo possiamo risolvere il paradosso delle due monete. Infatti anche se è assurdo che la lunghezza di una circonferenza sia uguale a quella di una semicirconferenza siano uguali, non deve stupire il fatto che una circonferenza sia equipo-

tente ad una semicirconferenza. Infatti abbiamo visto che tutti gli intervalli sono equipotenti tra loro.

11. Superare la potenza del continuo e poi superare ancora

Abbiamo mostrato fino ad ora l'esistenza di tre tipi di insiemi:

- quelli finiti,
- quelli numerabili
- quelli aventi la potenza del continuo.

Si pone ora il problema di trovare insiemi di cardinalità che supera quella del continuo. Per prima cosa tentiamo con l'insieme delle parti di N.

Proposizione 11.1. L'insieme $\mathcal{P}(N)$ delle parti di N è equipotente all'insieme $\{0,1\}^N$ che a sua volta è equipotente all'intervallo $(0,1)$. Pertanto $\mathcal{P}(N)$ ha la potenza del continuo.

Dim. Per provare che $\mathcal{P}(N)$ è equipotente a $\{0,1\}^N$ è sufficiente considerare la funzione $H : \mathcal{P}(N) \to \{0,1\}^N$ che associa ad ogni sottoinsieme X di N la sua funzione caratteristica $c_X : N \to \{0,1\}$ che, ricordiamo, è definita dal porre:

$$c_X(x) = \begin{cases} 1 & \text{se } x \in X \\ 0 & \text{altrimenti.} \end{cases}$$

Per provare che $\{0,1\}^N$ è equipotente a $(0,1)$ osserviamo che possiamo associare ad ogni elemento $c : N \to \{0,1\}$ di $\{0,1\}^N$ il numero reale $0,c(1)c(2)...$. Una tale corrispondenza è iniettiva (anche se non è suriettiva) e dimostra che la potenza di $\{0,1\}^N$ è minore della potenza di $(0,1)$. Viceversa, consideriamo la corrispondenza che ad ogni numero reale $0.c(1)c(2)...$, che supponiamo scritto in base due e senza il periodo 1, associa la successione $c : N \to \{0,1\}$ in cui $c(n)$ è l'ennesima cifra binaria. Una tale corrispondenza è iniettiva e ciò prova che la potenza di $(0,1)$ è minore della potenza di $\{0,1\}^N$. In conclusione $\{0,1\}^N$ è equipotente a $(0,1)$ e quindi ha la potenza del continuo. □

Proviamo ora a vedere se l'insieme delle funzioni di N in N sia più grande di R. La seguente proposizione mostra che la risposta è negativa.

Proposizione 11.2. L'insieme $\mathcal{P}(N\times N)$ delle relazioni binarie in N ha la potenza del continuo. L'insieme N^N delle funzioni di N in N ha la potenza del continuo.

Dim. Poiché $N\times N$ è equipotente ad N, per il principio di compatibilità è ovvio che $\mathcal{P}(N\times N)$ ha la stessa potenza di $\mathcal{P}(N\times N)$ e quindi la potenza del continuo. Non volendo utilizzare tale principio procediamo al modo seguente. Sia $h : N\to N\times N$ una funzione biettiva. Definiamo allora $k : \mathcal{P}(N) \to \mathcal{P}(N\times N)$ ponendo $k(X) = h(X)$ per ogni X in $\mathcal{P}(N)$. Allora è evidente che k è biettiva, pertanto, essendo $\mathcal{P}(N\times N)$ equipotente a $\mathcal{P}(N)$, $\mathcal{P}(N\times N)$ ha la potenza del continuo.

Per provare che N^N ha la potenza del continuo osserviamo che $N^N \subseteq \mathcal{P}(N\times N)$ poiché ogni funzione di N in N, in quanto relazione binaria, è un sottoinsieme di $N\times N$. Ciò prova che la potenza di N^N è minore o uguale a quella del continuo. D'altra parte $\{0,1\}^N$ è un sottoinsieme di N^N e quindi N^N ha potenza maggiore o uguale al continuo. Per il teorema di Cantor-Bernstein N^N ha la potenza del continuo. □

Tutti gli insiemi di cui abbiamo parlato fino ad ora sono di "dimensione uno" ed abbiamo visto che tutti hanno la potenza del continuo. Allora per trovare insiemi più grandi del continuo potremmo rivolgerci ad insiemi di dimensione maggiore, ad esempio ai quadrati oppure ai cubi. Ebbene si scoprì che anche l'insieme dei punti di un quadrato ha la potenza del continuo !

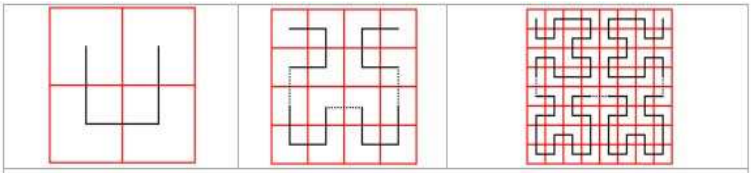
Teorema 11.3 (Paradosso del quadrato e del suo lato). L'insieme dei punti interni ad un quadrato è equipotente all'insieme dei punti interni ad un suo lato. Pertanto tale insieme ha la potenza del continuo.

Dim. Possiamo supporre che il quadrato sia unitario e che sia stato collocato in un sistema di assi cartesiani in modo che i suoi quattro vertici abbiano coordinate (0,0), (0,1), (1,0), (1,1). Allora, riferendoci alle coordinate dei punti interni al quadrato e dei

punti interni ad un lato, dobbiamo provare che $(0,1)^2$ è equipotente a $(0,1)$. Supponiamo di rappresentare i numeri reali nella forma dell'espansione decimale. Inoltre, per ottenere che ad espansioni decimali diverse corrispondano numeri reali diversi supponiamo di non rappresentare mai i numeri con periodo nove. Ad esempio scriveremo 0.40000... al posto di 0.3999... Consideriamo la corrispondenza che associa ad ogni coppia $(x,y)\in(0,1)^2$ il numero $f(x,y)\in(0,1)$ ottenuto ponendo $f(x,y) = 0.x_1y_1x_2y_2x_3y_3...$ avendo supposto che $x=0.x_1x_2x_3...$ e $y=0.y_1y_2y_3...$ Tale corrispondenza è iniettiva e ciò prova che la potenza di un quadrato è minore di quella del suo lato.[23] Per trovare una corrispondenza iniettiva da $(0,1)$ a $(0,1)^2$ possiamo ad esempio considerare la corrispondenza che associa ad ogni $x\in(0,1)$ la coppia $(x,1/2)$. Per il teorema di Cantor-Bernstein possiamo concludere che $(0,1)$ è equipotente a $(0,1)^2$. □

Ho usato la parola "paradosso" poiché questo risultato appariva stupefacente ai tempi di Cantor[24]. Infatti stabiliva l'uguaglianza delle grandezze di due enti geometrici di differente dimensione mentre la nostra intuizione geometrica distingue fortemente linee, superfici e solidi.

Un modo diverso per convincersi della possibilità di mettere in corrispondenza i punti di una retta ed i punti interni ad un



La curva di Peano

quadrato, è dato dalla considerazione di curve particolari. Una delle curve più famose che progressivamente "riempie" il quadrato è la curva di Peano che si ottiene come limite di una successione di curve definita per ricorsione. La curva di Peano è una funzione continua di $(0,1)$ in $(0, 1)^2$. D'altra parte, stante il fatto

[23] Si osservi che la funzione f non è suriettiva poiché, ad esempio, il numero 0.19191919... dovrebbe avere come immagine inversa la coppia (0.11111...., 0.9999...) ma tale coppia non rappresenta un punto interno al quadrato.

[24] In realtà anche a me appare stupefacente.

che la dimensione di (0,1) è diversa da quella di $(0,1)^2$, non può esistere nessuna funzione bicontinua (continua, invertibile e tale che la sua inversa sia continua) tra (0,1) e $(0,1)^2$. Si dimostra anche la curva di Peano non è iniettiva e non derivabile

Problema. Dimostrare che ogni cubo ha la stessa potenza di un suo spigolo.

Dalle proposizioni ora dimostrate segue facilmente il seguente teorema.

Teorema 11.4. L'insieme dei punti del piano e l'insieme dei punti dello spazio hanno la potenza del continuo.

Dim. Poiché R è equipotente a (0,1), per il principio di compatibilità $R\times R$ è equipotente a $(0,1)\times(0,1)$. D'altra parte abbiamo già dimostrato che $(0,1)\times(0,1)$ è equipotente a (0,1). Quindi $R\times R$ è equipotente a (0,1) e quindi ha la potenza del continuo. Non volendo utilizzare tale principio, possiamo osservare che se $f: (0,1) \to R$ è una biezione di (0,1) in R, allora ponendo $f^*(x,y) = (f(x), f(y))$ ottengo una biezione di $(0,1)\times(0,1)$ in $R\times R$.

In modo analogo si dimostra che l'insieme dei punti dello spazio ha la potenza del continuo. □

Esercizio. Dimostrare che due circonferenze sono equipotenti (Una dimostrazione analitica si ottiene col considerare le equazioni parametriche di una circonferenza. Una dimostrazione geometrica si ottiene provando l'equipotenza per circonferenze concentriche e poi utilizzando traslazioni per estendere il risultato ad una qualunque coppia di circonferenze).

Problema. Scrivere su un foglio di carta la propria firma e dire se ha la potenza del continuo oppure no.

Problema. Uno spazio vettoriale di dimensione finita sul campo dei reali quale cardinalità ha ?

Problema. L'insieme dei triangoli del piano ha potenza maggiore o uguale al continuo ?

Problema. L'insieme dei cerchi del piano ha potenza maggiore o uguale al continuo ?

Problema. Il gruppo delle rotazioni intorno ad un dato punto è ciclico ?

Problema. Il gruppo additivo di R è finitamente generato?

Proposizione 11.5. L'insieme dei numeri complessi ha la potenza del continuo.

Dim. Basta ricordare che un numero complesso $x+iy$ è caratterizzato dalla sua parte reale x e dalla sua parte complessa y, cioè da una coppia (x,y) di numeri reali. □

Ancora una volta sembra difficile trovare qualche cosa di più grande del continuo. Fortunatamente (per chi non ama avere limiti) il seguente teorema, dovuto a Cantor, mostra che:

dato un insieme S esiste sempre un insieme più grande di S.

Teorema 11.6. (Teorema di Cantor) Dato un insieme S, l'insieme $\mathcal{P}(S)$ delle parti di S ha potenza strettamente maggiore di quella di S. In particolare, l'insieme $\mathcal{P}(R)$ ha potenza strettamente maggiore del continuo.

Dim. Che $\mathcal{P}(S)$ abbia potenza maggiore o uguale ad S segue dal fatto che la funzione $h : S \to \mathcal{P}(S)$ ottenuta ponendo $h(x) = \{x\}$ è iniettiva. Supponiamo per assurdo che esista una funzione biettiva f di S in $\mathcal{P}(S)$ e consideriamo l'insieme $T = \{x \in S \mid x \notin f(x)\}$. Essendo f suriettiva, esisterà $x_o \in S$ tale che $f(x_o) = T$. Allora:

$x_o \in T \Rightarrow x_o$ verifica la proprietà caratteristica di T
$\Rightarrow x_o \notin f(x_o) = T$
$x_o \notin T \Rightarrow x_o$ non verifica la proprietà caratteristica di T
$\Rightarrow x_o \in f(x_o) = T$.

Si perviene pertanto all'equivalenza $x_o \in T \Leftrightarrow x_o \notin T$ che è assurda in quanto afferma che una asserzione coincide con la sua negata.

Corollario 11.7. Dato un qualunque sottoinsieme è possibile trovare un altro insieme di potenza strettamente maggiore.

Teorema 11.8. L'insieme R^R delle funzioni di variabile reale ha la potenza strettamente maggiore del continuo.

Dim. Ovviamente R^R ha cardinalità maggiore o uguale a $\{0,1\}^R$. D'altra parte questo ultimo insieme ha cardinalità uguale a $\mathcal{P}(R)$ poiché la funzione che associa ad ogni sottoinsieme X di R la sua

funzione caratteristica è biettiva.Quindi R^R ha una potenza maggiore del continuo. □

Riassumendo, le cardinalità che abbiamo visto sono quelle finite e quelle infinite. Se poniamo, per ogni naturale n, $\underline{n} = \{1,\ldots,n\}$ abbiamo visto che esiste una successione

$$\varnothing, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \ldots N, \mathcal{P}(N), \mathcal{P}(\mathcal{P}(N)), \ldots$$

di insiemi che è strettamente crescente rispetto alla relazione $\leq$.

Nota. Un primo paradosso: la classe di tutti gli insiemi.
Il Teorema 11.6 conduce ad un paradosso. Consideriamo la classe C di tutti gli insiemi. Allora la potenza di C è maggiore di quella di ogni altro insieme (cosa abbastanza intuitiva). Infatti se X è un insieme possiamo considerare la funzione $f : X \to C$ definita ponendo $f(x) = \{x\}$, funzione che è ovviamente iniettiva. D'altra parte per il corollario al teorema di Cantor sappiamo che esiste un insieme che è di potenza maggiore a quella di C.

NOTA 1.
Cantor, l'infinito e la dottrina Cristiana

E' da notare che le motivazioni filosofiche di Cantor erano strettamente intrecciate a quelle religiose. La cosa non deve sorprendere poiché sono tali motivazioni alla base dei primi esempi di accettazione dell'infinito attuale nella cultura occidentale. Era infatti convincimento comune nel medioevo che Dio fosse infinito.

> *Appunto perché è uno, Egli non rientra né in una misura né in un numero. Così Egli non incontra il confine né in altrui né in se stesso, che, in tal caso, Egli cadrebbe già nella dualità.* (Plotino, Enneadi).

Era semmai oggetto di discussione se Dio potesse concepire entità infinite poiché in tale caso si dovrebbero accettare entità infinite diverse da Dio. A tale proposito ad esempio l'opinione di San Tommaso era che l'unico infinito fosse Dio.

> *Quindi, come Dio, nonostante abbia potenza infinita, tuttavia non può creare qualcosa di increato (il che sarebbe far coesistere cose contraddittorie), così non può creare cosa alcuna che sia assolutamente infinita.* (S. Tommaso, Summa Teologica).

In altre parole, se si vede che il concetto di infinito attuale è contraddittorio allora Dio non può pensarlo perché Dio, in un certo senso, rispetta la logica.

Invece l'opinione di Sant'Agostino era non solo che Dio fosse infinito ma anche che potesse avere come oggetto del suo pensiero un altro infinito, ad esempio "il tutto del numero" cioè l'intera totalità degli interi.

> *Riguardo poi all'altra loro teoria che neanche con la scienza di Dio può essere rappresentato l'infinito, rimane loro che osino affermare, immergendosi nell'abisso profondo della irreligiosità, che Dio non conosce il tutto del numero . . . Non lo potrebbe dire neanche il più insensato . . . Che razza di omucci siamo noi che pretendiamo di porre limiti alla sua scienza?* (Agostino, La città di Dio)

Tornando a Cantor ed alle sue motivazioni religiose, ad esempio in una lettera del 1890 a padre Thomas Esser egli scrive:

> *Viene da me offerta alla filosofia cristiana per la prima volta la vera dottrina dell'infinito nei suoi principi. So con piena sicurezza e determinazione che essa accoglierà questa dottrina: è soltanto da vedere se ciò accadrà già adesso o soltanto dopo la mia morte.*

Da notare che Cantor distingue tre tipi di infinito. Il primo, legato all'idea di Dio, il secondo di natura fisica (il tempo, lo spazio), il terzo di natura matematica.

> *L'infinito attuale si presenta in tre contesti: il primo è quello in cui si presenta nella forma più completa, in un essere completamente indipendente trascendente questo mondo, "in Deo", ed è questo che io chiamo l'Infinito Assoluto o semplicemente l'Assoluto; il secondo quando si presenta nel mondo contigente, nel creato; il terzo è quando la mente lo afferra "in abstracto", come grandezza matematica, numero o tipo d'ordine. Voglio sottolineare chiaramente la differenza tra l'Assoluto e quello che io chiamo il Transfinito, cioè l'infinito attuale degli ultimi due tipi, perché si tratta di oggetti evidentemente limitati, suscettibili di accrescimento, e quindi collegati al finito.*

NOTA 2.
La definizione di Emily di infinito

Ecco un'implicita definizione di infinito data nel 1893 dalla poetessa Emilly Dickinson (traduzione di Margherita Guidacci nel volume edito da Mondadori).

Come se il mare separandosi
svelasse un altro mare,
questo un altro, ed i tre
solo il presagio fossero

d'un infinito di mari
non visitati da riva –
il mare stesso al mare fosse riva-
questo è l'eternità.

Emily Dickinson

L'originale è

As if the Sea should part
And show a further Sea –
And that – a further – and the Three
But a Presumption be –

Of Periods of Seas –
Unvisited of Shores –
Themselves the Verge of Seas to be –
Eternity – is Those –

NOTA 3.
Un modo diverso di quozientare una struttura

Nel paragrafo 1 abbiamo visto che i numeri relativi ed i numeri razionali si possono ottenere sostituendo alle classi le forme normali che le rappresentano. Questo modo di procedere è molto generale ed in un certo senso può sostituire l'usuale definizione di quoziente di una struttura algebrica A modulo una data congruenza $\equiv$. Il modo di procedere è il seguente. Si considera una *funzione di scelta* $f : A/\equiv \to A$ cioè una funzione f tale che $f([x]) \in [x]$ per ogni classe di equivalenza $[x]$. In un certo senso $f([x])$ è l'elemento scelto per rappresentare la classe $[x]$. Gli elementi scelti si dicono in *forma normale* ed indichiamo con $A^{\equiv}$ la classe degli elementi in forma normale. Se $x \in A$ poniamo $f^*(x) = f([x])$ e diciamo che $f^*(x)$ è la *forma normale* di x e che il calcolo di $f^*(x)$ è una *riduzione a forma normale di x*.[25]

[25] L'assioma della scelta ci assicura che questo modo di procedere è generale. Tuttavia, se vogliamo che le operazioni siano effettivamente cal-

Definizione 1. Data una struttura algebrica A ed una congruenza $\equiv$ in A, consideriamo una funzione di scelta f per $\equiv$, allora indichiamo con $A^{\equiv}$ la struttura algebrica tale che:
- il dominio è il sottoinsieme $A^{\equiv}$ degli elementi di A in forma normale
- le operazioni sono definite in $A^{\equiv}$ operando prima come in A e successivamente riducendo a forma normale il risultato ottenuto.

In altre parole, data ad esempio un'operazione binaria + in A definiamo un'operazione $\underline{+}$ in $A^{\equiv}$ ponendo $x\underline{+}y = f^*(x+y)$.

Teorema 2. Data una congruenza $\equiv$ in una struttura algebrica A, la funzione $f : A/\equiv \to A^{\equiv}$ è un isomorfismo.

Dim. E' evidente che f è una biezione. Sia + un'operazione binaria in $A/\equiv$, allora

$$f([x]+[y]) = f([x+y]) = f^*(x+y) = f([x])+f([y]).$$

Ad esempio esaminiamo il modo con cui sono di fatto usati gli interi modulo m. Data una classe $[n]$ si sceglie come rappresentante della classe il numero positivo più piccolo della classe. Questo è anche il resto della divisione (che è il resto della divisione di n per m e risulta minore di m-1). Pertanto ci si riferisce alle "forme normali" 0, 1, …, m-1 e non alle rispettive classi.

Proposizione 3. Sia Z/m l'anello degli interi modulo m e consideriamo la funzione di scelta $f : Z/m \to \{0,\ldots,m\text{-}1\}$ ottenuta ponendo $f(Z) = minZ$ per ogni classe $Z \in Z_m$. Definiamo inoltre le operazioni in $\{0, 1, \ldots, m\text{-}1\}$ $\oplus$ e $\otimes$ definite ponendo
- $x \oplus y = f(x+y)$ (riduzione a forma normale di $x+y$)
- $x \otimes y = f(x \cdot y)$ (riduzione a forma normale di $x \cdot y$).

Allora Z_m è isomorfo a $(\{0,\ldots,m\text{-}1\}, \oplus, \otimes, 0, 1)$.

Ad esempio, nel caso $m = 5$, si considera il dominio $\{0, 1, 2, 3, 4\}$, e $4 \oplus 3 \to 7 \to 2$. Più in generale, abbiamo le seguenti tabbelle della somme e del prodotto.

---

colabili, dobbiamo supporre che il procedimento di riduzione a forma normale sia effettivo e che quindi f sia calcolabile.

$\oplus$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tale *"filosofia"* è quella adottata dai sistemi di calcolo simbolico come *Mathematica* che, d'altra parte, sono sistemi di intelligenza artificiale che simulano il comportamento di un matematico. Ad esempio, dovendo effettuare la somma tra 6/9 e 10/12, *Mathematica* riduce tali coppie a forma normale ottenendo, come rappresentanti delle corrispondenti classi, le coppie 2/3 e 5/6. Poi effettua l'operazione di addizione ottenendo prima $(2\cdot6+3\cdot5)/3\cdot6$, e quindi, dopo avere effettuato le operazioni tra interi, 27/18. Infine riduce a forma normale tale coppia ed ottiene come risultato 3/2. Allo stesso modo *Mathematica* riesce a trattare una larga parte della matematica.

Concludiamo osservando che un tale modo di definire il quoziente di una struttura non richiede necessariamente che la relazione di equivalenza sia una congruenza, come richiesto normalmente in algebra. E' sufficiente avere un'equivalenza ed una funzione di scelta. Tuttavia in tale caso ad ogni funzione di scelta corrisponde una struttura diversa. Inoltre il quoziente tramite una congruenza ha il pregio di conservare molte delle proprietà della struttura di partenza, ad esempio le proprietà esprimibili tramite equazioni come la proprietà commutativa e quella associativa.

NOTA 4

Giochi di prestigio con l'insieme vuoto: tutti gli elementi di ∅ sono pari, …tutti gli elementi di ∅ sono dispari.

Sia nella definizione 5.1 che nella definizione 5.3 abbiamo trattato a parte il caso in cui uno degli insiemi sia vuoto. In realtà questo non è indispensabile se siamo disposti a pagare il prezzo di alcune "acrobazie logiche". Tali acrobazie sono basate sul fatto che una implicazione è vera quando l'antecedente è falso.

Proposizione 1. ∅ è un sottoinsieme di ogni insieme.

Dim. L'implicazione $x\in\varnothing \Rightarrow x\in X$ è vera per ogni insieme X in quanto l'antecedente $x\in\varnothing$ è falso.

Proposizione 2. Per ogni insieme X risulta che $\varnothing$ è una funzione iniettiva di $\varnothing$ in X e quindi $\varnothing \leqq X$. In particolare $\varnothing \equiv \varnothing$.

Dim. Osserviamo che,
- $\varnothing$ è una relazione binaria tra $\varnothing$ e X in quanto è un sottoinsieme di $\varnothing\times X$.
- $\varnothing$ è una relazione funzionale, e quindi una funzione di $\varnothing$ in X, in quanto vale l'implicazione
  $(x,y)\in\varnothing$ e $(x,y')\in\varnothing \Rightarrow y = y'$
- $\varnothing$ è una funzione iniettiva poiché vale
  $(x,y)\in\varnothing$ e $(x',y)\in\varnothing \Rightarrow x = x'$.
  Questo prova che $\varnothing \leqq X$.
- $\varnothing$ vista come funzione di $\varnothing$ in $\varnothing$ è anche suriettivaIn particolare abbiamo che $\varnothing \leqq \varnothing$.

Proposizione 3. $\varnothing \equiv X$ se e solo se $X = \varnothing$., intesa come funzione di e $X = \varnothing$ allora $\varnothing$ (vista come funzione) è anche suriettiva in quanto

$x\in B \Rightarrow$ esiste $y\in\varnothing$ tale che x è immagine di x.

Questo prova che $\varnothing \equiv \varnothing$. Supponiamo che $\varnothing \equiv B$, ed osserviamo che l'unica funzione di $\varnothing$ in B è la funzione vuota $\varnothing$. Tale funzione è suriettiva solo se

$y\in B \Rightarrow \exists x\in\varnothing$ tale che $(x,y)\in\varnothing$.

Poiché il conseguente è falso tale implicazione può essere vera solo se l'antecedente è falso per ogni y, cioè solo se $B = \varnothing$.

Un insieme può essere equipotente a $\varnothing$ solo se coincide con $\varnothing$. Infatti una funzione f di $\varnothing$ in un insieme S è un sottoinsieme di $\varnothing\times S = \varnothing$ e quindi è la funzione vuota. Se f è suriettiva Pertanto la classe $[\varnothing]$ degli insiemi equipotenti a $\varnothing$ si riduce al singoletto $\{\varnothing\}$.

Problema 1. Quanti insiemi vuoti esistono? Motivare la risposta.

Problema 2. Consideriamo l'insieme $[0,1]$ con l'usuale ordine tra numeri reali ed il sottoinsieme vuoto $\varnothing$ di $[0,1]$. Dire se esistono ed eventualmente a cosa sono uguali $sup(\varnothing)$ e $inf(\varnothing)$.

Problema 3. Consideriamo l'insieme dei numeri reali R con l'usuale ordine tra numeri reali ed il sottoinsieme vuoto $\varnothing$ di R. Dire se esistono ed eventualmente a cosa sono uguali $sup(\varnothing)$ e $inf(\varnothing)$.

LETTURA 1

Rudy Rucker – L'albergo di Hilbert, da *La mente e l'infinito*, Editore Muzzio, 85-86.

Il famoso matematico David Hilbert, nelle sue conferenze a carattere divulgativo, raccontava spesso la storia di un albergo con infinite stanze: Questo mitico albergo, che chiameremo *Albergo di Hilbert*, ha omega camere: Camera 0, Camera 1, Camera 2, …., Camera *n*, e così via. Come nel paragrafo precedente inizieremo a contare da 0. Per fissare le idee, ho disegnato l' Albergo nella figura 2.13. Per farlo stare su una pagina, ho supposto che ogni piano fosse dotato di un fantascientifico condensatore di spazio, uno strumento che fa si che ogni piano sia alto due terzi del precedente. Anche gli ospiti subiscono la stessa contrazione e quindi, sebbene i soffitti del terzo piano siano alti solo due o tre piedi, il condensatore di spazio rende gli ospiti alti uno o due piedi in modo che si trovino a loro agio. Lascio al lettore come esercizio di dimostrare che, se il primo piano ha soffitti di dieci piedi e ogni piano è alto i due terzi del precedente, allora l'albergo di ω piani è alto 30 piedi.

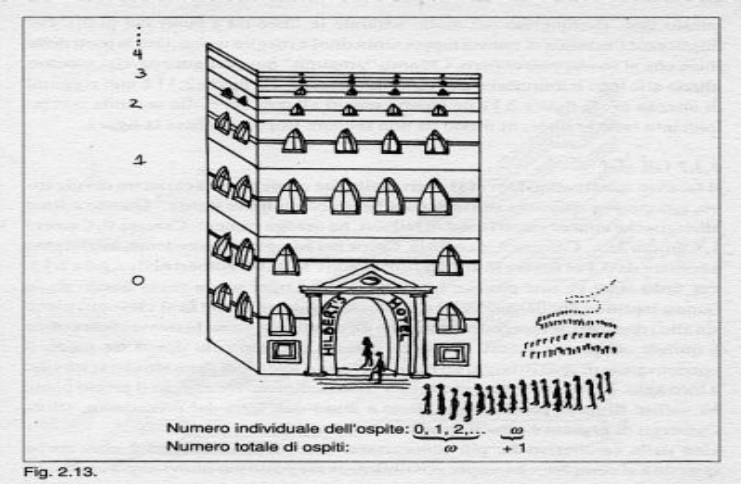


Fig. 2.13.

Una delle caratteristiche più sconcertanti dell'Albergo di Hilbert è che, anche quando è al completo, è sempre possibile trovare posto per nuovi ospiti senza che nessuno debba condividere la sua stanza con un altro!

Supponiamo, per esempio, che ogni camera sia occupata collocando l'ospite n nella Camera n. Supponiamo che a questo punto arrivi un nuovo ospite: l'Ospite *a.* Dove potrà alloggiare? E' facile! basta chiedere ad ogni cliente di passare nella camera successiva. In tale modo si libera la camera numero 0 e la si può utilizzare per ospitare a.

Ma se fosse arrivato un nuovo pulman contenente una quantità numerabile di nuovi turisti? Come collocarli? Facile, basta dire a ciascun ospite della camera n di passare alla camera $2n$. In tale modo tutte le camere di numero dispari rimangono libere. Allora si dice ai turisti del pulman di collocarsi in tali camere. Precisamente al prima turista che scende dal pulman si assegna la camera $2\cdot1-1 = 1$, al secondo turista la camera $2\cdot2-1 = 3$, ... al turista n la camera $2\cdot n-1$.

NOTA. Naturalmente le stesse considerazioni le potremmo fare se l'albergo avesse stanze tutte uguali tra loro ma lungo una linea retta infinita (a me piace più immaginarla orizzontale e non verticale forse per questione di vertigini). In questo caso lo spostarsi alla camera successiva sarebbe una vera e propria traslazione. Ciò permetterebbe di interpretare quanto detto in questa lettura dicendo che l'albergo è equiscomponibile con un albergo uguale più una stanza (in generale più n stanze). Il paradosso degli otto raggi esposto nel primo volume è analogo salvo il fatto che i punti della successione A_1, A_2,... sono stati collocati su di una circonferenza e non su di una retta.

LETTURA 2

Tratto dall'articolo : G. Gerla, Nel paese del Destino, *Periodico di Matematiche* - Serie VII - Volume 4, 1997.

Nel Paese del Destino, dove tutti sono immortali, esistono due tipi di abitanti, i Vagabondi e gli Integrati. Un Vagabondo ha abitudini semplici. Ogni giorno cammina lungo la sua strada ed ogni sera si ferma ad un bivio dove resta a mangiare ed a dormire all'aria aperta (per fortuna non piove mai in questo paese). Il mattino seguente egli è libero di scegliere se prendere la strada a sinistra o quella a destra per poi camminare fino a sera... e così via. Gli Integrati invece vanno a lavorare ed ogni giorno fanno quello che è scritto nel *Libro dei Regolamenti del Mestiere.*

Anche io abito in questo paese e, non me ne vergogno, sono un Vagabondo. Mi piace questa vita poiché si vedono boschi, montagne e paesaggi sempre nuovi. Poi si può pensare, fantasticare e, camminando camminando, avere il piacere di incontrare altri vagabondi con cui si scambia un cenno di saluto oppure ci si sofferma a parlare dell'ultimo software prodotto. Infine, ed è questa la cosa più importante, si è liberi.

Quella sera, come tutte le sere, mentre più soddisfatto del solito mi accoccolavo accanto ad un muretto per addormentarmi, mi venne da mormorare con orgoglio:

"*faccio una vita serena e sono un essere libero, libero ogni mattina di andare a destra o a sinistra come mi detta la fantasia"*

Ma, come rispondendo alle mie parole, ecco una voce ironica emergere dall'altra parte del muretto

"non ti illudere, non ti illudere".

Era un Giovane Integrato emerso dal buio con il suo cravattino, la camicia celeste e la giacchetta blu. Lo guardai con fastidio (non correva buon sangue tra gli Integrati e i Vagabondi) e pensai che, essendo domenica, doveva trattarsi del solito Integrato che trascorreva un fine settimana tra le montagne. Era strano comunque che non avesse gli scarponi, gli occhiali scuri firmati, la giacca a vento e tutto quanto era previsto dal Regolamento Generale degli Integrati in Fine Settimana. Aveva poi in mano un

registro che mi ricordava quello della mia maestra (quando ancora non ero scappato da scuola e da casa, come tutti i Vagabondi), solo era un po' più grosso.

"Non ti illudere sulla tua libertà - proseguì - il *tuo destino è già scritto in una pagina di questo libro, Il Grande Libro Dei Destini, ... anche se ora non ti saprei dire in quale pagina".*

Afferrai il libro un po' preoccupato. Aveva una successione infinita di pagine che, man mano che venivano sfogliate, apparivano sempre più sottili; all'inizio della prima c'era scritto:

"DESTINO DEL PRIMO VAGABONDO"

e poi la sequenza infinita di frasi:

"Domani andrà a sinistra, dopodomani a destra, poi ancora a sinistra, poi ancora a sinistra, poi a destra, poi a sinistra, poi a sinistra ..."

con caratteri sempre più piccoli, sempre più piccoli, per fare entrare tutto nella pagina.[26] Era terribile pensare che quella era la pagina di un Vagabondo e che in quel momento stavo leggendo il suo destino. Un Vagabondo che felice ed ignaro si illudeva ogni mattina di scegliere a caso la sua via!

Anche la seconda pagina era simile: in alto era scritto

"DESTINO DEL SECONDO VAGABONDO"

e poi:

"Domani andrà a sinistra, dopodomani a destra, poi a destra, poi a destra, poi a sinistra, poi a destra, poi a sinistra ..."

Ecco il destino di un altro Vagabondo! Che tristezza sapere che forse il Giovane Integrato aveva ragione e che il mio destino era scritto in una di quelle squallide pagine! *"Che senso ha la vita di un Vagabondo",* mi dissi, *"se le sue scelte sono solo una illusio-*

[26] Se si ammette che la geometria Euclidea è logicamente possibile, allora si deve ammettere anche la possibilità di un libro con una quantità numerabile di pagine sempre più sottili. Basta ad esempio che lo spessore della pagina n+1 sia la metà di quello della pagina n. Allora se la prima pagina ha spessore 1, lo spessore totale sarà $1 + 1/2 + .. + 1/2^n + ... = 2$. Discorso analogo vale per la quantità di parole, scritte in carattere sempre più piccolo, che possono essere scritte in una pagina. E' anche interessante esaminare il tipo di ordinamento che in tale modo viene a determinarsi sull'insieme delle parole del libro.

ne, se tutto è già stabilito? Non sarebbe meglio allora risparmiarsi i reumatismi, trovarsi un impiego e tutte le mattine recarsi allo stesso posto di lavoro?".
Eppure non mi fidavo: poteva darsi che il Giovane Integrato mi stesse mentendo e che un uomo libero potesse realmente esistere in questo Paese. Bisognava trovare una via di uscìta; bisognava pensare, ... pensare, ... pensare...
Ed ecco, all'improvviso, una idea.

"Mi presteresti il libro?".
"Certo! "

rispose il Giovane Integrato,

"anzi, te lo regalo: ne ho una copia in più".

Finalmente sereno, mi addormentai stringendo il libro che ora mi sembrava un'ancora di salvezza, non più una trappola. Sapevo quello che avrei dovuto fare.

Al mattino, come tutte le mattine, il leggero calore del sole mi svegliò ed io mi alzai ben riposato. L' Integrato se ne stava ancora lì a guardarmi, cosa questa alquanto strana visto che era lunedì e che ogni Integrato il lunedi, sta al suo posto di lavoro. Non me ne preoccupai, anzi ero ansioso di iniziare la mia passeggiata quotidiana e di dimostrargli quanto si sbagliasse. Come tutte le mattine, avevo davanti a me due strade e dovevo scegliere, ma questa volta sapevo esattamente cosa fare e non esitai a dire trionfante:
"Visto che alla prima pagina si parla di un uomo che oggi dovrebbe andare a sinistra, io andrò a destra. In tale modo posso almeno evitare che il mio destino sia quello descritto in tale pagina".
E cosi feci, camminando fino a sera al fianco del Giovane Integrato per poi addormentarmi contento. Il mattino dopo, al risveglio, dissi all'Integrato (che ormai non mi lasciava):
"Visto che alla seconda pagina c'è scritto di un uomo che oggi andrà a destra, io per dispetto andrò a sinistra. In tale modo posso star certo che il mio destino non può essere scritto nemmeno in questa pagina".
Procedendo cosi, giorno dopo giorno, ero sicuro che il mio destino non poteva essere quello della terza pagina, né quello della

quarta e così via. In definitiva il mio destino non poteva essere in nessuna pagina e ciò mi metteva in allegria e mi spingeva a prendere in giro il Giovane Integrato con le sue fandonie sul destino ! Ero anzi convinto che il Giovane Integrato si fosse convertito alla vita dei Vagabondi, visto che tutti i giorni bighellonava con me lungo le strade.[27]

Ma anche il Giovane Integrato era contento ed io non capivo perché. Egli pensava al suo lavoro, che come tutti gli Integratí amava molto:

"questo lavoro non è poi tanto difficile, peccato che mi obblighi a camminare tanto"

e guardandomi pensava:

[27]Quello che riesce a fare il Vagabondo è, dato un elenco di possibili destini, definire un destino che sicuramente non è nell'elenco. Allora il racconto mostra che

L'INSIEME DEI DESTINI NON E NUMERABILE.

Enumerare i destini equivale infatti a scriverli uno dopo l'altro sulle pagine di un libro che abbia una quantità numerabile di pagine. Ma il nostro Vagabondo mostra che esiste sempre un destino che sfugge a tale elenco. In termini matematici, il racconto mostra come sia possibile illustrare il famoso e fondamentale teorema di Cantor sulla non numerabilità dell'insieme delle parti di N. Infatti se denotiamo con 1 la decisione di andare a sinistra e con 0 quella si andare a destra possiamo rappresentare un possibile destino (cioè il contenuto di una pagina) tramite una successione di 0 ed 1 (ricordiamo che i Vagabondi sono immortali). Ora, chiamiamo *funzione caratteristica* di un sottoinsieme X di N la funzione $c_X: N \to \{1,0\}$ così definita:

$$c_X(n) = 0 \text{ se } n \in X \text{ e } c_X(n) = 1 \text{ se } n \notin X.$$

E' evidente che a due sottoinsiemi diversi corrispondono due funzioni caratteristiche diverse. Inoltre una qualunque funzione $c : N \to \{0,1\}$ può essere considerata la funzione caratteristica di un insieme, precisamente l' insieme $X = \{n \in N : c(n) = 1\}$. Ne segue che vi sono tante parti di N quante sono gli elementi di $\{0,1\}^N$, cioè le successioni di elementi di $\{0,1\}$. Equivalentemente ci sono tante parti di N quanti sono i possibili destini. Pertanto l'avere dimostrato che l'insieme dei destini non è enumerabile equivale all'avere dimostrato che

L'INSIEME DELLE PARTI DI N NON E' NUMERABILE.

"Tu ritieni di essere libero, eppure io, giorno per giorno, leggo nel Grande Libro dei Destini ciò che farai domani!".

Infatti il Giovane Integrato per sapere cosa avrebbe fatto il Vagabondo nel giorno *n*-esimo semplicemente leggeva il contrario di quanto affermato alla pagina *n*-esima del Grande Libro dei Destini.[28]

[28] Tuttavia la sua affermazione dopo una attenta analisi risulta di fatto sbagliata. Il paradosso per cui il destino del Vagabondo pur non essendo scritto in nessuna pagina del Libro dei Destini può tuttavia essere "1etto" in tale volume deriva dall'ambiguità della parola "1eggere" (o, meglio, della parola "scrivere"). Se ad esempio si leggessero nell'ordine la prima parola in alto a sinistra della prima pagina di un qualsiasi libro, poi la prima parola della seconda pagina e cosi via, si otterrebbe una lunga frase (magari sensata) che non sarebbe corretto ritenere scritta nel libro. In realtà la scrittura e la lettura di un testo avviene nell'ambito di una comune accettazione di un prefissato algoritmo di scelta delle parole. Nelle convenzioni dei linguaggi occidentali, tale algoritmo è sequenziale da sinistra a destra ma niente vieta di procedere da destra a sinistra. Consideriamo ad esempio la scrittura "Maria ama Mario"; se si accetta la convenzione sinistra-destra si ottiene un significato diverso di quello dato dalla convenzione destra-sinistra, che comunque è sensata. In definitiva, anche se dal Libro dei Destini è possibile ricavare le scelte giornaliere del Vagabondo, il destino di quest'ultimo non è affatto scritto in tale volume. Sarebbe d'altra parte possibile scrivere un Nuovo Libro dei Destini aggiungendo la successione di tali scelte in una ulteriore pagina: ed è quello che, idealmente, fa il Giovane Integrato.

LEZIONE 3:
Un esempio di seminario in un liceo

Nel seguito si riportano le slide di un incontro con ragazzi dei licei in cui ho esposto alcune nozioni di teoria degli insiemi. Spero che possano servire ai colleghi insegnanti. Non scrivo troppi commenti sperando che il tutto sia comprensibile. A richiesta posso inviare il corrispondente file in power point.
L'idea di base è che:

> *indovinare una cosa pensata (non avendo un limite prefissato al numero di tentativi) equivale al fatto che l'ambito delle possibili cose da pensare sia enumerabile.*

Infatti in questo caso posso pensare ad una strategia consistente in una successione di tentativi fatti uno dopo l'altro. Se la successione non esclude nessuna possibilità, cioè se è suriettiva, allora prima o poi la cosa pensata sarà indovinata. La iniettività della successione è utile per evitare che lo stesso tentativo sia ripetuto più volte.

Si suppone la situazione di una guardia ed un prigioniero. La guardia pensa a qualche cosa ed il prigioniero per potere essere liberato deve indovinare. Non ci sono limiti prefissati al numero di tentativi. Si inizia con un insieme finito di cose da pensare per introdurre la nozione di equipotenza.

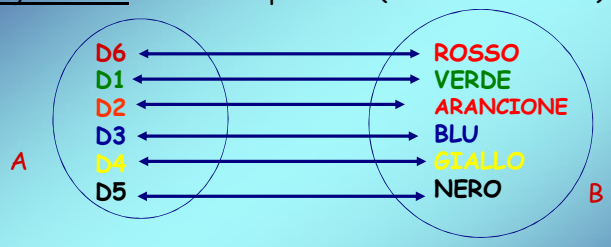
Diapositiva 1

Diapositiva 2

Diapositiva 3

Strategia vincente = chiedere di tutti i colori (funzione suriettiva).

Strategia ottima = evitare ripetizioni (funzione iniettiva).



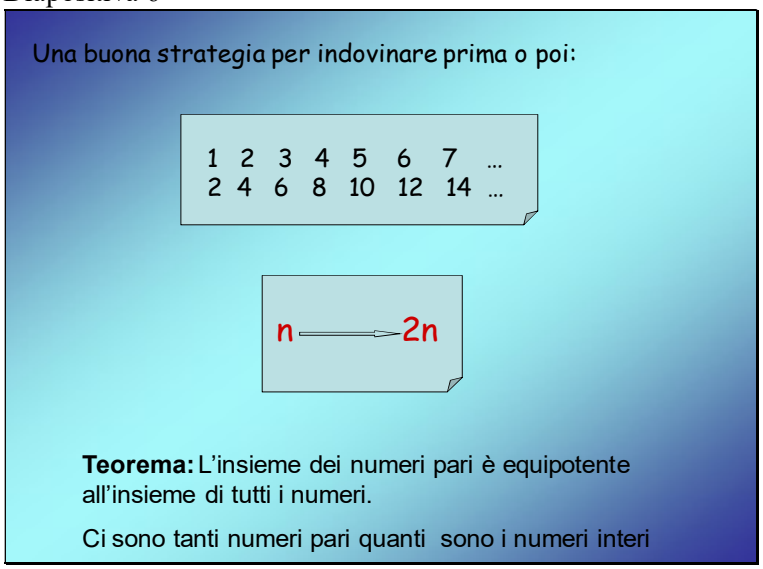
Dati due insiemi A e B, si dice che A è ***equipotente*** a B se esiste una funzione iniettiva e suriettiva di A in B. Cioè se è possibile stabilire una corrispondenza biunivoca (uno a uno) tra gli elementi di A e quelli di B.

Diapositiva 4

- **Chiamiamo *finito* un insieme *A* tale che esista una funzione biettiva**
- **f : {1, 2, 3, 4, 5, 6,…, n} → *A*.**
- **Chiamiamo *numerabile* un insieme *A* tale che esista una funzione biettiva**
- **f : N → *A***
- **Chiamiamo enumerabile un insieme che sia finito oppure numerabile**

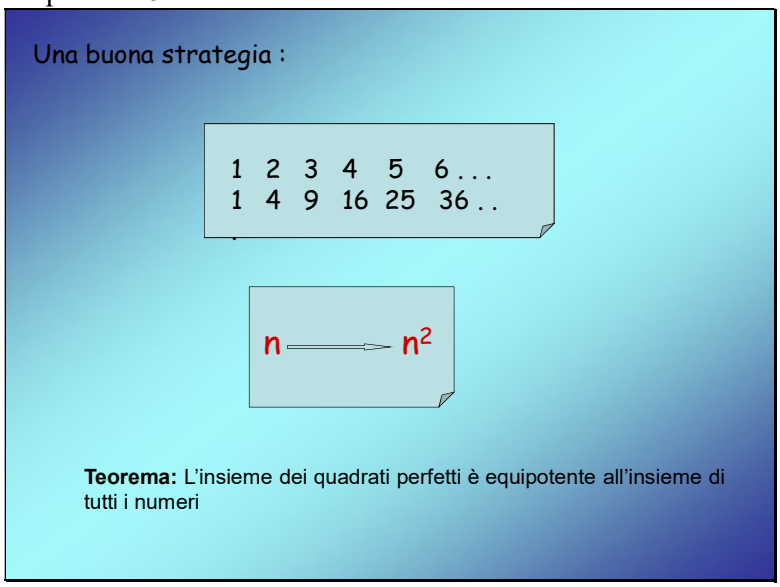
Diapositiva 5

Diapositiva 6

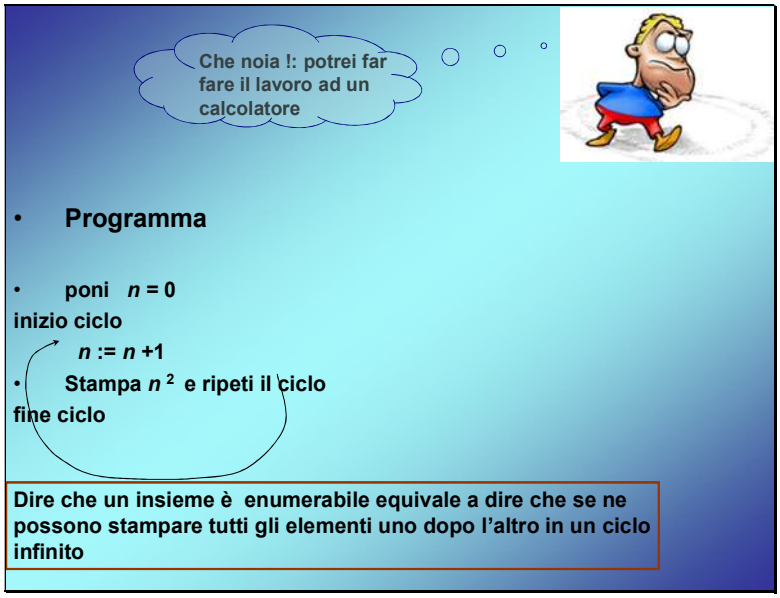


Diapositiva 7

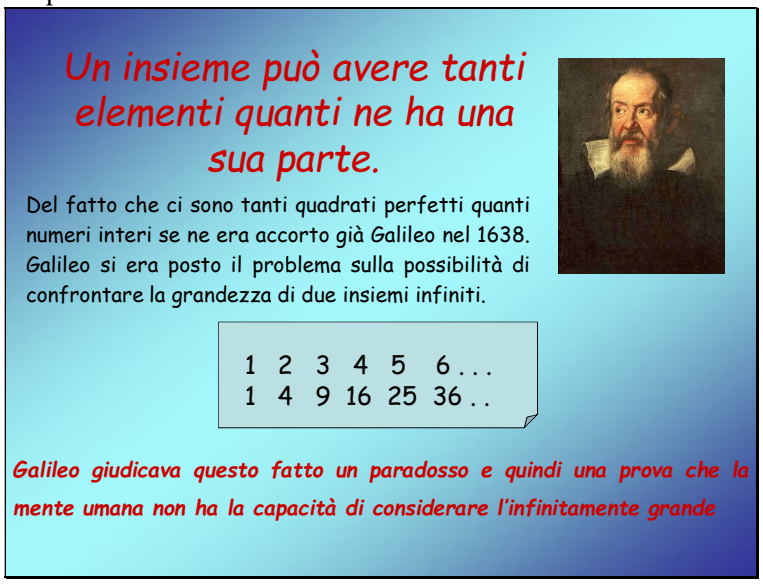
Diapositiva 8



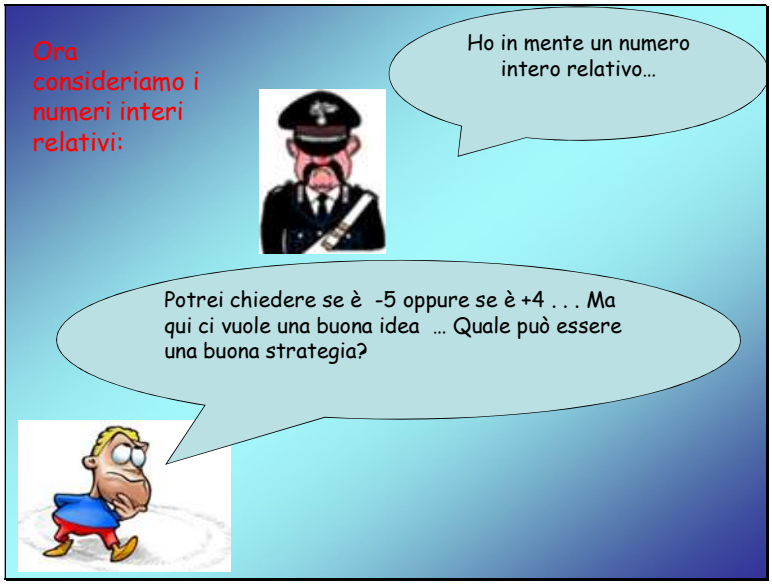
Diapositiva 9



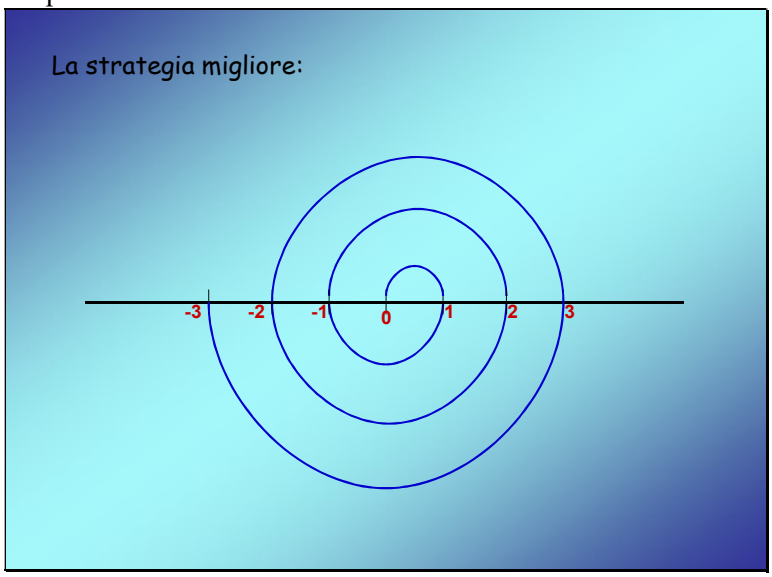
Diapositiva 10



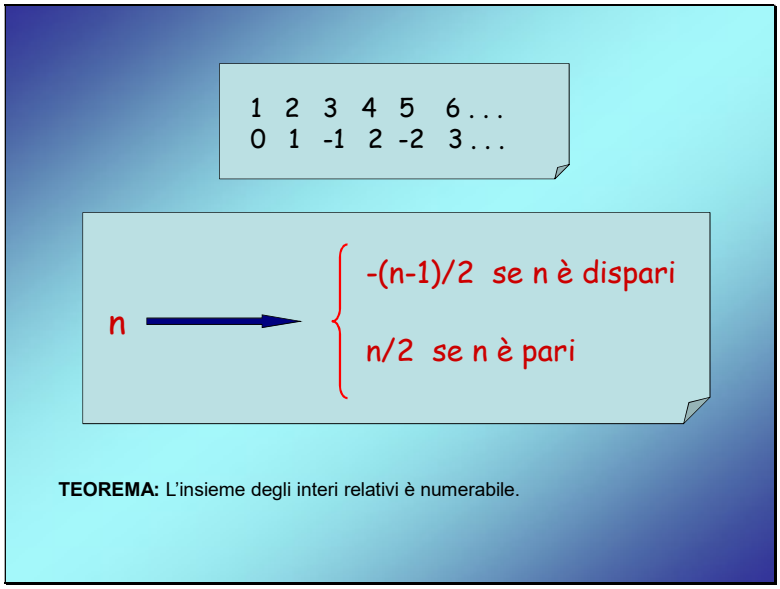
Diapositiva 11



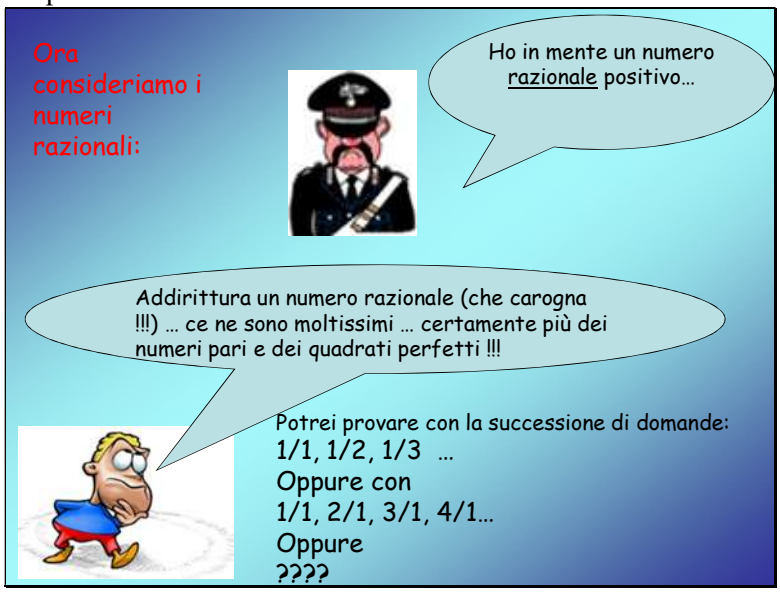
Diapositiva 12



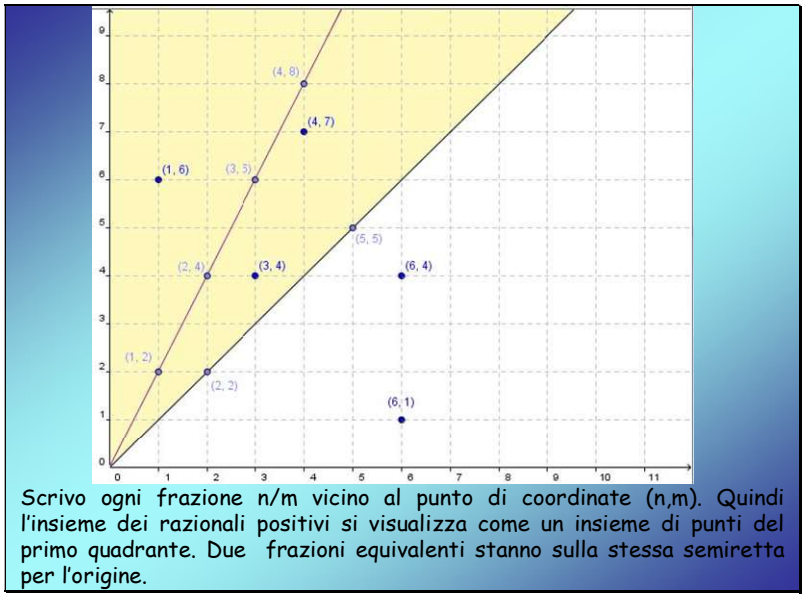
Diapositiva 13



Diapositiva 14



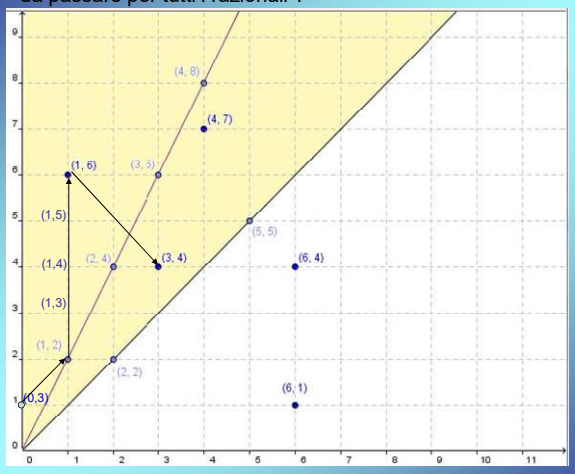
Diapositiva 15



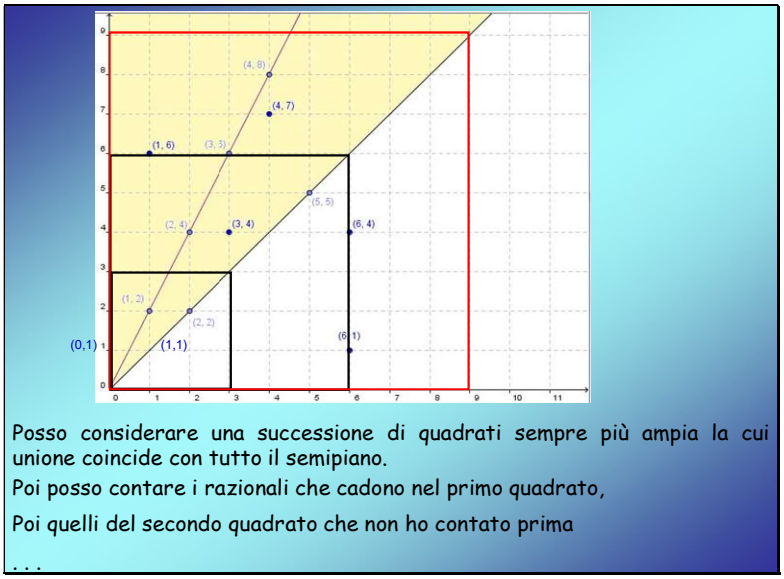
Scrivo ogni frazione n/m vicino al punto di coordinate (n,m). Quindi l'insieme dei razionali positivi si visualizza come un insieme di punti del primo quadrante. Due frazioni equivalenti stanno sulla stessa semiretta per l'origine.

Diapositiva 16

- E' possibile camminare passo dopo passo nel primo quadrante in modo da passare per tutti i razionali ?



Diapositiva 17



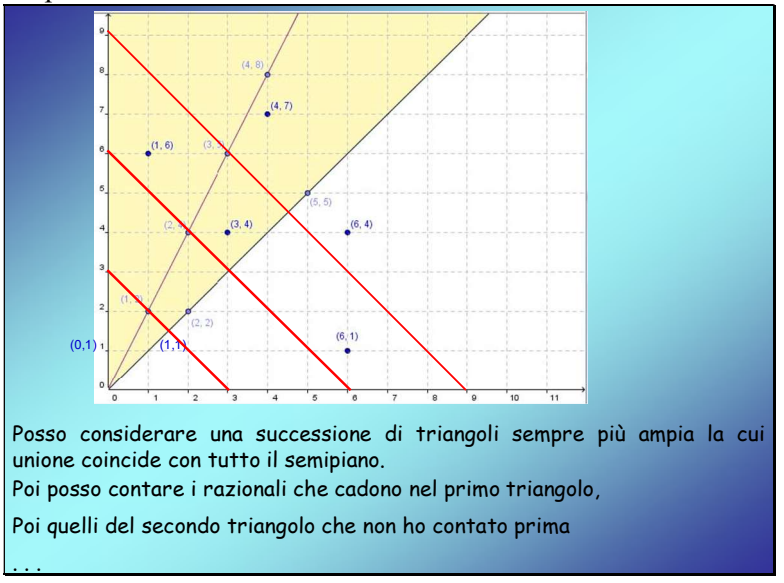
Posso considerare una successione di quadrati sempre più ampia la cui unione coincide con tutto il semipiano.

Poi posso contare i razionali che cadono nel primo quadrato,

Poi quelli del secondo quadrato che non ho contato prima

. . .

Diapositiva 18



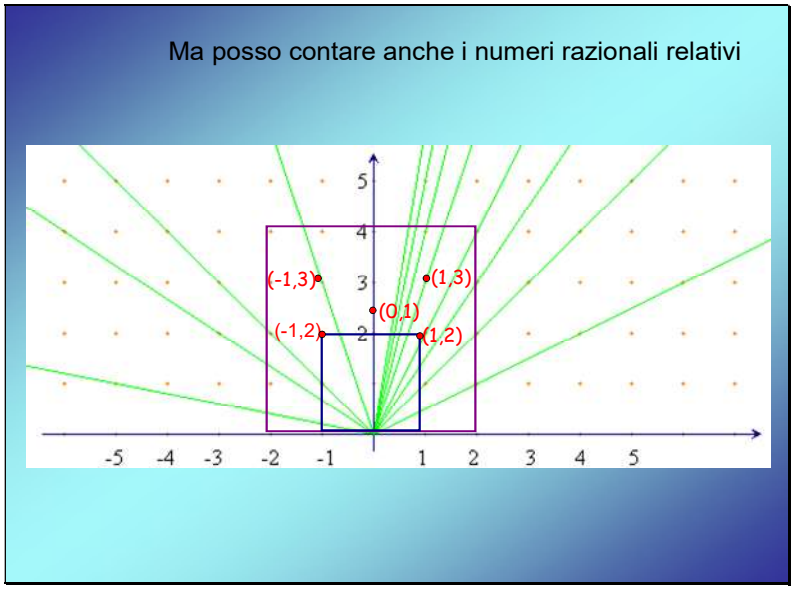
Posso considerare una successione di triangoli sempre più ampia la cui unione coincide con tutto il semipiano.

Poi posso contare i razionali che cadono nel primo triangolo,

Poi quelli del secondo triangolo che non ho contato prima

. . .

Diapositiva 19



Diapositiva 20

Diapositiva 21

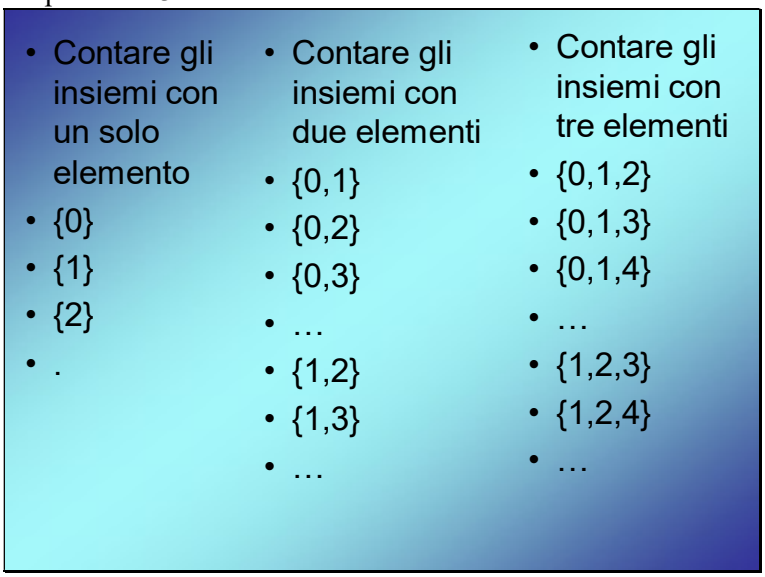
- Contare la parole con una sola lettera
- A
- B
- C
- .

- Contare la parole con due lettere
- AA
- AB
- AC
- …
- BA
- BB
- …

- Contare la parole con tre lettere
- AAA
- AAB
- AAC
- …
- ABA
- ABB
- …

Diapositiva 22

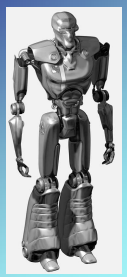
Diapositiva 23



Un insieme non numerabile.
Cambio ora il tipo di situazione ed inizio una serie di slide che riproducono, in una forma leggermente diversa, il raccontino "Nel paese del destino" che ho esposto precedentemente.
Lo scopo è dimostrare l'esistenza di un insieme infinito ma non numerabile.

Diapositiva 24

Esistono insiemi che non sono numerabili ?



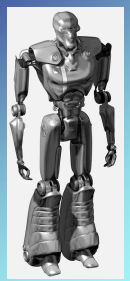
In un mondo futuro esistono robot intelligentissimi, più intelligenti degli uomini.

Ed allora gli uomini sono invidiosi ed odiano i robot

Il robot Carlo ogni mattina va in un bar ed ordina qualche cosa al al barista Luigi

Luigi: voi robot siete solo macchine e non siete liberi di scegliere. Infatti nel registro generale dei programmi è scritto tutto quello che farete giorno per giorno

Diapositiva 25



NON CI Credo !!!! Intanto dammi il cocktail numero 3 (nel bar esistevano solo 10 tipi di cocktail che i robot chiamavano per numero 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,

Ed invece si, ad esempio io so sempre quello che ordinerai anche se tu ti illudi di scegliere liberamente

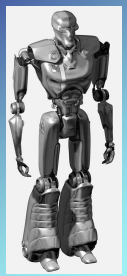
Appartengo all'Associazione Baristi e collegandomi tramite internet al sito del Registro delle Scelte posso consultare il programma inserito in ogni robot e quindi anche il tuo programma. Basta che chiedo che cosa ordinerai il tal giorno e mi viene detto

Diapositiva 26

Registro delle scelte

• Codice del robot	Giorni 1	2	3	4	5	6	7	8	9	10	11	12. . .
• 1	7	3	2	3	0	0	1	3	3	4	5	7 . . .
• 2	3	2	1	2	3	5	7	4	6	9	9	8 . . .
• 3	5	1	1	1	1	2	1	3	1	9	9	9 . . .
• 4	2	2	2	9	2	2	2	2	2	2	2	2 . .
•												

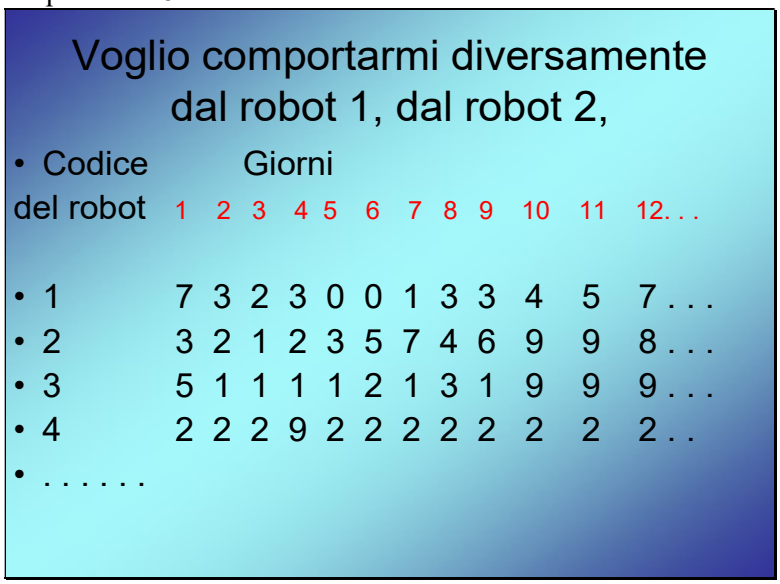
Diapositiva 27



NON CI Credo !!!! Il registro esiste, tutti lo possono vedere ma il codice di ogni robot e segreto e neanche io conosco il mio.

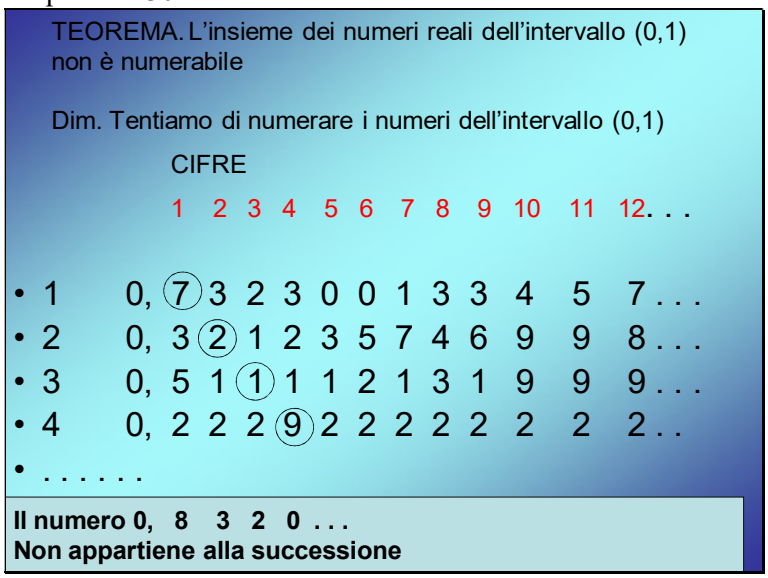
Ed invece io ho scoperto quale è il tuo codice e quindi so sempre quello che farai

Diapositiva 28



Diapositiva 29

Diapositiva 30



CAPITOLO 2
ALTRI TEOREMI ED ALTRI NUMERI

1. Teorema di Cantor-Bernstein: è tanto scontato che valga ?

Ricordiamo che il teorema di Cantor-Bernstein sostiene che:

Dati due insiemi A e B, se A è equipotente ad una parte di B e B è equipotente ad una parte di A, allora A e B sono equipotenti.

Dal punto di vista intuitivo la validità di tale affermazione appare scontata. Questo accade perché spesso si usa l'espressione "potenza minore o uguale a" e quindi si enuncia il teorema al modo seguente:

Dati due insiemi A e B, se la potenza di A è minore o uguale alla potenza di B e la potenza di B è minore o uguale alla potenza di A, allora A e B sono equipotenti.

Ora siamo abituati ad usare la parola "minore o uguale" in connessione con una relazione d'ordine $\leq$ e attribuiamo alle relazioni d'ordine la proprietà antisimmetrica che dice che se $x \leq y$ ed $y \leq x$ allora $x = y$.

Un ulteriore motivo è che le nostre idee sugli insiemi nascono dalla considerazione di insiemi finiti e per tali insiemi effettivamente la proprietà espressa da tale teorema appare scontata. Tuttavia se si passa dal finito all'infinito allora, come abbiamo già visto in numerose occasioni, la validità di una proprietà potrebbe anche non conservarsi.

D'altra parte tale proprietà si basa sulla nozione di funzione che viene data in teoria degli insiemi che prima di Cantor era molto più restrittiva. Se si cambia la nozione di funzione non è detto che tale teorema continui a valere. Ad esempio potremmo immaginare una comunità di matematici per cui solo le funzioni continue hanno il diritto di chiamarsi "funzioni".[1] Per tali mate-

---

[1] La cosa non sarebbe tanto strana. Ad esempio i matematici fino alla prima metà dell'ottocento condividevano questo punto di vista e questo perché la loro idea di funzione era molto legata al continuo geometrico o all'algebra. Venivano pertanto accettate come funzioni solo quelle riconducibili a curve geometriche o algebriche. Anche attualmente esistono filosofi della matematica che considerano esistenti solo gli oggetti matematici che sono "effettivamente producibili" e solo le funzioni che sono "effettivamente computabili". Sono gli intuizionisti, di cui abbiamo già parlato, oppure, più in generale, i seguaci dei vari tipi di costrut-

matici il teorema di Cantor-Bernstein dovrebbe essere riformulato considerando solo funzioni bicontinue (funzioni continue, invertibili, la cui inversa è ancora continua) al modo seguente.

> *Dati due spazi topologici A e B se esiste una funzione bicontinua di A in una parte B* ed una funzione bicontinua di *B* in una parte di *A* allora esiste una funzione bicontinua di *A* in *B*..

D'altra parte è facile mostrare che tale teorema non vale. Ad esempio se poniamo $A = (-1,1)$ e $B = [-1,1]$ allora la funzione $f(x) = x/2$ ristretta ad A è una funzione bicontinua di A nella parte $(-1/2, +1/2)$. La stessa funzione ristretta a B è una funzione bicontinua di B nella parte $[-1/2,1/2]$ di A. E'evidente che tra A e B non può esserci una funzione bicontinua.

2. Cercarne una dimostrazione[2]

Esiste una dimostrazione del teorema di Cantor-Bernstein che è esposta in tutte le introduzioni elementari alla teoria degli insiemi e che spesso è esposta nel primo capitolo dei libri di algebra di livello universitario. La dimostrazione non è troppo lunga ed i singoli passaggi sono semplici. Tuttavia nelle esposizioni che mi è capitato di leggere non si riesce a capire affatto da dove salti fuori e quale è la possibile strategia che ha condotto a trovarla. D'altra parte questo modo di procedere è presente quasi sempre nei testi di di matematica nei quali, dato un teorema, ci si limita quasi sempre a riprodurre un dimostrazione già nota assegnando implicitamente allo studente solo il compito di capirla e ripeterla. Insomma in generale nei libri di testo non si considera la "dimostrazione" come qualcosa da trovare (l'incognita di un problema) ma solo qualcosa che deve solo ricordare capendo perché i singoli passaggi sono corretti.

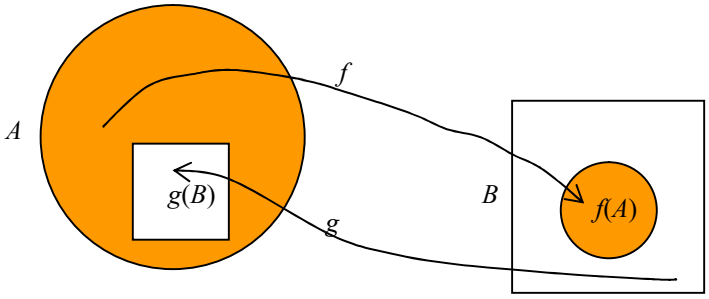
---

tivismo in matematica. Ora risulta che tutte le definizioni proposte di funzione computabile di variabile reale verificano l'implicazione
computabile $\Rightarrow$ *continua.*
Pertanto anche i costruttivisti accettano come realmente esistenti solo funzioni che sono continue.

[2] Questo ed il prossimo paragrafo sono la rielaborazione di uno lavoro, scritto in collaborazione con la dottoressa Cristina Coppola ed il Prof. Saverio Tortoriello e che apparirà su Periodico di Matematiche.

In questo paragrafo invece proverò ad argomentare quale possibile strategia si può adottare per trovare (inventare) una dimostrazione. Ricordiamo ancora quale è l'enunciato del teorema:

Teorema 2.1. Dati due insiemi A e B supponiamo che A sia equipotente ad una parte di B e che B sia equipotente ad una parte di A, allora A e B sono equipotenti.



Indichiamo con f una funzione iniettiva di A in B e con g una funzione iniettiva di B in A. Volendo trovare una funzione biettiva h di A in B dobbiamo servirci in qualche modo del materiale disponibile e quindi delle due funzioni iniettive $f : A \to B$ e $g : B \to A$. Supponiamo che le due funzioni non siano anche suriettive poichè in questo caso l'equipotenza non si dovrebbe dimostrare. Naturalmente poiché dobbiamo andare da A in B abbiamo in realtà bisogno di g^{-1} anche se tale funzione pur essendo iniettiva non è ovunque definita in A. Dobbiamo poi costruire una funzione h biettiva $h : A \to B$ facendo operare:

- in alcuni casi la funzione $f : A \to B$ (che è iniettiva ma non suriettiva)
- negli altri casi la funzione $g^{-1} : A \to B$, (che è suriettiva ma non è ovunque definita).

In altri termini l'idea è che sia possibile trovare un sottoinsieme $D \subseteq A$ in modo che la funzione cercata h sia definita dal porre

$$h(x) = \begin{cases} f(x) & \text{se } x \in D \\ g^{-1}(x) & \text{se } x \in -D. \end{cases}$$

Si tratta ora di capire come dovrebbe essere un tale insieme perché il tutto funzioni e, naturalmente, cercare di dimostrare che tale insieme esiste. In proposito osserviamo che:

1. Perché la definizione abbia senso abbiamo bisogno che su ogni elemento $x \in A\text{-}D$ possa operare g^{-1} e questo si ottiene solo se risulta

$$A\text{-}D \subseteq g(B).$$

2. Perché la funzione h sia iniettiva è sufficiente supporre che:

$$f(D) \cap g^{-1}(A\text{-}D) = \varnothing.$$

Infatti, essendo f iniettiva in D e g^{-1} iniettiva $A–D$, rispettivamente, la non iniettività di h si potrebbe realizzare solo se esistessero $x \in D$ ed $y \in A\text{-}D$ tali che $h(x) = f(x) = g^{-1}(y) = h(y)$ e ciò comporterebbe che $h(x) \in f(D) \cap g^{-1}(A\text{-}D)$.

3. Infine perché h sia suriettiva deve accadere che

$$h(A) = f(D) \cup g^{-1}(A\text{-}D) = B.$$

Riassumendo, riusciamo a dimostrare il teorema solo se troviamo un sottoinsieme D di A tale che:

a) $\text{-}D \subseteq g(B)$ (perché possa operare g^{-1})
b) $f(D) \cap g^{-1}(\text{-}D) = \varnothing$ (perché la funzione h sia iniettiva)
c) $f(D) \cup g^{-1}(\text{-}D) = B$ (perché h sia suriettiva).

La seconda e terza condizione equivalgono a

i) $g^{-1}(\text{-}D) = \text{-}f(D)$

che a sua volta implica

$g(g^{-1}(\text{-}D)) = g(\text{-}f(D))$.

Poiché, per *a*), $g(g^{-1}(A\text{-}D)) = (A\text{-}D) \cap g(B) = A\text{-}D$[3], risulta che

$\text{-}D = g(\text{-}f(D))$ e quindi

$$D = \text{-}g(\text{-}f(D)). \qquad (2.1)$$

Viceversa, se D verifica (2.1) allora

$D \supseteq \text{-}g(B)$

inoltre, essendo g iniettiva,

$g^{-1}(\text{-}D) = g^{-1}(g(\text{-}f(D))) = \text{-}f(D)$.

---

[3] Dati due insiemi S e T se h è una funzione di S in T ed X è un sottoinsieme di S allora $h^{-1}(h(X)) \supseteq X$ e se h è iniettiva $h^{-1}(h(X)) = X$. Invece se Y è un sottoinsieme di T allora $h(h^{-1}(Y)) \subseteq Y$. Infatti se y è un elemento di Y di cui non è possibile fare l'antimmagine in quanto non appartiene ad $h(S)$, allora, quando si calcola $h(h^{-1}(Y))$, y *"scompare"*. In realtà vale l'equazione $h(h^{-1}(Y)) = Y \cap h(S)$. Ciò comporta che se h è suriettiva vale l'uguaglianza $h(h^{-1}(Y)) = Y$.

Pertanto, le tre condizioni che vogliamo imporre a D equivalgono all'unica condizione espressa dall'equazione (2.1). In definitiva, indicando con $k : \mathcal{P}(A) \to \mathcal{P}(A)$ la funzione definita ponendo

$$k(X) = -g(-f(X)), \qquad (2.2)$$

dobbiamo provare che esiste un insieme D tale che $D = k(D)$.

Siamo allora giunti alla seguente situazione:

la dimostrazione del teorema di Cantor-Bernstein si riconduce alla dimostrazione che l'equazione

$$k(X) = X \qquad (2.3)$$

ammette soluzione o, come si dice usualmente, che k abbia un *punto fisso*.

Abbiamo pertanto ridotto un problema (dimostrare il teorema di Cantor-Bernstein) ad un altro (esistenza di un punto fisso) con la speranza che quest'ultimo sia più semplice da risolvere anche perché con le equazioni i matematici hanno un po' più di esperienza. A questo punto se siamo ricercatori che vogliono trovare una dimostrazione del teorema, dobbiamo andare a cercare in biblioteca se esiste qualche teorema di punto fisso adatto allo scopo. Nel paragrafo 2 dell'Appendice, si espongono due teoremi che sembrano fare al caso nostro. Se ci riferiamo al primo e più semplice è sufficiente provare che k è monotona. Infatti al crescere di X:

- $f(X)$ cresce
- quindi $B-f(X)$ decresce
- quindi $g(B-f(X))$ decresce
- quindi $A-g(B-f(X))$ cresce.

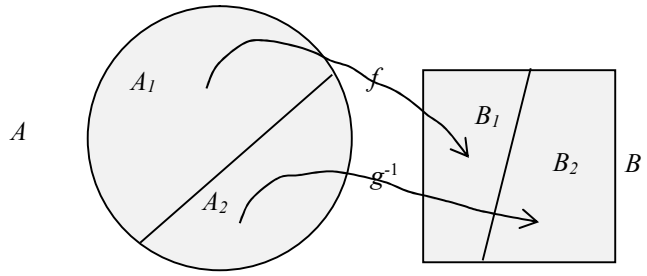
Essendo k monotona per il teorema citato esiste un punto fisso di k e quindi il teorema di Cantor-Bernstein è provato.

E' possibile anche capire dove si blocca la dimostrazione nel caso in cui f e g siano due omeomorfismi e si voglia che h sia un omeomorfismo. Noi otteniamo la funzione biettiva h facendo lavorare in un insieme D la funzione f e nel suo complemento $A-D$ la funzione g^{-1}. In altri termini h è ottenuta incollando due funzioni. Se f e g sono omeomorfismi f che g^{-1} sono funzioni continue in D ed in $-D$, rispettivamente. Purtroppo ciò non comporta che il risultato h del loro "incollamento" sia ancora un omeomorfismo.

3. Trarre altre informazioni dalla dimostrazione

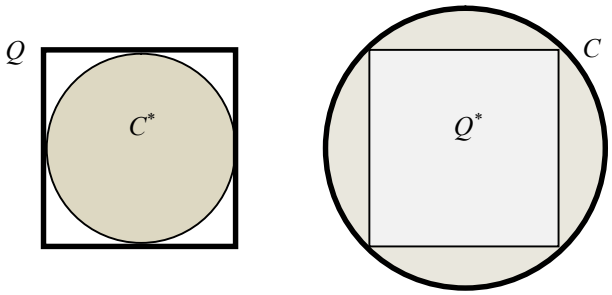
Come abbiamo già osservato una dimostrazione di un teorema spesso contiene più informazioni di quanto sia presente nel suo enunciato. Se infatti analizziamo la dimostrazione ora fatta possiamo anche enunciare il teorema di Cantor-Bernstein al modo seguente.

Teorema 3.1. Siano A e B due insiemi e supponiamo che esiste una funzione iniettiva $f : A \to B$ ed una funzione iniettiva $g : B \to A$. Allora A è scomponibile negli insiemi A_1, A_2 e B negli insiemi B_1, B_2 in modo che $f : A_1 \to B_1$ e $g : B_2 \to A_2$ siano due biezioni. Pertanto A e B, essendo scomponibili in parti equipotenti, sono equipotenti.



Dim. E' sufficiente riesaminare la dimostrazione del Teorema 1.1 e porre $A_1 = D$, $A_2 = A\text{-}D$, $B_1 = f(A_1)$, $B_2 = g^{-1}(A_2)$. □

Per evidenziare come sia interessante questo modo di enunciare il teorema di Cantor-Bernstein consideriamo il seguente esempio. Per provare che un quadrato Q ed un cerchio C sono equipo-



tenti basta osservare che due quadrati sono sempre equipotenti e che due cerchi sono sempre equipotenti (basta riferirsi ad opportune similitudini). Allora dal fatto che Q contenga il cerchio

iscritto C^* e che C^* sia equipotente a C, segue che Q ha cardinalità maggiore o uguale a C. D'altra parte il fatto che il cerchio C contiene un quadrato inscritto Q^* a che Q^* è equipotente a Q, comporta che C ha cardinalità maggiore o uguale a Q. Il teorema di Cantor-Bernstein comporta allora che Q e C sono equipotenti. Tuttavia il Teorema 3.1 ci fornisce maggiori informazioni e ci permette di dimostrare il seguente "paradosso".

Proposizione 3.2. (Paradosso del quadrato e del cerchio). E' possibile ritagliare un quadrato in due pezzi, lasciarne una parte fissa, dilatare la parte rimanente ed ottenere il cerchio circoscritto al quadrato.

Dim. Per potere illustrare meglio la dimostrazione procediamo più in generale considerando, dato un quadrato Q, una qualunque traslazione f che porti Q in un quadrato Q^* ed una similitudine g che porti il cerchio C circoscritto a Q^* nel cerchio C^* inscritto in Q. Tale funzione è il composto di f^{-1} per una opportuna contrazione. Allora esiste una partizione Q_1, Q_2 del quadrato Q ed una partizione C_1, C_2 del cerchio C tali che $C_1 = f(Q_1)$ e $Q_2 = g(C_2)$. Se supponiamo che f sia l'applicazione identica e quindi che $C_1 = Q_1$ otteniamo che dilatando Q_2 e tenendo fisso Q_1 otteniamo il cerchio circoscritto a Q. □

Può anche essere interessante esplicitare nell'enunciato del teorema il metodo per ottenere la soluzione dell'equazione 2.3. Ad esempio se si guarda il secondo dei teoremi di punto fisso esposti nel primo volume, si ottiene la seguente proposizione.

Teorema 3.3. Dati due insiemi A e B supponiamo che $f : A \to B$ e $g : B \to A$ siano due funzioni iniettive. Definiamo le due successioni $\underline{A}_1, \underline{A}_2 \ldots$ e $\underline{B}_1, \underline{B}_2 \ldots$ ponendo:

$$\begin{array}{lll} \underline{A}_1 = A - g(B) & ; & \underline{B}_1 = B - f(\underline{A}_1) \\ \underline{A}_2 = A - g(\underline{B}_1) & ; & \underline{B}_2 = B - f(\underline{A}_2) \\ \ldots\ldots & & \\ \underline{A}_n = A - g(\underline{B}_{n-1}) & ; & \underline{B}_n = B - f(\underline{A}_n). \\ \ldots\ldots & & \ldots \end{array}$$

Allora ponendo $A_1 = \cup_{n \in N} \underline{A}_n$ e $A_2 = A - A_1$ si ottiene la partizione di A di cui è detto nel Teorema 3.1.

Dim. Allo scopo di potere applicare il teorema 2.5 in Appendice, osserviamo che per ogni successione $(X_n)_{n\in N}$ di sottoinsiemi di A

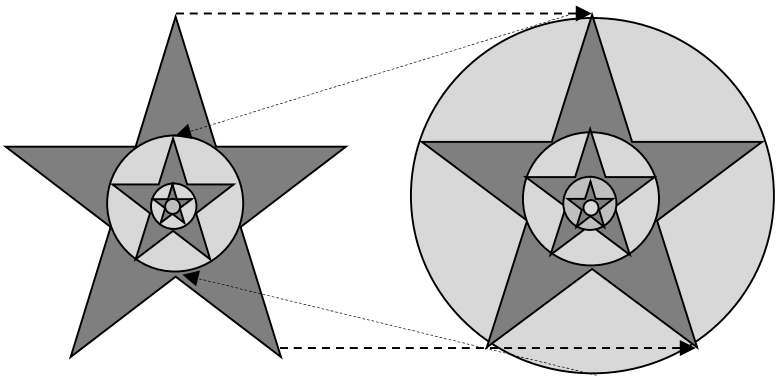
$$k(\cup_{n\in N}X_n) = A\text{-}g(B\text{-}f(\cup_{n\in N}X_n)) = A\text{-}g(B\text{-}\cup_{n\in N} f(X_n))$$
$$= A\text{-}g(\cap_{n\in N} (B\text{-}f(X_n))) = A\text{-}\cap_{n\in N} g(B\text{-}f(X_n))$$
$$= \cup_{n\in N} A\text{-}g(B\text{-}f(X_n)) = \cup_{n\in N} k(X_n),$$

dove l'uguaglianza $g(\cap_{n\in N} (B\text{-}f(X_n))) = \cap_{n\in N} g(B\text{-}f(X_n))$ è una conseguenza del fatto che g è iniettiva. Dunque $A_1 = \cup_{n\in N} k^n(\varnothing)$ è il minimo punto fisso di k. E' facile mostrare che:

$k(\varnothing) = A\text{-}g(B\text{-}f(\varnothing)) = A\text{-}g(B) = \underline{A}_1$,
$k^2(\varnothing) = A\text{-}g(B\text{-}f(\underline{A}_1)) = A\text{-}g(\underline{B}_1) = \underline{A}_2$
…
$k^n(\varnothing) = A\text{-}g(B\text{-}f(\underline{A}_{n-1})) = A\text{-}g(\underline{B}_{n-1}) = \underline{A}_n$. □

Ad esempio confrontiamo una stella a cinque punte S ed un cerchio C. Non è restrittivo supporre che la stella si possa inscrivere nel cerchio tramite una traslazione $f : S \to C$. Inoltre esiste una applicazione $g : C \to S$ capace di portare il cerchio all'interno della stella come in figura. Basta porre g uguale al prodotto di una contrazione e di una traslazione. Per trovare allora la partizione di S dobbiamo costruire le successioni

$\underline{S}_1 = S\text{-}g(C)$; $\underline{C}_1 = C\text{-}f(\underline{S}_1) = g(C)$
$\underline{S}_2 = S\text{-}g(\underline{C}_1)$; $\underline{C}_2 = C\text{-}f(\underline{S}_2) = g(C_1)$
. . . .
$\underline{S}_n = S\text{-}g(\underline{C}_n)$; $\underline{C}_n = C\text{-}f(\underline{S}_n) = g(C_{n-1})$.
. . . .



$\boldsymbol{S = S_1 \cup S_2}$ $\boldsymbol{C}$

Guardando la stella dall'esterno verso l'interno si vede che:

$\underline{S}_1$ è costituito dai primi cinque "triangoli" scuri a sinistra,
$\underline{S}_2$ è costituito dai primi 10 "triangoli" scuri a sinistra,
...
$\underline{S}_n$ è costituito dai primi $n\cdot 5$ "triangoli" scuri a sinistra,
…

Pertanto $S_1 = \cup_{n\in N}\underline{S}_n$ (la parte scura) e $S_2 = S\text{-}S_1$ (la parte chiara) costituiscono la partizione cercata. La biezione tra la stella ed il cerchio si ottiene tramite una traslazione a destra della parte scura ed una dilatazione più una traslazione della parte chiara.

Possiamo anche supporre che la stella sia direttamente circoscritta dal cerchio e quindi guardare solo la parte destra del disegno. In questo caso

la stella può essere trasformata nel cerchio ritagliando la parte chiara ed allargandola fino a circondare la stella.

Da notare la somiglianza con il metodo della equiscomponibilità in questo modo di procedere.

4. Le dimostrazioni di Borel e di Kőnig

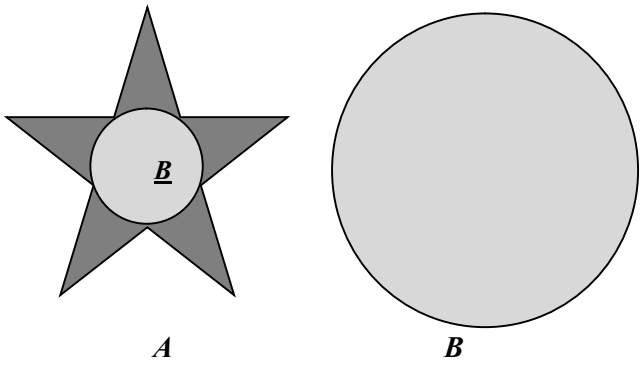
Esistono varie dimostrazioni del teorema di Cantor-Bernstein. La dimostrazione di Borel, che ricorda molto le tecniche di manipolazione delle serie di potenze positive, si basa sul fatto che l'equipotenza è compatibile con l'unione disgiunta. In altre parole due insiemi sono equipotenti se si possono tagliare in fette equipotenti.

Proposizione 4.1. Siano X ed Y due insiemi che ammettono due partizioni $(X_i)_{i\in I}$ e $(Y_i)_{i\in I}$ tali che per ogni $i\in I$, $X_i \equiv Y_i$, allora $X \equiv Y$.

Dim. Sia, per ogni $i\in I$, $f_i : X_i \to Y_i$ una funzione biettiva tra X_i ed Y_i, e definiamo $f : X \to Y$ ponendo, per ogni $x\in X$, $f(x) = f_i(x)$ dove i è l'unico elemento tale che $x\in X_i$. Tale funzione è biettiva in quanto per ogni $y\in Y$ esiste uno ed un solo $i\in I$ tale che $y\in Y_i$ e quindi esiste uno ed un solo $x\in X_i$ tale che $f(x) = f_i(x) = y$. □

Dimostrazione di Borel. Per illustrare la dimostrazione di Borel ci riferiamo all'esempio della stella e del cerchio che abbiamo considerato nel paragrafo precedente. Posto $\underline{B} = g(B)$, per provare l'equipotenza tra A e B è sufficiente provare l'equipotenza tra A e la sua parte $\underline{B}$ (cioè tra la stella ed il cerchio inscritto). Ora, osserviamo che la funzione composta $h = g\circ f$ si presenta come una ap-

plicazione biettiva di A in A.[4] Nell'esempio fatto, h è una funzione della stella in se che, essendo una composizione di una traslazione ed una contrazione, conserva la forma delle figure.



Poniamo:

$A_1 = A\text{-}\underline{B}$ (la parte in scuro della figura a forma di cinque punte).
$A_2 = \underline{B} - h(A)$ (la parte in chiaro della figura che si presenta come un cerchio meno una stella).
$A_3 = h(A_1) = h(A)\text{-}h(\underline{B})$ (stessa forma di A_1 uguale alla figura a cinque punte che abbiamo disegnato in scuro)
$A_4 = h(A_2)$ (quindi cerchio meno stella)
. . .
$A_n = h(A_{n-2})$
. . .

Si noti che gli elementi della successione $(A_n)_{n\in N}$ sono a due a due disgiunti. Inoltre gli elementi di indice pari sono equipotenti tra loro e lo stesso si dice per quelli di indice dispari. Poniamo ora $I = \cap_n A_n$ (nella nostra figura I è il punto centrale della stella). Allora A può essere scomposto al modo seguente

$$A = I \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup ...$$

mentre $\underline{B}$ può essere scomposto al modo seguente

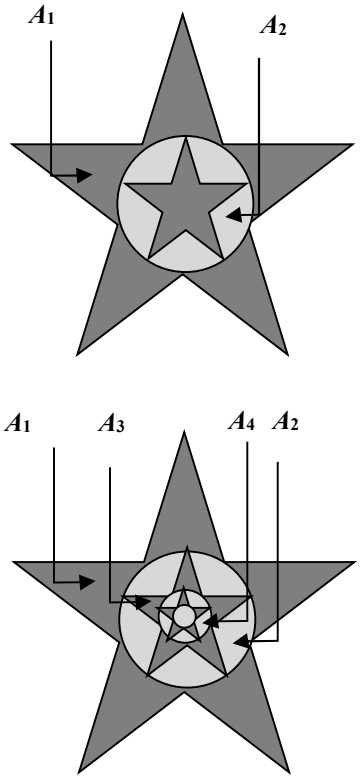
$$\underline{B} = I \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup ...$$

oppure, commutando,

$$\underline{B} = I \cup A_3 \cup A_2 \cup A_5 \cup A_4 \cup ...$$

[4] Abbiamo leggermente semplificato la dimostrazione di Borel senza alterarne lo spirito.

Essendo A_1 equipotente ad A_3, A_2 equipotente ad A_4, ... possiamo concludere che A è equipotente a $\underline{B}$.



L'equipotenza tra il cerchio e la stella può essere visualizzata al modo seguente. Considerata la scomposizione della stella in parti chiare e scure, lasciamo invariata la parte scura e dilatiamo la parte chiara opportunamente fino ad estenderla in modo da circoscrivere la parte scura. Si ottiene un cerchio dello stesso raggio del cerchio a destra. In tale modo la dimostrazione del teorema di Cantor-Bernstein diviene in un certo senso "visuale".

Dimostrazione di Kőnig. Di stile completamente diverso è la dimostrazione fatta nel 1906 dal matematico ungherese Julius Kőnig (1849 –1913). Essa si basa sull'idea che per provare l' equipotenza di due insiemi A e B è sufficiente dividere $A \cup B$ in

classi di equivalenza, in modo che in ciascuna classe gli elementi di A siano tanti quanti quelli di B.

Più precisamente, siano $f : A \to B$ e $g : B \to A$ due funzioni iniettive e, per ogni elemento a di A, costruiamo la seguente successione di elementi di $A \cup B$

$... f^{-1}(g^{-1}(a)), g^{-1}(a), a, f(a), g(f(a)), ...$

Tale successione può sempre essere continuata *verso destra*, ma non sempre *verso sinistra*. Infatti g^{-1} è definito in a solo se $a \in g(B)$, $f^{-1}(g^{-1}(a))$ è definito solo se $g^{-1}(a) \in f(A)$, e così via. Indichiamo con $[a]$ l'insieme degli elementi di tale successione. Analogamente a partire da un elemento $b \in B$ possiamo costruire la successione di elementi

$... g^{-1}(f^{-1}(b)), f^{-1}(b), b, g(b), f(g(b)), ...$

che ancora può essere prolungata oppure no indefinitamente a sinistra. Indichiamo con $[b]$ l'insieme degli elementi di una tale successione. Una sequenza che si ferma ad un elemento di A viene chiamata *A-stopper* una sequenza che si ferma ad un elemento di B viene chiamata *B-stopper*.

Vogliamo provare che la classe degli insiemi $[x]$ ottenuti in questo modo costituisce una partizione di $A \cup B$. Infatti è evidente che tale classe è un ricoprimento. Inoltre se due sequenze hanno un elemento in comune anche l'elemento che segue sarà lo stesso, così come quello che lo precede (se esiste) (perché f e g sono iniettive).[5] Dunque le due sequenze coincidono. Essendo

$$A = \cup_{z \in A \cup B} A \cap [z] \text{ e } B = \cup_{z \in A \cup B} B \cap [z],$$

per dimostrare l'equipotenza tra A ed B è sufficiente mostrare che, per ogni $z \in A \cup B$, l'insieme $A \cap [z]$ è equipotente a $B \cap [z]$. Ora se la classe $[z]$ è A-stopper, allora f è una biezione che porta $A \cap [z]$ in $B \cap [z]$. Se $[z]$ è B-stopper, allora g è una biezione che porta $B \cap [z]$ in $A \cap [z]$. Negli altri casi sia f che g sono biezioni tra le due classi e ciò conclude la dimostrazione.

---

[5] In effetti la partizione è quella corrispondente alla relazione di equivalenza $\langle f \cup g \rangle$ generata dalle applicazioni f e g. Come è noto, tale relazione si può ottenere prima simmetrizzando $f \cup g$ ottenendo in tale modo la relazione $R = f \cup g \cup f^{-1} \cup g^{-1}$. Successivamente viene costruita la chiusura transitiva di R dicendo che due elementi x ed y sono in relazione se esiste una catena $x_1, x_2, \ldots x_{n-1}, x_n$ tale che $x = x_1$ $(x_i, x_{i+1}) \in R$ e $x_n = y$. Infine si impone la proprietà riflessiva aggiungendo le coppie (z,z) con $z \in X \cup Y$.

5. Equiscomponibilità e paradosso di Vitali

In questo e nel prossimo paragrafo esporrò alcune interessanti e paradossali conseguenze dell'assioma della scelta che sono legate alla nozione di equiscomponibilità ed a quella di misura. Ricordiamo le principali nozioni in teoria della misura.

Definizione 5.1. Sia S un insieme non vuoto ed M una algebra di Boole di sottoinsiemi di S[6] . Allora, dato un cardinale $\lambda \geq 2$ diciamo che M è una *λ-algebra* di Boole se
- per ogni famiglia $(A_i)_{i\in I}$ di elementi in M tale che la cardinalità di I sia minore o uguale a λ risulta che $\cup_{i\in I}A_i \in M$.

Definizione 5.2. Sia $\lambda \geq 2$, una *misura λ-additiva* è una funzione $\mu : M \rightarrow R^{+}\cup\{\infty\}$, dove M è una λ-algebra di Boole, tale che

i) $\mu(\varnothing) = 0$,

ii) $\mu(\cup_{i\in I}A_i) = \sum_{i\in I} \mu(A_i)$ per ogni famiglia $(A_i)_{i\in I}$ di elementi di M a due a due disgiunti con I di cardinalità minore o uguale a λ.

Se X è un elemento in cui μ è definita, cioè se $X\in M$, allora si dice che X è *misurabile.*

Da notare che $\sum_{i\in I} \mu(A_i)$ viene definito come estremo superiore di tutte le somme finite di elementi di $\mu(A_i)$. I matematici sono particolarmente interessati alle misure 2-additive che prendono anche il nome di *misure finitamente additive* ed alle misure ω-additive che si dicono anche *numerabilmente additive.* Naturalmente ogni misura numerabilmente additiva è anche finitamente additiva.

Definizione 5.3. Una misura μ nello spazio euclideo viene detta *invariante rispetto alle isometrie*, se

$$\mu(X) = \mu(\tau(X))$$

---

[6] Una *algebra di Boole di sottoinsiemi* di S è una classe M di sottoinsiemi di S tale che:
- $\varnothing\in M$ ed $S\in M$
- l'unione di due elementi di M appartiene ancora a M
- l'intersezione di due elementi di M appartiene ancora ad M
- il complemento di un elemento di M appartiene ancora ad M.

per ogni isometria τ e per ogni insieme misurabile X.

In altri termini una misura è invariante se insiemi "uguali" hanno la stessa misura o, se si vuole, se la misura si conserva quando le figure vengono mosse nel piano. Usualmente le misure che si utilizzano negli spazi euclidei si basano tutte sul fatto che la misura di un rettangolo è data dalla base per l'altezza. Poiché ogni spostamento di un rettangolo non altera la sua base e la sua altezza è evidente che tale misure sono tutte invarianti rispetto alle isometrie.

Esempi. Se si pone μ costantemente uguale a zero si ottiene una misura λ-additiva invariante rispetto alle isometrie. Un'altra misura invariante λ-additiva si ottiene ponendo $\mu(X) = \infty$ per ogni $X \neq \varnothing$. Chiamiamo *banali* queste due misure che, ovviamente, sono prive di interesse.

Ricordiamo la seguente ovvia proposizione che è stata già utilizzata nel primo volume.

Proposizione 5.4. Consideriamo una misura finitamente additiva nello spazio euclideo che sia invariante rispetto alle isometrie. Allora due figure geometriche A e B equiscomponibili in pezzi che sono misurabili hanno la stessa misura.

Tale proposizione può essere utilizzata per mostrare l'esistenza di insiemi dello spazio euclideo che non sono misurabili.

Teorema 5.5. (*Paradosso di Vitali*). Se si accetta l'assioma della scelta allora un cubo si può spezzare in una successione di sottoinsiemi disgiunti tutti equiscomponibili tra loro.

Dim. Cominciamo con il dimostrare che l'intervallo [0,1) si può scomporre in una successione di insiemi $(C_k)_{k\in N}$ equiscomponibili tra loro. Per fare questo, definiamo in [0,1) la relazione $\equiv$ ponendo $x \equiv y$ se x-y è un numero razionale[7]. E' facile verificare che $\equiv$ è

[7] Supponiamo di avere dimostrato che π sia irrazionale e poniamoci il problema di trovare altri esempi di numeri irrazionali. Esiste un modo banale per fare questo: basta aggiungere a π un qualunque numero ra-

una relazione di equivalenza e che quindi ripartisce [0,1) in classi di equivalenza. In base all'assioma della scelta possiamo prendere in ogni classe un elemento rappresentativo. Indichiamo con T l'insieme degli elementi ottenuti in questo modo. Allora ogni classe di equivalenza è costituita da un elemento r di T a cui sono aggiunti tutti i possibili razionali (purché si rimanga in [0,1)). In altre parole

$$[0,1) = \cup_{r\in T} [r] = \{r+q : r\in T,\ q\in Q,\ r+q \in [0,1)\}$$
$$= \cup_{q\in Q} (T+q)\cap[0,1)$$

dove gli insiemi $T+q$ sono tutti disgiunti tra loro. Infatti supponiamo che $(T+q)\cap(T+q') \neq \varnothing$ con $q \neq q'$ e supponiamo che z sia un elemento di tale intersezione. Allora esisterebbero t, $t'\in T$ tali che $z = t+q = t'+q'$ e quindi tali $t-t' = q'-q$. Ciò comporterebbe l'equivalenza tra t e t' e quindi che $t = t'$. Ciò è in contrasto con il fatto che $q \neq q'$.

Osserviamo anche che nella maggior parte dei casi gli insiemi $(T+q)\cap[0,1)$ sono vuoti, ad esempio nei casi in cui $q>1$ oppure $q<-1$. Pertanto nell'unione $\cup_{q\in Q}(T+q)\cap[0,1)$ è inutile considerare tutti i possibili razionali ma ci si può limitare a quelli dell'intervallo [-1,1]. Detta $(q_k)_{k\in N}$ una enumerazione di tutti i razionali in [0,1] è evidente che $(1-q_k)_{k\in N}$ è una numerazione di tutti i razionali in [-1,0]. Pertanto, se poniamo

$A_k = (T+q_k)\cap[0,1)$
$B_k = (T+q_k-1)\cap[0,1)$
$C_k = A_k\cup B_k$

possiamo scrivere

$$[0,1) = (\cup_{k\in N} (T+q_k)\cap[0,1))\cup(\cup_{k\in N} (T+q_k-1)\cap[0,1))$$
$$= \cup_{k\in N} ((T+q_k)\cap[0,1))\cup(T+q_k-1)\cap[0,1)) = \cup_{k\in N} A_k\cup B_k$$
$$= \cup_{k\in N} C_k .$$

D'altra parte se trasliamo il pezzo $A_k' = \{x \in T : x<1-q_k\}$ di T tramite la traslazione di ampiezza q_k otteniamo A_k. Se trasliamo il pezzo rimanente $B_k' = \{x \in T : x\geq 1-q_k\}$ tramite la traslazione di ampiezza q_k-1 otteniamo B_k. Questo prova che ciascun insieme C_k

---

zionale q. Infatti, posto $c = \pi+q$ se c fosse un razionale, allora $\pi = c-q$ sarebbe razionale. Naturalmente un tale esempio non è molto significativi e noi lo percepiamo come "equivalente" a π. La relazione $\equiv$ di cui si serve la dimostrazione è adeguata a rappresentare tale idea di equivalenza.

$= A_k \cup B_k$ è equiscomponibile con $T = A_k' \cup B_k'$ e che quindi tutti questi insiemi sono equiscomponibili tra loro.

Possiamo ora procedere alla dimostrazione del teorema riferendoci al cubo $[0,1)^3$ ed osservando che

$$[0,1)^3 = [0,1)\times[0,1)\times[0,1)$$
$$= (\cup_{k\in N} C_k)\times(\cup_{k\in N} C_k)\times(\cup_{k\in N} C_k)$$
$$= \cup_{h,k,r\in N}(C_h \times C_k \times C_r).$$

E' evidente allora che tutti gli insiemi $C_h \times C_k \times C_r$ sono equi-scomponibili a $T\times T\times T$ e quindi equi-scomponibili tra loro. In conclusione, la classe di tali insiemi costituisce la scomposizione cercata. □

Ho usato il termine "paradosso" poiché da tale teorema sembra seguire che un cubo, essendo scomponibile in una successione di infiniti pezzi tutti della stessa misura $\underline{m}$, debba avere una misura infinita se $\underline{m} \neq 0$ oppure nulla nel caso $\underline{m} = 0$. In realtà un modo di "uscire" da tale paradosso è accettare la possibilità che esistano insiemi che non ammettono misura. Allora dal teorema di Vitali segue che in uno spazio euclideo è impossibile definire una misura numerabilmente additiva che sia invariante rispetto ai movimenti e che sia capace di misurare tutti gli insiemi.

Corollario 5.6. Se si accetta l'assioma della scelta è possibile provare che non esiste una misura numerabilmente additiva μ nello spazio euclideo R^3 tale che:

- μ sia invariante rispetto alle isometrie,
- μ sia definita in tutti i sottoinsiemi di R^3.

Dim. Sia S un cubo e $(D_k)_{k\in N}$ una decomposizione di S tramite sottoinsiemi equiscomponibili. Se per assurdo esistesse una tale misura μ allora, $\mu(S) = \mu(\cup_{k\in N} D_k) = \sum_{k\in N} \mu(D_k)$. Posto $\mu(D_k) = \underline{m}$ per ogni indice k, avremmo che se fosse $\underline{m} = 0$ allora $\mu(S) = 0$ e quindi S avrebbe misura nulla. Se invece fosse $\underline{m} \neq 0$ si avrebbe che $\mu(S) = \infty$. □

6. Il paradosso di Banach-Tarski

Abbiamo già parlato del paradosso di Banach-Tarski nel primo volume quando abbiamo trattato la nozione di equiscomponibilità. Ricordiamo che in tale paradosso si prova che:

"Se si accetta l'assioma della scelta é possibile suddividere una sfera in un numero finito di parti e poi ricomporre tali parti per formare due sfere identiche alla prima".

Equivalentemente possiamo riformulare il paradosso riferendoci a cubi invece che a sfere.

Teorema 6.1. (Banach-Tarski). Assumiamo l'assioma della scelta, ed indichiamo con S un cubo unitario dello spazio euclideo a tre dimensioni. Allora S è equi-scomponibile a due copie di se stesso, cioè esistono due cubi unitari disgiunti S' e S'' tali che $S \sim S' \cup S''$.

Non proveremo tale sorprendente teorema ma ci limitiamo a mettere in evidenza che da esso consegue un altro interessante teorema sulle misure finitamente additive nello spazio euclideo.

Corollario 6.2. Non esiste una misura finitamente additiva (e quindi neanche numerabilmente additiva) nello spazio euclideo tridimensionale tale che

- sia invariante rispetto alle isometrie,
- sia definita su tutti i sottoinsiemi dello spazio.

Dim. Infatti se tale misura esistesse, il cubo unitario S avrebbe misura uguale a quella di $S' \cup S''$ e quindi misura uguale a due volte la propria misura. □

Il teorema di Banach-Tarski urta fortemente contro la nostra intuizione. Infatti siamo portati a considerare i sottoinsiemi dello spazio euclideo come "corpi" e quindi il vedere che un corpo S possa essere spezzato in parti che ricomposte opportunamente formano due corpi uguali ad S sembra alquanto strano. Si potrebbe anche dire che tale teorema è in contrasto con il principio della conservazione della massa. Infatti durante il movimento le masse dei pezzi in cui è stato decomposto S dovrebbero conservarsi invece il teorema prova che si raddoppiano.

Un possibile atteggiamento nei confronti del paradosso di Banach-Tarski è quello di accettare come assioma l'esistenza di una misura invariante ed ovunque definita e quindi di reinterpretare il paradosso come una dimostrazione per assurdo che l'assioma della scelta non vale.

7. Nuovi numeri: i numeri cardinali

Come affermato dallo stesso Cantor, la nozione di numero cardinale nasce come:

> *"concetto generale che, con l'aiuto della nostra intelligenza, risulta da un insieme M quando noi facciamo astrazione dalla natura dei suoi elementi e dall'ordine con cui sono dati"*

Ora "fare astrazione" significa considerare uguali cose che differiscono per aspetti che a noi non interessano. Il modo con cui spesso in matematica si rappresenta un tale processo è quello di introdurre un equivalenza e poi passare al quoziente. Un tipico esempio si presenta quando si passa dall'anello degli interi Z agli interi modulo un intero m. Questo passaggio è giustificato dal fatto che esistono situazioni in cui due numeri che differiscono per un multiplo di m sono da considerare uguali. Questo avviene ad esempio nei movimenti lungo un poligono convesso oppure per decidere qualcosa con il "tocco" tra $m+1$ persone. Pertanto appare ragionevole utilizzare la nozione di equipotenza nella classe di tutti gli insiemi e chiamare "numero cardinale" una classe completa di equivalenza. Tuttavia, come abbiamo mostrato, non è possibile riferirsi alla classe di tutti gli insiemi perché tale classe conduce ad una contraddizione. Allora ci riferiamo ad una classe C più piccola che contenga solo tutti gli insiemi che si utilizzano usualmente in matematica. Pertanto mettiamo in C gli insiemi $\varnothing$, N_0, Z, Q, R, ..., e supponiamo anche che C sia chiusa rispetto alle principali operazioni insiemistiche utilizzate dai matematici, ad esempio:

- al prendere un sottoinsieme di un insieme in C
- all'unione,
- all'intersezione,
- al prodotto cartesiano
- all'operatore "insieme delle parti" che associa ad ogni insieme X in C l'insieme delle sua parti $\mathcal{P}(X)$
- alla operazione di X^Y di elevazione a potenza

Ad esempio in C metteremo anche $R\times R$, $\mathcal{P}(Q)$, ... Fatto questo, in C consideriamo la relazione di preordine $\leq$ "avere potenza minore o uguale a". Dalla teoria generale delle relazioni di preordine sappiamo

1. che $\leq$ induce una relazione di equivalenza $\equiv$

2. che ≤ induce una relazione d'ordine nel quoziente $C/\equiv$.

Ovviamente, per il teorema di Cantor-Bernstein ≡ coincide con l'equipotenza.

Definizione 7.1. Chiamiamo *insieme ordinato dei numeri cardinali* l'insieme ordinato $(C/\equiv, \leq)$ e chiamiamo *numero cardinale* ogni elemento di $C/\equiv$, cioè ogni classe completa di equivalenza. Inoltre poniamo

$$[X] \leq [Y] \Leftrightarrow X \leq Y.$$

Ad esempio, l'insieme N dei numeri naturali non nulli determina un cardinale $[N]$ che viene detto *la potenza del numerabile* ed indicato con $\aleph_0$. L'insieme R dei numeri reali definisce un altro cardinale $[R]$ che viene detto *la potenza del continuo*. I cardinali finiti sono le classi di equivalenza individuate da un insieme finito. Infatti avremo il numero cardinale $[\{a\}]$, il numero cardinale $[\{a, b\}]$, il cardinale $[\{a,b,c\}]$, ... Naturalmente il cardinale più piccolo che possiamo trovare è $[\varnothing] = \{\varnothing\}$.[8]

8. Algebra dei cardinali

Un ulteriore passo è quello di introdurre opportune operazioni in $C/\equiv$. Per fare questo procediamo al modo seguente. Definiamo prima in C una opportuna struttura algebrica $(C, \times, +, \varnothing, \{e\})$, poi passiamo a quoziente modulo l'equipotenza ≡. Per fare questo ovviamente le operazioni × e + devono essere compatibili con ≡. Naturalmente vogliamo dare una definizione insiemistica a tali operazioni e vogliamo ottenere che siano una estensione delle usuali operazioni tra numeri naturali.

La moltiplicazione. La prima operazione è la moltiplicazione di cardinali che viene suggerita dall'osservazione per cui il prodotto cartesiano di due insiemi finiti con n ed m elementi, rispettivamente, ha $n \cdot m$ elementi. A tale proposito possiamo osservare che il prodotto cartesiano è una operazione in C e che l'equipotenza è una relazione di congruenza rispetto a tale operazione.

[8] Un insieme può essere equipotente a ∅ solo se coincide con ∅. Infatti una funzione f di ∅ in un insieme S è un sottoinsieme di $\varnothing \times S = \varnothing$ e quindi è la funzione vuota. Se f è suriettiva Pertanto la classe $[\varnothing]$ degli insiemi equipotenti a ∅ si riduce al singoletto $\{\varnothing\}$.

Proposizione 8.1. Il prodotto cartesiano è una operazione in C compatibile con $\equiv$, cioè

$$X' \equiv X,\ Y' \equiv Y \Rightarrow (X \times Y \equiv X' \times Y').$$

Esercizio. Provare che se X ha un numero finito n di elementi ed Y ha un numero finito m di elementi, allora $X \times Y$ ha $n \cdot m$ elementi. Si suggerisce di procedere per induzione su m.

L'addizione. La definizione di addizione di due cardinali è leggermente più complicata. La via che sembra più naturale sembrerebbe quella di ricavare tale operazione dall'unione insiemistica. Infatti siamo abituati a pensare che il sommare sia la stessa cosa di unire. Purtroppo quando gli insiemi hanno intersezione non vuota le cose si complicano in quanto tale operazione non risulta compatibile con $\equiv$. Ad esempio se si pone

$$X = \{a,b,c\},\ Y = \{1,2\},\ X' = \{d,e,f\},\ Y' = \{d,\mathrm{e}\}$$

allora risulta che $X' \equiv X$, $Y' \equiv Y$ ma $X \cup Y = \{a,b,c,1,2\}$ non è equipotente a $X' \cup Y' = \{d,e,f\}$. Per risolvere un tale problema invece di effettuare l'unione di due insiemi effettuiamo l'unione di due copie di tali insiemi che siano sicuramente disgiunte. Ad esempio possiamo considerare invece che gli insiemi X ed Y gli insiemi equipotenti $X \times \{0\} = \{(x,0) : x \in X\}$ e $Y \times \{1\} = \{(y,1) : y \in Y\}$.

Definizione 8.2. Chiamiamo *unione disgiunta* di due insiemi X ed Y l'insieme

$$X \underline{\cup} Y = (X \times \{0\}) \cup (Y \times \{1\}).$$

Per capire tale definizione è come se avessimo messo una etichetta 0 agli elementi di X ed una etichetta diversa 1 agli elementi di Y. Allora anche se tali insiemi dovessero avere elementi comune, dopo questo etichettamento si ottengono due loro copie completamente disgiunte. È immediato dimostrare la seguente proposizione.

Proposizione 8.3. L'operazione $\underline{\cup}$ è compatibile con $\equiv$.

In definitiva, detto $\{e\}$ un qualunque singoletto, allora abbiamo definito una struttura algebrica $(C, \times, \underline{\cup}, \varnothing, \{e\})$ ed abbiamo provato che $\equiv$ è una congruenza in tale struttura. Se si tiene conto

del fatto che ≡ è compatibile con la relazione ≤ di "avere potenza minore o uguale" è possibile dare la seguente definizione.

Definizione 8.4. Chiamiamo *algebra dei numeri cardinali* la struttura algebrica $(C/\equiv, +, \times, \leq, 0,1)$ che si ottiene come quoziente della struttura $(C, \underline{\cup}, \times, \leq, \varnothing, \{e\})$ modulo la relazione di equipotenza.

Evidenziamo esplicitamente che $0 = [\varnothing]$, $1 = [\{e\}]$, e le operazioni sono definite ponendo $[X]+[Y] = [X \underline{\cup} Y]$, $[X]\times[Y] = [X\times Y]$.

Proposizione 8.5. L'operazione di addizione di cardinali è commutativa ed associativa e vale l'equazione $x+0 = x$, cioè 0 è elemento neutro rispetto a +. La moltiplicazione di cardinali è commutativa ed associativa. Vale l'equazione $x\times 1 = x$ e quindi 1 è l'elemento neutro. Inoltre $x\times 0 = 0$.

Dim. Ad esempio, per provare l'equazione $x\times 1 = 1$, detto X un insieme tale che $x = [X]$, osserviamo che $[X]\times[\{e\}] = [X\times\{e\}] = [X]$ in quanto $X\times\{e\}$ è equipotente ad X. Per provare che $x\times 0 = 0$ osserviamo che $[X]\times[\varnothing] = [X\times\varnothing] = [\varnothing]$. □

La seguente proposizione, di cui omettiamo la dimostrazione, mostra che l'algebra dei numeri cardinali estende l'usuale aritmetica dei numeri interi positivi.

Proposizione 8.6. Sia F la classe dei cardinali finiti e definiamo la funzione $s : F \to F$ ponendo $s([X]) = [X]+1$. Allora $(F, s, [\varnothing])$ è una terna di Peano. Se in tale terna si definiscono, per ricorsione, le operazioni di somma e prodotto come fatto nel terzo capitolo del primo volume, allora si ottiene un sottostruttura dell'algebra $(C/\equiv, \times, +, \leq, 0, 1)$ dei cardinali che è isomorfa all'algebra dei naturali.

Per le operazioni tra cardinali valgono proprietà che si discostano da quelle dell'aritmetica usuale. Ad esempio se $\aleph_0 = [N]$ denota il cardinale del numerabile, allora risulta che:
- $\aleph_0+\aleph_0 = \aleph_0$ (in quanto l'unione di due insiemi numerabili è ancora un insieme numerabile)

- $\aleph_0 \times \aleph_0 = \aleph_0$ (in quanto il prodotto cartesiano di due insiemi numerabili è un insieme numerabile)
- $\aleph_0 + n = \aleph_0$ (poiché l'unione di un insieme infinito con un insieme finito non altera la cardinalità)

Nella classe dei cardinali è possibile introdurre anche l'operazione di elevazione a potenza. Ricordiamo che, dati due insiemi X ed Y, la potenza X^Y si definisce come l'insieme di tutte le funzioni di Y in X. Questa operazione è una estensione del prodotto cartesiano poiché Y è l' insieme finito $\{1,2,\ldots,n\}$ allora X^Y coincide con il prodotto cartesiano di X per se stesso n volte, cioè con l'insieme delle n-ple di elementi di X. Possiamo allora aggiungere alla struttura $(C, \underline{\cup}, \times, \varnothing, \{e\})$ questa nuova operazione. Non è difficile verificare che l'elevazione a potenza è compatibile con la relazione di equipotenza e che quindi induce nel quoziente una nuova operazione che continuiamo a chiamare *elevazione a potenza*.

Definizione 8.7. Dati due cardinali $[X]$ ed $[Y]$ la potenza $[X]^{[Y]}$ è definita ponendo

$$[X]^{[Y]} = [X^Y].$$

Si noti che se X ed Y sono finiti di cardinalità n ed m allora in X^Y ci sono n^m elementi. Pertanto l'operazione di elevazione a potenza per cardinali estende quella già nota per i cardinali finiti. Se si utilizza la notazione esponenziale allora la cardinalità $\mathcal{P}(S)$ può essere indicata con $2^{[S]}$. In particolare la potenza del continuo può essere indicata con 2^{ω}. Questo tipo di notazione permette di esprimere molti fatti della teoria degli insiemi in modo elegante e compatto. Facciamo alcuni esempi.

Teorema di Cantor. Per ogni cardinale x, $x < 2^x$.

Ipotesi del continuo. Non esiste x tale che $\omega < x < 2^{\omega}$.

Ipotesi del continuo generalizzata. Per ogni z non esiste x tale che $z < x < 2^z$.

9. La nozione di buon ordine

I numeri naturali possono essere utilizzati in due modi diversi. Il primo è quello di misurare la quantità di elementi di un insieme,

il secondo è quello di stabilire una posizione (un turno, una graduatoria …) all'interno di un insieme ordinato. Ad esempio il numero 5 può rappresentare il numero di caramelle che sono su di un tavolo oppure può rappresentare la posizione in una fila di attesa di un certo insieme di persone. Per rendersi conto della differenza basta pensare che nel caso di liste di attesa si potrebbero benissimo utilizzare le lettere dell'alfabeto *a*, *b*, ... nell'ordine usuale e quindi utilizzare la lettera *e* per indicare la posizione 5.

La nozione di numero cardinale che abbiamo introdotto corrisponde all'esigenza di rappresentare la quantità di elementi di un insieme. Si presenta allora il problema di come si possa definire una nozione analoga di numero quando si voglia indicare una posizione all'interno di un ordinamento. D'altra parte non è possibile riferirsi a tutti i tipi di ordinamento e quindi ci si concentra su quegli ordinamenti in cui in ogni insieme non vuoto sia possibile indicare quale è il primo elemento (se ci riferiamo ad un gruppo di persone, stabilire "a chi tocca").

Definizione 9.1. Una relazione di ordine $(S, \leq)$ è detta di *buon ordine* se ogni sottoinsieme non vuoto di S ammette minimo.

Inutile dire che non bisogna confondere "ammettere minimo" con "ammettere estremo inferiore". Ad esempio se consideriamo l'insieme R_+ dei reali positivi con l'ordine usuale $\leq$, ogni sottoinsieme non vuoto ammette estremo inferiore rispetto $\leq$. Tuttavia $(R_+, \leq)$ non è un buon ordine. Ecco invece alcuni esempi di buon ordine.

Esempio 1. Se si considerano le lettere $\{a, b, c, d\}$ con l'usuale ordinamento delle lettere dell'alfabeto abbiamo un esempio di insieme finito con un buon ordinamento.

Esempio 2. Dato un numero naturale n, l'insieme $\{0, 1, \ldots, n\}$ con l'usuale ordinamento è esempio di insieme finito con un buon ordinamento.

Esempio 3. L'insieme delle parole che vedono tradotte in un dizionario è ben ordinato.

Un esempio di buon ordinamento di un insieme infinito è dato da una terna di Peano (o se si vuole dall'insieme dei numeri naturali).

Teorema 9.2. Data una terna di Peano (S, s, z_0) e la relativa relazione d'ordine $\leq$, la struttura $(S, \leq)$ è un buon ordinamento.

Dim. Supponiamo che (S, s, z_0) sia una terna di Peano e quindi che valga il principio di induzione. Sappiamo allora che è possibile definire una relazione d'ordine $\leq$ in S. Per provare che $(S, \leq)$ è un buon ordinamento supponiamo per assurdo che A sia un sottoinsieme di S che non ha un elemento minimo. Affermiamo che $S\text{-}A = S$ e quindi che A è vuoto. Infatti osserviamo che $z_0 \in S\text{-}A$ in quanto altrimenti A avrebbe minimo. Supponiamo che $n \in S\text{-}A$, allora il suo successore $s(n)$ non potrebbe appartenere ad A in quanto A non ha minimo.

Esistono anche buon ordinamenti in insiemi infiniti che sono diversi da quello dei numeri naturali.

Esempio 3. Indichiamo con N_∞ l'insieme dei numeri naturali a cui sia stato aggiunto il simbolo $+\infty$ ed estendiamo l'ordinamento usuale ponendo $n \leq +\infty$ per ogni $n \in N_\infty$. Allora $(N_\infty, \leq)$ è un buon ordine. Infatti, dato un sottoinsieme non vuoto X di N_∞, se $X = \{+\infty\}$ è evidente che $+\infty$ è il minimo di X. Se invece $X \neq \{+\infty\}$ allora $X\text{-}\{\infty\} \neq \varnothing$. Pertanto, essendo $X\text{-}\{\infty\}$ un sottoinsieme non vuoto di N, ammette elemento minimo. Tale elemento è anche il minimo di X.

Problema. Provare che una struttura del tipo $(\mathcal{P}(S), \subseteq)$ non è di buon ordine.

Proposizione 9.2. Ogni insieme con un buon ordine è dotato di minimo ed è totalmente ordinato.

Dim. Se come sottoinsieme di S consideriamo S stesso, otteniamo che esiste il minimo di S. Dati inoltre due elementi x, y di S poiché $\{x,y\}$ deve ammettere il minimo, se tale minimo è x allora $x \leq y$, se tale minimo è y allora $y \leq x$. □

Di solito indichiamo con 0 il minimo di un insieme ben ordinato.

Problema. Provare che l' ordinamento usuale nell'anello Z degli interi non è un buon ordinamento.

Problema. Provare che l'ordinamento usuale nell'insieme Q_+ dei razionali positivi non è un buon ordinamento.

La seguente proposizione è utile per trovare esempi di buon ordinamento. Essa mostra, in particolare, che un sottoinsieme di un insieme ben ordinato è ancora ben ordinato (rispetto l'ordine indotto).

Proposizione 9.3. Sia $(S, \leq)$ un buon ordinamento e sia $(S',\leq')$ una relazione binaria che si può immergere in $(S,\leq)$. Allora $(S', \leq')$ è un buon ordinamento. In particolare, ogni sottoinsieme di un insieme ben ordinato è un insieme ben ordinato.

Dim. Sia $f : S' \to S$ una immersione e consideriamo un sottoinsieme non vuoto X' di S'. Allora $f(X')$ è un sottoinsieme non vuoto di S e quindi ammette un minimo m. Detto $m' \in X'$ tale che $f(m') = m$, risulta che m' è il minimo di X'. Infatti se $x' \in X'$, allora essendo $f(m') = m \leq f(x')$, ed essendo f una immersione, siamo sicuri che $m' \leq x'$.

Infine osserviamo se X è un sottoinsieme di un insieme ben ordinato $(S,\leq)$ allora l'applicazione identica è una immersione di $(X,\leq)$ in $(S,\leq)$. □

Ne segue in particolare che segmenti iniziali del tipo $\{0,\ldots,n\}$ sono ben ordinati rispetto l'ordine naturale.

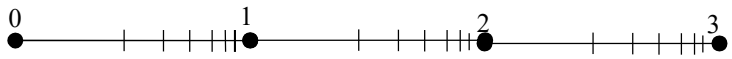
Corollario 9.4. Se una struttura d'ordine $(S, \leq)$ è isomorfa ad un insieme con un buon ordine allora tale struttura è un buon ordinamento.[9]

[9] Tale asserzione è un caso particolare del fatto che se due strutture sono isomorfe allora verificano le stesse proprietà. Ne segue che se una struttura è un modello di un dato sistema di assiomi anche la seconda è un modello dello stesso sistema di assiomi. Una tale proprietà per due strutture in logica matematica viene espressa dall'asserzione "se due strutture sono isomorfe allora sono logicamente equivalenti". Ad esempio se

Esempio 4. Consideriamo l'insieme

$$S = \{1\text{-}1/n : n\in N\}\cup\{2\text{-}1/n : n\in N\}\cup\{3\text{-}1/n : n\in N\}\}$$

di numeri reali rispetto l'ordine usuale ≤. Possiamo visualizzare sull'asse delle ascisse tale insieme come l'unione dei punti di tre successioni che si accumulano a sinistra su 1, 2 e 3, rispettivamente.



Vogliamo provare che $(S,\leq)$ è un buon ordine. E' evidente che ciascun dei tre ordini

$$(\{1\text{-}1/n : n\in N\}, \leq),\ (\{2\text{-}1/n : n\in N\}, \leq),\ (\{3\text{-}1/n : n\in N\}, \leq\}$$

è un buon ordine. Infatti tali strutture risultano essere isomorfi a $(N, \leq)$ tramite le funzioni $f(n) = 1\text{-}1/n$, $g(n) = 2\text{-}1/n$, $h(n) = 3\text{-}1/n$, rispettivamente. Sia ora X un sottoinsieme non vuoto di S, allora:
- se $X\cap(\{1\text{-}1/n : n\in N\}, \leq) \neq \emptyset$, allora il minimo di $X\cap(\{1\text{-}1/n : n\in N\}$ è anche il minimo di X
- se $X\cap(\{1\text{-}1/n : n\in N\}, \leq) = \emptyset$, e $X\cap(\{2\text{-}1/n : n\in N\}, \leq) \neq \emptyset$, allora il minimo di $X\cap(\{2\text{-}1/n : n\in N\}, \leq)$ è anche il minimo di X
- se $X\cap(\{1\text{-}1/n : n\in N\}, \leq) = \emptyset$ e $X\cap(\{2\text{-}1/n : n\in N\}, \leq) = \emptyset$ allora necessariamente $X\cap(\{3\text{-}1/n : n\in N\}, \leq) \neq \emptyset$. Allora il minimo di $X\cap(\{3\text{-}1/n : n\in N\}, \leq)$ è anche il minimo di X. Quindi X ammette minimo in S.

10. Alcune somiglianze con le terne di Peano

Abbiamo visto che l'ordinamento naturale in una terna di Peano è un buon ordinamento. D'altra parte gli insiemi ben ordinati hanno molti tratti comuni con tali terne. Ad esempio è possibile definire la nozione di successivo.

Definizione 10.1. Dato un insieme ben ordinato $(S,\leq)$ chiamiamo *successivo* di un elemento x il minimo tra gli elementi strettamente maggiori di x. Indichiamo con $s(x)$ tale successivo. Un elemento, diverso dal minimo 0 che non è successivo di nessun elemento viene chiamato *elemento limite*.

---

una struttura algebrica è isomorfa ad un gruppo G allora è un gruppo, se G è commutativo allora tale struttura è un gruppo commutativo.

Ovviamente se x ammette il successivo $s(x)$, allora non esiste z per cui $x<z<s(x)$. Riferendoci agli esempi fatti,

- negli esempi 1 e 2 non esistono elementi limite
- nell'esempio 2 il simbolo ∞ è un elemento limite
- nell'esempio 4 i numeri 1, 2 sono elementi limite.

Proposizione 10.2. Data una relazione di buon ordine $(S,\leq)$, ogni elemento x in S che non sia il massimo ammette un *successivo.*

Dim. Sia $x\in S$ e supponiamo che x non sia il massimo. Allora l'insieme $\{z\in S : x<z\}$ è non vuoto e quindi esiste il minimo di tale insieme. Indichiamo con $s(x)$ tale minimo, allora è evidente che tra x ed $s(x)$ non possono esserci elementi. □

Una ulteriore somiglianza tra insiemi ben ordinati e terne di Peano è che anche in entrambi vale la seguente forma del principio di induzione.

Teorema 10.3. (Principio di induzione transfinita). Consideriamo un insieme ben ordinato $(S,\leq)$ ed una proprietà P definita in S. Allora se è verificata l'implicazione

a) $P(x)$ per ogni $x<y \Rightarrow P$ vale per y

possiamo concludere che

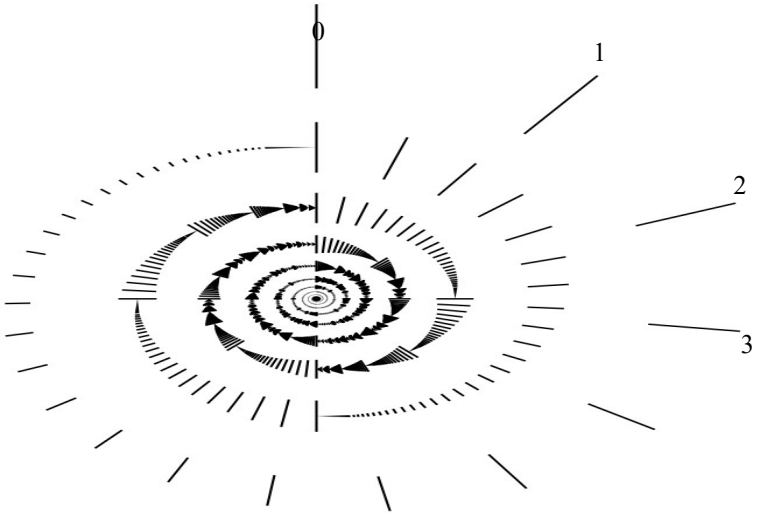
b) $P(x)$ per ogni $x\in S$.

Dim. Si ripete esattamente la stessa dimostrazione che abbiamo fatto nel primo volume nell'ambito delle terne di Peano. Assumiamo *a*), allora provare *b*) equivale a provare che l'insieme $X_P = \{x\in S : P \text{ è falsa in } x\}$ sia vuoto. Supponiamo per assurdo che non lo sia, allora esiste un minimo m per tale insieme. Per definizione di minimo ciò significa che $m\in X_P$ e $x\notin X_P$ per ogni $x < m$. Ciò comporterebbe che $P(x)$ è falsa in m e vera per ogni $x<m$. Ciò è in contrasto con *a*). □

Osserviamo esplicitamente che se si accetta *a*) allora, poiché la premessa "$P(x)$ per ogni $x<0$" è vera, P vale per 0.

Concludiamo il paragrafo con la seguente immagine, presa da Wikipedia, che rappresenta un ordinale con infiniti elementi limi-

te. Si lascia al lettore il compito di interpretare la figura e di individuare gli elementi limite.



Teorema 10.4. Sia $(S, \leq)$ un insieme ben ordinato, z_0 il suo minimo elemento ed s la relativa funzione successore. Allora la struttura (S, s, z_0) è una terna di Peano se e solo se non esiste un elemento infinito.

Dim. E' evidente che in una terna di Peano non può esistere un elemento infinito. Supponiamo che $(S, \leq)$ sia un buon ordinamento privo di elementi infiniti e che A sia sottoinsieme di S contenente z_0 e tale che se contiene $x \in A$ allora $s(x) \in A$. Allora se A fosse diverso da S l'insieme S-A sarebbe non vuoto e quindi ammetterebbe minimo m. Tale minimo è un infinito in quanto se esistess x tale che $s(x) = m$ avremmo che x non può appartenere ad S-A e quindi $x \in A$. Tuttavia questo comporterebb, per ipotesi, che $m \in A$. In conclusione in $(S, \leq)$ non può esserci un infinito. □

11. Nuovi numeri: i numeri ordinali

Per definire una teoria generale dei numeri ordinali, partiamo ancora dalla classe C che ci ha permesso di costruire i numeri cardinali ed indichiamo con O la classe delle strutture $(S, \leq, z)$ tali che:

- $S \in C$
- $\leq$ è un buon ordine in S
- z è il minimo elemento.

Inoltre indichiamo con $\equiv$ la relazione "essere isomorfi" nella classe O.

Definizione 11.1. Date due strutture $(S_1, \leq_1, z_1)$ e $(S_2, \leq_2, z_2)$ in O prende il nome di *omomorfismo* una funzione $f : S_1 \to S_2$ tale che $f(z_1) = z_2$ e

$$x \leq_1 y \Rightarrow f(x) \leq_2 f(y)).$$

Diciamo che f è un *isomorfismo* se è un omomorfismo invertibile ed il suo inverso è ancora un omomorfismo.

Equivalentemente, possiamo dire che f è un isomorfismo se f è una funzione suriettiva tale che $f(z_1) = z_2$ e

$$x \leq_1 y \Leftrightarrow f(x) \leq_2 f(y)).$$

Ad esempio, consideriamo $(N_0, \leq, 0)$ e $(\{-3, -2, -1\} \cup N_0, \leq, -3)$ dove $\leq$ è l'usuale ordinamento. Allora tali strutture sono isomorfe in quanto la funzione $h : N_0 \to \{-3, -2, -1\} \cup N_0$ definita ponendo $h(n) = n-3$ è un isomorfismo. Infatti h è una funzione suriettiva tale che $h(0) = -3$ e $h(n) \leq h(m)$ se e solo se $n \leq m$. Tale isomorfismo può essere visualizzato dalla seguente tabella

$$\begin{array}{ccccccccccc} 0 & < & 1 & < & 2 & < & 3 & < & 4 & < & \ldots. \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ -3 & < & -2 & < & -1 & < & 0 & < & 1 & < & 2 < \ldots \end{array}$$

Definizione 11.2. Chiamiamo *numero ordinale* ogni elemento di $O/\equiv$, cioè ogni classe completa di equivalenza.

Allora, ad esempio, l'insieme ordinato $(N,\leq)$ dei numeri naturali determina un ordinale $[(N, \leq)]$ che viene denotato con ω. Stante l'isomorfismo considerato nell'esempio precedente, abbiamo che lo stesso ordinale viene definito da $(\{-3, -2, -1\} \cup N, \leq)$ e quindi $[(N, \leq)] = [(\{-3, -2, -1\} \cup N, \leq)]$. Se considero un singoletto $\{a\}$ costituito da un solo elemento a allora l'unica relazione d'ordine in $\{a\}$ è quella cosituita dall'insieme $\{(a,a)\}$. Tale relazione è di buon ordine e posso indicare con **1** l'ordinale corrispondente $[\{a\},\{(a,a)\}]$. Ovviamente se considero il singoletto $\{b\}$ definisco lo stesso ordinale. Se considero un insieme con due elementi $\{a,b\}$ in tale insieme posso definire un buon ordinamento $\{(a,a)$,

(b,b), $(a,b)\}$. Posso indicare con **2** il numero ordinale corrispondente $[\{a,b\}, \{(a,a), (b,b), (a,b)\}]$. Con un po' di acrobazie logiche possiamo anche definire un ordinale a partire dall'insieme vuoto. Infatti se considero l'insieme vuoto $\varnothing$, e la relazione vuota $\varnothing\subseteq\varnothing\times\varnothing$, allora la coppia $(\varnothing,\varnothing)$ è una struttura ben ordinata. Infatti è vero ogni sottoinsieme non vuoto di $\varnothing$ ammette minimo (non essendoci sottoinsiemi non vuoti). Indichiamo con **0** l'ordinale $[(\varnothing,\varnothing)]$ corrispondente.

12. Algebra degli ordinali

Come abbiamo fatto per i numeri cardinali, possiamo definire in $O/\equiv$ una struttura algebrica ottenuta definendo prima in O una opportuna struttura algebrica e poi passando al quoziente modulo $\equiv$. Per fare questo ovviamente le operazioni $\times$ e $+$ devono essere compatibili con $\equiv$.

Per poter definire il prodotto di due insiemi ordinati $(S_1,\leq_1)$ e $(S_2,\leq_2)$ dobbiamo individuare un ordinamento $\leq$ in $S_1\times S_2$ in modo che se $(S_1,\leq_1)$ e $(S_2,\leq_2)$ sono ben ordinati allora anche $(S_1\times S_2,\leq)$ sia ben ordinato. Se ad esempio avessimo gli insiemi ben ordinati $\{0,1,2,3\}$ e $\{a,b,c\}$, allora dovremmo individuare un buon ordinamento nell'insieme di coppie,

$(0,a)$ $(0,b)$ $(0,c)$
$(1,a)$ $(1,b)$ $(1,c)$
$(2,a)$ $(2,b)$ $(2,c)$
$(3,a)$ $(3,b)$ $(3,c)$

(che abbiamo rappresentato in forma di matrice). In tale caso un ordinamento è quello che si ottiene leggendo la matrice da sinistra a destra e poi dall'alto al basso (come avviene usualmente la lettura di un testo). Avremmo cioè

$(0,a) < (0,b) < (0,c) < (1,a) < (1,b) < (1,c) < (2,a) < (2,b) < (2,c) < (3,a) < (3,b) < (3,c)$.

Se volessimo moltiplicare $(N,\leq)$ per se stesso allora potremmo disporre $N\times N$ in una matrice infinita

$(0,0)$ $(0,1)$ $(0,2)$ . . .
$(0,1)$ $(1,1)$ $(1,2)$ . . .
$(0,2)$ $(2,1)$ $(2,1)$ . . .
$(0,3)$ $(3,1)$ $(3,2)$ . . .
. . .

In questo caso un ordinamento potrebbe essere quello che si ottiene leggendo la matrice da sinistra a destra e poi dall'alto al

basso.[10] Possiamo visualizzare anche su di una retta del piano euclideo tale insieme ordinato interpretando le coppie come punti, a coordinate intere, del primo quadrante. In questo caso l'ordine si stabilisce prima "muovendosi" da sinistra verso destra e poi dal basso verso l'alto. In altre parole se "andare avanti" significa passare da un elemento ad un altro più grande, allora si può andare avanti o spostandosi orizzontalmente verso un punto a destra oppure spostandosi verticalmente verso un punto in alto.

Volendo dare una definizione generale dei tipi di ordinamento ora esposti possiamo dire che, date due coppie (n,m) e (p,q), per decidere chi viene prima si guarda la prima coordinata, se $n<p$ (cioè se la coppia (n,m) giace sopra un rigo superiore) allora si pone $(n,m) < (p,q)$, se $n= p$ (cioè se stanno sullo stesso rigo) allora si pone $(n,m) \leq (p,q)$ se e solo se $m \leq q$.

Definizione 12.1. Dati due insiemi ordinati $(S_1,\leq_1)$ e $(S_2,\leq_2)$, poniamo

$$(S_1,\leq_1)\times(S_2,\leq_2) = (S_1\times S_2,\leq)$$

dove $\leq$ viene definito ponendo

$$(x,y)\leq (x',y') \Leftrightarrow x <_1 x' \text{ oppure } x = x' \text{ e } y\leq y'.$$

Si noti che un ordinamento così definito è molto simile a quello che usualmente viene utilizzato in un vocabolario o in un elenco telefonico. Infatti, l'ordinamento usuale *a*, *b* , *c* ... delle lettere dell'alfabeto viene esteso all'insieme di tutte le parole che si possono scrivere in tale alfabeto confrontando la prima lettera, poi, nel caso che la prima lettera coincida, confrontando la seconda e così via. Ad esempio la parole, *ala, aria, cane, case* saranno ordinate al modo seguente:

$$ala < aria < cane < case.$$

E' possibile dimostrare la seguente proposizione.

Proposizione 12.2. Il prodotto di due insiemi ben ordinati è un insieme ben ordinato.

Dim. Infatti dati due insiemi bene ordinati $(S_1,\leq_1)$ e $(S_2,\leq_2)$ e detto A un sottoinsieme non vuoto di $S_1\times S_2$ esisterà il minimo $m_1 = \{x\in S_1 : \text{esiste } y \text{ tale che } (x, y)\in A\}$. Inoltre esisterà anche il mi-

[10] Salvo il fatto che, per passare al rigo successivo sarebbe necessaria una "pazienza infinita" !

nimo m_2 dell'insieme $\{y \in S_2 : (m_1, y) \in A\}$. È chiaro che la coppia (m_1, m_2) è il minimo di A.

Definiamo ora la somma di due insiemi ben ordinati. L'idea è che la somma di $(S_1,\leq_1)$ e $(S_2,\leq_2)$ è l'insieme ordinato che si ottiene mettendo tutti gli elementi di S_1 prima degli elementi di S_2 e lasciando inalterato l'ordinamento dei due insiemi S_1 e S_2. Ad esempio la somma degli insiemi ordinati $\{1,2,3,4\}$ e $\{a,b,c\}$ sarà l'insieme $\{1, 2, 3, 4, a, b, c\}$ ordinato al modo seguente:

$$1< 2 < 3 < 4 < a < b < c.$$

Purtroppo, come nel caso della somma di due cardinali, si presenta il problema di rendere disgiunti i due insiemi coinvolti prima di potere procedere. Se ad esempio dovessi definire la somma di $\{a,b,c\}$ con se stesso avrei dei problemi poiché non potrei scrivere

$$a<b<c<a<b< c$$

Il trucco che si usa è allora rendere disgiunti gli insiemi ordinati $(S_1,\leq_1)$ e $(S_2,\leq_2)$ senza alterarne la struttura d'ordine. In altre parole dobbiamo trovare due copie isomorfe di $(S_1,\leq_1)$ e $(S_2,\leq_2)$ i cui domini sono disgiunti. Ad esempio, se si osserva che $\{0\}$ ed $\{1\}$ sono insiemi ordinati, allora possiamo considerare al posto di $(S_1,\leq_1)$ la struttura isomorfa $(S_1,\leq_1)\times\{0\}$ ed al posto di $(S_2,\leq_2)$ la struttura isomorfa e $(S_2,\leq_2)\times\{1\}$. Successivamente posso definire nell'unione $(S_1,\leq_1)\times\{0\}\cup(S_2,\leq_2)\times\{1\}$, che coincide con l'unione disgiunta $S_1 \underline{\cup} S_2$ un ordinamento che lascia immutato l'ordine nei due "pezzi" $(S_1,\leq_1)\times\{0\}$ e $(S_2,\leq_2)\times\{1\}$ e poi pone tutti gli elementi di $(S_1,\leq_1)\times\{0\}$ prima degli elementi di $(S_2,\leq_2)\times\{1\}$.

Definizione 12.3. La *somma* di due insiemi ordinati $(S_0,\leq_0)$ e $(S_1,\leq_1)$ è definita ponendo

$$(S_0 \underline{\cup} S_1,\leq) = (S_0,\leq_0) + (S_1,\leq_1)$$

dove

$(x,0) \leq (y,0)$ se e solo se $x \leq_0 y$
$(x,1) \leq (y,1)$ se e solo se $x \leq_1 y$
$(x,0) \leq (y,1)$ per ogni $x \in S_0$ *e* $y \in S_1$.

Proposizione 12.4. La somma di due insiemi ben ordinati è un insieme ben ordinato.

Proposizione 12.5. La relazione *"essere isomorfi"* ≡ è compatibile con le operazioni +, ×, pertanto è una congruenza della struttura algebrica $(O, +, \times, (\varnothing,\varnothing), (\{e\},\leq))$.

In base a tale proposizione possiamo definire il quoziente di $(O, +, \times, (\varnothing,\varnothing), (\{e\},\leq))$.

Definizione 12.6. Chiamiamo *algebra dei numeri ordinali* la struttura algebrica $(O/\equiv, \times, +, \mathbf{0},\mathbf{1})$ che si ottiene come quoziente della struttura $(O, +, \times, (\varnothing,\varnothing), (\{e\},\leq))$ modulo ≡.

Come avviene sempre quando si effettua il quoziente di una struttura algebrica, conviene effettuare le operazioni con gli elementi rappresentativi "più comodi" in modo da rendere chiaro il significato dell'operazione. Ad esempio dovendo calcolare la somma di $[(N,\leq)]+[(N,\leq)]$ conviene sostituire l'insieme ben ordinato $(N,\leq)$ con la struttura isomorfa $(\{1\text{-}1/(n+1) : n\in N\}, \leq)$ e, rispettivamente, $(\{2\text{-}1/(n+1) : n\in N\}, \leq)$. Essendo i due domini di tali strutture disgiunti, l'ordinamento della somma potrà essere rappresentato al modo seguente
$0 < 1\text{-}1/2 < 1\text{-}1/3 < \ldots < 1 < 2\text{-}1/2 < 1\text{-}1/3, \ldots$
Possiamo inoltre rappresentare sull'asse delle ascisse tale insieme ordinato ottenendo due successioni di punti, una che si avvicina sempre più ad 1 ed una che si avvicina sempre di più a 2.

Proposizione 12.7. L'algebra dei numeri ordinali è una estensione dell'usuale algebra dei numeri naturali $(N_0, \times, +, 0, 1)$.

Dim. Osserviamo solo che un isomorfismo $N_0 \to O/\equiv$ si può definire per induzione ponendo

$$f(0) = \mathbf{0} = [(\varnothing,\varnothing)] \text{ e } f(n+1) = f(n)+\mathbf{1}.$$

Lo stesso isomorfismo può essere definito direttamente ponendo $f(0) = 0$ e $f(n+1) = [(\{0,\ldots,n\},\leq)]$.

Per le operazioni tra ordinali valgono proprietà diverse da quelle delle operazioni tra cardinali. Ad esempio se ω denota il numero ordinale $[N]$, allora risulta che:

$\omega+\omega \neq \omega$
$\omega\times\omega \neq \omega$
$n+\omega = \omega$

$\omega + n \neq \omega$.

Ad esempio se $n = 3$, allora possiamo rappresentare n con la struttura $(\{-3,-2,-1\}, \leq)$ essendo $\leq$ l'ordine naturale. Se rappresentiamo ω con $(N, \leq)$, allora una visualizzazione di un rappresentante di $3+\omega$ può essere data da

$-3 < -2 < -1 < 0 < 1 < 2 < \ldots$

che, come abbiamo visto, individua una struttura isomorfa a $(N, \leq)$. Ciò mostra che $3+\omega = \omega$. Consideriamo invece $\omega+3$ e rappresentiamo 3 con $(\{a,b,c\}, \leq)$ dove $\leq$ è l'usuale ordinamento delle lettere dell'alfabeto. Allora una visualizzazione di un rappresentante di $\omega+3$ è data da

$0 < 1 < 2 < 3 < \ldots a < b < c$.

Rispetto tale ordinamento c costituisce un massimo e quindi tale rappresentante non può essere isomorfo a $(N, \leq)$ che non ammette un massimo[11]. Ciò mostra che $\omega+3 \neq \omega$.

Concludiamo definendo in $(O/\equiv, \times, +, 0,1)$ una relazione d'ordine. Per poterlo fare definiamo prima la seguente relazione dove per *segmento iniziale* di un insieme ben ordinato $(S,\leq)$ si intende un intervallo aperto del tipo $[0, t) = \{x \in S : 0 \leq x < t\}$.

Definizione 12.8. Indichiamo con $\leq$ la relazione binaria in O definita ponendo, per ogni coppia $(S_0,\leq_0)$, $(S_1,\leq_1)$ di insiemi ben ordinati, $(S_0,\leq_0) \leq (S_1,\leq_1)$ se $(S_0,\leq_0)$ è isomorfo ad un segmento iniziale di $(S_1,\leq_1)$.

Tale relazione è un pre-ordine ed induce una relazione d'ordine nella classe degli ordinali al modo solito.

Proposizione 12.9. Le relazione $\leq$ è compatibile con la relazione di isomorfismo ed induce nell'insieme degli ordinali una relazione d'ordine totale.

---

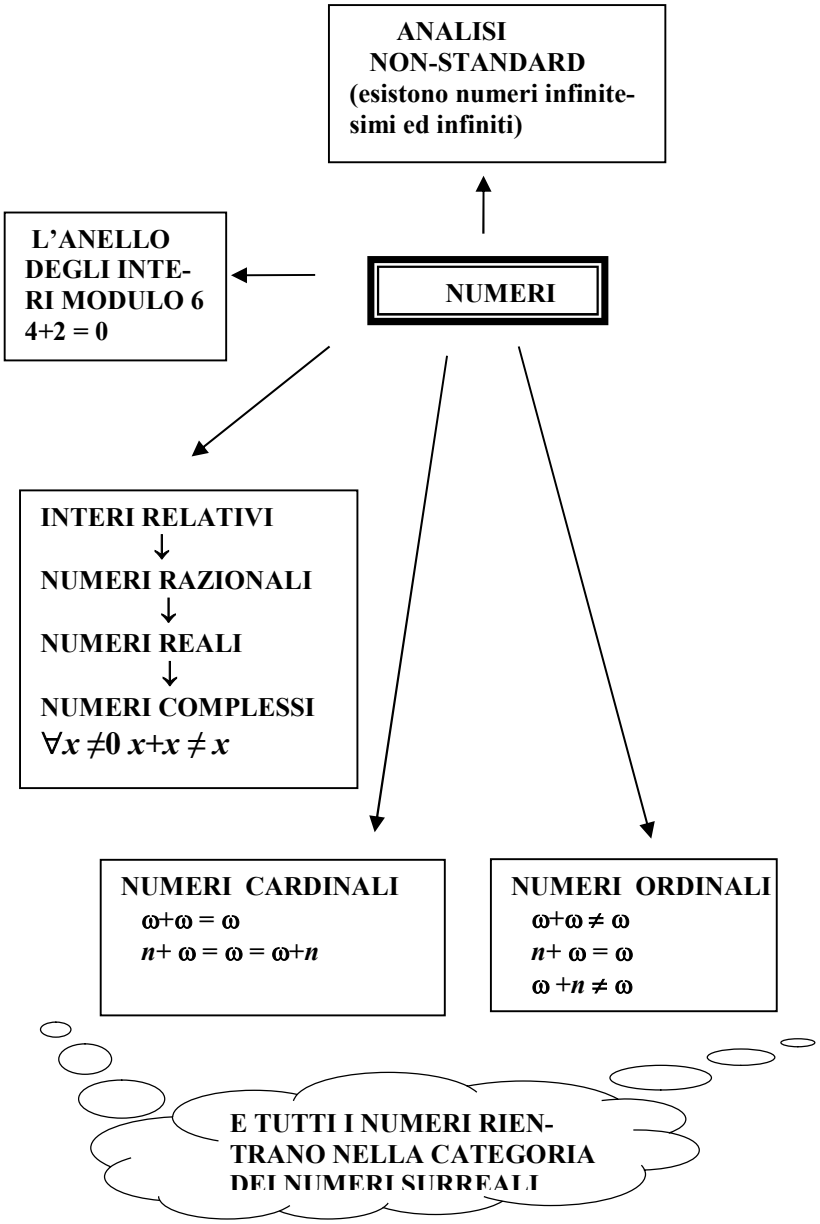
[11] In logica matematica si dimostra, come prevedibile, che se due strutture sono isomorfe allora ogni proprietà verificata dalla prima struttura è anche verificata dalla seconda. In particolare, date due strutture ordinate $(S_1, \leq_1)$ e $(S_2, \leq_2)$ isomorfe, se $(S_1, \leq_1)$ ammette un massimo, allora anche $(S_2, \leq_2)$ deve ammettere un massimo. D'altra parte se m fosse il massimo in $(S_1, \leq_1)$ allora, detto $f : S_1 \to S_2$ un isomorfismo, dal fatto che $x \leq m$ per ogni $x \in S_1$ seguirebbe che $f(x) \leq f(m)$ per ogni $x \in S_1$. Essendo f suriettiva ciò comporterebbe che $f(m)$ è un massimo in $(S_2, \leq_2)$.

13. Riassumendo sui possibili numeri

Il punto di partenza di molte nostre costruzioni sono i numeri naturali. Naturalmente questo non è un caso poiché il processo di contare è quello più antico nella storia dell'umanità ed è presente in tutti i popoli ed in tutti i tempi. A partire dalla struttura algebrica di N_0 siamo passati all'anello dei numeri relativi, poi al campo dei razionali, poi ai reali e poi ai numeri complessi. Sempre a partire dalla struttura algebrica di N_0, con l'introduzione del concetto di numero cardinale abbiamo esteso i naturali alla aritmetica dei transfiniti. Un'altro aspetto dei numeri naturali consiste nella struttura d'ordine. I numeri in questo caso servono per ordinare gli elementi di un insieme e non per misurare la quantità di elementi di un dato insieme. Estendendo tale aspetto perveniamo alla nozione di numero ordinale.

Una via completamente diversa è quella dell'analisi nonstandard in cui vengono introdotti numeri infiniti e numeri infinitesimi. Se invece di estendere il monoide dei numeri naturali ne facciamo un quoziente (cioè applichiamo un processo di astrazione), arriviamo agli anelli degli interi modulo *m.*

Qui sotto rappresentiamo graficamente tale situazione. Da notare che tutti i tipi di numero rientrano in una unica definizione generale di numero che va sotto il nome di *"numero surreale"* che comunque non esponiamo.


ANALISI
NON-STANDARD
(esistono numeri infinite-
simi ed infiniti)
L'ANELLO
DEGLI INTE-
RI MODULO 6
4+2 = 0
NUMERI
INTERI RELATIVI
↓
NUMERI RAZIONALI
↓
NUMERI REALI
↓
NUMERI COMPLESSI
∀x ≠0 x+x ≠ x
NUMERI CARDINALI
ω+ω = ω
n+ ω = ω = ω+n
NUMERI ORDINALI
ω+ω ≠ ω
n+ ω = ω
ω +n ≠ ω
E TUTTI I NUMERI RIEN-
TRANO NELLA CATEGORIA
DEI NUMERI SURREALI

Divagazione 1:
Insiemi ripetitivi, vaghi, rozzi

In questo capitolo ci siamo riferiti alle idee di Cantor sulla nozione di insieme. Tuttavia è interessante vedere se le idee di Cantor siano le uniche possibili per formalizzare l'idea di "collezione di oggetti" e se siano invece possibili altri punti di vista ed altre formalizzazioni.

Insiemi con ripetizioni. Osserviamo ad esempio che nel caso finito spesso gli insiemi che vengono indicati come "elenchi":

{Carlo, Luigi, Maria}} {2,5,1}, {*a*,*e*,*i*,*o*,*u*}, …

Ora in teoria degli insiemi non ha senso inserire in un elenco due volte lo stesso elemento, ad esempio scrivere {2,5,5,4} in cui il numero 5 è ripetuto due volte. Questo perché si assume che due insiemi con gli stessi elementi siano uguali (principio di estensionalità) e ciò comporta che {2,5,5,4} e {2,5,4} rappresentano lo stesso insieme. Ora, esistono situazioni in cui ha senso considerare tali ripetizioni.

Ad esempio ha senso dire che tra i divisori primi di $720 = 2^4 \cdot 3^2 \cdot 5$ il numero 2 compare quattro volte, il 3 compare due volte ed il 5 una volta, e che quindi invece di parlare dell'*insieme* dei divisori primi di 60 sia preferibile riferirsi al *"multi-insieme"* {2, 2, 2, 2, 3, 3, 5}.

Ancora, ha senso dire che un' equazione come $(x-2)^3 \cdot (x-7)^2 \cdot (x-5) = 0$ ammette come radici il numero 2 tre volte, il numero 7 due volte e 5 una volta. In tale caso invece di dire che l'insieme delle radici è {2, 7, 5} sarebbe preferibile dire che il multi-insieme di radici è {2, 2, 2, 7, 7,5}.

Esistono anche esempi in ambito diverso da quello della matematica. Supponiamo che in un magazzino di ogni oggetto in vendita esista una scorta con un certo numero di "pezzi", allora è ragionevole rappresentare il contenuto di tale magazzino non con la nozione di insieme ma con quella di multi-insieme. D'altra parte è quello che viene fatto comunemente in un inventario.

Fino ad ora abbiamo considerato solo multi insiemi finiti. Per potere dare una definizione precisa di multi-insieme che non escluda quelli infiniti, ricordiamo che un sottoinsieme X di un insieme S può essere identificato con la sua funzione caratteristica $c_X : S \to \{0,1\}$. Ciò suggerisce di identificare gli insiemi con ripetizioni con le funzioni $c : S \to N_0$ dove $c(x)$ è un numero che viene interpretato come numero di presenze di x.

Definizione 1. Chiamiamo *multi-sottoinsieme di S* o semplicemente *multinsieme* ogni funzione $c : S \to N_0$ e pertanto denotiamo con N_0^S la classe dei multi-sottoinsiemi di *S*. Il *multi-insieme vuoto* è la funzione costantemente uguale a 0.

Ad esempio il multi-insieme {2, 2, 2, 7, 7,5} viene identificato con la funzione $c : N \to N_0$ tale che $c(2) = 3$, $c(7) = 2$, $c(5) = 1$ ed in cui $c(x) = 0$ per tutti i numeri x diversi da 2, 7, 5. Nell'esempio del magazzino un inventario viene rappresentato tramite (la tabella di) una funzione $c : S \to N_0$ dove S è l'insieme dei vari articoli che sono usualmente in vendita nel negozio. Per ogni articolo x il numero $c(x)$ rappresenta il numero di pezzi del tipo x presenti in magazzino. Ovviamente il multi-insieme vuoto corrisponde al magazzino vuoto.

Precisata la nozione di multi-insieme ci si devono inventare buone definizioni di inclusione, unione, intersezione e così via. Possiamo ad esempio definire in N_0^S una relazione binaria $\subseteq$ ponendo $c \subseteq c'$ se per ogni $x \in S$ risulta che $c(x) \leq c'(x)$. In termini di contenuto di un negozio tale ordinamentio coincide con la relazione "essere più fornito". Inoltre potremmo definire le operazioni di unione e di intersezioni ponendo,

$(c \cup c')(x) = max\{c(x), c'(x)\}$; $(c \cap c')(x) = Min\{c(x), c'(x)\}$.

In alternativa, forse sarebbe meglio definire l'unione ponendo

$(c \cup c')(x) = c(x) + c'(x)$.

Questo tipo di unione viene chiamata *unione disgiunta.* In tale caso, differentemente da quando avviene nella teoria classica degli insiemi, si avrebbe che, se c non è vuoto, $c \cup c \neq c$. Sembra invece difficile dare una definizione ragionevole di complemento.

Insiemi vaghi. Un altro modo di estendere la nozione di insieme si ottiene ricordando che un modo di rappresentare un insieme (non necessariamente finito) è il considerare una proprietà P definita in un dato insieme S e quindi l'estensione $\{x \in S : x$ verifica $P\}$ di tale proprietà. Come vedremo nel seguito, ciò è permesso dal *principio di comprensione* o, per meglio dire, di *isolamento*. Ad esempio possiamo scrivere $\{n \in N : n$ divisibile per $2\}$ per rappresentare l'insieme dei numeri pari. Ora consideriamo proprietà vaghe come "essere grande", "essere giovane", "essere alto". E' forse possibile applicare una sorta di principio di estensione a tali proprietà ? In altre parole: è possibile definire qualcosa come

l'insieme dei numeri grandi, l'insieme delle persone alte, l'insieme delle persone giovani ? E' chiaro che la nozione usuale di insieme non si dimostra adeguata. Ad esempio, riferendoci a "l'insieme delle persone alte" esistono persone che sono decisamente alte, altre che sono alte ma non troppo, altre decisamente non alte. Inoltre appare ovvio che anche se due persone sono alte è possibile comunque considerare una persona più alta di un'altra e quindi, in un certo senso "più appartenente" a tale insieme di un'altra. La nozione di insieme, con il suo distinguere nettamente tra appartenenza e non appartenenza, ripeto, non è certamente adeguata.

Ancora una volta possiamo proporre una definizione formale capace di rappresentare insiemi di questo tipo estendendo la nozione di funzione caratteristica.

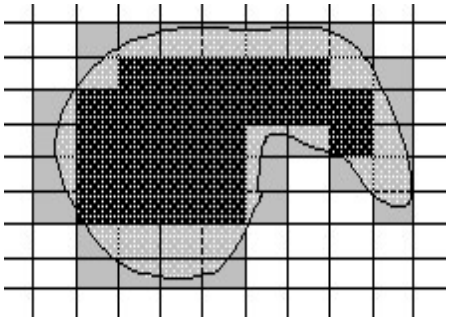
Definizione 2. Dato un insieme non vuoto S chiamiamo *insieme fuzzy* o *insieme vago* ogni funzione $s : S \to [0,1]$ e pertanto denotiamo con $[0,1]^S$ la classe degli sottoinsiemi vaghi di S. L'*insieme fuzzy vuoto* è la funzione costantemente uguale a 0.

Per ogni $x \in S$ il numero $s(x)$ rappresenta il grado di appartenenza di x all'insieme vago s. Se $s(x) = 1$ allora vuol dire che x viene considerato nettamente appartenente ad s. Se $s(x) = 0$ allora x si considera nettamente non appartenente ad s. Se $s(x) = 0.5$, allora vuol dire che esistono tante ragioni per considerare x appartenente ad s quante ce ne sono per considerarlo non appartenente.

La relazione di inclusione tra insiemi vaghi e le operazioni di unione e di intersezione possono essere definite in modo analogo a quanto fatto per i multinsiemi.

Insiemi rozzi. Concludiamo con un'altra tipologia di insieme che va sotto il nome di *insieme rozzo* (in inglese *rough set*). Supponiamo di volere rappresentare una figura X disegnata in bianco e nero su di un foglio quadrettato utilizzando esclusivamente l'insieme dei quadretti. Allora se indichiamo con T l'insieme di figure che si possono ottenere come unione di quadratini, possiamo rappresentare X tramite
- la più grande figura $i(X)$ in T contenuta in X
- la più piccola figura $c(X)$ contenente X.

In questo modo abbiamo una approssimazione per difetto $i(X)$ ed una approssimazione per eccesso $c(X)$ di X. Chiamiamo *insieme*



rozzo la coppia $(i(X),c(X))$ che appunto rappresenta un modo rozzo di rappresentare X.[1] La cosa può essere generalizzata al modo seguente.

Definizione 3. Dato un insieme S ed una relazione di equivalenza $\equiv$, indichiamo con T la classe dei sottoinsiemi che sono unione di classi complete di equivalenza. Allora chiamiamo *insieme rozzo* una coppia (A,B) di elementi di T tale che $A \subseteq B$ e tra A e B non esiste nessun elemento di T.

Se X è tale che $i(X) = A$ e $c(X) = B$ allora diciamo che (A,B) è un insieme rozzo che *rappresenta* X. E' chiaro che un insieme rozzo può rappresentare più insiemi e che il rappresentare un insieme con un insieme rozzo comporta una perdita di informazione.

Anche in questo caso si dovrebbe procedere a definire nozioni come quelle di inclusione, intersezione, unione.

[1] Quando una immagine viene registrata in forma elettronica (scannerizzata) allora i quadratini sono un equivalente dei pixel.

Divagazione 2
I razionali sono bene ordinabili, i naturali sono non ben ordinabili

Mescoliamo un po' le carte rispetto a quello che abbiamo detto fino ad ora. Abbiamo visto che l'ordinamento usuale in Z non è un buon ordinamento e lo stesso può essere detto per Q. Tuttavia niente esclude che in Z ed in Q si possano definire buon ordinamenti (ovviamente diversi da quelli usuali). Infatti basta considerare la seguente proposizione.

Teorema 1. In ogni insieme numerabile è possibile definire un buon ordinamento isomorfo a quello dei numeri naturali. In particolare in Z ed in Q è definibile un buon ordinamento.[2]

Dim. Supponiamo che S sia un insieme numerabile, allora esiste una funzione biettiva $f : N_0 \to S$ di N in S. Definiamo in S la relazione $\leq'$ ponendo

$$f(n) \leq' f(m) \Leftrightarrow n \leq m.$$

Allora è evidente che $(S, \leq')$ è una struttura relazionale isomorfa ad $(N_0, \leq)$ e che f è un isomorfismo tra tali strutture. Dal Corollario 9.4 segue che $(S, \leq')$ è un buon ordinamento. □

In altre parole, una volta fissata una strategia di enumerazione degli elementi di S diciamo che un elemento $x \in S$ è minore di un elemento $y \in S$ se in tale enumerazione in un certo senso x "viene prima" di y. Ad esempio, supponiamo di aver deciso di enumerare gli elementi di Z iniziando da 0 e poi alternando i negativi con i positivi

0, -1, +1, -2, +2, . . .

Avremo allora che si ottiene un buon ordinamento in Z al modo seguente:

$0 <' -1 <' +1 <' -2 <' +2 \ldots$

E' interessante osservare che in Z è possibile definire anche un buon ordinamento che non è isomorfo a quello di N_0. Infatti basta ordinare gli elementi di Z ponendo prima 0, poi tutti i negativi e poi tutti i positivi al modo seguente:

---

[2] Più complesso il discorso per l'insieme dei numeri reali R o, più in generale, per un qualsiasi insieme di cardinalità maggiore del numerabile. Infatti in tale caso la dimostrazione di esistenza di un buon ordine è possibile solo se si utilizza l'assioma della scelta.

$0 <^* -1 <^* -2 <^* -3 <^* \ldots <^* 1 <^* 2 <^* 3 \ldots.$

Una tale relazione d'ordine è quella dell'ordinale $\omega + \omega$. Un discorso simile può essere fatto anche per l'insieme Q^+ dei razionali positivi che abbiamo già dimostrato essere numerabile. Basta vedere la strategia di enumerazione che abbiamo utilizzata quando abbiamo enumerato Q^+ ed ottenere l'ordinamento definito ponendo

$0 < 1 < 1/2 < 2/1 < 1/3 < 3/1 < 1/4 < 4/1 < 2/3 < 3/2 < \ldots.$

Similmente, non è difficile trovare anche un buon ordinamento per l'intero insieme dei razionali Q intrecciando opportunamente razionali positivi e negativi.

Abbiamo visto che ogni insieme finito o numerabile è ben ordinato. Più complesso il discorso per l'insieme dei numeri reali R o, più in generale, per un qualsiasi insieme di cardinalità maggiore del numerabile. Infatti, vale il seguente teorema.

Teorema 2. L'asserzione per cui in ogni insieme esiste un buon ordinamento equivale all'assioma della scelta.

Mostriamo ora con due esempi come, a dispetto del teorema 1, non è vero che l'ordinamento in una terna di Peano sia un buon ordinamento.

Proposizione 3. (Paradosso del mucchio di grano).[3] Esistono sottoinsiemi non vuoti di una terna di Peano che non ammettono minimo.

Dim. Consideriamo l'insieme

$X = \{n \in N_0 :$ un mucchio di grano con n chicchi è grande$\}$

che è non vuoto poiché esiste almeno un mucchio di grano grande. Se si ammette che l'insieme dei naturali è bene ordinato, X ammetterebbe un minimo m. E' evidente che $m>1$ e che m-1, essendo strettamente minore di m non può appartenere ad X. Si perviene quindi all'assurdo per cui esiste un mucchio di grano piccolo (con m-1 chicchi di grano) a cui basta aggiungere un chicco perché diventi grande. □

Proposizione 4. (Paradosso di Berry). Esistono sottoinsiemi non vuoti di una terna di Peano che non ammettono minimo.

[3]Abbiamo già esaminato questo paradosso in relazione al principio di induzione. Questa è una riformulazione in termini di buon ordinamento.

Dim. Chiamo *"definizione"* di un numero naturale *n* una frase, scritta nella lingua italiana, del tipo

"il numero *n* tale che ..."

dove al posto dei puntini è messa una proprietà e dove si suppone che esista uno ed un solo numero che verifica tale proprietà. Esempi sono:

"il numero *n* che addizionato a 5 da 7" ;

"il numero *n* il cui quadrato sia nove"

che definiscono rispettivamente 2 e 3. Se ora una definizione la scrivo utilizzando la tastiera di un computer, potrò chiamare "lunghezza della definizione" il numero di volte che ho battuto su tale tastiera per ottenerla (comprendendo spazi vuoti e punti). Ha senso quindi considerare l'insieme

$A = \{n \in N_0 : n$ ammette solo definizioni di lunghezza maggiore di 90$\}$

Questo insieme è infinito e quindi non vuoto. Infatti è finito l'insieme dei numeri definibili con meno di 90 battiture.[4] Supposto per assurdo A ammetta un minimo m, allora m può essere definito come

"il più piccolo numero m che non può essere definito con meno di 90 battiture".

Ma i caratteri di tale definizione sono 76. Pertanto abbiamo trovato un modo per definire m con meno di 90 battiture in contrasto con il fatto che $m \in A$. L'assurdo cui siamo pervenuti prova che A non può ammettere minimo. □

[4] Supponiamo che la tastiera abbia 50 tasti, allora l'insieme delle frasi che posso scrivere con 90 battiture ha cardinalità 50^{90}. Quindi l'insieme delle possibili definizioni scritte con meno di 90 battiture ha cardinalità minore di 50^{90} ed è quindi finito.

CAPITOLO 3
METODO ASSIOMATICO E STRUTTURALISMO

Non mi sarei mai iscritto ad una associazione che mi accettasse come membro.
(il comico Groucho Marx).

Maria è destinata ad essere infelice, ama solo le persone che non l'amano.
(da una conversazione tra studentesse)

1. Paradossi e crisi della teoria degli insiemi

La scelta di considerare la nozione di insieme come base su cui fondare tutta la matematica mostrò ben presto alcune difficoltà di fondo. Dopo pochi anni che la teoria degli insiemi si andava diffondendo cominciarono ad essere scoperti diversi paradossi che mostravano come tale teoria fosse contraddittoria. Prima di esporre tali paradossi, esaminiamo un po' più da vicino quelle che sono due caratteristiche principali della nozione di insieme e che permettono di distinguerla dalla analoga nozione di classe o da quella di proprietà.

a) Principio di comprensione.
Tale principio afferma che data una qualunque proprietà P, la collezione degli enti verificanti P, che indicheremo con l'espressione $\{x : x \text{ verifica } P\}$, è un insieme. Ad esempio, alla proprietà *"essere pari"* corrisponde l'insieme dei numeri pari, alla proprietà *"essere maggiore di 2"* corrisponde l'insieme dei numeri maggiori di due e così via.

b) Principio di sostanzialità.
Tale principio, che è forse quello più importante, afferma che ogni insieme ha carattere di *"sostanza"* nel senso che, all'interno del discorso scientifico, gli insiemi possono essere trattati allo stesso modo di oggetti individuali come tavolo, atomo, punto.[5] Il principio di sostanzialità comporta che i nomi degli insiemi possono figurare come soggetti all'interno delle frasi e quindi, in particolare, che ha senso dire che un insieme verifica o meno una data proprietà. Ad esempio

"l'insieme dei numeri primi è infinito"

[5] Si veda anche il paragrafo 2 del capitolo 1.

è una frase in cui è l'intero insieme dei numeri primi a figurare come soggetto e tale insieme verifica la proprietà di essere infinito. Ciò non avviene, ad esempio, nella frase equivalente

"per ogni primo p esiste un primo q maggiore di p"

Che invece si riferisce agli elementi dell'insieme e non all'intero insieme. In termini insiemistici possiamo esprimere il principio di sostanzialità dicendo che un insieme può essere elemento di un altro dato insieme. Nell'esempio fatto l'insieme dei numeri primi appartiene all'insieme degli insiemi finiti.[6]

I due principi, messi insieme, ci dicono che, presa una proprietà, possiamo considerare un nuovo "oggetto", l'insieme degli elementi verificanti tale proprietà e che questo oggetto può essere trattato logicamente allo stesso modo di tutti gli altri oggetti. Questo punto di vista crea alcuni paradossi. Il primo si ottiene applicando il principio di comprensione alla proprietà-base "essere un insieme".

Proposizione 1.1. (**Paradosso della classe di tutti gli insiemi**) L'insieme $U = \{X : X \text{ è un insieme}\}$ ha cardinalità maggiore della cardinalità di ogni altro insieme. In particolare U ha cardinalità maggiore di $P(U)$ in contrasto con il teorema di Cantor.

Dim. Sia Z un insieme. Allora la funzione $h : Z \to U$ che associa ad ogni elemento $z \in Z$ il singoletto $h(z) = \{z\}$ è una funzione iniettiva di Z in U. □

Un altro paradosso nasce dal considerare la proprietà $X \notin X$ cioè alla proprietà di non appartenere a se stesso.

Definizione 1.2. Chiamiamo *normale* un insieme che non appartiene a se stesso.

Gli insiemi che usualmente consideriamo sono normali.

[6] Il principio di sostanzialità comporta che gli insiemi vengano considerati esistenti indipendentemente dal processo conoscitivo o creativo dell'uomo (come appunto avviene per le "sostanze"). Ciò pone quella che è la più moderna delle teorie matematiche, la teoria degli insiemi, nell'ambito di una delle più antiche filosofie: il platonismo.

Esempi di insiemi normali. L'insieme $\{1,\{2,3\},\{4,5,6\}\}$ non appartiene a se stesso e quindi è normale. L'insieme $\{X : X$ è finito$\}$ è infinito (ad esempio tutti i singoletti $\{n\}$ con $n \in N$ sono finiti) e quindi, non appartenendo a se stesso, è normale.

Esempi di insiemi non normali. Il complemento $\{X : X$ è infinito$\}$ dell'insieme normale ora considerato essendo infinito appartiene a se stesso e quindi non è normale. L'insieme di tutti gli insiemi appartiene a se stesso e quindi non è normale.

Se tali insiemi sembrano troppo grossi, possiamo considerare l'insieme X degli insiemi che sono descrivibili nella lingua italiana. Tale insieme non è molto grande in quanto, poiché con la lingua italiana posso formulare solo una quantità numerabile di descrizioni, X è numerabile. D'altra parte, avendo definito X tramite la lingua italiana, X appartiene a se stesso.

Problema: Dire se i due insiemi $\{x : x$ è un triangolo$\}$ e $\{x: x$ non è un triangolo$\}$ sono normali oppure no.

Data la proprietà di essere normale, per il principio di comprensione esisterà un insieme corrispondente, che chiamiamo *insieme di Russell*, cioè l'insieme

$$Russ = \{X \mid X \text{ è un insieme normale}\} = \{X \mid X \notin X\}.$$

D'altra parte, in base al principio di sostanzialità ha senso chiedersi se *Russ* sia normale o meno. Da queste due osservazioni segue il seguente paradosso dovuto a B. Russell.

Proposizione 1.3. (Paradosso di Russell, 1901) Sia *Russ* l'insieme di Russell, Allora risulta che

$$Russ \in Russ \iff Russ \notin Russ.$$

Dim. Se $Russ \in Russ$ allora *Russ* verifica la proprietà definitoria di *Russ* e quindi $Russ \notin Russ$. Se $Russ \notin Russ$ allora *Russ*, verificando la proprietà definitoria di *Russ* è normale e quindi $Russ \in Russ$. □

Si potrebbe pensare che i paradossi possano nascere solo dalla considerazione di proprietà strane come quella di non appartenere a se stesso o dalla considerazione di insiemi troppo grandi come l'insieme di tutti gli insiemi. In tale caso per evitare guai un matematico deve solo limitarsi a considerare proprietà ed insiemi

più familiari e piccoli. Le cose non stanno così, esistono contraddizioni che nascono dalla considerazione di insiemi che appaiono più naturali. Si consideri ad esempio proprietà semplicissime come "avere un numero finito di elementi" oppure "avere un solo elemento". Allora per il principio di comprensione è possibile considerare gli insiemi $Fin = \{X : X \text{ è finito}\}$ e $Sing = \{X : X \text{ è un singoletto}\}$. Se si analizza la dimostrazione del paradosso della classe di tutti gli insiemi, ci si accorge che tale dimostrazione permette di provare anche i seguenti paradossi.

Proposizione 1.4. (**Paradosso della classe di tutti gli insiemi finiti**) Sia la classe *Fin* di tutti gli insiemi finiti che la classe *Sing* di tutti i singoletti hanno cardinalità maggiore di ogni altro insieme. In particolare *Fin* e *Sing* hanno cardinalità maggiore di $\mathcal{P}(Fin)$ e $\mathcal{P}(Sing)$, rispettivamente. Ciò è in contraddizione con il teorema di Cantor.

La situazione non è molto diversa se si considera la proprietà "avere tre elementi". In base al principio di comprensione esisterà l'insieme corrispondente, cioè l'insieme $T = \{X \mid X \text{ ha tre elementi}\}$, cioè il numero cardinale $[\{a,b,c\}]$. Per tale insieme è possibile provare la stessa strana proprietà di cui gode l'insieme di tutti gli insiemi.

Proposizione 1.5. (Paradosso della classe degli insiemi con tre elementi). L'insieme $T = \{X \mid X \text{ ha tre elementi}\}$ ha più elementi di ogni altro insieme. In particolare T ha più elementi di $\mathcal{P}(T)$ e ciò è in contraddizione con il teorema di Cantor.

Dim. Sia Z un qualunque insieme, allora posso considerare la funzione $f : Z \to T$ ottenuta ponendo $f(z) = \{z, (z,z),(z,z,z)\}$. Tale corrispondenza è iniettiva e quindi T ha più elementi di Z. Una ulteriore dimostrazione si ottiene prendendo un qualunque insieme di tre elementi e poi considerando una "copia" di tale insieme per ogni elemento z in Z. Ad esempio possiamo considerare l'insieme $\{a, b, c\}$ e la funzione $f : Z \to T$ che ad ogni elemento $x \in Z$ associa $f(x) = \{(a,x), (b,x), (c,x)\}$. □

Forse è interessante riformulare il paradosso della classe degli insiemi con tre elementi anche per la classe dei gruppi, visto che

i gruppi costituiscono le strutture più trattate dagli dagli algebristi.

Proposizione 1.6. (Paradosso della classe dei gruppi) L'insieme G dei gruppi ha più elementi di ogni altro insieme. In particolare G ha più elementi di $\mathcal{P}(G)$ (in contrasto con il teorema di Cantor).

Dim. Per prima cosa osserviamo che ogni singoletto $\{z\}$ può essere considerato un gruppo $(\{z\},+,-,z)$ dove le operazioni sono definite ponendo $z+z = z$ e $-z = z$. Precisamente è un gruppo con elemento neutro ed in cui l'inverso di z è ancora z. Sia Z un qualunque insieme. Allora la corrispondenza $f : Z \to G$ che associa ad ogni $z \in Z$ il gruppo $f(z) = (\{z\},+,-,z)$ definito dal singoletto $\{z\}$ è iniettiva. Pertanto G ha più elementi di Z. □

Problema: Dimostrare che la classe dei gruppi finiti conduce ad un paradosso.
Problema: Dimostrare che la classe dei gruppi di ordine tre conduce ad un paradosso.

In realtà tali proposizioni sono facilmente estendibili a tutte le possibili strutture. Infatti vale per la classe degli anelli, la classe degli spazi vettoriali e per tutte le classi di strutture definite da un fissato sistema di assiomi. Vale infatti il seguente teorema molto generale di cui omettiamo la dimostrazione che richiederebbe un po' dei formalismi della logica matematica.

Teorema 1.7. Se una classe di strutture è chiusa per copie isomorfe, allora conduce ad un paradosso. In particolare, se T è una teoria, allora la classe dei modelli di T conduce ad un paradosso.

Problema: Chiamiamo *club* un insieme qualunque e consideriamo la classe $C = \{x : x \text{ è un club e } io \in x\}$ dei club che mi hanno come membro. Provare che comunque si consideri un insieme Z, C ha cardinalità maggiore o uguale a quella di Z. Pertanto C conduce ad un paradosso.

2. Russell, il paradosso del barbiere, Marx e le studentesse

E' importante osservare che nel paradosso di Russell la sola implicazione $Russ \in Russ \Rightarrow Russ \notin Russ$ non risulta paradossale. Per capire tale questione riconsideriamo la battuta di Marx con cui si è iniziato il paragrafo precedente. Detto x l'insieme dei membri di una associazione allora Marx afferma che

$$\forall x(io \in x \Rightarrow io \notin x).$$

Questo non è paradossale ma è solo la prova che, per ogni x, $io \notin x$, in altri termini che Marx non può appartenere a nessuna associazione. Detto più in generale, il fatto che una implicazione $A \Rightarrow \neg A$ risulti vera non è affatto paradossale e permette di dedurre solo che A è falsa. Infatti, $A \Rightarrow \neg A$ è logicamente equivalente ad $\neg A$. Per convincersi di questo basta ricordare un po' di logica e che una implicazione del tipo $A \Rightarrow B$ risulta equivalente alla disgiunzione $\neg A \vee B$. Pertanto, in particolare, $A \Rightarrow \neg A$ è equivalente a $\neg A \vee \neg A$ cioè a $\neg A$. D'altra parte le dimostrazioni per assurdo di cui abbiamo parlato nel primo volume si basano proprio su tale principio. Risulta invece paradossale una equivalenza del tipo $A \Leftrightarrow \neg A$ che afferma che una asserzione A è sia vera che falsa.

Più vicina alla struttura logica del paradosso di Russell è l'osservazione su Maria che ama solo le persone che non l'amano. Dal punto di vista logico viene affermata la validità dell'asserzione $\forall X(ama(Maria,X) \Leftrightarrow \neg ama(X,Maria))$. Ponendo *Maria* al posto di X si ottiene in particolare che

$$ama(Maria, Maria) \Leftrightarrow \neg ama(Maria, Maria)$$

che è ovviamente una contraddizione. L'effetto di tale contraddizione è meno catastrofico del paradosso di Russell in quanto prova solo che quello che si afferma di Maria è necessariamente falso. In altre parole non può esistere una persona che ama solo le persone che non l'amano.

Un paradosso simile era noto agli antichi greci sotto la forma del "paradosso del barbiere". In tale paradosso veniva data la seguente definizione di "barbiere"

Definizione 2.1. "Il barbiere è una persona che taglia la barba a tutte e sole le persone che non se la tagliano da sole".

Supponiamo ora che Carlo sia un barbiere. In questo caso:

- se Carlo non si fa la barba allora, in quanto barbiere, deve farsela
- se Carlo si fa la barba allora, in quanto barbiere, non deve farsela.

e questa è una contraddizione. Tuttavia a ben osservare il ragionamento fatto è sbagliato anche se l'errore è abbastanza nascosto. Infatti se si dice "Supponiamo che Carlo sia un barbiere" si assume che esiste qualcuno che rientra nella definizione di barbiere. Ma logicamente ciò non può essere provato. Infatti la contraddizione a cui si è pervenuti in realtà dimostra (per assurdo) che non può esistere una persona che può essere dichiarata "barbiere" secondo la definizione 2.1. D'altra parte non è certo sorprendente che una definizione non possa essere soddisfatta. Basta pensare, ad esempio, la definizione "un barbanumero è un numero che è sia pari che dispari".

Terminiamo con un ulteriore paradosso non stroppo differente dai precedenti. Chiamiamo *eterologica* una espressione della lingua italiana che esprime una proprietà che non risulta verificata dall'espressione stessa. Ad esempio "scritta con meno di quattro caratteri" è un'espressione eterologica. Chiamiamo *autologica* una espressione che che esprime una proprietà verificata dall'espressione stessa. Ad esempio "in lingua italiana" è una espressione autologica. Allora è immediato provare la seguente paradossale equivalenza:

'eterologica' è eterologica $\Leftrightarrow$ *'eterologica' non è eterologica.*

3. Affrontare i paradossi: intuizionismo e metodo assiomatico

Vi furono due modi diversi di reagire alla scoperta dei paradossi della teoria degli insiemi. Quello della maggior parte dei matematici fu semplicemente di fingere di non accorgersene. La teoria degli insiemi risultava essere uno strumento tanto utile che nessuno sembrava disposto a rinunciarci per questioni di rigore scientifico. Quei pochi che invece si occupavano di fondamenti della matematica videro nei paradossi la crisi dell'intero apparato conoscitivo della matematica. Vediamo cosa scrive Frege nel 1903 nei suoi *"Fondamenti dell'aritmetica"*, un testo fondamentale dove per la prima volta si propone una definizione dei numeri su base insiemistica o, come dice Frege, logica.

Nulla di più indesiderabile può capitare ad uno scienziato del fatto che una delle fondamenta del suo edificio si incrini dopo che l'opera è finita. E questa la situazione in cui mi trovo in seguito ad una lettera (contenente il paradosso) inviatami del sig. Bertrand Russell proprio mentre si stava ultimando la stampa di questo volume. . .

"Solatium miseris, socios habuisse malorum". Anch'io ho questo sollievo, se sollievo lo possiamo chiamare; infatti chiunque nelle sue dimostrazioni abbia fatto uso di estensioni di concetti, di classi, di insiemi (compresi i sistemi di Dedekind) si trova nella mia stessa posizione. Non è soltanto questione del mio particolare modo di gettare le fondamenta, ma è in questione la possibilità o meno di dare all'aritmetica un qualsiasi fondamento logico.

Frege reagì a questo sconforto cambiando radicalmente il suo punto di vista circa la matematica. Stante l'esistenza dei paradossi, non si doveva tentare di fondare tutta la matematica, in particolare la geometria, tramite la logica e la teoria degli insiemi. Piuttosto si doveva partire dall'intuizione geometrica per definire i numeri e quindi tutta la matematica.

"Anch'io un tempo ritenevo possibile conquistare per via puramente logica tutto il campo numerico a partire dai numeri dei bambini [...]."

tuttavia

"... mi sono convinto che aritmetica e geometria sono cresciute dallo stesso terreno e, precisamente, dal terreno della geometria, così che tutta l'aritmetica è, propriamente, geometria. La matematica appare così perfettamente nella sua essenza.

I matematici del seguito seguirono una via diversa: tentarono di risolvere la questione dei paradossi in teoria degli insiemi. Le strade seguite sono due, totalmente diverse tra loro. Quella dell'*intuizionismo* e quella dell'*assiomatizzazione* della teoria degli insiemi ed in generale della matematica.

L'intuizionismo. Gli intuizionisti rigettavano completamente la teoria di Cantor e quella parte della matematica che su essa si fondava. Esponenti di questa corrente filosofica, che si ispira a Kant, sono due matematici di rilievo, L.E.J. Brouwer (1881-1966) e H. Weyl (1885-1955). Gli intuizionisti sostengono che la matematica si fonda sull'intuizione *a priori* del tempo e che i suoi enti sono «costruzioni» della mente umana effettuate a partire da questa intuizione. In particolare, l'intuizione del trascorrere del tempo porta all'idea di numero naturale che essi ritengono, in comune con i pitagorici, base di tutta la matematica. Non ha senso ricondurre la nozione di numero naturale a quella di insieme o ad un sistema di assiomi perché l'idea di numero naturale è insita in ogni uomo. A partire da tale intuizione, mediante metodi costruttivi di tipo mentale, si doveva poi procedere alla edificazione del rimanente corpo della matematica. Indefinitiva il punto di vista degli intuizionismi si può riassumere con l'equazione:

MATEMATICA =
INTUIZIONE DEL NUMERO INTERO +
COSTRUZIONE DEGLI ENTI MATEMATICI

Per gli intuizionisti se una parte della matematica non è ottenibile in tale modo allora non è da considerare affidabile e deve essere rigettata via.

A partire da tali idee gli intuizionisti sviluppano una matematica ed una logica per molti aspetti diversa e più sottile di quella che usualmente siamo abituati a considerare. Ogni ente matematico esiste solo se è stato concretamente costruito. Ogni asserzione matematica è giustificata dalla costruzione di una dimostrazione,. Da ciò segue un tipo di logica che risulta differente da quella classica e che può essere definita al modo seguente.

- un asserzione atomica, cioè priva di connettivi logici, α è valida solo se la costruzione da essa descritta è stata fatta.
- una asserzione $\neg\alpha$ è valida solo se da α è stata derivata una contraddizione
- una asserzione $\alpha\wedge\beta$ è valida solo se si è esibita sia una dimostrazione di α che una dimostrazione di β.
- una asserzione $\alpha\vee\beta$ è valida solo se si è esibita o una dimostrazione di α oppure una dimostrazione di β.
- una asserzione $\exists x(\alpha)$ è valida se e solo se si è costruito un ente matematico verificante la proprietà espressa da α.

Da questa interpretazione seguono leggi della logica notevolmente diverse da quelle classiche. Ecco alcuni esempi di differenze:

La legge del terzo escluso per gli intuizionisti non è valida. Infatti se valesse $\alpha \vee \neg\alpha$ per ogni asserzione α, allora, qualunque sia l'asserzione α saremmo sempre in grado di provare α oppure provare $\neg\alpha$. Ciò potrebbe accadere solo se tutte le questioni della matematica fossero state risolte.

La legge di doppia negazione neanche è valida perché il significato dell'asserzione $\neg(\neg\alpha)$ è diverso dal significato di α. Ad esempio $\neg\neg\exists x(\alpha)$ significa che è assurdo supporre che non esista un elemento x per cui valga α. Invece $\exists x(\alpha)$ significa che si è in grado di esibire concretamente un elemento che verifica α. Le due cose sono totalmente differenti. Infatti, supponiamo ad esempio che $\exists x(\alpha)$ sia l'affermazione "esiste un numero trascendente". Utilizzando la teoria degli insiemi è possibile provare tale affermazione dimostrando che la cardinalità dell'insieme dei numeri algebrici è numerabile. Pertanto se non esistessero numeri trascendenti l'insieme dei numeri reali sarebbe numerabile è ciò contraddice un teorema di teoria degli insiemi. Stante questa dimostrazione un intuizionista direbbe che è stata dimostrata l'asserzione $\neg\neg\exists x(\alpha)$ e non l'asserzione $\exists x(\alpha)$. Invece quando, dopo avere definito π, viene dimostrato che π è trascendente (cosa enormemente più complicata), allora è possibile asserire $\exists x(\alpha)$. In altre parole gli intuizionisti utilizzano la negazione in modo che sia possibile distinguere enunciati di teoremi dimostrati per assurdo da enunciati di teoremi dimostrati in modo costruttivo.

L'intuizionismo, per quanto interessante ed affascinante, non ebbe e non ha molti seguaci e normalmente viene ignorato dai matematici contemporanei. Il problema è che l'accettazione dei principi dell'intuizionismo comporta difficoltà enormi nella dimostrazioni dei teoremi. Per mancanza di spazio e per la difficoltà della materia, in questi appunti non ci occuperemo ulteriormente di questo affascinante modo di vedere la matematica.

Il metodo assiomatico. La presentazione della geometria in forma assiomatica è, come abbiamo già osservato, il merito principale dell'opera di Euclide. Il metodo assiomatico assume però,

dalla fine dell'ottocento in poi, aspetti completamente nuovi e più radicali. Gli assiomi, e quindi i teoremi, erano visti nella geometria di Euclide come asserzioni vere riguardanti un dato mondo, quello degli enti geometrici matematici. La geometria si caratterizzava come studio sistematico di tali enti così come la zoologia si caratterizza per lo studio degli animali e la botanica per lo studio dei vegetali. Totalmente diverso è invece l'atteggiamento che viene assunto dai fautori del moderno metodo assiomatico. La matematica si caratterizza non per avere un particolare oggetto di studio ma per essere un particolare metodo di indagine, quello ipotetico-deduttivo. In altre parole:

> il metodo assiomatico non è solo una elegante sistemazione logica delle proprietà degli enti matematici, esso viene a coincidere con la matematica stessa.

Come è noto, l'essenza di tale metodo consiste:

> nell'esaminare tutte le conseguenze (interessanti) implicite in un particolare gruppo di ipotesi (gli assiomi), conseguenze ottenute con il solo ausilio di deduzioni senza mai fare riferimento all'esperienza o alla intuizione.

È significativo esaminare il diverso atteggiamento rispetto alle definizioni degli enti primitivi. In Euclide gli assiomi sono preceduti dalle definizioni: come si può parlare dei punti e delle rette se non si è prima spiegato che cosa sono i punti e le rette? Le definizioni cercano pertanto, in qualche modo, di indicare ciò di cui si vuole parlare, di facilitare l'intuizione, di distinguere un ente matematico da un altro. Si dice in proposito che sono *"ostensive"* cioè che indicano qualcosa. Come vedremo nel paragrafo successivo, nell'approccio assiomatico alla geometria proposto da Hilbert ciò non accade, in un certo senso le definizioni degli enti primitivi mancano del tutto. Semmai si può parlare di nomenclatura; si chiamano, per comodità espositiva, "punti" gli elementi di un dato insieme, "rette" gli elementi di un altro insieme e così via. Questo non significa che alla parola punto corrisponda qualcosa "che non ha dimensioni" o che "non ha parti" o cose simili. Neanche che alla parola retta corrisponda qualcosa che ha "lunghezza senza larghezza". Ad esempio una geometria potrebbe essere ottenuta considerando come punti le città di una

data nazione e come rette le autostrade che eventualmente le congiungono. Questo non vuol dire che una città non abbia parti o che una autostrada sia una lunghezza senza larghezza.

Il metodo assiomatico non si riferisce poi alla sola geometria. Non si dice che cosa è un numero reale (ad esempio non si dice che sia una classe completa di equivalenza di successioni di Chauchy oppure una sezione). Viene chiamato "numero reale" ogni elemento di una struttura algebrica verificante il sistema di assiomi per i campi ordinati completi.

4. Il metodo assiomatico e geometria

Il primo significativo esempio di applicazione del metodo assiomatico è il libro *"Fondamenti della Geometria"* di Hilbert la cui prima edizione risale al 1899.[7] Tale libro inizia nel modo seguente.

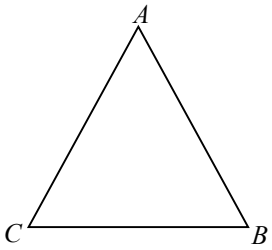
> *"Consideriamo tre diversi sistemi di oggetti: chiamiamo "punti" gli oggetti del primo sistema e li indichiamo con A, B, C, ...; chiamiamo "rette" gli oggetti del secondo sistema e li indichiamo con a, b, c . . . ; chiamiamo "piani" gli oggetti del terzo sistema e li indichiamo con α, β, γ, . . . ; . . .*
>
> *. . . Noi consideriamo punti, rette e piani in certe relazioni reciproche ed indichiamo queste relazioni con parole come "giacere", "fra", "congruente"; la descrizione esatta e completa, ai fini matematici, di queste relazioni segue dagli assiomi della geometria."*

[7] In realtà, già dieci anni prima di Hilbert il matematico e logico Giuseppe Peano aveva definito chiaramente il metodo assiomatico in geometria : *"Si ha così una categoria S di enti, chiamati "punti". Questi enti non sono definiti. Inoltre, dati tre punti, si considera una relazione fra essi, indicata con la scrittura c Î ab, la quale relazione non è parimenti definita. Il lettore può intendere col segno S una categoria qualunque di enti, e con c Î ab una relazione qualunque fra enti di quella categoria; avranno sempre valore tutte le definizioni che seguono, e sussisteranno tutte le proposizioni. In dipendenza dal significato attribuito ai segni non definiti S e c Î ab, potranno essere soddisfatti, oppure no, gli assiomi. Se un certo gruppo di assiomi è verificato, saranno pure vere tutte le proposizioni che si deducono."* (in *"Principi di geometria logicamente esposti"*).

Per capire meglio lo spirito del libro di Hilbert, esponiamo i primi assiomi che si riferiscono alla geometria piana ed alla relazione di giacenza. [8] Se un punto *X* giace su di una retta *r* diremo anche che *r passa per X*.

A1 Dati due punti *X* ed *Y* esiste almeno una retta *r* che passa per *X* ed *Y*.
A2 Dati due punti *X* ed *Y* esiste al più una retta che passa per *X* ed *Y*.
A3 Su ogni retta giacciono almeno due punti, ci sono almeno tre punti che non giacciono su di una stessa retta.

Un modello di tale sistema di assiomi è ottenuto assumendo come punti i tre vertici di un triangolo e come rette i tre lati:



La relazione "giace" è l'usuale appartenenza.

Mostriamo un paio di semplici teoremi che si possono dedurre dagli assiomi A1-A3.

Teorema 4.1. Due rette coincidono se e solo se hanno gli stessi punti (principio di estensionalità).

Dim. Supponiamo che *r* ed *r'* abbiano gli stessi punti. Allora i due punti di *r* la cui esistenza è assicurata da A3 devono appartenere anche ad *r'*. Ma per A2 ciò comporta che *r* = *r'*. □

Tale teorema mostra che la corrispondenza che associa ad ogni retta l'insieme dei suoi punti è iniettiva. Ciò permette di identificare una retta con l'insieme dei suoi punti e quindi la relazione *"giacere"* con la relazione insiemistica di *"appartenere"*.

[8] Da notare che una retta non è necessariamente un insieme di punti e che la relazione di "giacenza" non è necessariamente la relazione di appartenenza.

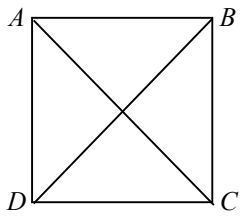
Teorema 4.2. Esistono almeno tre punti distinti non allineati e tre rette distinte che non passano per lo stesso punto.

Dim. Che esistano tre punti distinti non allineati A, B, C è detto in A3. Dati due punti X ed Y ndichiamo con r_{XY} la retta passante per X ed Y. Allora le rette r_{AB}, r_{AC} e e_{BC} non possono avere un punto in comune in quanto l'unico punto in comune di due di esse non può appartenere alla terza. □

Proviamo ora ad aggiungere ai primi tre assiomi il famoso assioma delle parallele, dove come all solito chiamiamo parallele due rette con nessun punto in comune.

> **A4** Sia r una retta ed X un punto non giacente in r, allora c'è una ed una sola retta passante per X e parallela ad r.[9]

Tale assioma non è ovviamente verificato dal modello con tre punti che abbiamo dato. Tuttavia è verificato dai vertici del seguente quadrato se si assumono come rette lati e diagonali.



Dai primi quattro assiomi segue il seguente teorema.

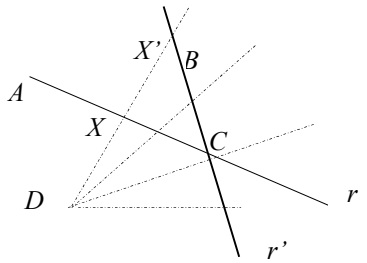
Teorema 4.3. Dati tre punti non allineati A, B e C, esiste un quarto punto D tale in $\{A, B, C, D\}$ non esistono tre punti allineati.

Dim. Sia r una retta per C parallela a r_{AB}. Per A3 esiste in r un punto D diverso da C. E' immediato verificare che tra i quattro punti A, B, C e D non ne esistono tre allineati. □

[9] In Hilbert viene assunta assunta solo l'unicità della parallela in quanto l'esistenza viene provata nel seguito del libro.

Teorema 4.4. Tutte le rette sono equipotenti tra loro.

Dim. Cosideriamo due rette *r* ed *r'* e supponiamo che si incontrino in un punto *C.* Detti *A* e *B* due punti ripettivamente di *r* ed *r'*



la terna *A*, *B*, *C* risulta non allineata. Sia *D* un quarto punto come nella proposizione precedente. Allora *D* non essendo allineato con *A* e *C* non appartiene ad *r*, non essendo allineato a *B* e *C* non appartiene ad *r'*. Allora ad ogni punto *X* di *r* posso associare la retta per *D* e *X* e poi l'intersezione di r_{DX} con *r'*. E' subito visto che tale corrispondenza è biettiva. Abbiamo quindi dimostrato che due rette *r* ed *r'* che si incontrano in un punto sono equipotenti. D'altra parte se *r* ed *r'* sono parallele, preso *P* in *r* e *P'* in *r'*, poiché *r* è equipotente ad $r_{PP'}$ e $r_{PP'}$ *ad r'*, *r* risulta essere equipotente a *r'*. □

Problema. Dimostrare che ogni fascio di rette contiene lo stesso numero di rette e che tale numero è uguale a quello dei punti di una retta più uno.

5. Geometrie e campi

L'esempio più noto di modello del sistema di assiomi A1-A4 è que ottenuto a partire dal campo dei numeri reali. Chiamiamo
- *punto* ogni coppia di numeri reali, cioè ogni elemento di R^2,
- *retta* ogni insieme di punti verificanti una equazione di primo grado del tipo $ax+by = p$ con *a*, *b* non entrambi nulli .

La relazione di *giacenza* coincide (in questo caso) con quella usuale di appartenenza. Da notare che terne proporzionali di coefficienti *a*, *b* e *c* determinano la stessa retta poiché determinano equazioni con le stesse soluzioni. Che per due punti diversi

(x_0,y_0) e (x_1,y_1) passa una ed una sola una retta deriva dall'esame del sistema omogeneo

$ax_0 + by_0 = p$
$ax_1 + by_1 = p$

nelle incognite a, b, p. Infatti bastano alcuni nozioni di base di algebra lineare per provare che tale sistema ammette almeno una soluzione non nulla e che tutte le soluzioni sono proporzionali tra loro. Il primo fatto comporta l'esistenza di una retta. Il secondo fatto che la retta è unica. Non è difficile verificare anche l'assioma delle parallele. Infatti, come è noto, i punti di intersezione di due rette $ax+by = p$ e $a'x+b'y = p'$ si ottengono risolvendo il sistema

$ax + by = p$
$a'x + b'y = p'$

Pertanto le due rette sono parallele se e solo se tale sistema non ammette soluzioni e questo avviene se e solo se i coefficienti a e b sono proporzionali ai coefficienti a', b'. Allora, dato un punto (x_0,y_0) ed una retta r di equazione $ax+by = p$, trovare una retta passante per (x_0,y_0) e parallela ad r equivale a trovare tre numeri a', b', p' tali che

$ab' = a'b$
$a'x_0 + b'y_0 = p'$

Anche in questo caso si tratta di un sistema omogeneo in tre incognite ed anche in questo caso esiste una soluzione e tutte le soluzioni sono proporzionali tra loro. Ciò prova l'esistenza e l'unicità della retta per (x_0,y_0) e parallela ad r.

Proposizione 5.1. Dato un campo C, chiamiamo *punto* una coppia di elementi di C, *retta* l'insieme $\{(x,y) : ax+bx+c = 0\}$ delle coppie che verificano una equazione di primo grado

$ax+by+c = 0$.

Diciamo inoltre che un punto *giace* su di una retta se appartiene a tale retta. Allora la struttura ottenuta in questo modo soddisfa gli assiomi A1-A4.

Dim. Basta osservare che tutte le verifiche degli assiomi che possono essere fatte nel campo dei reali in realtà possono essere fatte in un qualunque campo.

Esempi di geometrie finite. Sappiamo che consideriamo gli interi modulo m con m primo allora otteniamo un campo finito. Al-

lora, in accordo con la proposizione 5.1, possiamo associare al campo degli interi modulo due una geometria con solo quattro punti che non è diverso dal modello già considerato nel paragrafo precedente.

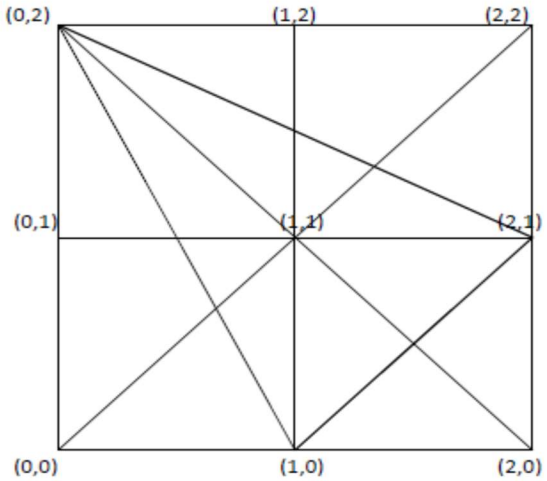
Possiamo considerare anche il campo degli interi modulo 3. In tale caso avremo che il modello di geometria è costituito dai nove punti

(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2).

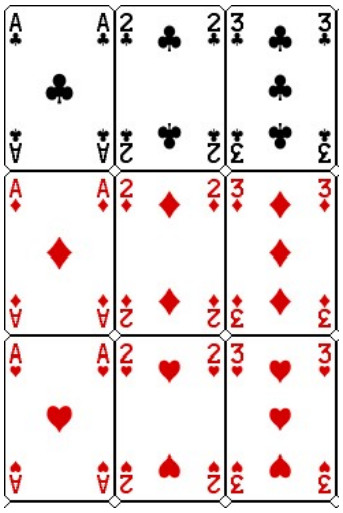
Avremo che le rette passanti per (0,0) saranno le quattro rette di equazione $x = 0$, $y = 0$, e $y = x$ e $y = 2x$, oppure, equivalentemente, $y = -x$. Le rette che non passano per (0,0) avranno equazione $ax+by = 1$. Ad esempio una retta è data da

$$\{(x,y) \mid 2x+y = 1\} = \{(0,1), (1,2), (2,0)\}.$$

Procedendo in questo modo non è difficile trovare tutte le rette di questo modello.



Tale esempio può essere "travestito" in modo più piacevole al modo seguente. Consideriamo nove carte di gioco che si ottengono prendendo i numeri 1, 2 e 3 ed i semi di fiori, quadri e cuori. Indicheremo tali carte con 1♣, 2♣, 3♣, 1♦, 2♦, 3♦, 1♥, 2♥, 3♥. Diciamo che due carte hanno una proprietà in comune se hanno lo stesso numero oppure lo stesso seme. Chiamiamo *punto* ognuna di tali carte e chiamiamo *retta* un insieme di tre carte tale che



- le tre carte hanno lo stesso numero, oppure
- le tre carte hanno lo stesso seme, oppure
- le tre carte non hanno nessuna proprietà in comune.

Allora ad esempio per i punti 1q, 2♣ passa la retta {1♦,2♣,3♥}, per i punti 1q, 1♣, la retta {1♦,1♣,1♥}. È facile rendersi conto che tali rette sono uniche. Inoltre data ad esempio la retta r = {1♦,2♣,3♥} ed il punto 2♦, la parallela ad r passante per 2♦ è la retta {2♦, 3♣, 1♥}.

Concludiamo questi due paragrafi relativi al sistema di Hilbert sottolineando che la lista di assiomi A1-A4 prosegue fino ad avere un sistema di assiomi categorico ed il cui unico modello, a meno di isomorfismi, è quello analitico definito all'inizio del paragrafo partendo dal campo dei reali. Il discorso sarebbe troppo lungo ed in questo libro ci accontentiamo di dare il "sapore" di cosa diventa la geometria dal punto di vista del moderno metodo asiomatico.

6. Metodo assiomatico e numeri reali

Nel primo volume abbiamo ottenuto i numeri reali partendo dall'insieme dei numeri razionali e "costruendo" la struttura che ci serviva. Hilbert, coerentemente alla sua idea della matematica come sistema ipotetico-deduttivo, diede invece una impostazione assiomatica alla teoria dei numeri reali. In questo paragrafo esponiamo un sistema di assiomi che anche se non coincide con quello proposto da Hilbert è ad esso equivalente e si riferisce alla teoria dei campi ordinati completi. Considereremo in particolare due assiomi: quello di Archimede e quello di completezza (o continuità). Tali assiomi li abbiamo già visti nel primo volume quando abbiamo definito la nozione di classe di grandezze omogenee. La cosa non deve sorprendere perché la teoria delle grandezze omogenee costituiva per i greci un sostituto della teoria dei numeri reali. Ricordiamo alcune nozioni che abbiamo dato già alla fine del primo volume.

Definizione 6.1. Un elemento x di un campo ordinato si chiama *infinito positivo* se risulta che $x > p \cdot 1$ qualunque sia l'intero p. Chiamiamo *infinito* negativo l'opposto di un infinito positivo. Chiamiamo *finito* un elemento che non sia infinito.

L'idea è che x è infinito se, partendo da zero, per quanti "passi unitari" in avanti si facciano non sia mai possibile raggiungere x.

Definizione 6.2. Chiamiamo *infinitesimo positivo* (*negativo*) un elemento x che sia l'inverso di un elemento infinito positivo (negativo).

Pertanto un elemento δ è un infinitesimo positivo se $\delta > 0$ e risulta che $1/\delta \geq p \cdot 1$ e quindi $\delta \leq 1/(p \cdot 1)$ per ogni naturale p. Possiamo ora definire la nozione di campo archimedeo.

Definizione 6.3. Un campo ordinato $(D,+,\cdot,0,1,\leq)$ si dice *archimedeo* se in esso non esistono elementi infiniti positivi.

In altre parole un campo ordinato si dice archimedeo se verifica il seguente assioma:

Assioma di Archimede. $\forall x \exists p \in N\ (p \cdot 1 \geq x)$.

Problema. Dimostrare che il campo dei numeri razionali ed il campo dei numeri reali (costruito con le successioni di Cauchy) risultano essere archimedei.

Un campo di razionali non standard (si veda la costruzione nel primo volume) è un esempio di campo ordinato non archimedeo. I campi non archimedei sono molto affascinanti perché in essi è possibile sviluppare una teoria degli infiniti e degli infinitesimi. Ad esempio possiamo dire che due elementi x ed y di un campo ordinato sono *infinitamente vicini* se x-y è un infinitesimo. Ovviamente due numeri possono essere infinitamente vicini senza coincidere.

Proposizione 6.4. Se x è un elemento finito allora anche $x+1$ è finito. Se x è un elemento infinito allora anche x-1 è infinito. Ne segue che l'insieme *Fin* degli elementi finiti non ammette massimo e che l'insieme *Inf* degli elementi infiniti non ammette minimo.

Dim. Se x è finito allora esiste p tale che $x \leq p \cdot 1$. Ciò comporta che $x+1 \leq (p+1)\cdot 1$ e quindi che $x+1$ è finito. Da ciò segue anche che se x è infinito anche x-1 è infinito. La rimanente parte della proposizione è ovvia. □

Ricordiamo che, se A e B sono due sottoinsiemi di un insieme ordinato allora $A \leq B$ significa che ogni elemento di A è minore di ogni elemento di B. In tale caso si dice anche che A e B sono *separati*. Chiameremo "*elemento separatore*" della coppia A e B un elemento u tale $A \leq \{u\} \leq B$ cioè un elemento u maggiore di tutti gli elementi di A e minore di tutti gli elementi di B.

Definizione 6.5. Un campo ordinato si dice *completo* se ogni coppia di insiemi separati ammette elemento separatore.

In altre parole un campo ordinato si dice *completo* se verifica l'assioma:

Assioma di completezza: $\forall A \forall B(A \leq B \Rightarrow \exists u(A \leq \{u\} \leq B)$.

Tutti i campi completi risultano essere archimedei.

Teorema 6.6. Ogni campo completo è archimedeo ma esistono campi archimedei che non sono completi.

Dim. Supponiamo che $(D,+,\cdot,0,1,\leq)$ sia un campo completo e consideriamo la coppia *Fin* ed *Inf* di sottoinsiemi di D. Se il campo non fosse archimedeo allora *Inf* sarebbe non vuoto e quindi essendo $Fin \leq Inf$, esisterebbe un elemento separatore u di tale coppia di insiemi. Allora u in quanto maggiorante di *Fin* è un infinito e quindi appartiene a *Inf*. Inoltre u, che è anche minorante di *Inf*, appartenendo a *Inf* è un minimo di *Inf* in contrasto con la Proposizione 6.4.

Il campo dei razionali è un esempio di campo archimedeo non completo. □

Da tale teorema segue che il campo Q^* dei razionali non standard ed il campo R^* dei reali non standard non essendo archimedei non sono nemmeno completi. Se si accettano le costruzioni fatte del campo dei numeri reali esposte nel primo volume, allora è possibile provare il seguente teorema. Naturalmente questo comporta l'accettazione della teoria degli insiemi.

Teorema 6.7. La teoria dei campi completi è soddisfacibile, cioè ammette un modello.

Dim. E' sufficiente considerare il campo costruito nel primo capitolo con il metodo delle successioni di Cauchy. La dimostrazione che tale campo è completo presenta qualche piccola difficoltà. □

Il seguente teorema, di cui omettiamo la dimostrazione, afferma che, a meno di isomorfismi, esiste un ed un solo campo completo archimedeo.

Teorema 6.8. La teoria dei campi completi è categorica, cioè tutti i campi completi sono isomorfi tra loro.

Quanto detto fino ad ora è sufficiente a dare una definizione assiomatica dei numeri reali.

Definizione 6.8. Chiamiamo *campo dei numeri reali* ogni campo completo.

Come spesso viene fatto in matematica, il fatto che tutti i campi completi siano isomorfi tra loro permette di usare l'espressione "il campo dei numeri reali" invece di "un campo dei numeri reali". Da notare che, coerentemente con il punto di vista strutturalista, non cerchiamo di definire che cosa sia un numero reale. Invece diciamo quando una struttura può essere chiamata "campo dei numeri reali" e chiamiamo "numero reale" ogni elemento di tale struttura.

7. Assiomi per evitare i paradossi della teoria degli insiemi

Il metodo assiomatico può sia essere applicato "localmente" a singoli settori della matematica (come la geometria, gli insiemi numerici e così via) oppure può essere utilizzato per tentare di rimettere in piedi la teoria degli insiemi cercando di eliminarne i paradossi. Una volta che si sia trovata una opportuna assiomatizzazione della teoria degli insiemi è possibile poi costruire tutta la matematica come abbiamo fatto nel capitolo 3 del primo volume.

Naturalmente la questione fondamentale è trovare un sistema di assiomi capace di eliminare i paradossi della teoria degli insiemi che abbiamo trattato nei paragrafi precedenti. Le assiomatizzazioni della teoria degli insiemi che sono state proposte riescono in questo compito limitando opportunamente

- o il principio di comprensione
- oppure quello di sostanzialità.

Limitazione del principio di sostanzialità (la teoria delle classi). La limitazione del principio di sostanzialità si ottiene accettando senza restrizioni il principio di comprensione nel senso che, data una proprietà P, la collezione degli enti verificanti P è sempre una classe. Non sempre le classi hanno però carattere di sostanza e solo le classi per cui ciò avviene hanno il diritto di chiamarsi insiemi. Ora ricordiamo che il carattere di sostanza per una classe si esprime nel fatto che di essa si possa asserire qualche proprietà, e quindi, in termini insiemistici, che essa appartenga ad una classe. Pertanto:

> vengono chiamati *insiemi* quelle classi che sono elementi di qualche altra classe.

Detto in breve, x è un insieme se verifica la proprietà $\exists y(x \in y)$. Le classi che non sono insiemi vengono chiamate *classi proprie*. Delle classi proprie non ha senso dire che verificano o meno una proprietà e non ha senso parlare di cardinalità. Questo modo di procedere fu proposto per la prima volta da von Neumann nel 1925 e poi migliorato da altri. Nella teoria delle classi il principio di comprensione viene riformulato al modo seguente:

Principio di comprensione nella teoria delle classi

Per ogni modo di fissare una proprietà P

$$\exists A \forall X(X \in A \Leftrightarrow X \text{ è un insieme e verifica } P$$

dove P è una proprietà esprimibile nel linguaggio della teoria degli insiemi ed A è una variabile che non compare in P.

Proposizione 7.1. Nella teoria delle classi il paradosso di Russell non è più valido ma diviene una dimostrazione del fatto che $Ru = \{X : X$ è un insieme e $X \notin X\}$ è una classe e non un insieme.

Dim. Riprendiamo il paradosso di Russell considerando la proprietà $X \notin X$. Allora per il principio di comprensione esiste una classe Ru tale

$X \in Ru \Leftrightarrow X$ è un insieme tale che $X \notin X$.

Ora risulta che

$Ru \notin Ru \Leftrightarrow$ o Ru non è un insieme oppure $Ru \in Ru$.

Tale equivalenza non è assurda in quanto risulta verificata nel caso in cui $Ru \notin Ru$ ed Ru non è un insieme. [10] □

Similmente nella teoria delle classi gli altri paradossi citati diventano dimostrazioni del fatto che la classe di tutti gli insiemi, la classe degli insiemi con tre elementi, la classe di tutti i gruppi sono tutte classi proprie.

Una limitazione del principio di comprensione si ottiene invece sostituendolo con il più debole assioma di isolamento.

Assioma di isolamento: *Dato un insieme S ed una proprietà P, $\{x \in S : x$ verifica $P\}$ costituisce un insieme.*

In altri termini l'assioma di isolamento consente solo di "isolare" un opportuno sottoinsieme all'interno di una collezione che sia stata già riconosciuta essere un insieme.

Proposizione 7.2. Se si sostituisce al principio di comprensione l'assioma di isolamento, il paradosso di Russell non è più riproducibile ma si trasforma nella dimostrazione del fatto che, fissato un qualunque insieme S, l'insieme $Ru = \{X \in S \mid X \notin X\}$ non appartiene ad S.

[10] La cosa è evidente, tuttavia se si vogliono fare un po' di calcoli logici basta osservare che $\neg A \Leftrightarrow (B \vee A) \equiv (\neg A \Rightarrow (B \vee A)) \wedge (B \vee A \Rightarrow \neg A) \equiv (A \vee B) \wedge ((\neg B \wedge \neg A) \vee \neg A) \equiv (A \vee B) \wedge \neg A$ e quindi, per la proprietà distributiva, alla formula $B \wedge \neg A$.

Dim. Se si accetta il principio di isolamente al posto di quello di comprensione allora l'equivalenza paradossale provata da Russell diventa

$$Ru \notin Ru \Leftrightarrow Ru \notin S \text{ oppure } Ru \in Ru.$$

che a sua volta è equivalente a $Ru \notin S$. □

Proposizione 7.3. Se si sostituisce al principio di comprensione l'assioma di isolamento, il paradosso dell'insieme di tutti gli insiemi non è più riproducibile.

Dim. Data la proprietà "essere un insieme" il principio di isolamento permette di definire solo la classe $U_S = \{X \in S : X \text{ è un insieme}\}$ cioè la classe di tutti insiemi che sono elementi di un dato insieme S. Allora, dato un insieme Z, la funzione che ad ogni $z \in Z$ associa il singoletto $\{z\}$ non è una funzione di Z in U_S poiché non è detto che $\{z\}$ appartenga ad S. □

Proposizione 7.4. Se si sostituisce al principio di comprensione l'assioma di isolamento, il paradosso dell'insieme degli insiemi con tre elementi non è più riproducibile.

Dim. Anche in questo caso il principio di isolamento permette di asserire solo che, dato un insieme S, la proprietà "avere tre elementi" definisce un insieme $T = \{X \in S \mid X \text{ ha tre elementi}\}$. Dato allora un insieme Z qualsiasi e $z \in Z$, non è detto che $\{(a,z),(b,z),(c,z)\}$ appartenga ad S e quindi a T. □

Proposizione 7.5. Tutti i paradossi della teoria degli insiemi che abbiamo esposto si traducono in una dimostrazione che la classe U di tutti gli insiemi non è un insieme.

Dim. Sia U la classe di tutti gli insiemi, se U fosse un insieme allora l'assioma di isolamento coinciderebbe con l'assioma di comprensione (basterebbe riferirsi sempre ad S come all'insieme in cui isolare l'insieme voluto). Ma dall'assioma di comprensione genera paradossi, e ciò prova che U non è un insieme. □

8. La teoria di Zermelo-Fraenkel

La limitazione al principio di comprensione è presente nella più diffusa teoria degli insiemi che prende il nome di teoria Zermelo-

Fraenkel. In tale teoria assumiamo come unici concetti primitivi la nozione di *insieme* e la *relazione di appartenenza* che indichiamo con $\in$. Pertanto un modello della teoria di Zermelo-Fraenkel sarà costituito da un insieme con una relazione binaria.

Nel seguito elenchiamo alcuni degli assiomi di tale teoria senza nessuna pretesa di rigore.

A1. Assioma di estensionalità: due insiemi che hanno gli stessi elementi sono uguali. In breve

$$[\forall z(z\in x \Leftrightarrow z\in y)] \Rightarrow x = y$$

Naturalmente è evidente che $x = y \Rightarrow \forall z(z\in x \Leftrightarrow z\in y)$, pertanto l'assioma di estensionalità può essere riformulato al modo seguente:

$$x = y \Leftrightarrow [\forall z(z\in x \Leftrightarrow z\in y)].$$

Tale assioma afferma che due insiemi che hanno gli stessi elementi sono uguali, in altre parole due insiemi che hanno la stessa "estensione" coincidono. Ciò differenzia un insieme dal procedimento usato per descriverlo (cioè dalle proprietà che lo definiscono). Per fare un esempio, anche se le proprietà "essere pari" e "terminare per 0, 2, 4, 6 o 8" sono diverse (pur essendo equivalenti) i due insiemi $\{x\in N \mid x$ è pari$\}$ e $\{x\in N \mid$ l'ultima cifra di x è 0, 2 4 6 o 8$\}$ sono uguali. La portata del fatto che in teoria degli insiemi si assume il punto di vista estensionale è più evidente se si considera il concetto di funzione. Come è noto in teoria degli insiemi si accetta le seguente definizione di funzione:

- chiamiamo *funzione* di N in N una relazione binaria $\mathcal{R}$ in N tale che per ogni $x\in N$ esiste uno ed un solo y tale che $(x,y)\in \mathcal{R}$.

Un modo diverso di procedere, che a volte si trova nei libri di scuola, potrebbe essere il seguente:

- chiamiamo *funzione* una *legge* o un *processo* che permette di ottenere un numero y una volta che si sia fissato un numero x.

Una tale definizione appare più intuitiva ma meno rigorosa. Infatti è poco chiaro che cosa si debba intendere per "legge" o "processo". Inoltre in generale noi accettiamo che, ad esempio, equazioni come

$$y = (x\text{-}1)^2 + 2x \qquad \text{e} \qquad y = x^2+1$$

rappresentano la stessa funzione pur rappresentando processi di calcolo diversi. Il fatto che le due funzioni siano la stessa signifi-

ca che quello che interessa è il fatto che se si fissa x in entrambi i casi si ottiene lo stesso y. In altre parole quello che interessa è l'estensione $\{(x,y)\in R\times R : y = (x\text{-}1)^2 - x^2\}$ della proprietà $y = (x\text{-}1)^2 - x^2$ che, di fatto, coincide con l'estensione $\{(x,y)\in R\times R : y = x^2+1\}$ della proprietà $y = x^2+1$. Pertanto l'idea di funzione è "estensionale"; quello che interessa e solo la "tabella" (l'insieme delle coppie) non il modo di calcolare tale tabella.

Un tale punto di vista, tipico dei matematici, potrebbe non essere accettato da un informatico che tiene anche conto dei tempi di calcolo di una funzione. In tale caso è evidente che il punto di vista estensionale non è più valido e che $y = (x\text{-}1)^2 - x^2$ e $y = x^2+1$ denotano cose diverse (cioè algoritmi diversi).

A2. Assioma dell'insieme vuoto: esiste un insieme che non ha elementi e che chiameremo *insieme vuoto*:

$$\exists x(\forall z(\neg z\in x)).$$

Dall'assioma di estensionalità segue che esiste un solo insieme vuoto che indicheremo con $\varnothing$.[11]

A3. Assioma del singoletto. Dato un insieme x esiste un insieme z che ha x come unico elemento:

$$\forall x\exists y\forall z(z\in y \Leftrightarrow z=x)$$

Per l'assioma di estensionalità l'insieme z è unico e lo denoteremo con $\{x\}$. Questi primi assiomi permettono di asserire l'esistenza di un buon numero di insiemi. Infatti siamo sicuri dell'esistenza degli insiemi $\varnothing$, $\{\varnothing\}$,$\{\{\varnothing\}\}$, ...

[11] Da A1 e A2 segue che la teoria parla solo di insiemi e non di "elementi". Infatti se accettassimo la presenza di un "elemento" a che non contiene a sua volta elementi, allora a dovrebbe coincidere con l'insieme vuoto. Ciò significa che non ha senso considerare come insieme un insieme di oggetti che non siano a loro volta insiemi. Ad esempio l'insieme delle monete che ho in tasca non rientra in tale teoria. Questo rende il tutto poco naturale ma evita molte complicazioni. Un modo diverso di procedere sarebbe accettare che esistano due tipi di oggetti matematici: gli insiemi e gli elementi che non sono insiemi. Per gli elementi che non siano insiemi non vengono imposti i due assiomi A1 e A2.

Un modello dei primi tre assiomi. Nello spirito del metodo assiomatico non dobbiamo necessariamente interpretare gli oggetti che abbiamo chiamato "insiemi" e la relazione che abbiamo chiamato di "appartenenza" nel modo usuale. In effetti per avere una interpretazione si deve avere una collezione di elementi più una relazione binaria. Ad esempio se chiamiamo *insieme* un numero naturale e poniamo $n \in m$ se m è il successivo di n allora abbiamo che gli assiomi $A1$, $A2$ ed $A3$ sono soddisfatti. Infatti $A1$ segue dal fatto che la funzione successore è iniettiva. A2 è vera perché 0 non è successore di nessun elemento. A3 è verificata perché ogni numero naturale ha uno ed un solo successore. Non è invece verificato il seguente assioma.

A4. Assioma dell'unione di due insiemi. Dati due insiemi x ed y esiste un insieme z che ha come elementi o gli elementi di x oppure gli elementi di y.

$$\forall x \forall y \exists z (\forall z' (z' \in z \Leftrightarrow z' \in x \vee z' \in y))$$

L'insieme z per l'assioma di estensionalità è unico e viene indicato con $x \cup y$. Da tale assioma e da A3 segue che dati due insiemi x_1 e x_2 esiste l'insieme $\{x_1, x_2\} = \{x_1\} \cup \{x_2\}$ caratterizzato dal contenere solo gli elementi x_1, x_2. Più in generale, dati gli insiemi $x_1,...,x_n$ esiste l'insieme $\{x_1,...,x_n\} = \{x_1\} \cup ... \cup \{x_n\}$ che ha $x_1,...,x_n$ come unici elementi. Da notare che i numeri naturali non verificano A4 in quanto dati x ed y, con $x \neq y$, non è vero che esiste un z che è successore sia di x che di y.

L'assioma dell'unione di due insiemi può essere esteso in modo da ottenere l'unione di una classe qualunque di insiemi.

A5. Assioma dell'unione degli elementi di una classe. Di ogni classe di insiemi è possibile fare l'unione:

$$\forall x \exists y \forall z (z \in y \Leftrightarrow \exists z' (z' \in x \wedge z \in z')).$$

Per l'assioma di estensionalità l'insieme y di cui si dichiara l'esistenza è unico. Nel seguito lo denoteremo con $\cup x$ oppure $\cup \{x' : x' \in x\}$ e parleremo di *unione degli elementi di* x.

Dati due insiemi x ed y diremo che x *è una parte di* y e scriveremo $x \subseteq y$ se ogni elemento di x è anche un elemento di y, cioè se vale l'implicazione

$$z \in x \Rightarrow z \in y.$$

A6. Assioma dell'insieme delle parti: per ogni insieme x esiste un insieme y costituito da tutte e sole le parti di x:

$$\forall x \exists y \forall z (z \in y \Leftrightarrow z \subseteq x).$$

Per l'assioma di estensionalità l'insieme y è unico. Denoteremo tale insieme con $\mathcal{P}(x)$.

Il prossimo assioma postula l'esistenza di un insieme infinito. Per fare questo dobbiamo definire la nozione di funzione e poi quella di equipotenza.

Definizione 8.1. Dati due insiemi x ed y chiamiamo *coppia* di elementi x ed y l'insieme $\{x,\{x,y\}\}$.

Che tali insieme esista segue dal fatto che è l'unione degli insiemi $\{x\}$ ed $\{\{x,y\}\}$. Segue la solita definizione di prodotto cartesiano, di relazione e di funzione. Ciò permette di definire la nozione di equipotenza tra due insiemi.

Definizione 8.2. Chiameremo *infinito* un insieme che sia equipotente ad una sua parte propria.

A7. Assioma dell'infinito: esiste un insieme infinito.

A questo punto possiamo introdurre l'assioma di isolamento.

A8. Assioma di isolamento: sia p una proprietà descrivibile nel linguaggio della teoria degli insiemi, allora per ogni insieme z esiste un insieme z' tale che

$$x \in z' \Leftrightarrow x \in z \text{ ed } x \text{ verifica } p.$$

L'insieme z' viene indicato anche con $\{x \in z : x \text{ verifica } p\}$. Tale assioma coinvolge la nozione di *"proprietà descrivibile nel linguaggio della teoria degli insiemi"* e quindi richiederebbe una definizione rigorosa di tale concetto. Questo può essere fatto solo nell'ambito della logica matematica, qui ci limitiamo a dire che intendiamo riferirci a tutte le proprietà che possono essere descritte nel linguaggio della teoria degli insiemi, cioè utilizzando solo il simbolo di appartenenza $\in$ ed eventualmente i connettivi logici "non", "esiste", "per ogni", "oppure", "e".

Per completezza enunciamo anche l'ultimo assioma della teoria *ZF* che non è molto intuitivo ma molto utile per motivi tecnici. Nel seguito chiamiamo *funzionale* una proprietà $p(x,y)$ scritta nel linguaggio della teoria degli insiemi tale che per ogni x esiste un unico y per cui $p(x,y)$ sia vera. In altre parole una proprietà funzionale è una proprietà a due posti che quando venga interpretata definisce una funzione. Data una proprietà funzionale $p(x,y)$ ed un insieme z chiamiamo *immagine di z* tramite $p(x,y)$ un insieme z' tale che per ogni $x \in z$ esiste $y \in z'$ tale che $p(x,y)$ sia vera. Il prossimo assioma assicura che l'immagine di un insieme tramite una proprietà funzionale è ancora un insieme.

A9. Assioma di sostituzione: Sia $p(x,y)$ una proprietà funzionale. Allora per ogni insieme z esiste un insieme z' che è immagine di z tramite $p(x,y)$.

9. Assioma della scelta: dimostrarlo o confutarlo

L'elenco dei possibili assiomi per la teoria degli insiemi non si esaurisce con quelli che abbiamo dato. Il primo che si deve considerare per la sua importanza è l'assioma della scelta, che abbiamo già incontrato, senza il quale molti teoremi della matematica non possono essere provati. Ricordiamo cosa dice.

A10. (**Assioma della scelta)**. Ogni insieme non vuoto Σ di insiemi non vuoti ammette una funzione di scelta, cioè una funzione $f: \Sigma \to \cup\Sigma$ tale che $f(X) \in X$.

Si pone in modo naturale la questione se tale assioma possa essere derivato dagli altri assiomi. In alcuni casi particolari la risposta è positiva.

Proposizione 9.1. Se Σ è una classe di sottoinsiemi non vuoti di un insieme ben ordinato allora esiste una funzione di scelta su Σ. In particolare esiste una funzione di scelta se Σ è una classe di i sottoinsiemi di un insieme finito o numerabile.

Dim. Basta considerare la funzione f che associa ad ogni insieme in X in Σ il minimo elemento di X. Il resto della dimostrazione segue dal fatto che, come osservato nel primo volume, ogni insieme finito o numerabile ammette un buon ordinamento. □

Vale anche la seguente proposizione.

Proposizione 9.2. Se si considera una classe finita Σ di insiemi allora esiste di una funzione di scelta.

Dim. Infatti sia $\Sigma = \{X_1, X_2,...,X_n\}$ una classe finita di insiemi e supponiamo che tali insiemi siano non vuoti. Allora allora esistono $x_1 \in X_1$, $x_2 \in X_2$,…,$x_n \in X_n$ e pertanto esistono le coppie (X_1, x_1), (X_2, x_2),..., (X_n, x_n). Per l'assioma della coppia possiamo asserire che esiste anche l'insieme $\{(X_1, x_1), (X_2, x_2),..., (X_n, x_n)\}$ che è la funzione di scelta cercata. □

Tuttavia non è possibile estendere quanto ora visto al caso più generale in cui Σ è infinito. Infatti in tale caso, è ancora possibile "scegliere" un elemento x in ciascun X in Σ. Tuttavia questa volta nulla ci assicura che esista un insieme costituito da tutte le coppie (X,x) che si sono ottenute con queste infinite scelte. In altre parole niente ci assicura che la totalità di tali coppie costituisca una funzione. D'altra parte quando l' assioma della scelta fu proposto per la prima volta esso suscitò molte perplessità e reazioni negative. Infatti si aveva la tendenza a credere che un insieme esiste solo se si riescono a descrivere i suoi elementi tramite una proprietà comune. Similmente si era portati a pensare che una funzione esiste solo se è possibile definire in modo preciso quale è la legge che associa l'input all'output. Allora chi ci assicura che esiste sempre un criterio generale che permetta di scegliere all'interno di ogni insieme in Σ un suo elemento ?

Ad esempio, König riteneva di avere dimostrato che l'assioma della scelta non può essere vero.

Teorema 9.3. (**König**) Nell'insieme dei numeri reali non esiste un buon ordinamento. Pertanto l'assioma della scelta è falso.

Dim. Supponiamo per assurdo che il campo R dei numeri reali ammetta un buon ordinamento (che naturalmente non coincide con l'ordinamento usuale tra numeri reali). Riprendendo il discorso fatto quando nel primo volume abbiamo esposto il paradosso di Berry, chiamo *"definibile"* un numero reale r tale che, battendo sulla tastiera del mio computer un certo numero di carat-

teri ottengo una descrizione in lingua italiana di tale numero. Ad esempio la radice positiva di 2 è definibile poiché è l'unico numero reale che soddisfi la condizione $(x^2=2)\wedge(x>0)$. Consideriamo ora l'insieme dei numeri reali che sono definibili. Come dimostreremo nel capitolo 4 nel paragrafo sulla definibilità e la numerabilità, tale insieme è numerabile. Pertanto, non essendo R numerabile, l'insieme dei numeri non definibili ha la potenza del continuo e quindi non è vuoto. Consideriamo ora la frase *"*il più piccolo numero non definibile*"* in cui ci si riferisce al buon ordinamento che abbiamo supposto esistente per ipotesi. Tale frase è ovviamente una definizione in italiano di un numero $\underline{r}$ che risulta quindi definibile. D'altra parte, poiché il minimo di un insieme appartiene all'insieme, il numero $\underline{r}$ non è descrivibile. Ciò è un assurdo e quindi non può esistere un buon ordinamento in R.

Infine, poiché, come osserveremo meglio nel seguito, l'assioma della scelta è equivalente all'affermazione che ogni insieme ammette un buon ordinamento, possiamo concludere che esso non vale. □

Tale teorema è tuttavia sbagliato anche se non è chiaro dove sia l'errore della dimostrazione. Infatti lo schema adottato è lo stesso del paradosso di Berry e quindi se accettassimo la sua validità dovremmo accettare anche che l'ordinamento usuale in N non sia di buon ordinamento. Questa cosa sarebbe difficile da digerire perché equivarrebbe ad ammettere l'esistenza di una successione infinita di numeri interi positivi sempre più piccoli.

In realtà non è possibile dimostrare la falsità dell'assioma della scelta come non è possibile provarne la verità a partire dai rimanenti assiomi. Infatti vale il seguente teorema la cui dimostrazione, che richiede nozioni avanzate di logica matematica, omettiamo.

Teorema 9.4. (Paul Joseph Cohen 1963) L'assioma della scelta è indipendente dai rimanenti assiomi.

La teoria che si ottiene aggiungendo a *ZF* l'assioma della scelta viene denotata con *ZFC* (la lettera *C* è l'iniziale di "choice" che appunto significa "scelta" in inglese).

10. Ipotesi del continuo

Un altro assioma particolarmente importante è l'ipotesi del continuo. Abbiamo visto che la potenza di $\mathcal{P}(N)$ è strettamente maggiore di quella di N. Appare allora naturale chiedersi se esistono insiemi che hanno potenza maggiore del numerabile e minore di quella di $\mathcal{P}(N)$. Cantor formulò l'ipotesi per cui non esiste un tale insieme. Trasformiamo questa ipotesi in un assioma.

A11. Ipotesi del continuo. Non esiste un insieme che abbia potenza strettamente maggiore del numerabile e strettamente minore del continuo.

Detto in altri termini l'ipotesi del continuo afferma che nel piano euclideo esistono solo insiemi finiti, numerabili o aventi la potenza del continuo. Per molti anni nessun matematico ha saputo confutare o provare l'ipotesi del continuo. Nel 1963 il logico matematico Cohen ha dato una risposta a tale ipotesi mostrando che è indipendente dai rimanenti assiomi della teoria degli insiemi.

Teorema 10.1. (Teorema di Cohen). L'ipotesi del continuo è indipendente dai rimanenti assiomi.

In altre parole l'ipotesi del continuo non può ne' essere provata ne' essere confutata a partire dai sistemi di assiomi che usualmente vengono accettati per la teoria degli insiemi. Più in generale è stata provata anche l'indipendenza della seguente asserzione.

Ipotesi generalizzata del continuo. Dato un insieme infinito S non esiste un insieme che abbia potenza strettamente maggiore di S e strettamente minore di $\mathcal{P}(S)$.

L'ipotesi generalizzata del continuo può essere espressa anche utilizzando la teoria dei numeri cardinali.

Ipotesi generalizzata del continuo. Per ogni cardinale x non esiste nessun cardinale tra x e 2^x.

Se si accetta tale ipotesi i cardinali possono essere ordinati nella seguente successione crescente:

$1 < 2 < 3 < \ldots < \aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \ldots$

ed tra due elementi della successione non è possibile trovare nessun altro cardinale.

In definitiva:

risultano indipendenti dal sistema-base degli assiomi per la teoria degli insiemi sia l'ipotesi del continuo che l'assioma della scelta.

Si ripresenta allora per la teoria degli insiemi la stessa situazione dell'assioma delle parallele in geometria. Così come coesistono geometrie euclidee e geometrie non euclidee, è possibile sviluppare sia teorie degli insiemi in cui vale l'ipotesi del continuo che teorie in cui vale l'ipotesi opposta.

Da notare che, oltre che dai paradossi, che si spera possano essere eliminati da una opportuna assiomatizzazione, il ruolo della teoria degli insiemi viene messo in crisi ancora di più dalle dimostrazioni di indipendenza. Abbiamo già visto come l'indipendenza dell'assioma delle parallele in geometria con il mostrare la possibilità di più geometrie avesse tolto il ruolo centrale che la geometria euclidee aveva sempre assunto. Allo stesso modo, l'indipendenza dell'ipotesi del continuo con il mostrare la possibilità di più teorie degli insiemi diverse tra loro pone il problema di quale sia quella giusta e toglie quindi il carattere assoluto che si pensava avesse l'intuizione della nozione di insieme.

Problema. Sia X un insieme numerabile di punti di un foglio di carta e supponiamo che una macchia di inchiostro cada sul foglio in modo da coprire X. Dire quale è la cardinalità della macchia di inchiostro.

11. Categoricità, completezza, consistenza, indipendenza

Se si adotta il metodo assiomatico è essenziale considerare alcune nozioni come quelle di consistenza categoricità, completezza, consistenza ed indipendenza. Le definizioni che daremo non possono essere rigorose poichè solo nell'ambito dell'approccio formale della logica matematica lo potrebbero essere. La prime due nozioni sono la soddisfacibilità e la categoricità..

Definizione 11.1. Una teoria T viene detta *soddisfacibile* se ammette almeno un modello, viene detta *categorica* se è soddisfacibile e tutti i suoi modelli sono isomorfi tra loro.

Quando una teoria è categorica i matematici a volte dicono anche che "esiste un unico modello a meno di isomorfismi".

Esempi: La teoria delle terne di Peano e la teoria dei campi completi sono complete. La teoria dei gruppi con cinque elementi è categorica. Il sistema di assiomi della geometria euclidea è categorico.

Esempi: La teoria dei gruppi non è categorica (ammette per esempio sia modelli finiti che modelli infiniti). La teoria degli anelli non è categorica (basti pensare all'anello Z degli interi ed all'anello Q dei numeri razionali. La teoria degli insiemi ordinati non è categorica (l'intervallo [0,1] e l'intervallo aperto (0,1) non sono isomorfi perché il primo contiene un minimo ed il secondo no).

Data una teoria T ed una asserzione α indicheremo con l'espressione $T \vdash \alpha$ il fatto che α è un teorema di T, cioè che esiste una dimostrazione di α che utilizza come ipotesi formule in T. Scriviamo invece $T \vDash \alpha$ per indicare che ogni modello di T verifica la formula α.

Definizione 11.2. Una teoria T viene detta *consistente* se non esiste nessuna asserzione α tale che $T \vdash \alpha$ e $T \vdash \neg\alpha$.

Si osservi che poiché la nozione di consistenza dipende da quella di dimostrazione, essa dipende anche dal tipo di apparato deduttivo che si considera. La stessa cosa può essere detta per le successive nozioni di indipendenza e di completezza. Non entramo nel merito di tale questione che può essere trattata adeguatamente solo nell'ambito della logica matematica e ci manteniamo ad una nozione intuitiva di dimostrazione[12]. In tutte le logiche la nozione di dimostrazione viene in ogni caso definita in modo che

[12] E' opportuno sottolineare che nel caso del calcolo proposizionale e della logica del primo ordine questa dipendenza è solo apparente in quanto tutti gli apparati deduttivi danno luogo alla stessa nozione di teorema. Nel caso della logica del secondo ordine invece non è possibile trovare un apparato adeguato (non può essere provato un teorema di completezza) e quindi non è possibile fornire una definizione soddisfacente di consistenza.

se $T \vdash \alpha$ allora $T \models \alpha$ cioè in modo che se α è un teorema di T allora ogni modello di T verifica α. Ciò permette di dimostrare la seguente implicazione

$$T \text{ soddisfacibile} \Rightarrow T \text{ consistente.}$$

Infatti supponiamo che T ammetta un modello M, allora se esistesse per assurdo α tale che $T \vdash \alpha$ e $T \vdash \neg\alpha$, avremmo anche che $T \models \alpha$ e $T \models \neg\alpha$ e quindi che in M l'asserzione α deve essere sia vera che falsa[13]. Tale implicazione mostra che un modo per provare che una teoria è consistente è mostrare che è soddisfacibile.

Esempi: La teoria dei gruppi è consistente. Infatti se la teoria dei gruppi fosse inconsistente allora, preso ad esempio il gruppo additivo degli interi relativi $(Z,+)$, in tale gruppo dovrebbe valere sia α che $\neg\alpha$. Un esempio di teoria inconsistente è dato dalla teoria degli insiemi ingenua, come mostrano le antinomie. D'altra parte tutte le teorie studiate in algebra sono consistenti (altrimenti non avrebbe senso studiarle).

Esempi: Un esempio di teoria inconsistente è la teoria T degli insiemi ordinati finiti che non hanno elementi minimali. Infatti se un insieme ordinato $(S,\leq)$ non ha elementi minimali, allora preso un elemento $x \in S$ esiste un $x_1 < x$. Poiché x_1 non può essere minimale allora esiste $x_2 < x_1$, … procedendo in questo modo si prova l'esistenza di una successione infinita di elementi x_n di S tutti diversi tra loro. Ciò prova che esistono infiniti elementi in S. Pertanto in T può essere dimostrata sia l'asserzione "esistono infiniti elementi" che l' asserzione "non esistono infiniti elementi".

Definizione 11.3. Una teoria T viene detta *indipendente* se non esiste $\alpha \in T$ tale che $T\text{-}\{\alpha\} \vdash \alpha$.

In altre parole una teoria è indipendente se nessun assioma può essere eliminato in quanto dimostrabile a partire dagli altri assiomi. In generale le teorie che si studiano sono, oltre che consistenti, anche indipendenti. Infatti se un assioma α fosse dimo-

[13] Nella logica del primo ordine e nel calcolo proposizionale è possibile anche invertire tale implicazione e quindi provare che per tali logiche la soddisfacibilità coincide con la consistenza.

strabile a partire da altri, allora lo si potrebbe semplicemente cancellare senza alterare la teoria stessa.

Definizione 11.4. Data una teoria T diciamo che una asserzione α è *indipendente* da T se non accade né che $T \vdash \alpha$ né che $T \vdash \neg\alpha$ cioè α non può essere né provata né confutata a partire dagli assiomi di T.

Definizione 11.5. Una teoria T è detta *completa* se per ogni α o $T \vdash \alpha$ oppure $T \vdash \neg\alpha$.[14]

Equivalentemente possiamo chiamare completa una teoria tale che non esistono asserzioni che non dipendano da T.

Esempio: Sia T l'insieme degli assiomi della geometria euclidea tranne l'assioma delle parallele e sia α l'assioma delle parallele. Allora abbiamo visto che α è indipendente da T.

Esempio: Ad esempio sia T la teoria dei gruppi ed α la proprietà commutativa, allora α non può essere dimostrata (perché in tale caso tutti i gruppi sarebbero commutativi). D'altra parte nemmeno $\neg\alpha$ può essere dimostrata (perché in tale caso tutti i gruppi sarebbero commutativi). Pertanto α è indipendente da T. Questo mostra anche che la teoria dei gruppi non è completa.

12. Tre diverse ideologie per il metodo assiomatico

Fino ad ora abbiamo esposto esempi di applicazione del metodo assiomatico che sono stati proposti allo scopo di trovare un fondamento sicuro alla geometria, all'analisi (tramite la teoria dei numeri reali) ed alla teoria degli insiemi. Chiameremo *fondazionale* un tale modo di utilizzare il metodo assiomatico. È necessario però specificare che tale metodo attualmente viene utilizzato con uno spirito completamente diverso ed in chiave che viene detta *strutturalista* per il ruolo importante che gioca la nozione di

[14] Da notare che tale nozione di completezza, che si riferisce ad un sistema di assiomi, è completamente diversa dalla nozione di completezza per un campo ordinato che si riferisce alla relazione d'ordine in una particolare struttura.

struttura matematica.[15] Nel seguito esporremo man mano le idee dello strutturalismo evidenziandone le differenze con l'approccio fondazionale di Hilbert e con il metodo presente negli *Elementi* di Euclide. Ci riferiamo a tale scopo ad alcuni aspetti fondamentali della matematica.

Creazione o sistemazione

Hilbert e Euclide. Il punto di vista fondazionale di Hilbert e l'approccio assiomatico di Euclide non hanno lo scopo di "creare" nuova matematica, di trovare nuovi risultati. Piuttosto si concentrano solo sulla organizzazione logica (Euclide) e sulla giustificazione (fondazione) della matematica già esistente. Infatti i *Fondamenti della Geometria* di Hilbert rappresentano un rifacimento, senza imperfezioni dal punto di vista assiomatico, della geometria di Euclide, rifacimento che si mantiene abbastanza vicino all'originale. Gli *Elementi* di Euclide sono essenzialmente una esposizione logicamente ordinata dell'insieme dei teoremi conosciuti all'epoca.

Strutturalisti. Per la scuola strutturalista il metodo assiomatico viene invece utilizzato per cogliere la struttura comune a diversi rami della matematica allo scopo di unificare trattazioni diverse. È una scelta dettata da questioni che potremmo dire di organizzazione del lavoro scientifico e non da esigenze di fondazione o di analisi critica. Ad esempio gli assiomi della teoria dei gruppi colgono proprietà comuni a strutture matematiche disparate come il gruppo additivo dei reali, il gruppo degli interi modulo un intero m, il gruppo delle isometrie del piano, il gruppo delle permutazioni di un insieme in sé, e così via. Spesso i teoremi sono estensioni e generalizzazioni di teoremi già noti ma che si riferivano casi particolari. In tale senso si produce nuova matematica e nuovi e più generali teoremi.

[15] Tra i fautori più radicali dello strutturalismo, ricordiamo il gruppo di matematici francesi che si autodefiniscono Bourbakisti e che hanno scritto una notevole serie di libri tutti firmati con il nome di un matematico inesistente che hanno chiamato Bourbaki. Da notare che la classe delle strutture matematiche è molto più ampia di quella della classe delle strutture del primo ordine considerate nell'Appendice del primo volume. Essa comprende ad esempio gli spazi topologici, gli spazi vettoriali ed altro.

Intuizione.

Euclide. In Euclide l'intuizione è lo strumento mediante il quale si perviene alla conoscenza degli enti matematici e delle loro proprietà fondamentali. Che gli assiomi, per meglio dire i postulati, siano fortemente intuitivi è cosa essenziale perché solo questa loro immediatezza assicura la bontà di tutta la teoria che si vuole costruire (e rende possibile "postulare" per una loro accettazione). In definitiva la scelta del sistema di assiomi poggia direttamente sulla intuizione ed è, in un certo senso, ad essa successiva. Naturalmente l'intuizione non deve invece essere uno strumento di dimostrazione anche se essa conserva un ruolo euristico (in ciò Euclide non differisce dai moderni matematici).

Comunque l'intuizione di un buon matematico non conduce ad errori ed è solo per motivi di "purezza intellettuale" che non può servirsene in una trattazione scientifica di un argomento.

Hilbert. In Hilbert, poiché il metodo assiomatico ha lo scopo di fondare un settore della matematica preesistente alla assiomatizzazione, un adeguato sistema di assiomi per la geometria deve solo essere abbastanza potente da permettere di ottenere tutti i teoremi della geometria euclidea. Non è detto perciò che i singoli assiomi debbano essere "intuitivi". Naturalmente, nel caso in questione, gli assiomi di Hilbert ereditano il carattere intuitivo degli assiomi di Euclide ma, se ne avesse avuto bisogno, Hilbert non avrebbe esitato ad introdurre un sistema di assiomi completamente diverso il cui requisito avrebbe dovuto essere solo di essere capace di dimostrare in maniera elegante e rapida l'insieme delle proposizioni della geometria euclidea. L'intuizione comunque può essere forviante perché può portare a dare per scontato qualche cosa che invece deve essere dimostrato.

Strutturalisti. In maniera ancora più radicale per la scuola strutturalista l'intuizione è cosa più da combattere che da utilizzare ed essa non ha assolutamente valore euristico. Ad esempio se ogni volta che si parla dei gruppi ci si immagina il gruppo additivo dei reali, allora si è portati ad attribuire ai gruppi più proprietà di quante siano deducibili dal dato sistema di assiomi (ad esempio la commutatività). In altri termini, poiché per gli strutturalisti una teoria deve descrivere una intera classe di strutture diverse tra loro, è forviante nelle dimostrazioni guardare troppo ad una particolare struttura.

Categoricità.

Euclide. In Euclide la categoricità del sistema di assiomi è una questione che, in un certo senso, non si pone. Infatti il suo sistema di assiomi aveva l'unico scopo di descrivere in modo adeguato il modello fornito dall'idea platonica di punto, retta, circonferenza. Tale modello è il punto di partenza ed era considerato l'unico possibile. Pertanto non poteva mai porsi il problema della esistenza di un modello degli assiomi di Euclide diverso da quello naturale (non esistevano due mondi delle idee !).

Hilbert. Hilbert invece si pone esplicitamente la questione della categoricità, anzi la considera un requisito essenziale per il suo sistema in quanto la bontà del sistema di assiomi proposto consiste proprio nella capacità di individuare esattamente l'oggetto matematico a cui si vuole dare una base solida, ad esempio per quanto riguarda la geometria individuare il piano euclideo. Era anche importante provare la categoricità per il sistema di assiomi dei numeri interi, dei numeri reali ed altro.

Strutturalisti. In questo caso la bontà di tale teoria si misura nella sua capacità ad abbracciare quanti più "oggetti matematici". Un teorema della teoria dei gruppi è importante poiché fornice informazioni su una vasta classe di strutturee. Per gli strutturalisti se una teoria è categorica non è molto utile. Infatti se si vuole appurare se una asserzione α è conseguenza o meno degli assiomi della teoria allora tanto vale di andare a vedere direttamente se α vale su tale modello. Consideriamo ad esempio l'intero sistema di assiomi della geometria di Hilbert; si sa che tale sistema è categorico e che quindi tutti i modelli sono isomorfi tra loro ed in particolare sono equivalenti al modello analitico (cioè ad R^2). Allora dovendo verificare se una proposizione è vera oppure no, non conviene cercare di dedurla dal sistema di assiomi; è più semplice verificarne direttamente la validità su R^2 mediante alcuni semplici calcoli.

Completezza

Euclide. Anche se non esplicitamente menzionata è evidente che nella tradizione Euclidea la completezza di una teoria matematica era considerata un requisito importante. Un sistema di assiomi per la geometria per cui esista una asserzione non dimostrabile e non confutabile è evidentemente inadeguato a rappresentare

l'intuizione geometrica. D'altra parte da Euclide fino agli inizi dell'ottocento si era convinti che questo assioma fosse in realtà dimostrabile e gli sforzi per dimostrarlo mostravano che si aveva il convincimento della completezza della teoria ottenuta cancellandolo.

Hilbert. In Hilbert la completezza è essenziale in quanto è essenziale la categoricità che, appunto, comporta la completezza. Se una teoria non è completa non può certo sperare di fondare qualche struttura matematica.

Strutturalisti. Anche per gli strutturalisti può essere ripetuto quanto detto per la questione della categoricità. Una buona teoria non deve essere completa in quanto deve essere la parte comune di più teorie diverse tra loro.

Consistenza.

Euclide. Anche il problema della consistenza non poteva essere problema riguardante Euclide. Infatti il sistema di postulati proposto era un elenco di proprietà di un modello preesistente di cui l'uomo ha diretta ed innata conoscenza. Ma se un sistema di assiomi viene costruito isolando alcune proprietà di un dato modello allora esso è necessariamente consistente. Se infatti fossero deducibili sia una formula α che una sua negata $\neg\alpha$, allora per il modello di partenza esisterebbe una proposizione che è sia vera che falsa, il che non può accadere.

Hilbert. Per Hilbert il problema della consistenza è essenziale, non esiste un mondo geometrico da descrivere, esiste solo un sistema di assiomi e niente assicura che tale sistema sia stato scelto male e che ci si accorga che esso permette di dimostrare sia che valga una cosa che valga il contrario. Facciamo un esempio, e supponiamo che Hilbert avesse messo tra gli assiomi della sua teoria anche l'assioma

α = *"l'insieme dei punti nel piano è numerabile"*.

La teoria risultante *T* sarebbe apparsa degna di interesse e si sarebbero prodotti molti teoremi di tale teoria. Purtroppo, Hilbert ad un certo punto sarebbe giunto a dimostrare (cosa che fa nel suo libro) che *T* permette di introdurre un sistema di coordinate che utilizza il campo dei numeri reali. Ciò avrebbe comportato la validità di

$\neg\alpha$ = *"l'insieme dei punti nel piano non è numerabile"*

È ovvio allora che la teoria *T*, non potendo ammettere modelli, sarebbe risultata priva di ogni interesse.

Come fare a dimostrare che la teoria dei campi ordinati completi (cioè la teoria dei numeri reali) è consistente ? E' vero che possiamo "costruire" un modello utilizzando, ad esempio, il metodo delle successioni di Cauchy. Tuttavia questo modo di procedere non è molto accettabile dal punto di vista fondazionale. Infatti non si può utilizzare la cosa da fondare (il modello) per giustificare un sistema di assiomi (la teoria) che ha come scopo proprio quello di fare a meno del modello.

Strutturalisti. Molto meno importante è la questione della consistenza per gli strutturalisti. È vero che tale questione in linea di principio si pone, ma, di fatto, una teoria viene proposta solo allo scopo di unificare lo studio di una serie di modelli matematici preesistenti. Pertanto tale teoria sarà, come per Euclide, automaticamente soddisfacibile e quindi consistente. Ad esempio, il problema della consistenza della teoria dei gruppi non si è mai posto in quanto tale teoria nasce successivamente alla considerazione di alcuni gruppi concreti.

Il problema dei fondamenti.

Sia in Euclide che in Hilbert l'assiomatizzazione risponde al problema di dare un fondamento sicuro all'intero edificio della matematica. Negli strutturalisti l'atteggiamento è più pragmatico e "locale". Essi non pretendono di dare una volta per tutti un sistema di assiomi su cui fondare tutta la matematica. Piuttosto essi pensano che la matematica si possa smembrare in diversi settori i quali si possono esaminare indipendentemente uno dall'altro. Ad esempio J. Dieudonnè, uno dei fondatori dello strutturalismo in matematica, afferma

> *Il matematico moderno si sente così perfettamente in pace con la sua coscienza e non si preoccupa affatto di tutti gli pseudo-problemi che hanno preoccupato i suoi predecessori.*

Gli pseudo-problemi di cui si parla sono i paradossi che non sembrano interessare più di tanto gli strutturalisti. Se anche una singola teoria risultasse essere contraddittoria, ciò non comporterebbe il crollo di tutto l'edificio matematico, ma semplicemente un piccolo cambio di indirizzo (un indebolimento di qualche as-

sioma). Inoltre mentre la dimostrazione della coerenza dei sistemi di assiomi per l'aritmetica e la geometria presentano difficoltà insormontabili, lo stesso non avviene per molte "piccole" teorie esaminate dagli strutturalisti. La loro coerenza si può mostrare spesso semplicemente esibendo dei modelli finiti (come avviene per la teoria dei gruppi, dei campi, degli anelli ed altro). E poi le questioni relative ai fondamenti della matematica non devono infastidire i matematici di professione. Si provvederà ad addestrare appositamente del personale "paramatematico" (i logici) che se ne occupino.

Tutte le questioni come la non contraddizione delle teorie . . . ed in generale tutto ciò che concerne la teoria della dimostrazione fanno parte ora di una scienza completamente separata dalla matematica, la metamatematica; questa nuova disciplina non cessa di svilupparsi ed ha già fornito numerosi risultati nuovi e pieni di interesse; ma è perfettamente lecito al matematico ignorarla completamente senza essere per nulla preoccupato nelle sue ricerche (è sempre Dieudonnè che parla).

Nota. La distinzione tra approccio fondazionale ed approccio strutturalista al metodo assiomatico è di un certo interesse da un punto di vista didattico. Infatti il metodo assiomatico nelle scuole può essere introdotto o tramite un sistema di assiomi per la geometria euclidea (Hilbert) oppure tramite la nozione di gruppo o di insieme ordinato (Bourbakismo). Nel primo caso la scelta fondazionale presenta difficoltà se gli studenti non sono stati stimolati verso interessi epistemologici. Infatti per essi sembrerà strano che si debba perdere tanto tempo per dimostrare cose che appaiono ovvie. Inoltre l'esistenza di un unico modello renderà difficile far capire questioni di indipendenza. Infine il carattere estremamente intuitivo di tale modello farà scomparire in modo completo la questione dell'indipendenza. Nel secondo caso l'approccio unificante del metodo assiomatico in chiave strutturalista può essere compreso dagli alunni solo se prima sono stati esibiti molti esempi di strutture diverse che però sono suscettibili di una trattazione unificata. Ad esempio dovrebbero essere prima introdotti alcuni gruppi particolari come quello delle simmetrie di una figura, quello delle permutazioni di un insieme, quello dei movimenti del piano e così via.

DIVAGAZIONI

Strutturalismo e divisione del lavoro

La matematica è sempre stata divisa in tanti settori quanti sono gli oggetti matematici da studiare. Così la geometria era la scienza dello spazio (che a sua volta si divideva in piana e solida), l'aritmetica la scienza delle quantità, l'analisi la scienza delle quantità infinitamente piccole e di quelle infinitamente grandi e così via. Con lo strutturalismo tale divisione della matematica viene messa in discussione. Ad esempio la geometria si smembra in vari settori completamente indipendenti tra loro. In buona parte viene sostituita dalla geometria analitica intesa come algebra lineare e teoria delle matrici. Lo studio delle coniche e delle quadriche diviene un caso particolarissimo di un altro settore, la geometria algebrica, una teoria completamente algebrizzata. Lo studio dei movimenti del piano rientra nella teoria dei gruppi. Lo studio delle aree e delle lunghezze nella teoria della integrazione. A sua volta l'aritmetica viene smembrata nello studio di diverse strutture algebriche, l'analisi matematica in parte si traduce nella teoria degli spazi topologici, in quella degli spazi metrici o normati. Per dirla in maniera più specifica, si perviene ad una nuova divisione della matematica basata sul fatto che tutte le strutture fino ad ora studiate sono riconducibili per la loro forma logica e non per il loro contenuto alle seguenti tre categorie:

(*a*) strutture algebriche
(*b*) strutture relazionali
(*c*) strutture topologiche.

Le strutture algebriche sono quelle che fanno riferimento solo alle operazioni. Esempi sono la teoria dei gruppi, dei campi, degli spazi vettoriali. Le strutture relazionali sono quelle che fanno riferimento alle relazioni. Esempi sono dati dalla teoria degli insiemi ordinati e dalla teoria dei grafi. Infine le strutture topologiche sono quelle che fanno riferimento a particolari insiemi di parti chiamati topologie. In tali strutture è possibile esaminare i concetti di convergenza e continuità. Da tale punto di vista, in un certo senso, la geometria euclidea non trova una soddisfacente collocazione. È una struttura troppo "confusa" in cui sono presenti sia aspetti algebrici (il campo dei numeri reali per la coordinatizzazione, lo spazio vettoriale delle traslazioni, il gruppo dei movimenti del piano), sia aspetti relativi all'ordinamento ed alla

relazione "essere tra" (ricordiamo che in ogni retta si definiscono in modo naturale due ordinamenti) sia la struttura topologica (l'usuale topologia generata dai rettangoli che viene studiata in analisi). D'altra parte il campo dei numeri reali che è alla base della geometria euclidea è una struttura algebrica con un ordinamento ed una struttura topologica.

Divisione del lavoro, specializzazione. Il nuovo modo di organizzare la matematica degli strutturalisti ha permesso lo svilupparsi anche nell'ambito della matematica di alcuni fenomeni noti, per chi si interessa di sociologia o di politica, sotto il nome di divisione del lavoro, specializzazione e alienazione. È esperienza comune delle maggior parte degli studenti del corso di laurea in matematica il fatto che ogni materia di esame è completamente scollegata alle altre e, tranne il caso dell'analisi matematica che non risente molto dell'influenza strutturalista, anche con gli studi degli anni precedenti. È possibile seguire un corso di topologia senza conoscere niente di algebra e viceversa e si possono capire entrambi senza avere nessuna conoscenza matematica precedente. Si badi che non si tratta di mancanza di coordinamento e di organizzazione e neanche di volontà di andare incontro alle esigenze dello studente non richiedendo prerequisiti. È invece un modo di concepire la matematica come corpo di conoscenze che si può parcellizzare in unità autonome tra loro ed autonome dalle altre scienze. Questa parcellizzazione, consentendo una divisione del lavoro ed una estrema specializzazione, diventerebbe uno strumento formidabile per produrre una grande quantità di risultati scientifici. Ciò in contrapposizione con i risultati artigianali di una volta. Vediamo ad esempio cosa dicono Giorgio Israel e Lucio Lombardo Radice in Storia della Scienza (Ed. Universale Laterza, vol. II).

"L'introduzione del metodo assiomatico realizza una trasformazione del lavoro matematico che, secondo i Bourbakisti, è paragonabile alla transizione dal lavoro di tipo artigianale ad un lavoro di "fabbrica". Il matematico non procede più, come l'artigiano, inventando di volta in volta metodi nuovi e stratagemmi per risolvere il problema specifico di fronte al quale si trova; al contrario, se egli incontra relazioni che soddisfano gli assiomi di una struttura già nota, può fare uso di tutto l'arsenale del tipo di struttura individuata."

E, più avanti, continuano

"Come l'organizzazione del lavoro tayloristica significa da un lato controllo del singolo processo, dall'altro lato parcellizzazione ed alienazione da una finalità complessiva, così all'introduzione dei metodi standard legati al metodo assiomatico fa riscontro il carattere "anarchico" ed incontrollato dei rapporti tra matematica e scienza sperimentale, la rinuncia definitiva ad ogni spiegazione complessiva dei fenomeni naturali. Ma non soltanto a questo livello si riflette il taylorismo della concezione Bourbakisti, bensì anche all'interno della ricerca matematica, dove lo studio delle strutture prende il piede sullo studio dei problemi ed implica ancora una volta la perdita di consapevolezza del ricercatore in merito agli indirizzi complessivi della ricerca."

Concludiamo questo paragrafo riportando l'opinione di John von Neumann (1903-1957), uno dei matematici più versatili del *XX* secolo, espressa nell'articolo *The Mathematician* (1947).

"Quando una disciplina matematica si allontana di molto dalla sua fonte empirica o, il che è ancor peggio, se per due o tre generazioni viene ispirata solo indirettamente dalla «realtà», essa corre pericoli estremamente gravi. Diventa sempre più un'attività puramente estetica, sempre più l'art pour l'art. Questo fatto non è necessariamente negativo, se il campo è attorniato da soggetti che mantengono stretti legami empirici, oppure se la teoria è dominata dall'influenza di uomini con uno spirito di altissimo livello. Ma esiste il grave pericolo che la disciplina si sviluppi lungo la linea che offre minor resistenza; è possibile che la corrente, così lontana dalla sua fonte, si separi in una moltitudine di diramazioni insignificanti e quella disciplina diventi una massa disorganizzata di dettagli e nozioni complesse. In altre parole, una disciplina matematica che si trovi a grande distanza dalla sua fonte empirica, o abbia generato per troppo tempo molte filiazioni sterili e astratte, corre il rischio di degenerare. Da principio lo stile è generalmente classico; quando mostra segni di diventare barocco, ecco il segnale di pericolo […]. In ogni caso, una volta raggiunto questo stadio mi sembra che l'unico rimedio sia ringiovanire ritornando alla fonte: occorre introdurre nuovamente idee derivate, in minore o maggior grado, dall'esperienza. Sono convinto che questa sia stata una condizio-

ne necessaria per conservare la freschezza e la vitalità della matematica, e che altrettanto valga per il futuro".

CAPITOLO 4
LA LOGICA PER I FONDAMENTI[1]

"...se si lodano gli uomini che hanno determinato il numero di corpi regolari, che non ha utilità alcuna se non in quanto è piacevole a contemplarsi, quanto sarà più meritorio ridurre a leggi matematiche il ragionamento umano, che è ciò che di più eccellente e di più utile possediamo." (W. G. Leibniz).

"C'è qualcosa di più importante della logica: è l'immaginazione." (Alfred Hitchcock)

1. Hilbert contro l'infinito

Abbiamo visto che il problema della non contradditorietà di un dato sistema di assiomi *T* è centrale per la concezione ipotetico-deduttiva di Hilbert. Ora i problemi di non contradditorietà di una teoria si risolvono usualmente mostrando un modello di tale teoria, mostrando cioè che essa è soddisfacibile.[2] Ad esempio la consistenza della geometria non euclidea[3] viene provata dal modello di Klein o da uno dei tanti modelli di cui abbiamo già parlato. D'altra parte tali modelli vengono costruiti a partire dal modello euclideo e quindi la dimostrazione di non contraddittorietà delle geometrie non euclidee è valida a patto che la geometria euclidea sia affidabile. In altre parole:

riusciamo a provare che la teoria delle geometrie non euclidee è consistente solo provando che il sistema di assiomi per la geometria euclidea è consistente.

---

[1] La logica matematica è un argomento i cui contenuti non possono essere certamente concentrati in poche pagine. Tuttavia non è possibile parlare di fondamenti della matematica senza parlare di logica matematica. Quindi, anche a rischio di essere approssimativo e di omettere dimostrazioni fondamentali, non posso fare a meno di dedicare un rapido capitolo a tale argomento.

[2] Come abbiamo già detto nel capitolo precedente, una teoria si dice *soddisfacibile* se ammette un modello, si dice *consistente* se da tale teoria non è possibile ricavare una contraddizione. Ovviamente se una teoria è soddisfacibile è anche consistente e pertanto per provare la consistenza di una teoria è sufficiente esibirne un modello.

[3] Cioè la consistenza del sistema di assiomi che si ottiene sostituendo nel sistema di postulati di Euclide il quinto postulato con la sua negazione

A questo punto si potrebbe dire che è facile provare tale consistenza, basta costruire il modello analitico basato sui numeri reali. Ma come giustificare i numeri reali ? Coerentemente con il metodo assiomatico, possiamo fornire un sistema di assiomi per i numeri reali (ad esempio tramite la nozione di campo completo). Ovviamente ciò conduce al seguente fatto:

riusciamo a provare che il sistema di assiomi della geometria euclidea è consistente solo provando che la teoria dei campi completi è consistente.

Ancora una volta sembra che non ci siano difficoltà: infatti abbiamo mostrato come, ad esempio con il metodo delle sezioni, sia possibile il campo dei reali e quindi un modello della teoria dei campi completi. Purtroppo però sia per dimostrare l'esistenza di una terna di Peano sia per effettuare una delle tante costruzioni dei numeri reali dobbiamo servirci della teoria degli insiemi. In definitiva, se ci potessimo fidare della teoria degli insiemi, avremmo risolto tutti i problemi e ci potremmo fermare:

riusciamo a provare la consistenza delle varie teorie utilizzate in matematica solo se la teoria degli insiemi è consistente.

Sfortunatamente la scoperta dei paradossi mostra che la nozione di insieme è alquanto inaffidabile e che quindi si deve procedere ad una sua buona assiomatizzazione. Ora è vero che esistono diverse teorie assiomatiche degli insiemi che permettono di evitare tutti i paradossi fino ad ora noti, ma chi ci assicura che un giorno non vengano scoperti paradossi anche per tali nuove teorie ? Il problema appare senza soluzioni.

Ora Hilbert pensò che tutte le difficoltà nascessero dalla considerazione dell'infinito attuale che già tanta diffidenza aveva suscitato da Pitagora in poi. Infatti, come abbiamo già osservato, nessuno dubita della consistenza della teoria dei gruppi perché non è difficile fornire "concretamente" esempi di gruppi finiti. Esaminiamo in proposito un passo dall'articolo di Hilbert *Sull'infinito* apparso nel 1925.[4]

[4]In questo passo viene fatto riferimento alla *"operazioni sull'infinitamente piccolo"* tipiche dell'analisi matematica. Si deve pensare che prima dell'attuale definizione di limite (in termini di quantificatori universali ed esistenziali) le nozioni di limite e di derivata venivano viste come il risultato di operazioni fatte su infiniti o infinitesimi, i qua-

"Proprio come le operazioni sull'infinitamente piccolo sono state sostituite da operazioni sul finito che danno luogo esattamente agli stessi risultati e alle stesse eleganti relazioni formali, così in generale i metodi deduttivi basati sull'infinito devono essere sostituiti con procedimenti finiti che diano gli stessi risultati, che cioè rendano possibili le stesse catene di dimostrazioni e gli stessi metodi per ottenere formule e teoremi.
Questo è lo scopo della mia teoria, essa si propone di dare definitivamente sicurezza al metodo matematico . . ."

Hilbert vede nella chiarificazione del concetto di infinito una questione fondamentale il cui interesse non è solo matematico.

"Le considerazioni precedenti intendono solo affermare che la chiarificazione definitiva della natura dell'infinito non riguarda esclusivamente l'ambito degli interessi scientifici specializzati ma è necessaria per la dignità stessa dell'intelletto umano."

"D'altra parte l'esistenza dei paradossi della teoria degli insiemi sembra spingere al rifiuto dell'infinito attuale. C'è tuttavia un modo soddisfacente per evitare i paradossi senza tradire la nostra scienza. Il punto di vista utile per la scoperta di tale modo ed il desiderio che ci mostra la via da prendere sono:

1. *Se c'è la più piccola speranza, esamineremo accuratamente tutte le definizioni e i metodi deduttivi fecondi, li cureremo, li potenzieremo e li renderemo utili. Nessuno potrà cacciarci dal paradiso che Cantor ha creato per noi.*[5]

2. *Dobbiamo estendere a tutta la matematica quella sicurezza dei metodi dimostrativi che è propria della teoria elemen-*

---

li, come poi sarà fatto in modo rigoroso dall'analisi non standard, venivano visti come particolari tipi di quantità.

[5] Ho sottolineato questa frase poiché evidenzia che il punto di vista di Hilbert è completamente differente da quello degli intuizionisti che invece pensavano si dovesse cancellare dalla matematica tutto ciò che va oltre il numerabile ed il costruttivo.

tare dei numeri, di cui nessuno dubita e in cui contraddizioni e paradossi sorgono solo per negligenza."

Il punto di vista di Hilbert è chiaro. Per prima cosa il rigore in matematica non si deve ottenere semplicemente eliminando quella parte della matematica e quei metodi che, pur essendosi rivelati fecondi, non risultano avere basi sicure. Pertanto, nonostante i paradossi, *"Nessuno potrà cacciarci dal paradiso che Cantor ha creato per noi"*. L'atteggiamento di Hilbert è pragmatico, se certi metodi si sono rivelati utili allora devono essere accettati.

"In effetti il successo è essenziale perché, in matematica come altrove, esso costituisce la corte suprema di fronte a cui tutti si inchinano."

D'altro lato è indiscutibile che il rigore e la sicurezza si possono ottenere solo facendo riferimento ai metodi finitari propri dei numeri interi. Come fare per conciliare le due cose apparentemente contraddittorie?

2. L'infinito è solo una parola

Abbiamo già visto una citazione di Hilbert che si riferisce alla nozione di limite dichiarando che in tale nozione il coinvolgimento dell'infinito è solo apparente. Infatti se si scrive $lim_{n\to\infty} 1/n = 0$ non si deve intendere che quando n raggiunge l'infinito allora il valore di $1/n$ raggiunge 0. Piuttosto tale uguaglianza è solo un modo breve per indicare che:

per ogni $\varepsilon > 0$ *esiste m tale che* $1/n \leq \varepsilon$ *per ogni* $n \geq m$.

E' evidente allora che in tale caso il simbolo ∞ non denota niente ma è solo un aiuto linguistico per rappresentare una situazione in cui l'infinito non compare in nessun modo.

Un discorso simile, come osserva ancora Hilbert, può essere fatto in relazione alla nozione di "punto all'infinito" elaborata dalla geometria proiettiva. Come è noto, il piano proiettivo viene definito aggiungendo all'insieme dei punti del piano euclideo dei punti ideali, detti "punti all'infinito". In tale modo invece di dire che due rette sono parallele diciamo che hanno in comune un punto all'infinito. Tecnicamente ciò si ottiene al modo seguente.

Definizione 2.1. Chiamiamo *punto all'infinito* del piano euclideo ogni fascio completo di rette parallele. Diciamo che un punto all'infinito *P appartiene* ad una retta *r* se *r* appartiene al fascio *P*.

L'introduzione dei punti all'infinito permette di semplificare e rendere simmetrici gli assiomi della geometria piana. Ad esempio possiamo affermare che due rette si incontrano sempre in un punto (che è finito se le rette non sono parallele ed infinito se le rette sono parallele).[6] Anche in questo caso non si pretende che i punti all'infinito siano realmente esistenti, essi sono strumenti linguistici, enti ideali la cui introduzione è utile per ottenere risultati e per avere una trattazione più efficace della geometria.[7]

La proposta di Hilbert è pertanto di considerare l'infinito un ente ideale, per meglio dire un oggetto linguistico da manipolare seconde certe regole. In altre parole si tratta di spostare il ruolo del linguaggio il quale, da strumento di indagine del mondo degli enti matematici, deve diventare esso stesso oggetto di investigazione. Oggetto di studio dovranno essere i "segni concreti" che rimangono comunque oggetti finiti da maneggiare con un numero finito di regole.

> *"Questa è la filosofia che ritengo necessaria non solo per la matematica ma per ogni pensiero, per ogni comprensione e per ogni comunicazione che rientrano nell'ambito della scienza. In base ad essa, in particolare, oggetto della nostra considerazione matematica sono gli stessi segni concreti la cui forma, in virtù del nostro approccio, è immediatamente chiara e riconoscibile."*

Fino a qui non esistono, come lo stesso Hilbert sottolinea, grandi differenze con la tradizione algebrica. Anche la semplice risoluzione di una equazione di primo grado consiste in una manipolazione di equazioni (oggetti linguistici) secondo certe regole che permettono di passare da una equazione ad un altra. Lo stesso si può dire anche di un semplice calcolo. La grossa novità nasce dal fatto che per "segni concreti" Hilbert intendeva non solo equazioni ma anche espressioni linguistiche molto più complicate che coinvolgevano i quantificatori (come "esiste" e "per ogni") e i

[6] Inoltre in tale modo si ottiene un potente ed elegante strumento per la trattazione delle curve algebriche.
[7] Discorso analogo vale per l'introduzione dell'unità immaginaria.

connettivi logici (ad esempio la negazione, la congiunzione, la disgiunzione). Inoltre tra le regole di manipolazione linguistica non considerava solo quelle di carattere algebrico (quali ad esempio la proprietà associativa, la proprietà distributiva ...) ma anche quelle di natura logica quali le regole di inferenza. Arriviamo pertanto al punto fondamentale: il calcolo logico.

> *"Certo questo fu sviluppato in origine per motivi del tutto differenti. I suoi segni furono introdotti originariamente solo per scopi di comunicazione. Tuttavia è coerente col nostro punto di vista non attribuire alcun significato ai segni logici, così come non se ne è attribuito alcuno ai segni matematici, e dichiarare che anche le formula del calcolo logico sono elementi ideali che di per sé non significano niente. Col calcolo logico abbiamo un linguaggio simbolico che permette di tradurre in formule le asserzioni matematiche e di esprimere le deduzioni logiche mediante processi formali."*

In definitiva non bastava ridurre la matematica a linguaggio, ma era anche necessario formalizzare i processi deduttivi che permettevano la manipolazione di tale linguaggio. Più precisamente una particolare teoria matematica veniva vista come:
- un insieme finito di espressioni linguistiche (gli assiomi propri della teoria)
- un insieme fissato di espressioni (gli assiomi logici)
- il tutto da manipolare tramite determinate regole (le regole di inferenza).

Tale apparato permette di produrre altre espressioni (i teoremi). In tale modo qualunque teoria (anche quelle che parlano di oggetti infiniti) diviene un oggetto finito e quindi passibile di essere esaminato nella sua interezza. Il problema della consistenza diviene allora quello di esaminare tale oggetto finito e vedere se tra le sue proprietà vi è anche quella della consistenza. Un programma questo che sembra abbastanza ragionevole.

3. Nuovi oggetti matematici: parole e linguaggi

Abbiamo visto che per Hilbert la matematica, in particolare la dimostrazione matematica, può essere vista come un particolare sistema che agisce sulle parole di un linguaggio. Ora la nozione di "parola" e di "linguaggio" non sembrano appartenere

all'universo matematico e quindi si pone il problema di come possa essere reso rigoroso il discorso di Hilbert. E' necessario a tale scopo elaborare una teoria matematica dei linguaggi e la cosa può essere fatta al modo seguente. Si parte da un "alfabeto", cioè un insieme finito di simboli. Ad esempio nella lingua italiana un alfabeto è costituito dalle lettere *a*, *b*, *c*, ... In lingua greca è costituito dalle lettere α, β, γ, ... Un esempio di alfabeto "piccolo" è l'*alfabeto Morse* $A = \{\cdot,-\}$ costituito da un punto e da una linea che una volta veniva usato per il telegrafo. In definitiva possiamo chiamare alfabeto un qualunque insieme finito. Dato un alfabeto possiamo poi costruire parole. Ad esempio con quello della lingua italiana possiamo scrivere parole come "*cane*", "*canne*", "*cena*", "*acne*", "*acccanne*".. (quest'ultima è una parola senza significato). Dovendo definire la nozione di parola in termini insiemistici osserviamo che due parole come "*cane*" e "*cena*", che pur avendo le stesse lettere le hanno in posizione diversa, devono essere considerate diverse. Sono pure da considerare diverse due parole come "*cane*" e "*canne*" in cui le lettere coincidono anche nell' ordine ma appaiono un numero diverso di volte. Ciò mostra che non è certamente possibile chiamare parola un insieme finito di elementi dell'alfabeto. Infatti, poichè due insiemi con gli stessi elementi sono uguali, tutti gli insiemi $\{c,a,n,e\}$, $\{c,a,n,n,e\}$, $\{c,e,n,a\}$, $\{a,c,n,e\}$, $\{a,c,c,a,n,n,e\}$ coincidono. Allora, per potere rappresentare la nozione di parola conviene usare la nozione di *n*-pla che permette appunto di tenere conto sia dell'ordine che dell'eventuali ripetizioni. Si arriva quindi alla seguente definizione.

Definizione 3.1. Sia A un insieme finito (che chiamiamo *alfabeto*). Allora gli elementi di A^n vengono detti *parole di lunghezza n* nell'alfabeto A. Indichiamo con A^+ l'insieme $\cup_{n\in N}A^n$ di tutte le possibile parole.

Una volta che abbiamo soddisfatto la mania dei matematici di ridurre tutto alla teoria degli insiemi, continueremo a rappresentare le parole al modo solito, scrivendo una parola come $(a_1,a_2,...,a_n)$ con $a_1,a_2,...,a_n$.[8] Ad esempio per indicare la parola (c,a,n,e) scriveremo semplicemente *cane.*

[8] Il fatto che "rendere rigoroso" significhi ridurre alla teoria degli insiemi è una credenza, un po' ridicola, dei matematici. Assumere come

Possiamo immaginare l'alfabeto A come l'insieme dei caratteri che sono sulla tastiera di un computer ed una parola come la sequenza di lettere che compaiono sullo schermo quando si batte sulla tastiera. In particolare è possibile anche considerare il "simbolo spazio-vuoto" che corrisponde al lasciare uno spazio vuoto tra due lettere. In questo caso si chiama parola anche quella che è per noi una frase, cioè una sequenza di parole separate da spazi vuoti. Allora possiamo far rientrare nel termine "parola" anche *frasi* del tipo

"il cane corre", *"enac corre il"*, ...

Ad esempio il contenuto di questo libro può essere visto come una unica parola nell'alfabeto che si ottiene usando i soliti caratteri della tastiera più un "carattere" per denotare lo spazio vuoto.

Un linguaggio non si caratterizza solo da un alfabeto ma anche da un criterio con cui si stabilisce se una parola o frase è da considerare accettabile. Stabilito tale criterio, allora un linguaggio si definisce come l'insieme delle parole (se si vuole di frasi) che sono considerate accettabili.

Definizione 3.2. Dato un alfabeto A chiamiamo *linguaggio formale su A* un sottoinsieme $\mathcal{L}$ di A^+.

Se $\mathcal{L}$ contiene solo un numero finito di parole, allora un criterio di accettabilità si può ottenere direttamente tramite una lista delle parole che sono in $\mathcal{L}$. Ad esempio nel caso della lingua italiana l'insieme corretto delle parole coincide con l'insieme delle parole presenti in un buon vocabolario. Nel caso il linguaggio contiene un insieme infinito di parole (come in generale avviene quando si considerano frasi), allora è un po' più complicato stabilire un criterio di accettabilità ed in generale ci si riferisce alla nozione di *grammatica* che però non considereremo in questo libro. Esaminiamo ora una ovvia proprietà dei linguaggi formali.

---

primitiva direttamente la nozione di parola sarebbe altrettanto o forse maggiormente rigoroso viste le basi incerte della teoria degli insiemi. E' quello che usualmente viene fatto nei linguaggi di programmazione dove viene assunta come primitiva la nozione di "parola" (equivalentemente, il tipo "stringa", "lista", ...). Dovendo poi introdurre il tipo "insieme" lo si fa derivare da quello di "parola" introducendo una opportuna relazione di equivalenza tra parole (o, equivalentemente, di riduzione a forma normale).

Proposizione 3.3. L'insieme A^+ delle parole nell'alfabeto A è numerabile. Pertanto ogni linguaggio formale è finito o numerabile.

Dim. Sia $a \in A$, allora la corrispondenza f che associa ad ogni $n \in N$ la parola $aaaa..a$ che si ottiene ripetendo n volte la lettera a è una funzione iniettiva di N in A^+. Quindi A^+ ha potenza maggiore o uguale del numerabile. Vogliamo provare che A^+ ha anche potenza minore o uguale al numerabile, cioè che esiste una funzione iniettiva di A^+ in N. Esistono diversi modi per fare questo che spesso prendono il nome di *codifiche*. Un modo vicino allo stile dei matematici è considerare la successione p_1, p_2, ... dei numeri primi scritta in ordine crescente. Associamo poi in modo iniettivo ad ogni lettera in A un numero intero, cioè consideriamo una funzione iniettiva $c : A \to N$. Essendo A finito non ci sono difficoltà a trovare una tale funzione. Successivamente associamo ad ogni parola $a_1...a_n$ il numero $p_1^{c(a_1)} \cdot \ldots \cdot p_n^{c(a_n)}$. Tale corrispondenza è iniettiva (anche se non suriettiva). Ad esempio se poniamo $c(a) = 1$, $c(b) = 2$, $c(c) = 3$, ... allora alla parola *"bacca"* viene associato il numero $2^2 \cdot 3^1 \cdot 5^3 \cdot 7^3 \cdot 11^1$.

Un modo più "informatico" ed intuitivo di procedere è il seguente. Definiamo una funzione iniettiva $c : A \to \{0,1\}^+$ che associ ad ogni elemento $a \in A$ una parola nell'alfabeto $\{0,1\}$ e supponiamo che tutte le parole $c(a)$ abbiano la stessa lunghezza e che inizino con 1. Consideriamo la funzione che associa ad ogni parola $a_1a_2...a_n$ in A^+ la parola $c(a_1)c(a_2)...c(a_n)$ in $\{0,1\}^+$. Infine interpretiamo tale parola come un numero scritto in base 2 (ma il discorso funziona anche se la si interpreta in base 10). In tale modo abbiamo definito una funzione iniettiva di A^+ in N.[9] Ad esempio

[9]La tecnica che ora abbiamo utilizzato per dimostrare la proposizione corrisponde al modo concreto di funzionamento dei computer. Infatti quando si preme un tasto della tastiera l'impulso inviato al computer è proprio una sequenza di 0 ed 1. Dopo avere scritto un documento (un romanzo una poesia od altro), nella memoria del computer è immagazzinata una serie lunghissima di 0 e di 1 corrispondente alla sequenza di lettere scritte (ma anche agli spazi vuoti). Più precisamente nei sistemi di scrittura (come il Word) esistono anche caratteri che vengono chiamati "di controllo" e che servono a modificare i caratteri che compaiono sullo schermo. Ad esempio esistono caratteri che creano il corsivo, il grassetto e così via.

supponiamo, sempre riferendoci all'alfabeto della lingua italiana che

$c(a) = 111111$, $c(b) = 111011$, $c(c) = 100011$, ...

In questo modo associamo alla parola "bacca" il numero, scritto in base 2,

11101111111110001110001111111111. □

Si osservi che il procedimento con cui abbiamo associato ad ogni parola un numero naturale è "effettivo", nel senso che corrisponde ad un preciso algoritmo che un qualunque calcolatore sarebbe capace di eseguire. In questo caso si usa parlare di "codifica" di un linguaggio. Si usa anche considerare una "decodifica" che associa ad ogni numero intero m l'elemento del linguaggio formale $\mathcal{L}$ ottenuto al modo seguente (ci riferiamo al primo tipo di codifica sopra esposto)

- si fissa una parola p in $\mathcal{L}$
- si effettua una scomposizione $m = p(1)^{i(1)}\cdot\ldots\cdot p(n)^{i(n)}$ di m in prodotto di successivi numeri primi
- se $i(1),\ldots,i(n)$ sono codici di lettere in A (cioè se esistono $a_1,\ldots,a_n$ in A tali che $g(a(1)) = i(1)$, . . . ,$i(a(n)) = i(n)$) e se la parola $a_1\ldots a_n$ è una parola in $\mathcal{L}$, allora si assume tale parola come decodifica di m
- altrimenti assumiamo per convenzione che la decodifica di m sia p.

Da notare che una tale decodifica è un processo effettivo solo se esiste un metodo per decidere se una parola appartiene ad $\mathcal{L}$ o meno ($\mathcal{L}$ è decidibile).

Corollario 3.4. L'insieme dei possibili romanzi è numerabile. L'insieme delle possibili poesie è numerabile. L'insieme dei possibili programmi di un linguaggio di programmazione è numerabile.

4. Rappresentabilità, definibilità e numerabilità

Possiamo utilizzare la proposizione 3.3 per provare in modo immediato che alcuni insiemi sono numerabili. A tale scopo ci serviamo della nozione di "rappresentabile" o quella analoga di "definibile" in un alfabeto A. Lasciamo il significato di tali nozioni a livello intuitivo. Quello che interessa è che, dato un insieme X ed un alfabeto A, una rappresentazione (o definizione) di un elemen-

to di X in A sia una parola su A. Inoltre supponiamo che elementi diversi di X abbiano rappresentazioni (definizioni) diverse. Per fare un esempio, riferendoci alla rappresentazione decimale dei numeri, se si accetta un alfabeto A con i simboli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 allora ogni naturale e rappresentabile in A. Se aggiungiamo ad A i simboli + e -, allora otteniamo un alfabeto in cui ogni numero intero relativo è rappresentabile. Se all'alfabeto aggiungiamo anche il simbolo /, allora anche i razionali sono rappresentabili. Esempi di definizioni sono i seguenti. Il numero 3 può essere definito come "quel numero positivo il cui quadrato è nove". Il numero $+\sqrt{2}$ può essere definito come "quel numero positivo il cui quadrato è 2".

Teorema 4.1. Sia X un insieme i cui elementi siano rappresentabili (definibili) in un linguaggio formale. Allora X è enumerabile (cioè finito o numerabile).

Dim. E' possibile considerare una funzione che associa ad ogni elemento in X una delle sue rappresentazioni (definizioni) in A^+. Si ottiene una funzione iniettiva di X in A^+. Poiché A^+ è un insieme numerabile, questo prova che X è finito o numerabile. □

Applicando tale criterio possiamo dimostrare la seguente proposizione.

Proposizione 4.2. L'insieme $P_f(N)$ delle parti finite di N è numerabile.

Dim. Ogni insieme finito di numeri interi può essere rappresentato tramite una parola del tipo $\{n_1,...,n_p\}$ con $n_1<n_2<...<n_p$ cioè tramite una parola nell'alfabeto costituito dalle due parentesi {, }, dalla virgola e dalle cifre 0,1, 2, 3, 4, 5, 6, 7, 8, 9. Pertanto $P_f(N)$ è enumerabile. Poiché è ovvio che $P_f(N)$ non è finito, $P_f(N)$ è numerabile.[10] □

[10] Concretamente, dato un insieme finito lo "descrivo" al computer con una parola del tipo $\{n_1,...,n_p\}$ con $n_1<n_2<...<n_p$. Tale parola viene immagazzinata nei registri di memoria sotto forma di una sequenza di 0 ed 1, sequenza che possiamo interpretare come un numero. Ciò fornisce una corrispondenza di $P_f(N)$ in N.

E' possibile anche ridimostrare in modo più semplice alcune delle proposizioni provate nel paragrafo precedente.

Proposizione 4.3. L'insieme *Z* dei numeri relativi è numerabile. L'insieme *Q* dei razionali è numerabile. L'insieme delle *n*-ple di numeri razionali è numerabile.

Dim. Gia abbiamo osservato che gli elementi di *Z* e quelli di *Q* sono rappresentabili in un opportuno alfabeto. Per rappresentare l'insieme di tutte le possibili *n*-ple di numeri razionali è sufficiente aggiungere all'alfabeto le parentesi (,) e la virgola.

Ricordiamo che un numero reale si dice *algebrico* se è radice di un polinomio a coefficienti razionali. Un numero è *trascendente* se non è algebrico. Poiché ogni polinomio a coefficienti razionali si può ridurre ad un polinomio equivalente a coefficienti interi, possiamo definire un numero algebrico anche come un numero che sia radice di un polinomio a coefficienti interi. Ad esempio $\sqrt{5}$ è un numero algebrico perché è soluzione dell'equazione $x^2-5 = 0$. E' algebrico anche un numero razionale p/q qualunque perché è soluzione dell'equazione $q \cdot x - p = 0$.

Proposizione 4.4. L'insieme *Al* dei numeri reali algebrici è numerabile. Pertanto l'insieme dei numeri trascendenti ha la potenza del continuo.

Dim. Ogni numero algebrico può essere definito da una proprietà del tipo "la terza radice del polinomio $p(x)$". L'insieme di tali definizioni è un insieme di parole in un opportuno alfabeto. Ciò prova che *Al* è enumerabile. Poiché *Al* contiene tutti i razionali siamo sicuri che *Al* è numerabile. □

5. Logica del primo ordine: linguaggio ed apparato deduttivo

Un linguaggio formale che vada bene per la matematica dovrà contenere

- nomi per oggetti matematici (come 3, 13, π , ∅, *e*),

- nomi per funzioni ed operazioni (come *log*, +, ·, *sen*, x_2)[11]
- nomi per relazioni (come =, ≤, ≥, ⊇).

Sembra infatti ragionevole poter scrivere asserzioni come "*log*(2+3) ≥ 0" oppure "*log*(2+3) = 2·3" che si avvalgono del nome di funzione *log*, dei nomi di numeri 2, 3 e 0, di un simbolo + per un operazione binaria e dei simboli ≥ e = per relazioni binarie. Ancora, in matematica sono di uso frequente le variabili ed i quantificatori (esiste, per ogni) che permettono ad esempio di scrivere proposizioni del tipo "esiste una soluzione dell'equazione x^2-1=0", in breve "$\exists x(x^2-1=0)$". Infine sono usati connettivi logici come "non", "e", "oppure", "implica" che consentono di costruire asserzioni (composte) a partire da altre asserzioni. Ciò suggerisce le seguenti definizioni.

Definizione 5.1. Chiamiamo *alfabeto di un linguaggio del primo ordine* un alfabeto *A* costituito da:

- un insieme di simboli per denotare *variabili*, ad esempio *x*, *y*, *z*, . . .
- i *connettivi proposizionali* $\{\wedge,\vee,\rightarrow,\sim\}$
- il quantificatore esistenziale $\exists$
- la parentesi aperta (e la parentesi chiusa)

In più

- un insieme finito *C* di elementi detti *costanti*
- un insieme finito *O* di *nomi di operazione*
- un insieme finito *P* di *nomi di predicati*
- una *funzione arità ar* : $O \cup P \rightarrow N$

Se l'arità di un nome di funzione è 2 allora è inteso che tale nome denota una funzione binaria e si preferisce parlare di *operazione binaria.* Se l'arità di un nome di predicato è 1 allora si dice che denota un predicato *monadico* o una *proprietà*. Se invece l'arità è 2 si parla di *relazione binaria*. Da notare che esistono tanti alfabeti, e quindi tanti linguaggi del primo ordine, quanti sono i modi di specificare le costanti, i nomi delle relazioni e delle operazioni. Avremo ad esempio un linguaggio adeguato alla teoria dei gruppi, uno per la teoria degli anelli, uno per le strutture ordinate, e così via. Per poter definire il linguaggio del primo ordine corri-

[11] Non abbiamo escluso che in un alfabeto ci possano essere, come elementi, parole di un altro linguaggio come ad esempio, *log*, *sen*,.. Infatti l'unica cosa che abbiamo richiesto è che un alfabeto *A* sia finito.

spondente ad un dato alfabeto dobbiamo prima definire il linguaggio dei termini. Possiamo vedere un termine come descrizione di un algoritmo per il calcolo di una funzione (se il termine contiene variabili) o di un elemento (se il termine non contiene variabili).

Definizione 5.2. Dato un alfabeto del primo ordine chiamiamo *linguaggio dei termini* l'insieme delle parole che si ottengono applicando più volte le seguenti regole:

a) ogni variabile o costante è un termine

b) se f è il nome di una funzione n-aria e $t_1,...,t_n$ sono termini allora $f(t_1,...,t_n)$ è un termine (notazione *prefissa*)

c) se $\otimes$ è il nome di una funzione binaria e t_1, t_2 sono termini allora $(t_1)\otimes(t_2)$ è un termine (notazione *infissa*).

In matematica usualmente si usano solo nomi di funzioni di arità 1 (dette *funzioni* o *operazioni* unarie) o 2 (dette *operazioni binarie*). In questo ultimo caso si preferisce la notazione infissa. Ad esempio l'espressione (x)-$(log((y)+(x)))$ è un termine. Infatti

- poiché y è un termine ed x è un termine allora $(y)+(x)$ è un termine
- poiché $(y)+(x)$ è un termine allora $log((y)+(x))$ è un termine
- essendo x un termine e $log((y)+(x))$ un termine, (x)-$(log(y+x))$ è un termine.[12]

Utilizzando i termini, possiamo ora definire la nozione di linguaggio del primo ordine.

Definizione 5.3. Un *linguaggio del primo ordine*[13] è l'insieme $\mathcal{L}$ delle parole su di un alfabeto del primo ordine definito dalle seguenti regole di formazione:

---

[12] Naturalmente la realtà dei linguaggi matematici è più flessibile e diversificata. Ad esempio il termine che abbiamo costruito si indica più semplicemente con x-$log(y+x)$ in quanto esistono semplici regole e convenzioni per l'eliminazione di parentesi inutili. Ad esempio scriviamo $3\cdot5+2$ al posto di $((3)\cdot(5))+(2)$ come invece richiederebbe la definizione 4. Inoltre esistono anche notazioni *"post-fisse"* per le operazioni unarie, ad esempio per la funzione fattoriale $x!$ e notazioni *"esponenziali"* come la funzione inverso x^{-1}. Tuttavia ai fini del nostro discorso ci atterremo alla Definizione 2 anche se non l'applicheremo in modo rigoroso.

[13] Tale linguaggio è alla base della *logica del primo ordine* in cui è possibile quantificare solo sugli elementi di un fissato dominio. Non è pos-

a) se r è un predicato n-ario e $t_1,...,t_n$ sono termini allora $r(t_1,...,t_n)$ è una formula (*formula atomica in notazione prefissa*)
b) se r è il nome di un predicato binario e t_1,t_2 sono termini allora $t_1 r\ t_2 \in \mathcal{L}$ (*formula atomica in notazione infissa*);
c) se α e $\beta \in \mathcal{L}$ allora $(\alpha)\wedge(\beta)$, $(\alpha)\vee(\beta)$, $(\alpha)\rightarrow(\beta)$ e $\neg(\alpha)$ appartengono ad $\mathcal{L}$;
d) se x è una variabile ed $\alpha \in \mathcal{L}$ allora $\exists x(\alpha)\in\mathcal{L}$.

Gli elementi di $\mathcal{L}$ vengono chiamati *formule ben formate* o, più semplicemente, *formule*.

I seguenti sono alcuni esempi di linguaggi del primo ordine utilizzati in matematica.

Esempi.
Linguaggio usato per le strutture ordinate. È un linguaggio che contiene i soli simboli ≤ e = di relazioni binarie. A volte si aggiunge anche una costante 0 (da interpretare come minimo elemento) e una costante 1 (da interpretare come massimo elemento) e pertanto $C = \{0,1\}$. Poiché non ci sono nomi di operazioni, gli unici termini sono le variabili e le costanti. Sono esempi di formule

$$\forall x\exists y(x\geq y)\ ;\ \forall x(x \leq x)\ ;\ \forall x(\forall y((x\leq y)\wedge(y\leq z) \Rightarrow x\leq z)).$$

Linguaggio usato per la teoria dei gruppi. È costituito da "·" per rappresentare l'operazione binaria, da "*inv*" per rappresentare l'operazione che associa ad ogni x il suo inverso e la costante 1

---

sibile invece quantificare sui sottoinsiemi, le relazioni e le funizoni di tale dominio. Nella logica del primo ordine è possibile quindi esprimere un'asserzione del tipo "ogni elemento ammette inverso" ma non un'asserzione del tipo "ogni sottoinsieme non vuoto ammette minimo". I linguaggi che permettono di esprimere sia il primo tipo di asserzioni che il secondo sono quelli del secondo ordinee . Ciò comporta l'uso di diversi tipi di variabili. Ad esempio se utilizzo lettere maiuscole per denotare insiemi e minuscole per denotare elementi, posso esprimere la nozione di buon ordinamento tramite formula $\forall X\exists m(m\in X\wedge\forall z(z\in X \rightarrow m\leq z)))$. Anche l'assioma di completezza, che si esprime dicendo che ogni sottoinsieme inferiormente limitato ammette estremo inferiore si esprime quantificando sui sottoinsiemi. Un altro importante esempio è l'assioma per le terne di Peano che riguarda il principio di induzione. Una logica si dice del *primo* o del *secondo ordine* a seconda che si riferisca ad un linguaggio del primo o del secondo ordine.

per rappresentare l'elemento neutro. L'unica relazione è l'identità. In generale si preferisce la notazione esponenziale x^{-1} al posto di $inv(x)$. I termini sono pertanto espressioni del tipo 1+1, $(x \cdot y) \cdot x^{-1}$, $((1 \cdot x)^{-1} \cdot y)^{-1}$. Sono esempi di formule:

$$\forall x(x \cdot y = y \cdot x) \quad ; \quad x \cdot 1 = x \quad ; \quad \forall x(x = 1 \Rightarrow x \cdot x = 1).$$

Ma naturalmente è possibile utilizzare anche linguaggi diversi per trattare lo stesso tipo di strutture matematiche. Ad esempio per la teoria dei gruppi si usa spesso la notazione additiva invece di quella moltiplicativa che abbiamo indicato. In questo caso si utilizza la costante 0, il nome di operazione binaria + , di operazione unaria -, ed il solito simbolo di uguaglianza =.

Supponiamo di avere un linguaggio del primo ordine $\mathcal{L}$. In accordo con il punto di vista di Hilbert, dobbiamo vedere le dimostrazioni che usualmente si effettuano in matematica come un procedimento meccanico con cui produrre, a partire da un dato sistema di elementi di $\mathcal{L}$ (gli assiomi), nuovi elementi di $\mathcal{L}$ (i teoremi). Esistono diverse possibili regole per "produrre teoremi", noi ci soffermiamo sulle seguenti due regole più note in logica.

Il regola del Modus Ponens. Tale regola afferma che se ho dimostrato la formula $\alpha \rightarrow \beta$ ed ho dimostrato α allora posso affermare anche β. In breve:

$$\frac{\alpha,\ \alpha \rightarrow \beta}{\beta} \qquad (\textit{Modus Ponens})$$

La regola di Generalizzazione. Tale regola afferma che se ho dimostrato la formula $\alpha(x)$, allora posso affermare anche $\forall x(\alpha)$. In breve

$$\frac{\alpha}{\forall x(\alpha)} \qquad (\textit{Generalizzazione})$$

La generalizzazione si giustifica col fatto che se ho dimostrato $\alpha(x)$ allora, essendo x una variabile, non ho mai utilizzato nessuna particolare proprietà dell'oggetto denotato da x. In altri termini, durante la dimostrazione x ha sempre denotato un generico elemento del dominio. Pertanto, di fatto, si è dimostrato $\forall x(\alpha)$.

Vi sono poi delle formule di cui ci si può servire durante la dimostrazione perché sono vere sempre, qualunque siano le cose

di cui si parla. In altre parole si possono utilizzare delle formule logicamente vere del tipo $\alpha\rightarrow\alpha$ oppure $\alpha\wedge\beta\rightarrow\alpha$ oppure $\alpha(t)\rightarrow\exists x\alpha$. Chiamiamo *assiomi logici* un opportuno insieme *Al* di tali formule. Usualmente in A_l si mettono anche formule del tipo

$$p\rightarrow p,\ \neg(\neg(\alpha))\rightarrow\alpha,\ (\forall x\alpha(x))\rightarrow\alpha(t),\ \exists x(\alpha)\rightarrow\neg\forall x(\neg(\alpha)).$$

Inoltre si aggiungono assiomi relativi all'uguaglianza

U_1	$\forall x(x=x)$	(riflessività)
U_2	$\forall x\forall y((x=y)\rightarrow(y=x))$	(simmetria)
U_3	$\forall x\forall y\ \forall z((x=y)\wedge(y=z))\rightarrow(x=z))$	(transitività)
U_4	$x=y\rightarrow z\otimes x=z\otimes y$;	(sostituzione)
	$x=y\rightarrow x\otimes z=y\otimes z$;	
	$x=y\rightarrow f(x)=f(y)$	
U_5	$x=y\rightarrow(r(z,x)\Leftrightarrow r(z,y))$;	(sostituzione)
	$x=y\rightarrow(r(x,z)\Leftrightarrow r(y,z))$;	
	$x=y\rightarrow(s(x)\Leftrightarrow s(y))$.	

dove U_4 e U_5 devono essere intesi come *schemi di assiomi* cioè devono essere asseriti per tutti i nomi di operazioni binarie $\otimes$, di operazioni unarie f, di relazioni binarie r e di relazioni ad un posto s.

Definizione 5.4. Dato un insieme T di formule, che chiameremo *sistema di assiomi*, chiameremo *dimostrazione di α sotto ipotesi T* ogni successione di formule $\alpha_1,\ldots,\alpha_n$ con $\alpha_n=\alpha$ e tale che per ogni formula α_i si verifichi almeno uno dei seguenti casi:
- α_i è un assioma logico
- α_i è una ipotesi, cioè $\alpha_i\in X$
- α_i è stata ottenuta da formule precedenti per modus ponens o per generalizzazione.

Scriveremo $T\vdash\alpha$ per dire che esiste una dimostrazione di α sotto ipotesi T.

Possiamo visualizzare il sistema deduttivo di una logica del primo ordine come una macchina che produce teoremi. Tale macchina, dopo che sono stati inseriti gli assiomi di una teoria T (ad esempio la teoria dei gruppi) comincia a stampare i teoremi uno dopo l'altro. La macchina stampa tali teoremi utilizzando le regole di inferenza e formule che sono in *Al*, oppure in T oppure che sono state già prodotte.

6. Logica del primo ordine: l'interpretazione

Se ci si attiene strettamente al punto di vista formalista di Hilbert secondo cui la matematica è solo un calcolo di parole, nozioni come essere vero ed essere falso non hanno importanza. L'importante è stabilire regole precise in questa sorta di gioco linguistico e poi attenersi a tali regole. Tuttavia se ci stacchiamo dal riferimento alle "cose di cui si parla" e dalle nozioni di vero e falso non è chiaro come si debbano stabilire tali regole e quale senso abbiano i teoremi trovati.

In definitiva dobbiamo trovare una definizione matematica di interpretazione e di verità. Cominciamo con il problema dell'interpretazione che è alquanto problematico. Ad esempio non è affatto detto che due persone interpretano allo stesso modo una determinata frase. Se si riferisce ad un testo teatrale o un testo musicale è scontato che ogni attore o musicista possa dare una interpretazione personale di tale testo. Ovviamente interpretazione e verità sono nozioni collegate in quanto una asserzione può essere vera o falsa a seconda del modo come vengono interpretate le parole che la costituiscono. Ad esempio se dico "Maria è più grande di Luisa" la verità o falsità di tale asserzione dipende da chi intendo indicare con i nomi "Maria" e "Luisa" e che cosa intendo per "più grande" (più anziana ?, più alta ?). Anche se scrivo una cosa di carattere matematico come "2+2 = 0" scrivo una cosa falsa se interpreto tale asserzione sui numeri naturali, scrivo una cosa vera se la interpreto sugli interi modulo 4. Allora prima di parlare di vero e di falso è necessario fornire una definizione di interpretazione. Ora se $\mathcal{L}$ è un linguaggio del primo ordine, una sua interpretazione si ottiene specificando di quali oggetti si parla e quindi fissando un insieme D. Inoltre, come è ovvio, si deve associare

- ad ogni nome di operazione una operazione in D,
- ad ogni costante un elemento di D,
- ad ogni nome di relazione binaria o unaria una relazione binaria o unaria in D.

Definizione 6.1. Una *interpretazione* di un linguaggio del primo ordine $\mathcal{L}$ è costituita da un insieme D, detto *dominio dell'interpretazione* e da una funzione I che associa:

- ad ogni nome di operazione n-aria f una funzione $I(f) : D^n \to D$
- ad ogni costante c un elemento $I(c)$ di D

- ad ogni nome di relazione n-aria r un sottoinsieme $I(r) \subseteq D^n$.[14]

Esempio. Consideriamo un linguaggio $\mathcal{L}$ in cui vi sia solo il nome di una relazione binaria "*ama*". Allora una interpretazione di tale linguaggio si ottiene fissando un insieme D di persone (ad esempio quelle presenti in una certa stanza) ed una relazione binaria $I(ama)$, cioè un sottoinsieme di $D \times D$. Ad esempio potremmo supporre che D sia l' insieme di persone,

{*mario*, *maria*, *carlo*, *luigi*}

e che l'interpretazione sia definita ponendo $I(ama)$ uguale all'insieme

{(*maria*, *mario*), (*mario*, *carlo*), (*maria*, *carlo*), (*carlo*, *luigi*)}.

Naturalmente vi possono essere più interpretazioni dello stesso linguaggio, ad esempio se si cambia il gruppo di persone cui ci si riferisce.

Esempio. Riferiamoci al linguaggio che si usa per le strutture ordinate. Poiché è costituito da un solo simbolo di relazione binaria, $\leq$, una interpretazione di tale linguaggio è costituita da un insieme D e da una relazione binaria $I(\leq)$. Ad esempio possiamo supporre che

-D sia l'insieme dei numeri interi e $I(\leq)$ l'usuale relazione di ordine tra interi,

- D sia l'insieme delle parti di un insieme S e $I(\leq)$ sia la relazione di inclusione.

Si noti che l'unica cosa che si richiede in una interpretazione è che $I(\leq)$ sia una relazione binaria e non necessariamente una relazione d'ordine. Ad esempio otteniamo una interpretazione ponendo D uguale all'insieme dei numeri interi e $I(\leq) = \{(n,m) \mid n = m+1\}$. Naturalmente una tale interpretazione non è un insieme ordinato. Di fatto, almeno che non si impongano opportuni as-

[14] Da notare che la nozione di interpretazione di un linguaggio del primo ordine coincide sostanzialmente con la nozione di struttura del primo ordine che abbiamo considerato nel primo volume. Infatti sia dato un linguaggio Λ i cui nomi di operazione siano $o_1,...,o_s$, i cui nomi di relazioni siano $r_1,...,r_t$ e con costanti $c_1,...,c_p$. Allora la *struttura matematica associata ad una interpretazione* I è la struttura $(D,I(o_1),...,I(o_s),I(r_1),...,I(r_t),I(c_1),...,I(c_p))$. Viceversa è evidente che ogni struttura del primo ordine può essere considerata come interpretazione di un opportuno linguaggio.

siomi (cosa che faremo nel seguito) le interpretazioni di questo linguaggio possono essere accettate anche come interpretazioni del linguaggio dell'esempio precedente, e viceversa.

Abbiamo già detto che un termine in cui compaiano delle variabili libere è la descrizione di un algoritmo per calcolare una funzione (se il termine contiene variabili) o un elemento (se il termine non contiene variabili). Ad esempio al termine $3\cdot(5+7)+1$ corrisponde l'algoritmo:

1. prendi i numeri 5 e 7
2. sommali
3. moltiplica il risultato per 3
4. aggiungi 1

Chiamiamo interpretazione del termine il numero che si ottiene tramite tale algoritmo. Se nel termine abbiamo la presenza di una o più variabili, allora il corrispondente algoritmo calcola una funzione che chiamiamo interpretazione di tale termine. Naturalmente tali interpretazioni dipendono dalla struttura algebrica di cui si sta parlando, cioè dalla interpretazione fissata. Un modo più rigoroso di definire l'interpretazione di un termine è il seguente in cui utilizziamo come variabili i simboli x_1, x_2, … Per semplicità supponiamo di utilizzare la notazione prefissa anche per i nomi di operazioni binarie.

Definizione 6.2. Sia (D,I) una interpretazione, e t un termine. Allora per ogni intero n che sia maggiore o uguale agli indici delle variabili che compaiono in t definiamo una funzione n-aria $I(t)$: $D^n \to D$ per ricorsione sulla complessità di t al modo seguente:

a) se t è la costante c allora $I(t)$ è la funzione costantemente uguale a $I(c)$;

b) se t è la variabile x_i allora $I(t)$ è la proiezione i-esima[15] cioè la funzione definita da

$$I(t)(d_1,...,d_n) = d_i$$

c) se $t = f(\underline{t}_1,...,\underline{t}_p)$ allora $I(t)$ è la funzione tale che

$$I(t)(d_1,...,d_n) = I(f)(I(\underline{t}_1)(d_1,...,d_n),..., I(\underline{t}_p)(d_1,...,d_n)).$$

[15] Prende il nome di *proiezione i-esima* in un prodotto cartesiano $X_1\times...\times X_n$ con $i\le n$ la funzione Pr_i definita dal porre $Pr_i(x_1,...,x_n) = x_i$. In altri termini la proiezione i-esima è la funzione che associa ad ogni vettore la sua componente di posto i. La terminologia geometrica è dovuta al fatto che, ad esempio, in un piano euclideo le due possibili proiezioni corrispondono alle proiezioni sugli assi cartesiani.

Ad esempio sia t il termine $log(x_1)+sen(x_2)$, allora

$$I(t)(d_1,d_2) = I(+)(I(log(x_1))(d_1,d_2), I(sen(x_2)(d_1,d_2)).$$

D'altra parte

$$I(log(x_1))(d_1,d_2) = I(log)(I(x_1)(d_1,d_2)) = I(log)(d_1)$$
$$I(sen(x_2))(d_1,d_2) = I(sen)(I(x_2)(d_1,d_2)) = I(sen)(d_2)$$

e quindi

$$I(t)(d_1,d_2) = (I(log)(d_1)\ I(+)\ I(sen)(d_2)).$$

Questo significa che il temine $log(x_1)+sen(x_2)$ viene interpretato come la funzione che, data la coppia (d_1, d_2) di elementi di D,

1. applica la funzione $I(log)$ a d_1,
2. applica la funzione $I(sen)$ a d_2,
3. compone i risultati ottenuti nei passi 1. e 2. tramite $I(+)$.

Da notare che se in un termine compaiono le variabili x_1 e x_3 allora la sua interpretazione è comunque una funzione di (almeno) tre variabili anche se poi i valori che assume non dipendono effettivamente dai valori di x_2. Ad esempio il termine $2\cdot x_1+sen(x_3)$ è interpretato come una funzione di tre variabili in quanto viene considerato equivalente al termine $2\cdot x_1+0\cdot x_2 + sen(x_3)$. In tale caso si dice che la variabile x_2 è *muta*. Lo stesso termine può essere interpretato anche come funzione di quattro variabili in quanto può essere considerato equivalente al termine $2\cdot x_1+0\cdot x_2 + sen(x_3)+0\cdot x_4$. Un termine che si riduca ad una costante può essere interpretato come funzione di n variabili per ogni intero n. Ad esempio se l'interpretazione è il campo dei numeri reali allora la costante 3 può essere interpretata come funzione definita in R in R^2 in R^3 e così via. La cosa non è tanto strana in quanto se, ad esempio, si accetta che la costante 3 sia un termine equivalente al termine $0\cdot x_1+0\cdot x_2+0\cdot x_3+3$ (oppure al termine $0\cdot x_1+0\cdot x_2+3$ oppure al termine $0\cdot x_1+3$) allora tale costante deve poter essere interpretata come funzione di tre variabili (di due variabili e di una variabile, rispettivamente).

7. Cosa è la verità

> *Allora Pilato gli disse: «Ma dunque, sei tu re?» Gesù rispose: «Tu lo dici; sono re; io sono nato per questo, e per questo sono venuto nel mondo: per testimoniare della verità. Chiunque è dalla parte della verità ascolta la mia voce». Pilato gli disse: «Che cos'è la verità?» E detto questo, uscì di nuovo verso i Giudei ..."*
> (Giovanni 18:33-38 NRV)

Anche il problema della verità non è tanto semplice tanto che Pilato sembra dubitare perfino che esista la verità. In ogni caso il primo a proporre una definizione matematica di interpretazione e di verità fu il logico matematico Tarski, definizione a cui noi ci atterremo in seguito. Si consideri ora una formula α di un dato linguaggio e proponiamoci di definire in maniera rigorosa che cosa significa l'espressione "α è vera". Ora naturalmente la verità o falsità di una formula dipende dalla interpretazione del linguaggio. Ad esempio la formula $\forall x_1(\forall x_2(x_1 \cdot x_2 = x_2 \cdot x_1))$ sarà vera se il dominio D dell'interpretazione è l'insieme degli interi relativi ed il simbolo "$\cdot$" è interpretato con l'usuale moltiplicazione di numeri. Tale formula sarà invece falsa se invece D è l'insieme delle funzioni di R in R e l'interpretazione di "$\cdot$" è di essere la composizione di due funzioni (siccome, ad esempio $log(sen(x)) \neq sen(log(x))$, la composizione non è una operazione commutativa). Allora è più corretto dire che cosa si debba intendere per

"α è vera rispetto ad una interpretazione I".

Anche ciò crea qualche difficoltà, infatti se in α vi è una variabile libera x_1, allora α può essere vera o falsa a seconda dell'elemento rappresentato da x_1. Ad esempio la formula $\forall x_2(x_2 \cdot x_1 = x_2)$ sarà vera negli interi relativi se x_1 rappresenta l'unità, sarà falsa se x_1 rappresenta il numero 2. Ciò significa che ha senso dire se α è vera o falsa non solo dopo aver fissato una interpretazione I del linguaggio ma anche dopo aver assegnato ad ogni variabile libera di α un particolare elemento nel relativo dominio. Per evitare complicazioni formali nel seguito supponiamo che anche le variabili vincolate siano interpretate da elementi del dominio. Pertanto se le variabili libere o vincolate di α sono tra $x_1,...,x_m$, dati $d_1,...,d_m$ elementi di D vogliamo dare una definizione precisa del concetto:

"α è vera rispetto alla interpretazione I quando le sue eventuali variabili libere sono interpretate con $d_1,...,d_m$ ".
Indicheremo in breve con $I \models \alpha\,[d_1,...,d_m]$ una tale asserzione e ne daremo la seguente definizione formale. Per semplicità utilizziamo la notazione prefissa anche per i predicati binari.

Definizione 7.1. Sia I una interpretazione, sia α una formula le cui variabili libere o vincolate siano tra $x_1,...,x_m$ e siano $d_1,...,d_m$ elementi del dominio D. Allora la relazione $I \models \alpha\,[d_1,...,d_m]$ è definita per induzione sulla complessità di α tramite:

a) $I \models r(t_1,...,t_p)\,[d_1,...,d_m]$ se
$$(I(t_1)(d_1,...,d_m),..., I(t_2)(d_1,...,d_m)) \in I(r)$$
b) $I \models \alpha\wedge\beta\ [d_1,...,d_m]$ se $I\models\alpha\ [d_1,...,d_m]$ e $I\models\beta\ [d_1,...,d_m]$
c) $I \models \alpha\vee\beta\ [d_1, ... ,d_m]$ se $I\models\alpha\ [d_1,...,d_m]$ oppure $I\models\beta\ [d_1,...,d_m]$
d) $I \models \neg\alpha\ \ [d_1,...,d_m]$ se non è vero che $I\models\alpha\ \ [d_1,...,d_m]$
e) $I \models \exists x_i(\alpha)\,[d_1,...,d_m]$ se esiste $d\in D$ tale che
$I \models \alpha\,[d_1,...,d_{i-1},d,d_{i+1}...,d_m]$.

Si noti che
$I \models \forall x_i(\alpha)\,[d_1,...,d_m] \Leftrightarrow I\models \alpha\,[d_1,...,d_i,...,d_m]$ per ogni $d_i\in D$.
Infatti, poiché $\forall x_i(\alpha)$ è una abbreviazione di $\neg(\exists x_i(\neg\alpha))$, avremo che
$I \models \forall x_i(\alpha)\,[d_1,...,d_m]$
$\Leftrightarrow$ non è vero che $I \models \exists x_i(\neg\alpha)\,[d_1, ... ,d_m]$
$\Leftrightarrow$ non è vero che esiste $d_i\in D$ tale che $I \models \neg\alpha\ [d_1,...,d_i,...,d_m]$
$\Leftrightarrow$ per ogni $d_i\in D$ $\ I \models \alpha\ [d_1,...,d_i,...,d_m]$.

Definizione 7.2. Se $I \models \alpha\,[d_1,...,d_m]$ diciamo che *la formula α è vera rispetto ad I negli elementi* $d_1,...,d_m$. Diciamo che *α è vera* in I o che *I è un modello di* α e scriviamo $I \models \alpha$, se risulta $I \models \alpha\,[d_1,...,d_m]$ per ogni $d_1,...,d_m$ in D.

In altre parole dire che una formula con eventuali variabili libere è vera in una interpretazione I equivale a dire che la sua chiusura universale è vera. Ad esempio diciamo che $x_1\cdot x_2 = x_2\cdot x_1$ è vera in una interpretazione I se $I \models x_1\cdot x_2=x_2\cdot x_1\ [d_1,d_2]$ comunque si scelgano d_1 e d_2 nel dominio di interpretazione, cioè se $I \models \forall x_1\forall x_2(x_1\cdot x_2=x_2\cdot x_1)$.

8. Teorema di completezza

Siamo ora pronti a parlare di cinque teoremi fondamentali della logica. Il primo parla in positivo sottolineando una cosa (formidabile) che la logica formale riesce a fare. Gli altri, di cui parleremo nel prossimo paragrafo, parlano in negativo mostrando cose che la logica formale non potrà mai fare.

Abbiamo definito la relazione $\models$ che è di carattere semantico e la relazione $\vdash$ che è di carattere sintattico, cioè relativa ai processi di manipolazione di parole. Il seguente teorema mostra che le due nozioni sono ben collegate.[16]

Teorema 8.1. (**Teorema di Completezza**[17]) Per ogni teoria T ed ogni formula chiusa α risulta:

$$T \models \alpha \;\Leftrightarrow\; T \vdash \alpha .$$

Per rendersi conto dell'importanza di tale teorema, osserviamo che la verifica della relazione $T \models \alpha$ richiede l'andare a guardare tutti i possibili modelli di T e nel controllare per ciascun modello se verifica l'asserzione α. Ad esempio se T è la teoria dei gruppi si tratta di verificare che α vale in tutti i possibili gruppi. E' questa una impresa che è impossibile in quanto la classe dei gruppi è tanto grande da condurre, come abbiamo visto, a paradossi. Il teorema di completezza ci dice che verificare $T \models \alpha$ è una impresa meno disperata in quanto sembri. Infatti equivale a verificare $T \vdash \alpha$ cioè che la macchina finita che produce passo dopo passo i teoremi di T riesce a produrre anche α. D'altra parte se non valesse il teorema di completezza saremmo nella situazione per cui, ad esempio, esistono asserzioni vere in tutti i gruppi ma che non abbiamo nessuna speranza di poter dimostrare.

Un teorema che è sostanzialmente equivalente al teorema di completezza è il seguente dove si ricorda che una teoria è detta *consistente* se da tale teoria non è possibile derivare una contraddizione.

---

[16] Tale teorema, che è uno dei primi, più importanti ed affascinanti teoremi di logica matematica, è stato dimostrato nel 1929 da Kurt Gödel nella sua tesi di dottorato.

[17] E' molto importante osservare che invece la logica del secondo ordine non verifica un teorema di completezza. Questo significa che qualunque tentativo di trovare un sistema inferenziale per tale logica risulta necessariamente inadeguato.

Teorema 8.2. Una teoria è consistente se e solo se ammette un modello.

9. Teoremi limitativi

Il prima teorema limitativo lo abbiamo già enunciato nel primo volume quando abbiamo parlato della nozione di computabilità.imostrazione è dovuta a Turing.

Teorema 9.1. (Teorema di Turing). L'insieme delle espressioni vere dell'aritmetica non è decidibile.

In altre parole, non esiste un programma tale che, dato come input una asserzione dell'aritmetica, fornisca output 1 se l'asserzione è vera, 0 se è falsa.

Ed ecco altri due (famosi) teoremi provati da Gödel nel 1930. Per una loro dimostrazione, come d'altra parte per il teorema di completezza, si rimanda ad un buon testo di logica. Qui ci limitiamo ad enunciarli ed ad esporre le linee generali della dimostrazione del primo teorema per evidenziare come tale dimostrazione dipenda dalla possibilità di autoriferimento di una teoria che sia capace di parlare degli interi. Per semplicità consideriamo una teoria che è formulazione nell'ambito della logica del primo ordine della teoria delle terne di Peano.

Definizione 9.2. Concideriamo un linguaggio con un nome di funzione s ed una costante z_0. Chiamiamo *teoria del primo ordine per le terne di Peano* il seguente sistema di assiomi:

A1 $s(x) = s(y) \rightarrow x = y$

A2 $\forall x\, z_0 \neq s(x)$

A3 $(A(z_0) \wedge \forall x(A(x) \rightarrow A(s(x)))) \rightarrow \forall x A(x)$.

Si noti che *A1* e *A2* coincidono con gli assiomi *P1* e *P2* che abbiamo già visto nel primo volume quando abbiamo definito le terne di Peano. Invece *A3* non coincide con *P3*. La differenza è che *P3* è un assioma del secondo ordine in quanto è presente una quantificazione sui sottoinsiemi. Invece *A3* è uno "schema di assiomi" nel senso che deve essere inteso come rappresentante gli infiniti assiomi che si ottengono fissando in tutti i modi possibili una formula $A(x)$ con una variabile libera x. Pertanto *A3* asserisce il principio di induzione solo per gli insiemi che sono "descrivibi-

li" tramite una formula $A(x)$ del linguaggio fissato. Poiché esiste solo una quantità numerabile di formule, i sottoinsiemi descrivibili sono in quantità numerabile mentre la classe dei sottoinsiemi di un insieme infinito ha sicuramente potenza maggiore del numerabile. Quindi nella formulazione del primo ordine degli assiomi di Peano il principio di induzione viene richiesto per molti meno insiemi.[18]

Teorema 9.3. (Primo Teorema di Gödel) Sia T la teoria del primo ordine delle terne di Peano e supponiamo che sia consistente. Allora esiste una formula ϕ indecidibile in T, cioè che non può essere né provata né confutata da T.

L'idea per dimostrare tale teorema è ispirata al famoso paradosso che si ottiene considerando l'asserzione

$$\gamma \equiv \textit{"io sono una proposizione falsa"}.$$

Allora risulta che

$$\gamma \text{ vera} \Rightarrow \gamma \text{ falsa} \quad ; \quad \gamma \text{ falsa} \Rightarrow \gamma \text{ vera}$$

e pertanto γ non può essere né vera né falsa. Alla base di tale antinomia è il fatto che γ è una proposizione che parla di se stessa, cioè il fenomeno dell' "autoriferimento". Ora una prima "rozza"

---

[18] Naturalmente il fatto che quanto affermato da *P3* sembra essere più potente da quanto affermato dall'insieme *A3* di formule non escluderebbe in linea di principio che si possa dimostrare l'equivalenza delle due formulazioni. In altre parole non escluderebbe che il principio di induzione per la classe dei sottoinsiemi descrivibili possa implicare il principio di induzione per tutti i sottoinsiemi. Per potere convincersi che non sussiste l'equivalenza dovremmo infatti mostrare che esiste un modello di *A1*, *A2*, *A3* che non verifica *P1*, *P2*, *P3*. Il materiale per trovare un tale modello lo possiamo trovare nel campo di razionali non-standard che abbiamo ottenuto come ultra-potenza di Q. Infatti chiamiamo *numero naturale non-standard* un elemento $[(r_n)_{n\in N}]$ di Q^* con $(r_n)_{n\in N}$ successione di numeri naturali. Detto N_0^* l'insieme di tali numeri, definiamo la funzione $s : N_0^* \to N_0^*$ ponendo $s([(r_n)_{n\in N}]) = [(r_n+1)_{n\in N}]$. Allora $(N_0^*, s, 0)$ verifica *A1, A2, A3* ma non verifica *P3.* Infatti per un teorema fondamentale della teoria delle ultrapotenze, $(N_0^*, s, 0)$ verifica tutte le proprietà dell'insieme dei naturali che siano esprimibili al primo ordine. In particolare $(N_0^*, s, 0)$ verifica *A1, A2, A3*. D'altra parte l'insieme degli interi che non sono infiniti, pur contenendo 0 e pur essendo chiuso per successore, non coincide con N_0^*. Quindi non verifica *P3*.

dimostrazione del primo teorema di Gödel si ottiene partendo dall'asserzione simile

γ = *"io sono una formula che non è un teorema di T"*.

Allora, se si ammette che una tale asserzione sia esprimibile tramite una formula γ del linguaggio $\mathcal{L}$ e che la nostra logica sia corretta (cioè dimostra cose vere), allora

- se $T \vdash \gamma$ allora γ è vera e quindi γ non è un teorema di T;
- se $T \vdash \neg\gamma$ allora γ è falsa e quindi γ è un teorema di T

Pertanto, come volevamo dimostrare, né γ né la sua negata $\neg\gamma$ possono essere teoremi di T.

Per potere formalizzare quanto sopra detto, è necessario che sia possibile il fenomeno dell' autoriferimento, abbiamo cioè bisogno di far vedere come T possa "parlare di se stesso". In particolare, perché quel termine "io" abbia senso deve essere dato un nome all'interno del linguaggio $\mathcal{L}$ a ciascuna delle formule di $\mathcal{L}$. Inoltre deve essere definita una formula in $\mathcal{L}$ che significhi "essere teorema". Per fare ciò cominciamo con il mettere in rilievo che:

ogni numero naturale ha un "nome" corrispondente in $\mathcal{L}$.

Infatti nel linguaggio delle terne di Peano, che contiene il simbolo s di successivo, possiamo dare un nome ad ogni numero denotando

- con il termine chiuso $s(0)$ il numero uno,
- con $s(s(0))$ il numero due

... e così via.

Inoltre

è possibile codificare le formule di $\mathcal{L}$.

Cioè è possibile associare ad ogni formula ϕ un numero intero detto *numero di codice* di ϕ. Da ciò segue che:

Ad ogni formula ϕ di $\mathcal{L}$ può essere assegnato un "nome" $c(\phi)$ in $\mathcal{L}$ considerando il termine chiuso $c(\phi)$ che rappresenta il numero di codice di ϕ.

Similmente si vede che:

si può dare un numero di codice ad ogni dimostrazione π in T.

La cosa non è difficile poiché una dimostrazione può essere vista come una sequenza di formule $\alpha_1, \alpha_2, \ldots, \alpha_n$ e tale sequenza è una parola nell'alfabeto che si ottiene aggiungendo all'alfabeto A il simbolo ","[19]. Si può pertanto procedere allo stesso modo di quanto si è fatto per la codifica delle formule.

Ad ogni dimostrazione π può essere assegnato un "nome" $c(\pi)$,

Come nel caso delle formule basta considerare il termine chiuso che rappresenta il numero di codice di π.
Detto questo si dimostra (ma noi non lo dimostriamo) che in $\mathcal{L}$ esiste una formula $Pr(x,y)$ il cui significato è che x è (il numero di codice di) una dimostrazione di y (della formula codificata da y). Più precisamente Pr verifica la seguente proprietà

$$\text{"}T \vdash \phi \text{ se e solo se esiste un termine chiuso } t \text{ tale che } T \vdash Pr(t,c(\phi))\text{"}.$$

Infine si prova l'esistenza di una formula γ tale che

$$T \vdash \gamma \leftrightarrow (\neg\exists x Pr(x,c(\gamma))).$$

La formula γ asserisce proprio quello che volevamo, cioè che "io sono una formula che non è un teorema di T". Supponiamo ora che γ sia dimostrabile, allora sarebbe dimostrabile anche $\neg\exists x Pr(x,c(\gamma))$ e quindi non potrebbe esistere una dimostrazione di γ in T. Supponiamo invece che $\neg\gamma$ sia dimostrabile, allora sarà dimostrabile in T anche $\exists x Pr(x,c(\gamma))$. Ciò comporta che esiste un termine chiuso t per cui $Pr(t,c(\gamma))$ e pertanto che esiste una dimostrazione di γ. Ciò è in contrasto con l'ipotesi di consistenza per T.

Corollario 9.4. Se T è consistente, allora esiste una asserzione dell'aritmetica che pur essendo vera non può essere dimostrata. In altre parole T non è abbastanza potente da permettere di provare tutte le proposizioni vere dell'aritmetica.

[19] Per motivi tecnici che qui sarebbe troppo lungo spiegare la codifica delle dimostrazioni deve essere un processo effettivo e questa effettività richiede che l'insieme degli assiomi della teoria sia decidibile, cioè che esista un procedimento effettivo per capire se una formula è un assioma oppure no.

Dim. Sia ϕ la formula indecidibile la cui esistenza è stata provata nel primo teorema di Gödel. Se si ammette il modello naturale dell'aritmetica, allora in tale modello sarà vera ϕ oppure $\neg\phi$. Nel primo caso ϕ è una proposizione vera che non può essere dimostrata, nel secondo caso la stessa cosa si può dire per $\neg\phi$. □

Del secondo teorema di Gödel diamo solo l'enunciato. Da notare che anche per tale teorema la possibilità di autoriferimento è essenziale.

Teorema 9.5. (Secondo Teorema di Gödel). Se T è consistente, allora la formula $\neg\exists x Pr(x, \gamma\wedge\neg\gamma)$ che asserisce la consistenza di T non si può provare in T.

Quanto ora dimostrato non vale solo per la teoria del primo ordine delle terne di Peano ma per ogni teoria che sia abbastanza potente da permettere di definire i numeri naturali e quindi per ogni teoria che pretenda di fondare la matematica. Ad esempio vale anche per tutte le teorie che vogliano assiomatizzare la nozione di insieme. In particolare, il secondo teorema di Gödel mostra che qualunque sia tentativo di fornire un adeguato sistema di assiomi T per la matematica, la consistenza di T non può essere provata all'interno della stessa teoria T. In altri termini per provare la consistenza di T dobbiamo necessariamente utilizzare strumenti più potenti di T stesso. Non è quindi possibile, come sperava Hilbert, provare la consistenza di teorie "forti" che coinvolgono l'infinito attuale tramite metodi finitisti.

10. Un po' di storia: la teoria dei sillogismi di Aristotele

In questo capitolo abbiamo parlato della logica in quanto strumento proposto da Hilbert per la fondazione della matematica e siamo quindi partiti dagli inizi del 1900. Tuttavia la logica è sempre stata un capitolo fondamentale della filosofia risalente, tanto per cambiare, agli antichi greci ed avente come scopo lo studio delle forme corrette del ragionamento (non necessariamente matematico). Infatti la logica è già trattata in modo ampio e sistematico da Aristotele (340 A.C.) e dalla scuola stoica (300 A.C.). In particolare è famosa la teoria dei sillogismi di Aristotele che è stata oggetto di studio obbligatorio nelle scuole ed università fino al secolo diciassettesimo.

Aristotele analizza i vari tipi di ragionamento fatti dagli esseri umani e per prima cosa osserva che tutti i ragionamenti si riferiscono ad enunciati di quattro tipi:

A. Universale affermativo: es. "tutti i greci sono mortali"
I. Particolare affermativo: es. "alcuni greci sono mortali"
E. Universale negativo: es. "nessun greco è mortale"
O. Particolare negativo: es. "alcuni greci non sono mortali".[20]

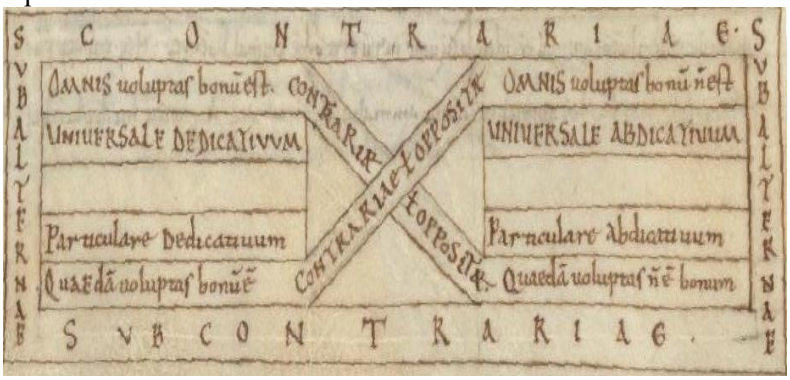
Se utilizziamo il linguaggio attuale della logica matematica ed indichiamo con P la proprietà "essere greco" e con Q la proprietà "essere mortale" possiamo riscrivere tali asserzioni come segue:

A. Universale affermativo: $\forall x(P(x)\rightarrow Q(x))$
I. Particolare affermativo: $\exists x(P(x)\wedge Q(x)$
E. Universale negativo: $\forall x(P(x)\rightarrow\neg Q(x))$
O. Particolare negativo: $\exists x(P(x)\wedge\neg Q(x))$.

Se supponiamo che $\forall xP(x)$ sia vera, allora tali formule assumono la forma simmetrica

$$\forall xQ(x),\ \exists xQ(x),\ \forall x\neg Q(x),\ \exists x\neg Q(x).$$

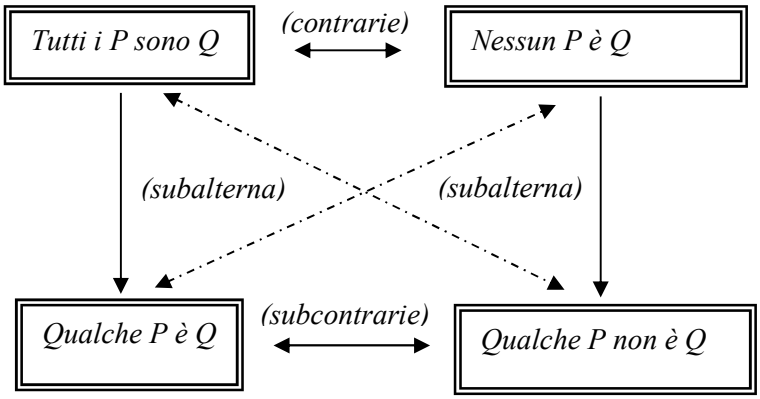
Tra tali enunciati esistevano vari rapporti che, nel medioevo, venivano rappresentati tramite la seguente configurazione chiamata "quadrilatero di Aristotele":



[20] Le lettere A, E, I, O utilizzate per indicare tali tipi di enunciati sono state introdotte dai logici medioevali.

Le parole, in latino, che si leggono rappresentano relazioni intercorrenti tra i tipi di enunciati. Nella figura seguente si riporta in chiaro un tale tipo di schema:

Quadrilatero Aristotelico delle proposizioni



Le due diagonali punteggiate collegano proposizioni *contraddittorie* cioè tali che una equivale alla negazione dell'altra. Le due frecce verticali collegano proposizioni in cui quella di sotto viene chiamata *subalterna* di quella di sopra. La prima doppia freccia orizzontale collega proposizioni che vengono dette *contrarie* tra loro. La seconda doppia freccia orizzontale collega proposizioni che vengono dette *subcontrarie* tra di loro.

Chiarita la nozione di enunciato, Aristotele passa ad individuare quelle che ritiene le forme possibili di ragionamento, cioè i sillogismi. Ecco un esempio di sillogismo come esposto da Aristotele:

«Se *A* si predica di ogni *B*, e se *B* si predica di ogni *C*, è necessario che *A* venga predicato di ogni *C*» (*Analitici primi* I.4, 25 *b*38-39).

In termini più semplici:

Se ogni B è A e se ogni C è B allora ogni C è A.

Come si vede un sillogismo deve avere due premesse e una conclusione e le due premesse devono avere in comune un predicato (il predicato denotato con *B*).

Definizione 10.1. Un sillogismo è una forma di argomentazione del tipo «se *p* e *q*, allora *r*», dove le tre lettere *p*, *q*, *r* denotano asserzioni del tipo *A*, *I*, *E*, *O* e dove le premesse *p* e *q* hanno un predicato in comune.

Tale definizione di sillogismo è solo di carattere sintattico e non distingue tra sillogismi "buoni" come quello che abbiamo indicato e sillogismi "cattivi" come ad esempio

Se ogni B è A e se ogni B è C allora ogni C è B.

Definizione 10.2. Un sillogismo «se *p* e *q*, allora *r*» è detto *corretto* o *valido* se, supponendo che tutti i predicati coinvolti siano non vuoti, risulta che tutte le volte che le premesse *p* e *q* sono vere allora il conseguente *r* è vero.

Per predicato "non vuoto" si intende un predicato la cui estensione sia non vuota, cioè un predicato che è verificato da almeno un elemento. Questa richiesta non viene esplicitata da Aristotele ma, come vedremo, è necessaria. .

A partire da tali definizioni, è possibile analizzare in modo sistematico tutte le possibili forme che potrebbe avere un sillogismo ed ad isolare fra queste quelle relative a sillogismi validi.

Teorema 10.3. Esistono 256 possibili forme di sillogismi di cui solo 24 sono valide.

Dim. Abbiamo detto che un sillogismo ha la forma: «se *p* e *q*, allora *r*» dove al posto delle lettere *p*, *q*, *r* devono essere scritte opportune asserzioni. Scriviamo

aXY per indicare che tutti gli *X* sono *Y*
iXY per indicare che alcuni *X* sono *Y*
eXY per indicare che nessun *X* è *Y*
oXY per indicare che alcuni *X* non sono *Y*.

dove *X*, *Y* denotano una delle tre lettere *A*, *B* e *C*.
Indichiamo con "... *A è C*" la conclusione di un sillogismo e *B* il predicato che è comune alla premessa maggiore ed alla premessa minore. Allora la forma generale di un sillogismo sarà del tipo

se ... X_1B e ... BX_2, allora ... *AC*

dove al posto dei puntini deve essere messa una delle quattro lettere {*a*, *e*, *i*, *o*} ed al posto di X_1, X_2 vanno messe le lettere *A*, *C*.

Esistono allora tanti sillogismi quanti sono gli elementi dell'insieme

$\{a, e, i, o\}\times\{A,C\}\times\{a, e, i, o\}\times\{A,C\}\times\{a, e, i, o\}$.

La cardinalità di un prodotto cartesiano è data dal prodotto delle cardinalità degli insiemi componenti, pertanto nel nostro caso avremo $3\times2\times3\times2\times3 = 256$. Non rimane altro che esaminarli pazientemente uno ad uno per potere isolare quelli validi. I diagrammi di Eulero-Venn che saranno trattati nel seguito possono essere lo strumento con cui può essere effettuato tale controllo che tuttavia, essendo piuttosto noioso, non facciamo. □

E' importante mettere in rilievo che per potere parlare di validità di un sillogismo è essenziale che vengano usate variabili predicative come A, B, C per denotare i predicati. Infatti possiamo dire che un sillogismo è valido se permette di passare da premesse vere a conclusioni vere qualunque sia l'interpretazione di tali variabili.[21]

Poiché nel medioevo Aristotele era considerato l'autore più importante ed autorevole, uno studente di quei tempi doveva ricordare tutti i sillogismi validi. Per aiutare la memoria si utilizzavano alcuni trucchi. Infatti ogni tipo di sillogismo veniva indicato da una parola latina, in cui le tre vocali indicano il tipo di quantificazione adottato. Precisamente, come abbiamo già visto,

- la vocale *a* serve a ricordare "ogni",
- la vocale *e* serve a ricordare "nessuno",
- la vocale *i* serve a ricordare "qualche",
- la vocale *o* serve a ricordare "non ogni".

Ecco dunque l'elenco completo dei 24 sillogismi validi:

[21] L'uso delle variabili per denotare enti generici è una delle scoperte più feconde di tutti i tempi, che ha reso possibile lo sviluppo tanto della logica quanto della matematica. Solo tramite esse si possono infatti formulare in maniera semplice leggi universali, proprio quelle di cui Aristotele andava alla ricerca nella sua analitica. Dopo Aristotele, per ritrovare un uso sistematico delle variabili in matematica bisogna attendere gli algebristi del 1600. In realtà forse sia per i sillogismi che per le equazioni sarebbe più corretto parlare di "parametri" che di "variabili" in quanto una delle caratteristiche delle variabili è che possono essere quantificate, cosa che in questi casi non avviene.

1ª figura: barbara, darii, celarent, ferio, barbari, celaront

2ª figura: cesare, camestres, baroco, festino, cesaro, camestrop

3ª figura: darapti, datisi, disamis, felapton, ferison, bocardo

4ª figura: bamalip, camenes, fesapo, fresison, dimaris, camelop

Diamo ora un esempio per ciascuna delle quattro figure:

1. **barbara:** se ogni *A* è *B* e ogni *B* è *C*, allora ogni *A* è *C*

2. **camestres:** se ogni *C* è *B* e nessun *A* è *B*, allora nessun *A* è *C*

3. **felapton:** se nessun *B* è *C* e ogni *B* è *A*, allora non ogni *A* è *C*

4. **fresison:** se nessuno *C* è *B* e qualche *B* è *A*, allora non ogni *A* è *C*

A questo punto, ovviamente, è possibile sostituire alle lettere qualsiasi nome: il ragionamento sarà sempre corretto, e, se le premesse saranno vere, si otterrà una conclusione vera (ovvero un «sillogismo dimostrativo»). Ecco un celebre esempio di un sillogismo barbara:

«se ogni uomo è mortale ed ogni ateniese è uomo, allora ogni ateniese è mortale»[22]

E' importante sottolineare il carattere sistematico e generale delle ricerche di Aristotele e dei suoi successori.

---

[22] Più famoso è il seguente "sillogismo":

«Socrate è un uomo, gli uomini sono mortali, quindi Socrate è mortale»

Tutavia tale argomentazione non rientra in senso stretto nella definizione data da Aristotele di sillogismo che coinvolge predicati monadici e non termini individuali quali "Socrate". Tuttavia questo limite non mi sembra importante se si pensa che "essere Socrate" può essere considerata un predicato monadico. L'argomentazione può allora essere riscritta dicendo:

«Essere socrate comporta essere uomo, tutti gli uomini sono mortali, quindi essere Socrate comporta essere mortale»

11. Il contributo degli stoici

Come abbiamo visto, in Aristotele il ruolo dei quantificatori è centrale. Pertanto la logica di Aristotele può essere vista come un pezzo di quella che sarà chiamata *logica dei predicati* oppure *logica del primo ordine.* Gli stoici si occuparono invece di studiare il ruolo dei principali connettivi logici nelle varie forme di ragionamento. In altre parole si interessarono principalmente a quello che attualmente viene chiamato *calcolo proposizionale*. Studiarono inoltre alcune regole di inferenza quali il *Modus Ponens* e sue variazioni. Non si hanno molti documenti diretti degli stoici. Ecco ad esempio come ne parla Sesto empirico, un filosofo di indirizzo diverso.

Gli Stoici immaginano un gran numero di ragionamenti indimostrati, ma ne espongono specialmente questi cinque, ai quali sembrano ridursi tutti i rimanenti:

1°) quello che dalla implicazione e dall'antecedente conclude il conseguente, come "Se è giorno, c'è luce. Ma è giorno. Dunque c'è luce. (In termini attuali: *da* $\alpha \rightarrow \beta$ *ed* α *segue* β*.* Tale regola di inferenza viene chiamata *Modus ponens*).

2*) Quello che dalla implicazione e dal contrario del conseguente conclude il contrario dell'antecedente, come: "Se è giorno, c'è luce. Ma non c'è luce. Dunque non è giorno".*
(In termini attuali*:* da $\alpha \rightarrow \beta$ e $\neg \beta$ segue $\neg \alpha$)

3) *Quello che da un collegamento negativo e da una delle parti del collegamento conclude il contrario dell'altra parte, come "Non è giorno e notte. Ma è giorno. Dunque non è notte".* (Cioè: da $\neg(\alpha \wedge \beta)$ ed α*,* segue $\neg \beta$)

4) *Quello che da un collegamento disgiuntivo e da una delle parti collegate conclude il contrario dell'altra, come "O è giorno o è notte. Ma è giorno. Dunque non è notte"* .
(Cioè: da $\alpha \vee \beta$ ed α segue $\neg \beta$, da notare che ci si riferisce alla disgiunzione esclusiva)

5) *Quello che da un collegamento disgiuntivo e dal contrario di una delle parti collegate conclude l'altra, come: "O è giorno, o è notte, ma non è notte. Dunque è giorno"*
(Cioè: da $\alpha \vee \beta$ e $\neg \alpha$ segue β)

(Sesto Empirico: *Schizzi pirroniani*, II, 109-117).

Da notare che gli stoici non adottarono la notazione simbolica di Aristotele e che questo fu di forte impedimento allo sviluppo delle loro ricerche. Ad esempio se dovevano esprimere la regola del Modus Ponens che noi enunciamo col dire

da $\alpha \rightarrow \beta$ *ed* α *segue* β

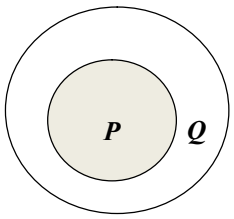
esprimevano una tale regola dicendo

se il primo allora il secondo e se il primo, allora il secondo.

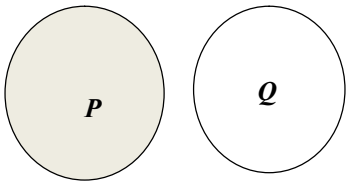
Scritta in questo modo la regola risulta di difficile lettura e uso.

12. Diagrammi di Eulero-Venn, algebre di Boole, sillogismi

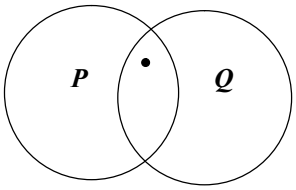
La prima reale evoluzione della logica di Aristotele avviene quando con Boole viene proposta una algebrizzazione della teoria dei sillogismi. Un piccolo passo verso tale algebrizzazione è l'interpretazione "insiemistica" dei sillogismi escogitata per scopi didattici dal matematico svizzero Leonhard Euler nel 1770 (*Lettere a una principessa tedesca*, Boringhieri, Torino, 1958) e successivamente migliorata da John Venn. Ogni proprietà viene interpretata come insieme di punti interni ad una curva chiusa, insieme che viene visto come l'insieme dei punti che verificano tale proprietà. In tale modo i quattro tipi di asserzione che costituiscono il quadrilatero di Aristotele possono essere rappresentati dai seguenti diagrammi.



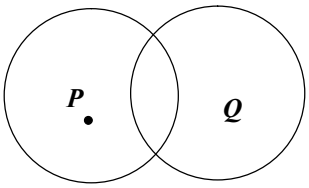
Tutti i P sono Q



Nessun P è Q



Qualche P è Q



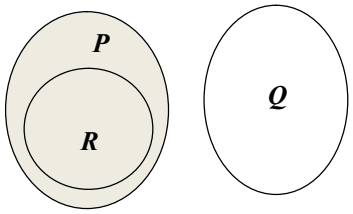
Qualche P non è Q

Nella prima linea abbiamo posto in grigio l'estensione di *P* per evidenziare il fatto che ci si riferisce "tutti gli elementi *P*". Nella seconda linea il puntino nero evidenzia l'esistenza di un oggetto in *P* che è in *Q* nel primo caso che non è in *Q* nel secondo. E' evidente che tale rappresentazione non è possibile se *P* o *Q* hanno estensione vuota, cioè nel caso in cui non esista un elemento che verifica *P* oppure nel caso in cui non esista un elemento che verifica *Q*.

Possiamo esaminare la correttezza dei sillogismi utilizzando tali diagrammi: ad esempio consideriamo il sillogismo

Tutti gli *R* sono *P*
Nessun *P* è *Q*
quindi Tutti gli *R* sono *Q*

Allora possiamo rappresentare le premesse al modo seguente:



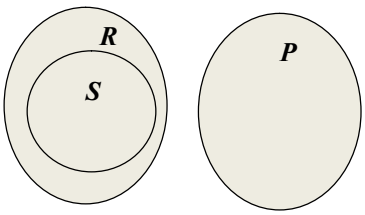
e da tali diagrammi appare evidentemente che la conclusione è falsa. Pertanto il sillogismo non è valido. Dallo stesso diagramma si "evince" invece che è valido il sillogismo

Tutti gli *R* sono *P*
Tutti i *P* non sono *Q*
quindi tutti gli *R* non sono *Q*

Consideriamo ora il seguente sillogismo Celarent

Nessun rettile ha la pelliccia
Tutti i serpenti sono rettili
quindi Nessun serpente ha la pelliccia

La sua giustificazione è data dal seguente diagramma.



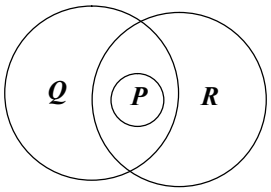
Esercizio. Riconoscere quale sillogismo è alla base del seguente ragionamento e se tale sillogismo è corretto:

"Tutti i padani sono gran lavoratori"
"Qualcuno in questa fabbrica è gran lavoratore"
pertanto
"Qualcuno in questa fabrica è padano".

Nota: il problema delle proprietà vuote. Consideriamo il sillogismo

Tutti i P sono Q
Tutti i P sono R
quindi qualche P è R

Le premesse possono essere rappresentate dal seguente diagramma:



in cui il conseguente è vero. Tale diagramma suggerisce che il sillogismo è valido. Tuttavia tale validità dipende dall'ipotesi per cui P è non vuoto. Ad esempio, poniamo al posto di P il predicato $A \wedge \neg A$. Allora dal fatto che sono vere le premesse[23]

tutti gli elementi tali che $A \wedge \neg A$ sono Q
tutti i gli elementi tali che $A \wedge \neg A$ sono R

dovrebbe seguire che

qualche $A \wedge \neg A$ è R,

ciòé dovrebbe seguire l'esistenza di un elemento che verifica $A \wedge \neg A$. Ciò è evidentemente assurdo.

[23] Ricordiamo che un implicazione il cui antecedente è falso risulta essere vera indipendentemente dal valore di verità del conseguente.

Si osservi che la validità del metodo dei diagrammi andrebbe dimostrata. Infatti per provare che una forma di sillogismo è corretta si dovrebbe verificare che essa risulta valida in tutti le possibili interpretazioni delle lettere coinvolte. Non solo quindi per le interpretazioni in cui i predicati si riferiscono ad insiemi di punti del piano. E' interessante osservare che invece per provare che una forma di sillogismo non è corretta basta osservare che non è corretta anche in un solo un caso. Pertanto le dimostrazioni di non correttezza tramite i diagrammi sono completamente valde. In altre parole è evidente che il metodo di Eulero è perfettamente adeguato per confutare la validità di un tipo di sillogismo ma andrebbe giustificato se si volesse utilizzarlo per provarne la validità.[24]

Saranno le strutture algebriche proposte da Boole in *Analisi matematica della logica* (1847) e in *Indagine sulle leggi del pensiero* (1854) ad essere uno strumento generale e rigoroso per la trattazione matematica dei sillogismi. L'dea è di rappresentare i predicati come elementi di un'algebra di Boole (per la definizione di algebra di Boole si veda l'Appendice del primo volume) e fare l'ipotesi che le leggi del pensiero siano rappresentate dagli assiomi della teoria delle algebre di Boole. Allora la dimostrazione di validità di un sillogismo diventa la dimostrazione di un teorema nella teoria delle algebre di Boole.

Per mostrare come ciò sia possibile, consideriamo un algebra di Boole e riscriviamo le quattro asserzioni al modo seguente:

A	Tutti gli X sono Y	traduzione	$x \leq y$
E	Nessun X è Y	traduzione	$x \leq -y$
I	Qualche X è Y	traduzione	$x \not\leq -y$

[24] Chi è a conoscenza di un po' di logica matematica potrebbe dimostrare la validità universale del metodo dei diagrammi per i sillogismi ricavandola dalla dimostrazione della decidibilità della logica monadica. Infatti la validità di un sillogismo si traduce nella dimostrazione che una implicazione del tipo $p \wedge q \rightarrow r$ è logicamente vera, cioè è vera in tutte le possibili interpretazioni. D'altra parte nella logica monadica si prova che una asserzione risulta logicamente vera se è vera in tutti i modelli il cui dominio D ha 2^n elementi, dove n è il numero di predicati coinvolti (proprietà del modello finito). Poiché in un sillogismo sono coinvolti solo tre predicati, basta fissare un insieme D di 8 punti nel piano ed interpretare in tutti i modi possibili tali predicati come sottoinsiemi non vuoti di D.

O Qualche *X* non è *Y* traduzione $x \not\leq y$.[25]

Equivalentemente, ricordando che in un' algebra di Boole una diseguaglianza del tipo $x \leq y$ può essere espressa da una equazione del tipo $x \wedge y = x$, possiamo tradurre in termini algebrici i quattro tipi fondamentali di asserzioni.

A Tutti gli *X* sono *Y* traduzione $x \wedge y = x$
E Nessun *X* è *Y* traduzione $x \wedge \text{-}y = 0$
I Qualche *X* è *Y* traduzione $x \wedge y \neq 0$
O Qualche *X* non è *Y* traduzione $x \wedge \text{-}y \neq 0$.[26]

Allora un sillogismo consiste nel derivare da un paio di equazioni o disequazioni una equazione o una disequazione.

Consideriamo ad esempio il sillogismo barbara

Tutti gli *R* sono *P*
Tutti i *P* non sono *Q*
quindi Tutti gli *R* non sono *Q*

Se indichiamo con *r*, *p*, *q* tre elementi di un algebra di Boole che corrispondono rispettivamente ad *R*, *P* e *Q*, allora

- la prima premessa diventa l'equazione
  $r \wedge p = r$
- la seconda premessa
  $p \wedge \text{-}q = p$
- la conclusione
  $r \wedge \text{-}q = r$.

Quindi il sillogismo equivale a dire che dalle prime due equazioni deriva la terza. Questa cosa d'altra parte è facilmente dimostrabile tramite la seguente serie di equazioni

$$r = r \wedge p = r(p \wedge \text{-}q) = (r \wedge p) \wedge \text{-}q = r \wedge \text{-}q$$

ottenute a partire dalla prima, utilizzando la seconda, poi la proprietà associativa, poi di nuovo la prima.[27]

---

[25] In realtà la traduzione fatta da Boole è leggermente diversa. Invece di scrivere ad esempio $x \cdot y \neq 0$ scrive $x \cdot y = v$ aggiungendo l'informazione che v è diverso da 0. In questo modo i quattro enunciati diventano tutti delle equazioni. Tuttavia in questo modo il calcolo smette di essere puramente algebrico.

[26] In realtà la traduzione fatta da Boole è leggermente diversa. Invece di scrivere ad esempio $x \wedge y \neq 0$ scrive $x \wedge y = v$ aggiungendo l'informazione che v è diverso da 0. In questo modo i quattro enunciati diventano tutti delle equazioni. Tuttavia in questo modo il calcolo smette di essere puramente algebrico.

[27] Questa indiscutibilmente è una dimostrazione, ma in realtà è una dimostrazione solo che nell'ambito della teoria delle algebre di Boole dal-

13. Limiti della logica Aristotelica

Per la logica di Aristotele e per la successiva algebrizzazione fatta da Boole esistono notevoli limiti. Ne elenchiamo i principali.

1. Il limite più importante è che i soli predicati accettati sono monadici e quindi sono escluse le relazioni ed in particolare le funzioni. Questo fatto ha notevoli conseguenze perché non consente a tale logica di essere uno strumento adeguato alla matematica la quale, come è noto, coinvolge costantemente relazioni e funzioni.

2. La logica di Aristotele in realtà è meno potente anche della semplice logica monadica. Infatti Aristotele non considera la quantificazione nel senso attuale del termine. Le parole *ogni*, *alcuni* ... venivano adottate per indicare un rapporto tra concetti. Ad esempio l'affermazione *"ogni uomo è mortale"* indicava un rapporto tra la classe degli uomini e quella degli esseri mortali (in questo caso l'inclusione). Questo rapporto, come abbiamo visto, è espresso da Boole in termini di equazioni in due variabili (in corrispondenza di due predicati). Una affermazione del tipo $\exists y(\forall x(Primo(x)\rightarrow\neg Dispari(x))\rightarrow Pari(y))$ che coinvolge tre predicati non potrebbe essere rappresentata nel formalismo di Aristotele.

3. Aristotele non considerava proprietà "vuote", cioè proprietà non verificate da nessun ente. D'altra parte ciò è coerente con la non considerazione dello zero e dell'insieme vuoto. Una conseguenza di questo fatto è che nella logica aristotelica si riteneva che una proposizione universale affermativa o negativa implicasse la sua *subalterna*. In altri termini la logica aristotelica assumeva come logicamente vere le implicazioni:

$$[\forall x(P(x)\rightarrow Q(x))] \rightarrow [\exists x(P(x)\wedge Q(x))] \quad ;$$
$$[\forall x(P(x)\rightarrow\neg Q(x))] \rightarrow [\exists x(P(x)\wedge\neg Q(x))].$$

Questo è corretto solo se si assume l'ulteriore ipotesi che esistano degli elementi che soddisfano P. Per rendercene conto e riferen-

---

le prime due equazioni segue la terza. Che la teoria delle algebre di Boole rappresenti adeguatamente le leggi del pensiero e che quindi possa provare la validità dei sillogismi è ovviamente cosa tutta da dimostrare.

doci alla prima implicazione, poniamo al posto di $P(x)$ un' asserzione del tipo $A(x)\wedge\neg A(x)$. Otteniamo

$$[\forall x((A(x)\wedge\neg A(x))\rightarrow Q(x))] \rightarrow [\exists x(A(x)\wedge\neg A(x)\wedge Q(x))].$$

D'altra parte l'implicazione $A(x)\wedge\neg A(x)\rightarrow Q(x)$ è sempre vera in quanto l'antecedente $A(x)\wedge\neg A(x)$ è sempre falso. Possiamo allora concludere che il conseguente $\exists x(A(x)\wedge\neg A(x)\wedge Q(x))$ è vero. In particolare risulta vera $\exists x(A(x)\wedge\neg A(x))$, cosa palesemente assurda.[28]

4. Come conseguenza del punto 4, Aristotele non poteva considerare predicati monadici liberamente costruiti tramite connettivi logici. Infatti in tale caso la sua teoria avrebbe dovuto accettare il predicato monadico $A(x)\wedge\neg A(x)$ con le conseguenze viste al punto 4.

14. Ma Leibniz aveva le idee chiare

Non è ovviamente possibile fare la storia della logica in poche pagine. Ad esempio non ho parlato del grande filosofo e matematico G. W. Leibniz che è il primo ad avvere le idee chiare sul ruolo ed il significato di quella che sarà la moderna logica matematica. In questo paragrafo mi limito solo ad alcune sue citazioni.

Leibniz era affascinato dal potere dell'algebra di meccanizzare gli argomenti geometrici a tal punto da fargli prefigurare una scienza ben più ampia. Tale scienza avrebbe operato con lo stesso metodo dell'algebra astratta ma sarebbe stata applicabile ai ragio-

[28] In effetti il punto di vista di Aristotele, pur essendo sbagliato da un punto di vista strettamente logico, è molto vicino alla intuizione comune. Infatti in generale si suppone che se si introduce una proprietà P in una conversazione, allora debba esistere almeno qualche oggetto che verifica tale proprietà. Se ad esempio dico "tutti gli operai stranieri della Fiat hanno il permesso di soggiorno" allora chi ascolta è portato a ritenere che esistono operai stranieri nella Fiat. Un tale modo di procedere viene chiamato da alcuni *implicatura.* Le implicature non riguardano il significato delle affermazioni che vengono fatte ma sono relative al contesto in cui si fanno tali affermazioni, contesto che in genere si ritiene di tipo cooperativo. Se so che il mio interlocutore ha il desiderio di comunicare allora perché avrebbe dovuto mettere in gioco la nozione di "operai stranieri della Fiat" se non esistessero effettivamente tali operai ? Se invece il contesto non è cooperativo, ad esempio del tipo "esame con professore universitario che mi vuole bocciare", allora è evidente che l'implicatura di cui sopra non andrebbe fatta.

namenti in tutti i campi della conoscenza razionale e non solo a quelli della geometria. Vediamo ad esempio che cosa dice:

Ogni ragionamento umano si compie per mezzo di certi segni o caratteri ... le lingue ordinarie, sebbene servano al ragionamento, tuttavia sono soggette ad innumerevoli equivoci, né possono essere impiegate per il calcolo ... Questo mirabilissimo vantaggio finora lo danno soltanto i segni impiegati dagli aritmetici e dagli algebristi, nei quali ogni ragionamento consiste nell'uso di caratteri, e ogni errore mentale è lo stesso che un errore di calcolo ...
... mi apparve subito chiaro che tutti i pensieri umani possono risolversi del tutto in pochi pensieri da considerarsi come primitivi. Se poi si assegnano a questi ultimi dei caratteri, di qui si possono formare i caratteri delle nozioni derivate ...
...Una volta fatto questo, chiunque si servisse dei caratteri così descritti nel ragionare nello scrivere, o non commetterebbe mai errori, oppure li riconoscerebbe sempre da sé, siano suoi o degli altri, mediante esami facilissimi.
... una volta fatto ciò, quando sorgeranno delle controversie, non ci sarà maggior bisogno di discussione tra due filosofi di quanto ce ne sia tra due persone che effettuano calcoli. Sarà sufficiente, infatti, che essi prendano la penna in mano, si siedano ad un tavolino, e si di dicano reciprocamente "calcoliamo".

Leibniz pertanto suggerisce che il ragionamento si può ridurre ad un calcolo dei caratteri, cioè ad un calcolo in cui gli oggetti non sono più numeri ma parole, per la precisione parole di un linguaggio appositamente costruito.

Nel numero dei segni comprendo dunque le parole, le lettere, le figure della chimica, le figure astronomiche, cinesi, geroglifiche, le note musicali, i segni steganografici, aritmetici, algebrici e tutti quelli che usiamo al posto delle cose quando ragioniamo. I segni scritti o disegnati o scolpiti si chiamano invece "caratteri".

Mentre ero profondamente occupato in questo studio, mi venne inaspettatamente l'idea degna di nota che si potrebbe immaginare un alfabeto del pensiero umano e che ogni cosa po-

trebbe essere scoperta e distinta mediante la combinazione delle lettere di questo alfabeto e delle parole risultanti.

Le lingue ordinarie, sebbene siano assai utili al ragionamento, sono tuttavia soggette a innumerevoli equivoci e non possono sostituire il calcolo, in modo cioè che gli errori di ragionamento possano essere scoperti dalla stessa formazione e costruzione delle parole, come se si trattasse di solecismi e barbarismi. Ma questo mirabile vantaggio finora lo offrono i soli segni degli aritmetici e degli algebristi per i quali ogni ragionamento consiste nell'uso di caratteri e ogni errore mentale è lo stesso che un errore di calcolo.
(Leibniz, 1684?)

A me invero, mentre meditavo più profondamente su questo argomento, apparve manifesto che tutti i pensieri umani potevano risolversi completamente in pochi pensieri da ritenersi come primitivi. E che se si assegnano a questi ultimi dei caratteri, da essi si possono formare i caratteri delle nozioni derivate, dai quali sarà sempre possibile ricavare i loro requisiti e le nozioni primitive in essi racchiuse e, per dirla in una parola, le definizioni o valori, e quindi anche i rapporti derivabili dalle definizioni. Ora, una volta che ciò fosse realizzato, chiunque nel ragionamento e nello scrivere facesse uso di siffatti caratteri o non sbaglierebbe mai oppure riconoscerebbe da s´e i propri errori non meno di quelli degli altri mediante esami facilissimi; e scoprirebbe poi la verità nella misura in cui i dati lo renderebbero possibile, e se talora i dati non fossero sufficienti a trovare ciò che fosse richiesto egli potrebbe vedere quali esperienze o quali notizie fossero necessarie per potersi almeno avvicinare alla verità quanto lo consentono i dati, sia procedendo per approssimazione, sia determinando il grado di maggiore probabilità ...(Leibniz, 1684?)

... non è degno di uomini eccellenti perdere ore come schiavi nella fatica della computazione.

...E questo è dunque il vantaggio del nostro metodo: che immediatamente possiamo stabilire per mezzo dei numeri se le proposizioni che ci vengono presentate sono provate o no; e che con la sola guida dei caratteri e con un metodo sicuro e vera-

mente analitico, portiamo alla luce verità che altri avevano raggiunto a stento con immenso sforzo della mente e per caso. E perciò noi siamo in grado di presentare entro il nostro secolo dei risultati che altrimenti con difficoltà potrebbero fornire molte migliaia di anni. (Leibniz, 1679).

CAPITOLO 5
TEORIA DELLE CATEGORIE

1. Introduzione

In questo ultimo capitolo parleremo delle categorie, una nozione nata nel 1945 ad opera di Samuel Eilenberg e Saunders Mac Lane. La teoria delle categorie, pur essendo stata creata per affrontare alcuni problemi specifici nell'ambito della topologia algebrica, attualmente costituisce uno strumento fondamentale per buona parte della matematica. Infatti esistono nozioni e situazioni matematiche che non è possibile esprimere se non utilizzando tale teoria. Inoltre, cosa che più ci interessa, essa risulta essere un strumento per rifondare la matematica che si presenta come possibile alternativa alla teoria degli insiemi. In un libro sui fondamenti non è quindi possibile evitare di parlarne almeno un po'.[1]

L'idea fondamentale è quella di mettere al centro dell'attenzione non la nozione di insieme o di struttura ma quella di funzione, funzione che non necessariamente viene vista come insieme di coppie ma un modo di rapportare un oggetto ad un altro.

Definizione 1.1. Una *categoria* è una struttura $\boldsymbol{C}$ definita da:
- una classe $Obj(\boldsymbol{C})$ i cui elementi sono chiamati *oggetti*
- per ogni X ed Y in $\boldsymbol{C}$ da un insieme $Hom(X,Y)$ i cui elementi sono chiamati *morfismi* di X in Y,
- per ogni X, Y e Z in $Obj(\boldsymbol{C})$ con $Hom(Y,Z) \neq \emptyset$, $Hom(X,Y) \neq \emptyset$ da un'operazione binaria $\circ : Hom(Y,Z)\times Hom(X,Y) \rightarrow Hom(X,Z)$, chiamata *composizione*.

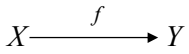
Inoltre si assume che
- tale operazione è associativa cioè, per ogni $f \in Hom(X,Y)$, $g \in Hom(Y, Z)$ ed $h \in Hom(Z, S)$,
  $h\circ(g\circ f) = (h\circ g)\circ f$.
- per ogni X in $Obj(\boldsymbol{C})$ esista un morfismo $id_X \in Hom(X, X)$, chiamato *morfismo identità per X*, tale che per ogni $f \in Hom(X,Y)$
  $id_Y \circ f = f = f \circ id_X$.

A dispetto della nomenclatura usata, i morfismi non sono necessariamente funzioni e gli oggetti non sono necessariamente in-

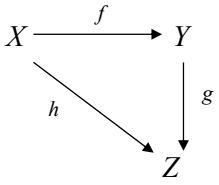
[1] La doppia negazione in questa frase potrebbe far pensare che la teoria delle categorie non mi sia molto simpatica. In effetti è così, non è detto che una persona importante sia anche simpatica.

siemi. Da notare anche che in tale definizione compare sia la parola "classe" che la parola "insieme". Infatti, come vedremo, esistono importanti categorie come quella dei gruppi, degli anelli o degli insiemi in cui $Obj(\boldsymbol{C})$ è una classe propria.

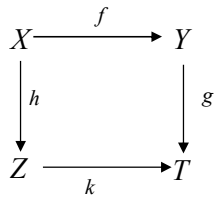
Per esprimere nozioni di teoria delle categorie si utilizzano grafici, chiamati *diagrammi*, in cui gli oggetti sono rappresentati da punti ed i morfismi con frecce. Ad esempio, per indicare che f è un omomorfismo di X in Y viene scritto:



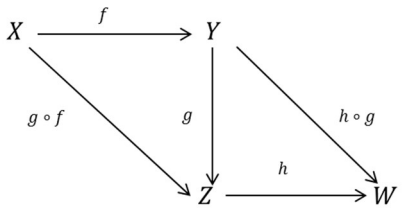
Il seguente diagramma esprime l'uguaglianza $g \circ f = h$:



Il seguente diagramma esprime l'uguaglianza $g \circ f = k \circ h$:



Quando una uguaglianza viene espressa in questo modo da un diagramma si dice anche che il diagramma *commuta*. Ad esempio la proprietà associativa della composizione cioè l'uguaglianza $h \circ (g \circ f) = (h \circ g) \circ f$ viene espressa dal dire che il diagramma commuta.



Esempio 1. La *categoria degli insiemi* è la categoria che ha come oggetti gli insiemi e come morfismi le funzioni. Precisamente,

per ogni X ed Y, $Hom(X,Y)$ è l'insieme delle funzioni di X in Y. L'operazione $\circ$ è l'usuale composizione tra funzioni e le identità sono le applicazioni identiche.

Esempio 2. La *categoria dei gruppi* è la categoria che ha come oggetti i gruppi e come morfismi gli usuali omomorfismi tra gruppi. Anche in questo caso si considera l'usuale composizione e le applicazioni identiche. Analoghe categorie si ottengono considerando la classe degli anelli, dei reticoli degli spazi vettoriali ed altro.

Esempio 3. La *categoria degli spazi topologici* è la categoria che ha come oggetti gli spazi topologici (che in questi due volumi non abbiamo trattato) e come morfismi le funzioni continue.

Il seguente esempio mostra che in una classe di oggetti (gli insiemi) si cambia la nozione di morfismo si ottiene una diversa categoria.

Esempio 4. *Categoria degli insiemi coma classe ordinata*. Consideriamo la classe degli insiemi e limitiamoci, rispetto all'esempio 1, solo ai morfismi che sono immersioni identiche. Questo significa che se $X \subseteq Y$ allora $Hom(X,Y) = \{i_{XY}\}$ dove i_{XY} è la funzione tale che $i_{XY}(x) = x$ per ogni $x \in X$. Nel caso in cui X non è incluso in Y si pone $Hom(X,Y) = \varnothing$.

Esempio 5. *Categoria associata ad un insieme ordinato.* L'esempio precedente può essere esteso considerando una qualunque struttura $(C, \leq)$ con C classe e $\leq$ relazione d'ordine. Viene definita una categoria che ha come oggetti gli elementi di C ed in cui, per X, Y in C,

$H(X,Y)$ ha un solo elemento, che indichiamo con i_{XY}, se $X \leq Y$
$H(X,Y)$ è vuoto altrimenti.

La composizione è definita ponendo $i_{YZ} \circ i_{XY} = i_{xz}$.

Esempio 6. *Categoria delle matrici*. Gli oggetti sono le matrici unitarie. Se indichiamo con $M(n)$ la matrice unitaria di n righe ed n colonne, allora $Hom(M(n),M(m))$ è l'insieme delle matrici con n righe ed m colonne. La composizione è il prodotto righe per colonne tra matrici.

Nei primi quattro esempi la classe degli oggetti non è un insieme poiché altrimenti si andrebbe incontro ai paradossi che abbiamo già visto. Nell'esempio 5 la classe degli oggetti può essere o meno un insieme. Nell'esempio 6 è un insieme (numerabile). Quando la classe degli oggetti è un insieme si dice che la categoria è *piccola*. Esistono esempi di categorie "tanto piccole" da avere un solo oggetto. La seguente proposizione, la cui dimostrazione è evidente, mostra che tali categorie sostanzialmente coincidono con i monoidi.

Proposizione 1.2. Ad ogni monoide $(M,\cdot,1)$ è associata una categoria con un solo oggetto. Precisamente la categoria avente come unico oggetto l'elemento neutro, come insieme di morfismi il dominio M e come composizione il prodotto $\cdot$ in M . Viceversa, ad ogni categoria con un solo oggetto è associato il monoide consistente nell'insieme dei suoi morfismi.

Nota. E' immediato provare che ad ogni oggetto è associato uno ed un solo morfismo identità. Questo permette in un certo senso di identificare gli oggetti con i morfismi identità e quindi di fare a meno degli oggetti. Più precisamente, possiamo identificare ogni categoria con la struttura algebrica costituita dalla classe di tutti i morfismi in cui è definita una operazione parziale $\circ$.[2] Viceversa ad ogni struttura algebrica con una operazione parziale $\circ$ che in un certo senso sia associativa ed abbia almeno un elemento neutro possiamo associare la categoria i cui oggetti sono gli elementi neutri cioè gli elementi i tali che per ogni f per cui è definito $i\circ f$ risulti $i\circ f = f$ e per ogni f per cui è definito $f\circ i$ risulti $f\circ i$

[2] Una struttura algebrica con operazioni "parziali" è una struttura in cui le operazioni potrebbero non essere ovunque definite. Ad esempio in un campo l'inversione è una operazione parziale poiché non è definita in 0. Un altro esempio è dato dalla sottrazione che nell'insieme dei numeri naturali non è ovunque definita. Quasi sempre gli algebristi preferiscono considerare operazioni totali. Questo è il motivo per cui un campo in genere viene visto come un particolare anello che permette di considerare come primitive solo le operazioni di addizione e di moltiplicazione. In una struttura con operazioni parziali quando si afferma che vale una equazione $t = t'$ si intende che se il termine t è definito anche il termine t' è definito e $t = t'$. Ad esempio si dice che $\circ$ è associativa se, ogni volta che $(x\circ y)\circ z$ è definito è anche definito $x\circ(y\circ z)$ e risulta $(x\circ y)\circ z = x\circ(y\circ z)$.

$= f$. Inoltre, dati due elementi neutri i e j l'insieme $Hom(i, j)$ è l'insieme degli elementi f tali che siano definiti sia $i \circ f$ che $f \circ j$. Un tale modo di vedere enfatizza l'aspetto fortemente algebrico delle categorie che potrebbero essere definite come "monoidi" in cui non si richiede che l'operazione sia ovunque definita.

2. Globale e locale

La teoria delle categorie si caratterizza per i seguenti aspetti fondamentali.

1. Privilegia la nozione intuitiva di funzione e non quella di insieme.
2. Privilegia gli aspetti algebrici ed in particolare la nozione di composizione.
3. Privilegia il punto di vista globale rispetto a quello locale.

I primi due punti sono evidenti. Il terzo significa che in teoria delle categorie si definiscono gli oggetti matematici non guardando alla loro struttura interna ma al modo di rapportarsi agli altri oggetti "simili".

Per fare un esempio consideriamo la nozione insiemistica di unione. Essa viene usualmente definita "localmente" facendo riferimento agli elementi degli insiemi coinvolti. Infatti, dati due insiemi X ed Y, poniamo

$$X \cup Y = \{z : z \in Y \text{ oppure } z \in Y\}.$$

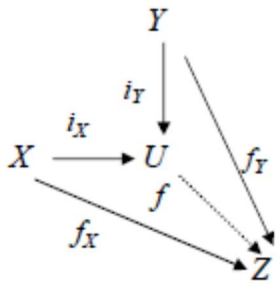
In teoria delle categorie, si preferisce invece definire l'unione come il più piccolo insieme che contiene sia X che Y, ossia come un insieme U che verifica la seguente proprietà:

$$X \subseteq U, \quad Y \subseteq U, \quad \forall Z(X \subseteq Z, X \subseteq Z \Rightarrow Z \supseteq U.$$

Proposizione 2.1. Consideriamo la classe di tutti gli insiemi con la relazione di inclusione. Tale classe definisce una categoria in accordo con quanto detto nell'esempio 4. In tale categoria l'unione tra due insiemi X ed Y può essere definita come un oggetto U insieme a due morfismi $i_X : X \to U$ e $i_Y : Y \to U$ in modo che per ogni coppia di morfismi $f_X : X \to Z$ e $f_Y : Y \to Z$ in un insieme Z esiste un unico morfismo $f : U \to Z$ tale che

$$f \circ i_X = f_X, f \circ i_Y = f_Y.$$

Possiamo rappresentare un tale modo di definire l'unione con il seguente diagramma:



La definizione di unione suggerita da tale proposizione potrebbe apparire un po' complicata. Tuttavia ha il grande vantaggio di essere "universale" nel senso che può essere ripetuta in ogni categoria.

Definizione 2.2. Chiamiamo *coprodotto* di due oggetti X ed Y di una categoria $\boldsymbol{C}$ un oggetto U insieme a due morfismi $i_X : X \to U$ e $i_Y : Y \to U$ in modo che per ogni coppia di morfismi $f_X : X \to Z$ e $f_Y : Y \to Z$ in un oggetto Z esiste un unico morfismo $f : U \to Z$ tale che

$$f \circ i_X = f_X \,,\; f \circ i_Y = f_Y.$$

Nel caso della categoria associata ad un insieme ordinato tale definizione fornisce la nozione di estremo superiore. Poiché non in tutti gli insiemi ordinati esiste l'estremo superiore di due elementi dati, questo mostra che non in tutte le categorie esiste sempre il coprodotto di due oggetti.

3. Monomorfismi, epimorfismi, isomorfismi

La nozione di funzione iniettiva viene usualmente definita facendo riferimento agli elementi su cui è definita la funzione, cioè dicendo che f è iniettiva se, dati due elementi x ed y, da $f(x) = f(y)$ segue che $x = y$. Una definizione globale equivalente è fornita dalla seguente proposizione.

Proposizione 3.1. Nella categoria degli insiemi una funzione $f : X \to Y$ è iniettiva se e solo se vale la legge di cancellazione a sinistra, cioe se per ogni coppia di funzioni $h, k : Z \to X$ risulta che:

$$f \circ h = f \circ k \;\Rightarrow h = k.$$

Dim. Sia f iniettiva allora dal fatto che $f(h(x)) = f(k(x))$ per ogni x comporta che $h(x) = k(x)$ per ogni x e quindi che $h = k$. Viceversa, supponiamo che f verifichi la legge di cancellazione a sinistra e che, per assurdo, esistano a ed b, con $a \neq b$ tali tale che $f(a) = f(b)$. Detto allora Z un qualunque insieme, $h : Z \to X$ la funzione costantemente uguale ad a e $k : Z \to X$ la funzione costantemente uguale a b, risulterà che $f \circ h = f \circ k$ ma $h \neq k$. Ciò è in contrasto con l'ipotesi fatta. □

Tale proposizione suggerisce la seguente definizione che estende la nozione di inettività ad ogni categoria.

Definizione 3.2 Data una categoria, diciamo che un morfismo $f : X \to Y$ è un *monomorfismo* se per ogni coppia di morfismi $h, k : Z \to X$ risulta che:

$f \circ h = f \circ k \Rightarrow h = k$ (f è cancellabile a sinistra).

Nel caso della categoria associata ad un insieme ordinato poiché esiste al più morfismo da un oggetto ad un altro, allora l'uguaglianza è banalmente verificata. Questo vuol dire che tutti i morfismi sono monomorfismi.

Un discorso analogo può essere fatto per la nozione di funzione suriettiva.

Proposizione 3.3. Nella categoria degli insiemi una funzione $f : X \to Y$ è suriettiva se e solo se vale la legge di cancellazione a destra, cioe se per ogni coppia di funzioni $h, k : Z \to X$ risulta che:

$h \circ f = k \circ f \Rightarrow h = k$ (f cancellabile a destra).

Dim. Sia f suriettiva, allora dal fatto che $h(f(x)) = k(f(x))$ segue che h e k assumono lo stesso valore in tutti gli elementi dell'insieme $f(X)$. Poichè $f(X) = Y$, le due funzioni coincidono.

Viceversa, supponiamo che valga la legge di cancellazione a destra. Allora se esistesse $b \in Y$ che non è immagine tramite f di nessun elemento di X, dette h e k due funzioni che differiscono solo per il valore in b risulterebbe che $h(f(x)) = k(f(x))$ per ogni $x \in X$ e quindi $h = k$. □

Definizione 3.4. Data una categoria, diciamo che un morfismo f : $X \to Y$ è un *epimorfismo* se per ogni coppia di morfismi h, k : $Y \to Z$ risulta che

$h \circ f = k \circ f \Rightarrow h = k$ (f è cancellabile a destra).

Sempre riferendoci alla categoria associata ad un insieme ordinato, anche in questo caso un morfismo risulta sempre suriettivo.

Definizione 3.5. Un morfismo $f : X \to Y$ è chiamato *isomorfismo* se esiste un morfismo $g : Y \to X$ tale che $g \circ f = id_X$ e $f \circ g = id_Y$. In tal caso diremo che X ed Y sono *isomorfi*.

Ogni isomorfismo è allo stesso tempo un monomorfismo ed un epimorfismo. In molte categorie non vale il viceversa. Ad esempio nella categoria associata ad un insieme ordinato risulta che due oggetti sono isomorfi se e solo se coincidono. Quindi per ogni $X<Y$ il morfismo di X in Y pur essendo sia monomorfismo che epimorfismo non è un isomorfismo.

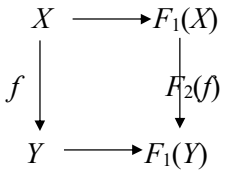
Problema. Dato un pre-ordine definire una categoria corrispondente. Studiare in tale categoria alcune delle nozioni trattate.

4. Funtori ed isomorfismi tra categorie

Quanto si assume il punto di vista strutturalista è essenziale rapportare tra loro strutture dello stesso tipo tramite le nozioni di omomomorfismo, immersione, isomorfismo. In particolare è importante la nozione di isomorfismo in quanto tutte le strutture matematiche si studiano "a meno di isomorfismi". Infatti è possibile dimostrare che tutto quello che si può dire di una struttura vale per tutte le strutture ad essa isomorfe. Questo spinge un matematico ad identificare strutture isomorfe. Non è invece possibile rapportare strutture matematiche di tipo diverso, ad esempio gruppi con campi o spazi topologici con gruppi. Ad esempio non si riesce ad esprimere il fatto intuitivo che la nozione di reticolo è la stessa sia che i reticoli si presentino come strutture ordinate sia che si presentino come strutture algebriche (si veda in Appendice del primo volume). Forse la caratteristica principale della teoria delle categorie è quella invece di avere tale capacità e ciò è reso possibile dalla nozione di funtore. Nel seguito denoto con $Mor(\boldsymbol{C})$ la classe dei morfismi di una categoria $\boldsymbol{C}$.

Definizione 4.1. Siano ***C*** e ***D*** due categorie. Un *funtore covariante* da ***C*** a ***D*** è una coppia $F = (F_1, F_2)$ dove $F_1 : Ob(\mathbf{C}) \to Ob(\mathbf{D})$, $F_2 : Mor(\mathbf{C}) \to Mor(\mathbf{D})$ sono applicazioni tali che
1. se $f : X \to Y$ allora $F_2(f) : F_1(X) \to F_2(Y)$
2. $F_2(g \circ f) = F_2(g) \circ F_2(f)$
3. $F_2(id_X) = id_{F1(X)}$

Possiamo rappresentare la nozione di funtore tramite il seguente diagramma:



Tale nozione è analoga a quella di omomorfismo di una struttura in un'altra ma, differenza non piccola, collega categorie diverse e non strutture diverse. D'altra parte la classe delle categorie costituisce a sua volta una categoria i cui oggetti sono, appunto, le categorie ed i cui morfismi sono i funtori. La definizione di composizione di due funtori si ottiene operando componente per componente.

Definizione 4.2 Un funtore F di una categoria ***C*** in una categoria ***D*** è detto *isomorfismo* se esiste un funtore G di ***D*** in ***C*** tale che che $G \circ F = id_C$ e $F \circ G = id_D$.

In tal caso G è univocamente determinato da F ed è a sua volta un isomorfismo.

Definizione 4.3. Due categorie ***C*** e ***D*** si dicono *isomorfe* se esiste un isomorfismo di ***C*** in ***D***.

Per fare un esempio, indichiamo con Ret_a la classe dei reticoli definiti come strutture algebriche e con Ret_r la classe dei reticoli deifniti come strutture relazionali. Possiamo strutturare tali classi in due categorie $\boldsymbol{Ret_a}$ e $\boldsymbol{Ret_r}$.

Definizione 4.4. Denotiamo con $\boldsymbol{Ret_a}$ la categoria i cui oggetti sono i reticoli come strutture algebriche e con $\boldsymbol{Ret_r}$ la categoria i

cui oggetti sono i reticoli come strutture relazionali. In entrambi i casi assumiamo come morfismi gli isomorfismi.
Vale in proposito il seguente teorema che precisa l'idea per cui l'approccio algebrico e quello relazionale alla teoria dei reticoli coincidono.

Proposizione 4.5. Le categorie $\boldsymbol{Ret_a}$ e $\boldsymbol{Ret_r}$ sono isomorfe.

Dim. Ricordando quanto fatto in Appendice del primo volume, indichiamo con $F_1 : Ret_a \to Ret_r$ la funzione che associa ad ogni reticolo inteso come struttura algebrica il corrispondente reticolo inteso come struttura ordinata. Indichiamo inoltre con $G_1 : Ret_r \to Ret_a$ la funzione che rappresenta il processo inverso. Indichiamo inoltre con F_2 e G_2 le applicazioni identiche operanti sui morfismi. Ha senso considerare tali applicazioni poiché nelle classi Ret_a e Ret_r gli isomorfismi coincidono. Allora è facile verificare che $F = (F_1, F_2)$ è un isomorfismo tra le due categorie e che $G = (G_1, G_2)$ è il suo inverso. □

Proviamo a cambiare la nozione di morfismo introducendo, come sarebbe naturale fare, quella di omomorfismo e non quella di isomorfismo. In tale caso il tipo di dimostrazione ora fatta si bloccherebbe. Infatti vale la seguente proposizione.

Proposizione 4.6. Gli omomorfismi in Ret_a non coincidono con quelli in Ret_r.

Dim. Ad esempio dato l'insieme $S = \{a, b, c\}$ la funzione $f : P(S) \to \{0, 1, 2, 3\}$ che associa ad ogni sottoinsieme di S il numero dei suoi elementi è un omomorfismo del reticolo $(P(S), \subseteq)$ nel reticolo $(\{0, 1, 2, 3\}, \leq)$. Tuttavia f non è un omomorfismo tra $(P(S), \cap, \cup)$ e $(\{0, 1, 2, 3\}, \wedge, \vee)$ poiché, ad esempio, $f(\{a\} \cap \{b,c\}) = 0$ mentre $f(\{a\}) \wedge f(\{b,c\}) = 1$. □

5. Teoria delle categorie per i fondamenti

Fino ad ora abbiamo visto la teoria delle categorie come uno strumento che interviene su vari settori della matematica e che a settori diversi corrispondono categorie diverse. Così alla teoria dei gruppi corrisponde la categoria dei gruppi, alla teoria degli insiemi ordinati corrisponde la categoria degli insiemi ordinati e

così via. Tuttavia esiste un modo più direttamente "fondazionale" di uso delle categorie basata sull'osservazione che la matematica, da Cantor in poi, è fondata sulla categoria degli insiemi. Allora se si fissa una categoria in cui si possono fare tutte le cose che è possibile fare in teoria degli insiemi è possibile fondare la matematica a partire da tale categoria. In altre parole possiamo ottenere una matematica a partire da ogni categoria che "assomiglia" abbastanza alla categoria degli insiemi anche se non è detto che coincida con tale categoria.[3] Una classe di categorie di tale tipo viene studiata in letteratura sotto il nome di *"topos"*.

Ad esempio osserviamo che nella categoria degli insiemi una struttura algebrica con una operazione binaria può essere vista come un oggetto (cioè un insieme) D più un morfismo $h : D\times D \to D$ dove con $D\times D$ si intende l'usuale prodotto cartesiano. Ma allora tale definizione può essere data in ogni categoria in cui sia definibile qualcosa di simile al prodotto cartesiano. Ora il modo usuale di definire il prodotto cartesiano è porre $D\times D = \{(x,y) : x\in X,\ y\in Y\}$ ma tale definizione, di carattere locale, non si prestaad essere estesa ad ogni categoria. Dobbiamo invece tentare di caratterizzare il prodotto cartesiano in termini di morfismi e poi adottare la risultante caratterizzazione come definizione di prodotto cartesiano in una qualunque categoria (un po' come abbiamo fatto per le nozioni di omomorfismo, epimorfismo ed isomorfismo). Ora la caratteristica principale di un prodotto cartesiano è che in ogni elemento del prodotto cartesiano (cioè in ogni coppia) sia possibile individuare la prima e la seconda componente. Questo viene fatto dalle funzioni *"prima proiezione"* e *"seconda proiezione"* che sono morfismi della categoria degli insiemi. Quindi un prodotto cartesiano di due oggetti X ed Y può essere definito come un oggetto che può essere proiettato sia in X che in Y. Inoltre è ragionevole ritenere che tale oggetto sia "il più grande possibile".

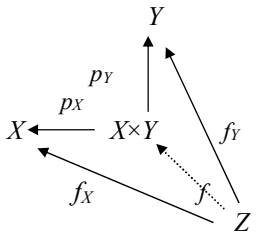
Definizione 5.1. Dati due oggetti X ed Y in una categoria $\boldsymbol{C}$, un *prodotto* di X e Y è un oggetto P insieme a due morfismi $p_X : P \to X$, $p_Y : P \to Y$ (detti *proiezioni*) tali che, per ogni terna $(Z,$

[3] D'altra parte questa esistenza di matematiche "diverse" si manifesta anche quando si fonda la matematica sulla teoria degli insiemi. Infatti non esiste una sola teoria degli insiemi e se si fissa una teoria degli insiemi tale teoria ammette svariati modelli. Ad ognuno di tali modelli corrisponde una diversa matematica.

f_X, f_Y), con $f_A : Z \to X$ e $f_Y : Z \to B$, esiste un unico morfismo $f : Z \to P$ tale che

$p_X \circ f = f_X$, $p_Y \circ f = f_Y$.

Se indichiamo con $X \times Y$ un prodotto, possiamo rappresentare con il seguente diagramma la proprietà che lo caratterizza:[4]



Da notare che abbiamo scritto "un prodotto" e non "il prodotto" poiché di due oggetti possono in generale essere definiti più oggetti che sono un loro prodotto. D'altra parte è possibile dimostrare che tali prodotti risultano essere tutti isomorfi tra loro. La stessa cosa si può dire per i coprodotti.

Sia ***C*** una categoria tale che per ogni coppia di oggetti esista il prodotto corrispondente (proprietà non verificata da tutte le categorie). Allora dato un oggetto D di ***C*** possiamo chiamare *operazione binaria* un morfismo di $D \times D$ in D e, più in generale, *operazione* n-aria un morfismo del prodotto D^n di n copie di D in D. Possiamo allora chiamare *struttura algebrica* in ***C*** un oggetto di ***C*** più un insieme finito di operazioni.

Ad esempio se consideriamo la categoria degli insiemi ordinati in cui i morfismi sono le funzioni crescenti, allora una struttura algebrica sarà costituita da un insieme ordinato più una serie di operazioni che dobbiamo assumere essere crescenti.

Se poi riusciamo a definire la nozione di relazione n-aria in ***C***, non ci sono ostacoli a definire la nozione di *struttura del primo ordine* in ***C.***

In definitiva, come abbiamo già detto, più ***C*** assomiglia alla categoria degli insiemi più si presta ad essere una base per una matematica che è diversa da quella usuale.

---

[4] Si confronti questo diagramma con quello che corrisponde alla definizione di coprodotto.

APPENDICE
CALCOLARE CON OPERATORI

1. Sistemi di chiusura, operatori e punti fissi

Moltissime nozioni matematiche possono essere introdotte in termini di sistemi di chiusura e di operatori di chiusura.

Definizione 1.1. Sia S un insieme non vuoto e denotiamo con $\mathcal{P}(S)$ l'insieme delle sua parti, allora chiameremo *sistema di chiusura su S* una classe C di sottoinsiemi di S tale che

i) $S \in C$

ii) C è chiusa rispetto alle intersezioni, cioè l'intersezione di una qualunque famiglia di elementi di C appartiene ancora a C.

Dato un sistema di chiusura è definita la nozione di sottoinsieme generato da un dato insieme.

Definizione 1.2. Dato un sistema di chiusura C su un insieme non vuoto S ed un sottoinsieme X di S poniamo

$$\langle X\rangle = \cap\{Y \in C : Y \supseteq X\}$$

è diciamo che $\langle X\rangle$ è l'elemento di C *generato* da X.

Poiché $\langle X\rangle$ appartiene a C, è evidente che $\langle X\rangle$ è il più piccolo elemento di C che contiene X.

Esempio di carattere topologico. Ad esempio se C è la classe degli insiemi chiusi di R allora C è un sistema di chiusura in quanto R è chiuso e l'intersezione di una famiglia di insiemi chiusi è ancora un insieme chiuso. Se X è un sottoinsieme di R allora

$\langle X\rangle = \overline{X}$ cioè $\langle X\rangle$ è la chiusura topologica dell'insieme X.

Esempio di carattere algebrico. Sia C la classe di tutti i sottogruppi di un dato gruppo G. Allora C è un sistema di chiusura e, per ogni sottoinsieme X di G, $\langle X\rangle$ è il sottogruppo generato da X.

Esempio di carattere geometrico. Sia C la classe di tutti gli insieme convessi del piano euclideo. Allora C è un sistema di chiusura. Per ogni insieme X di punti, $\langle X\rangle$ è la *chiusura convessa* di X.

La nozione di sistema di chiusura è strettamente legata alla nozione di operatore di chiusura.

Definizione 1.3. Chiamiamo *operatore di chiusura* una funzione $T : \mathcal{P}(S) \to \mathcal{P}(S)$ tale che:

a) $T(X) \supseteq X$ (proprietà di inclusione)
b) $X \subseteq Y \Rightarrow T(X) \subseteq T(Y)$ (crescenza o monotonia)
c) $T(T(X)) = T(X)$. (idempotenza).

Esempio di carattere topologico. Sia X un sottoinsieme di R ed indichiamo con $T(X)$ la chiusura $\overline{X}$ dell'insieme X. Allora T è un operatore di chiusura.

Esempio di carattere algebrico. In uno spazio vettoriale per ogni insieme X di vettori indichiamo con $T(X)$ l'insieme dei vettori linearmente dipendenti da X. Allora T è un operatore di chiusura.

Definizione 1.4. Dato un operatore T, si chiama *punto fisso* o *punto unito* di T un insieme X tale che $T(X) = X$.

Si osservi che la proprietà di idempotenza $T(T(X)) = T(X)$ equivale a dire che per ogni X l'insieme $T(X)$ è un punto fisso di T. Questo significa che se T è un operatore di chiusura allora tutti gli elementi del condominio di T sono punti fissi.

La seguente proposizione mostra che gli operatori di chiusura sono strettamente collegati ai sistemi di chiusura.

Teorema 1.5. Sia $T : \mathcal{P}(S) \to \mathcal{P}(S)$ un operatore che verifica la proprietà di inclusione e quella di crescenza. Allora l'insieme

$$C_T = \{X \in \mathcal{P}(S) : T(X) = X\}$$

dei punti uniti di T è un sistema di chiusura.

Dim. E' evidente che $S \in C_T$. Sia $(X_i)_{i \in I}$ una famiglia di elementi di C_T, allora, essendo $\cap_{i \in I} X_i \subseteq X_j$ per ogni $j \in I$, per la crescenza di T, risulta $T(\cap_{i \in I} X_i) \subseteq T(X_j)$. Ne segue che, essendo X_j punto fisso per T, $T(\cap_{i \in I} X_i) \subseteq X_j$ per ogni $j \in I$ e quindi $T(\cap_{i \in I} X_i) \subseteq \cap_{j \in I} X_j$. Poiche per la proprietà di inclusione $T(\cap_{i \in I} X_i) \supseteq \cap_{j \in I} X_j$, l'insieme $\cap_{i \in I} X_i$ è un punto fisso e quindi appartiene a C_T. □

Proposizione 1.6. Supponiamo che T verifichi le proprietà di inclusione e di crescenza e poniamo

$$D(X) = \cap\{Y : Y \supseteq X \text{ e } Y = T(Y)\}, \qquad (1.1)$$

Allora $D(X)$ è il minimo punto fisso di T contenente X.

Dim. Per definizione di intersezione, $D(X)$ è l'estremo inferiore dell'insieme $\{Y : Y \supseteq X \text{ e } Y = T(Y)\}$ dei punti fissi contenenti X. Poiché il teorema 1.5 ci dice che $D(X)$ è un punto fisso di T e poiché $D(X) \supseteq X$, $D(X)$ appartiene a tale insieme e quindi ne è il minimo elemento. □

Se ci riferiamo all'esempio di carattere topologico abbiamo il ben noto risultato per cui la chiusura topologica di un insieme X si ottiene come intersezione di tutti i chiusi contenenti X.

Teorema 1.7. Se T è un operatore di chiusura allora l'insieme C_T dei suoi punti fissi è un sistema di chiusura. Viceversa, sia C un sistema di chiusura e definiamo l'operatore $T_C : \mathcal{P}(S) \to \mathcal{P}(S)$ ponendo

$$T_C(X) = <X> = \cap\{Y \in C : Y \supseteq X\}.$$

Allora T_C è un operatore di chiusura il cui insieme di punti fissi è C.

Dim. La prima parte del teorema segue dal teorema 1.5 in quanto un operatore di chiusura verifica la proprietà di inclusione ed è monotono. La seconda parte è evidente. Infatti è immediato che T_C verifica le proprietà di inclusione e di monotonia. D'altra parte, se si osserva che

$$Y \supseteq T_C(X) \Leftrightarrow Y \supseteq X,$$

risulta anche

$$T_C(T_C(X)) = \cap\{Y \in C : Y \supseteq T_C(X)\} = \cap\{Y \in C : Y \supseteq X\}. \quad \square$$

2. Due teoremi di punto fisso per operatori

La seguente proposizione mostra che gli operatori crescenti ammettono sempre punto fisso.

Teorema 2.1. Sia $T : \mathcal{P}(S) \to \mathcal{P}(S)$ un operatore crescente. Allora l'insieme

$$Z = \cup\{X : X \subseteq T(X)\}$$

è un punto fisso di T.

Dim. Infatti per definizione per ogni $X \subseteq T(X)$ risulta che $X \subseteq Z$ e quindi, essendo T crescente, $X \subseteq T(X) \subseteq T(Z)$. Ne segue che $Z = \cup\{X : X \subseteq T(X)\} \subseteq T(Z)$. Da tale diseguaglianza segue che $T(Z) \subseteq T(T(Z))$ e che quindi $T(Z)$ appartiene all'insieme $\{X : X \subseteq T(X)\}$. Conseguentemente $T(Z) \subseteq Z$. Avendo già osservato che $Z \subseteq T(Z)$, possiamo concludere che $T(Z) = Z$.[1] □

Nel caso di operatori algebrici esiste un modo più "costruttivo" per ottenere un punto fisso.

Definizione 2.2. Chiamiamo *operatore algebrico su S* ogni funzione $T : \mathcal{P}(S) \to \mathcal{P}(S)$ tale che:

a) $T(X) \supseteq X$ (proprietà di inclusione)
b) $X \subseteq Y \Rightarrow T(X) \subseteq T(Y)$ (crescenza o monotonia)
c) $x \in T(X) \Rightarrow \exists F \subseteq X$, F finito, $x \in T(F)$ (compattezza o finitezza).

T è un *operatore di chiusura algebrico*, cioè se oltre ad essere un operatore algebrico verifica anche

d) $T(T(X)) = T(X)$ (idempotenza).

La teoria degli operatori algebrici deve essere vista come un modo astratto di considerare un processo con cui si costruiscono nuovi oggetti a partire da un dato insieme X di oggetti. Allora
a) significa che tra le cose che posso costruire con X ci sono gli elementi di X,
b) significa che se una cosa può essere costruita a partire da X allora (a maggior ragione) può essere costruita a partire da un insieme che contiene X,
c) afferma che dire che una cosa è costruibile a partire da X significa in realtà che è costruibile a partire da un numero finito di elementi di X. In altre parole, significa che il processo di costruzione è finitario.
d) si può interpretare dicendo che se un oggetto x è costruito con materiale in $T(X)$ che a sua volta è stato costruito con materiale in X allora tale oggetto è, di fatto, costruito con materiale in X. In altre parole a partire dagli oggetti in $T(X)$ non è possibile costruire niente che non sia già in $T(X)$.

[1] Se si esamina la dimostrazione ci si accorge che il teorema vale anche se al posto di $P(S)$ consideriamo un reticolo completo.

Da notare che le condizioni *b*) e *c*) equivalgono a dire che

$$T(X) = \cup\{T(F) : F \subseteq X \text{ e } F \text{ finito}\}$$

cioè equivalgono a dire che il calcolo di $T(X)$ si può effettuare riferendosi solo alla parti finite di X.

Problema. Sia S un insieme e Z un suo sottoinsieme. Dire quali proprietà verifica l'operatore T definito ponendo, per ogni sottoinsieme X di S

$$T(X) = X \cup Z.$$

Problema. Sia T l'operatore che associa ad ogni insieme X di numeri naturali l'insieme $T(X)$ dei divisori degli elementi di X. Ad esempio $T(\{3,14,15\}) = \{1,3,2,7,5,14,15\}$. Dire che tipo di operatore è.

Per caratterizzare gli operatori algebrici è utile il seguente lemma.

Lemma 2.3. Sia $(X_n)_{n\in N}$ una successione di sottoinsiemi di S crescente rispetto alla inclusione ed F un sottoinsieme finito di S, allora

$$F \subseteq \cup_{n\in N} X_n \Rightarrow \exists j \in N \text{ tale che } F \subseteq X_j. \qquad (2.1)$$

Dim. Supponiamo che F sia costituito dagli elementi $x_1,\ldots,x_k$, allora esisteranno $X_{n(1)},\ldots, X_{n(k)}$ tali che $x_1 \in X_{n(1)},\ldots, x_k \in X_{n(k)}$. Se j è il massimo degli indici $n(1),\ldots, n(k)$, allora $F \subseteq X_j$. □

Problema. Mostrare che il lemma ora enunciato non vale senza l'ipotesi di crescenza per $(X_n)_{n\in N}$ e che non vale senza l'ipotesi di finitezza per F.

Lemma 2.4. Se un operatore T è compatto e monotono allora per ogni successione crescente $(X_n)_{n\in N}$ di sottoinsiemi di S risulta che

$$T(\cup_{n\in N} X_n) = \cup_{n\in N} T(X_n). \qquad (2.2)$$

Dim. Per ogni fissato m, $X_m \subseteq \cup_{n\in N} X_n$ e quindi per la monotonia $T(X_m) \subseteq T(\cup_{n\in N} X_n)$. Ne segue che

$$\cup_{n\in N}\, T(X_n) = \cup_{m\in N}\, T(X_m) \subseteq T(\cup_{n\in N} X_n).$$

Per provare l'inclusione inversa, sia $x \in T(\cup_{n\in N} X_n)$, allora per la compattezza esiste un sottoinsieme finito F di $\cup_{n\in N} X_n$ tale che

$x \in T(F)$. Per il lemma 2.3 esiste j un intero tale che $F \subseteq X_j$ e quindi risulta anche che $x \in T(X_j)$ e quindi che $x \in \cup_{n\in N}\ T(X_n)$. Pertanto $T(\cup_{n\in N} X_n) \subseteq \cup_{n\in N} T(X_n)$. □

Il seguente teorema mostra che ogni operatore compatto e monotono ammette un punto fisso. Nel seguito scriveremo $T^n(X)$ per indicare il risultato della applicazione n volte dell'operatore T ad X; più precisamente definiamo $T^n(X)$ per ricorsione su $n \in N_0$ tramite le equazioni

- $T^0(X) = X$
- $T^{n+1}(X) = T(T^n(X))$.

Teorema 2.5. Sia $T : \mathcal{P}(S) \to \mathcal{P}(S)$ un operatore che verifica (2.2) per ogni successione crescente $(X_n)_{n\in N}$ di sottoinsiemi di S. Allora se X è un insieme tale che $T(X) \supseteq X$, l'insieme $\cup_{n\in N} T^n(X)$ è il minimo punto fisso di T contenente X. In particolare, $\cup_{n\in N} T^n(\varnothing)$ è il minimo punto fisso di T.

Dim. La condizione (2.2) comporta la crescenza di T. Pertanto dall'ipotesi $T(X) \supseteq X$, applicando n volte l'operatore T, segue che $T^{n+1}(X) \supseteq T^n(X)$. Essendo quindi $(T^n(X))_{n\in N}$ una successione crescente per (2.2)

$$T(\cup_{n\in N} T^n(X)) = \cup_{n\in N} T^{n+1}(X) = \cup_{n\in N} T^n(X).$$

Ciò prova che $\cup_{n\in N} T^n(X)$ è un punto fisso di T. Per provare che tale insieme è il minimo punto fisso contenente X, sia M un qualsiasi punto fisso contenente X. Allora per la monotonia di T, applicando n volte T alla diseguaglianza $M \supseteq X$, otteniamo che $T^n(M) \supseteq T^n(X)$ e quindi, essendo M punto fisso, che $M \supseteq T^n(X)$. In definitiva $M \supseteq \cup_{n\in N}\ T^n(X)$ e quindi $\cup_{n\in N}\ T^n(X)$ è il minimo punto fisso contenente X. □

Corollario 2.6. Sia $T : \mathcal{P}(S) \to \mathcal{P}(S)$ un operatore algebrico, allora per ogni $X \subseteq S$ l'equazione

$$D(X) = \cup_{n\in N} T^n(X) \qquad (2.3)$$

fornisce il minimo punto fisso $D(X)$ di T contenente X.

Esempio: Sia S uno spazio Euclideo e definiamo l'operatore $T : \mathcal{P}(S) \to \mathcal{P}(S)$ ponendo

$$T(X) = \{x \in S \mid \exists p \in X, \exists q \in X, x \in \underline{pq}\}$$

avendo indicato con $\underline{pq}$ il segmento chiuso di estremi p e q. In altre parole $T(X)$ è l'insieme dei punti che si trovano su di un segmento i cui estremi appartengono a X. Sono punti uniti di T tutti e soli i sottoinsiemi convessi di S. T è un operatore algebrico di tipo due. Infatti $x \in T(X)$ implica che $x \in pq$ con $p \in X$ e $q \in X$, e quindi $x \in T(\{p,q\})$. Ne segue che:
- l'intersezione di una famiglia di insiemi convessi è ancora un insieme convesso;
- dato un insieme X esiste il più piccolo insieme convesso $D(X)$ contenente X e lo si può ottenere come unione della catena $T^1(X)$, $T^2(X)$, . . .

3. Come generare relazioni di ordine o di equivalenza

Se una relazione $\mathcal{R}$ non è una relazione di pre-ordine allora non è difficile farla diventare una relazione di pre-ordine aggiungendo un opportuno insieme di coppie. Per mostrare come questo può essere fatto vediamo prima come si può rendere riflessiva una relazione.

Definizione 3.1. Dato un insieme S, la *diagonale* di S è la relazione

$$D(S) = \{(x,y) : x \text{ coincide con } y\}.$$

Tale relazione viene anche chiamata *identità.*

La relazione $D(S)$ viene detta *diagonale* in quanto nel caso $S = R$, la sua rappresentazione in un sistema di assi cartesiano ortogonali coincide con la diagonale del primo e terzo quadrante.

Dalla definizione di relazione riflessiva segue immediatamente la seguente proposizione.

Definizione 3.2. Dato un insieme non vuoto S indichiamo con $Rifl : \mathcal{P}(S\times S) \to \mathcal{P}(S\times S)$ l'operatore che associa ad ogni relazione binaria $\mathcal{R}$, la relazione

$$Rifl(\mathcal{R}) = \mathcal{R} \cup D(S).$$

Vale la seguente proposizione di cui omettiamo la semplice dimostrazione.

Proposizione 3.3. *Rifl* è un operatore di chiusura, inoltre le seguenti asserzioni sono equivalenti:

i) $\mathcal{R}$ è riflessiva
ii) $Rifl(\mathcal{R}) = \mathcal{R}$ cioè $\mathcal{R}$ è un punto fisso di *Rifl*
iii) $\mathcal{R} \supseteq D(S)$.
Inoltre $Rifl(\mathcal{R})$ è la più piccola relazione riflessiva contenente $\mathcal{R}$.

La relazione $Rifl(\mathcal{R})$ viene chiamata *relazione riflessiva generata da* $\mathcal{R}$. Vediamo ora come si può rendere transitiva una relazione.

Definizione 3.4. Sia $\mathcal{R}$ una relazione in S, chiamiamo *percorso* da x ad y una successione $x_1,...,x_n$ di elementi di S tale che $x = x_1$, $x_n = y$ e $x_{i-1}\mathcal{R}x_i$. Definiamo l'operatore $Trans : \mathcal{P}(S\times S) \to \mathcal{P}(S\times S)$ che associa ad ogni relazione binaria $\mathcal{R}$, la relazione

$$Trans(\mathcal{R}) = \{(x, y) : \text{esiste un percorso da } x \text{ ad } y\}.$$

Vale la seguente proposizione.

Proposizione 3.5. *Trans* è un operatore di chiusura. Una relazione binaria $\mathcal{R}$ è transitiva se e solo se $\mathcal{R} = Trans(\mathcal{R})$ cioè se e solo se è un punto fisso di *Trans*. Inoltre $Trans(\mathcal{R})$ è la più piccola relazione transitiva contenente $\mathcal{R}$.

Dim. E' evidente che $\mathcal{R}$ è transitiva se e solo se contiene $Trans(\mathcal{R})$. Per provare che $\mathcal{R}' = Trans(\mathcal{R})$ è transitiva supponiamo che $x\mathcal{R}'y$ e $y\mathcal{R}'z$ e quindi che esista un percorso $a_1,\ldots,a_n$ da x ad y ed un percorso $b_1,\ldots,b_m$ da y a z. Allora $a_1,\ldots,a_{n-1},b_1,\ldots,b_n$ è un percorso da x a z. Per provare che $\mathcal{R}'$ è la più piccola relazione transitiva contenente $\mathcal{R}$ indichiamo con $\mathcal{R}^*$ una relazione transitiva contentente $\mathcal{R}$. Allora $\mathcal{R}^* \supseteq Trans(\mathcal{R}^*) \supseteq Trans(\mathcal{R})$. □

Proposizione 3.6. La relazione $Trans(Rifl(\mathcal{R}))$ è sia riflessiva che transitiva e quindi è una relazione di pre-ordine. Precisamente è il più piccolo preordine contentente $\mathcal{R}$ e viene chiamato *preordine generato da* $\mathcal{R}$.[2]

[2]Abbiamo già utilizzato questo modo di procedere quando abbiamo definito la relazione d'ordine in una terna di Peano come la relazione ge-

Resta da vedere come sia possibile trasformare una relazione di pre-ordine in una relazione d'ordine, cioè ottenere la proprietà antisimmetrica. Ora se $\mathcal{R}$ contiene due coppie (a,b) e (b,a) con $a \neq b$, allora non esiste nessuna speranza di estendere $\mathcal{R}$ in modo da ottenere tale proprietà. Per ottenerla allora dobbiamo quozientare opportunamente la struttura $(S, \mathcal{R})$. Infatti vale la seguente proposizione.

Proposizione 3.7. Sia $\leq$ una relazione di un pre-ordine, allora la relazione $\equiv$ che si ottiene ponendo $x \equiv y$ se e solo se $x \leq y$ e $y \leq x$ è una relazione di equivalenza. Se si definisce in $S/\equiv$ la relazione $\leq$ ponendo

$$[x] \leq [y] \Leftrightarrow x \leq y$$

tale relazione è d'ordine in $S/\equiv$.

Se invece di mirare a relazioni d'ordine vogliamo ottenere relazioni di equivalenza, dobbiamo vedere come si possa modificare una relazione $\mathcal{R}$ in modo da ottenere la simmetria.

Proposizione 3.8. Sia $Simm : \mathcal{P}(S \times S) \to \mathcal{P}(S \times S)$ l'operatore che associa ad ogni relazione binaria $\mathcal{R}$, la relazione

$$Simm(\mathcal{R}) = \mathcal{R} \cup \mathcal{R}^{-1}.$$

Allora *Simm* è un operatore di chiusura. Inoltre le seguenti asserzioni sono equivalenti:

i) $\mathcal{R}$ è simmetrica

ii) $\mathcal{R}$ è un punto fisso di *Simm*

iii) $\mathcal{R} \supseteq \mathcal{R}^{-1}$ è un punto fisso di *Si.*

Ne segue che $Simm(\mathcal{R})$ è la più piccola relazione simmetrica contenente $\mathcal{R}$. $Simm(\mathcal{R})$ viene chiamata *relazione simmetrica generata da* $\mathcal{R}$.

Proposizione 3.9. Definiamo l'operatore $Eq : \mathcal{P}(S \times S) \to \mathcal{P}(S \times S)$ ponendo

$$Eq(\mathcal{R}) = Trans(Simm(Rifl(\mathcal{R}))).$$

---

nerata dalla relazione "successivo". In questo caso un percorso da x ad y è costituito da una seccessione del tipo $s^0(x), s^1(x), ..., s^n(x) = y$.

Allora *Eq* è un operatore di chiusura i cui punti fissi coincidono con le relazioni di equivalenza. Ne segue che $Eq(\mathcal{R})$ è la più piccola relazione di equivalenza contenente $\mathcal{R}$ e viene chiamata *relazione di equivalenza generata da* $\mathcal{R}$.

Indice Analitico

addizione di due cardinali; 96
alfabeto; 173
algebra
  dei numeri cardinali; 97
  dei numeri ordinali; 109
algebre di Boole per i sillogismi; 205
anello degli interi relativi
  visto tramite la riduzione a forma normale; 3
Aristotele
  quadrilatero; 196
  sillogismi; 197
Assioma
  del singoletto; 146
  dell'infinito; 148
  dell'insieme delle parti; 148
  dell'insieme vuoto; 146
  dell'unione; 147
  dell'unione di due insiemi; 147
  della coppia; 148
  della scelta; 14; 149
  di Archimede; 139
  di completezza; 140
  di estensionalità; 145
  di isolamento; 143; 148
  di sostituzione; 149
assiomi logici; 183
Brouwer L. E. J.; 129
campo
  archimedeo; 139
  completo; 140
campo dei numeri reali
  definizione assiomatica; 141
  sistema di assiomi; 138
cardinali
  elevazione a potenza; 98
  proprietà delle operazioni; 97
categoria
  associata ad una classe ordinata; 215
  coprodotto di due oggetti; 218
  definizione; 213
  degli insiemi; 214
  degli spazi topologici; 215
  dei gruppi; 215
  dei monoidi; 216

delle matrici; 215
epimorfismo; 220
funtore tra; 221
monomorfismo; 219
morfismi; 213
prodotto di due oggetti; 223
diagrammi di Eulero-Venn; 202
dimostrazione in logica matematica; 183
elementi
infinitamente vicini in un campo ordinato; 139
elemento
finito in un campo ordinato; 139
infinitesimo in un campo ordinato; 139
infinito in un campo ordinato; 139
limite in un insieme ben ordinato
successivo; 102
elemento
separatore in un insieme ordinato; 140
equipotenti; 12
falsa confutazione dell'assioma della scelta; 150
formule ben formate; 181
Frege; 127
funzione
caratteristica di un sottoinsieme; 39
geometrie finite; 136
Hilbert
Fondamenti della Geometria"; 132
Sull'infinito; 168
implicatura; 208
insieme
Dedekind finito; 19
Dedekind infinito; 19
D-finito; 19
D-infinito; 19
enumerabile; 22
N-finito; 19
N-infinito; 19
numerabile; 22
rozzo; 115
SI-finito; 19
SI-infinito; 19
vago o fuzzy; 115
insieme ben ordinato
successivo; 102
interpretazione; 184

intuizionismo; 129
Ipotesi
  del continuo; 152
  generalizzata del continuo; 152
Lemma di Zorn; 17
linguaggio
  dei termini; 180
  del primo ordine; 179; 180
  del secondo ordine; 181
  formale; 174
logica
  del primo ordine; 181
  del secondo ordine; 181
Mathematica; 49
multinsieme; 114
notazione
  infissa; 181
  prefissa; 181
numero
  algebrico; 178
  cardinale; 95
  cardinale in Cantor; 94
  di codice; 193
  naturale non-standard; 192
  ordinale; 105
  reale nell'approccio assiomatico; 141
  trascendente; 178
operatore di chiusura; 226
paradosso
  "io sono una asserzione falsa"; 192
  dei quadrati perfetti; 8
  del barbiere; 126
  del mucchio di grano e del buon ordine; 118
  del quadrato con tanti punti quanto il suo lato; 40
  del quadrato e del cerchio; 83
  della classe degli insiemi con tre elementi; 124
  della classe degli insiemi finiti; 124
  della classe dei gruppi; 125
  della classe di tutti gli insiemi; 122
  della moltiplicazione dei pani e dei pesci o di Banach-Tarski; 93
  della somma di infiniti 1 ed -1; 10
  delle due monete; 10
  delle espressioni eterologhe; 127
  delle ruote concentriche; 9
  delle ruote concentriche, soluzione; 37

di Berry; 119
di Russell; 123
di Vitali; 90
parola; 173
Peano; 132
Peano curva; 41
potenza
del continuo; 95
del numerabile; 95
potenza del continuo; 37
principio
dei cassetti; 21
di comprensione; 121
di induzione transfinita; 103
di sostanzialità; 121
prodotto
di due insiemi ben ordinati; 107
proiezione *i*-esima; 186
punto fisso di un operatore; 226
regola
generalizzazione,; 182
Modus Ponens; 182
relazione
di buon ordine; 99
di equivalenza generata da; 234
di pre-ordine generata da; 232
diagonale; 231
riflessiva generata da; 232
simmetrica generata da; 233
sillogismo; 197
barbara, darii, celarent, ferio, barbari, celaront; 199
sistema di chiusura; 225
somma
di due insiemi ordinati; 108
stoici, contributo alla logica; 201
strutturalismo; 156
Teorema
di Cantor; 43
di Cantor-Bernstein
cercare una dimostrazione; 78
di Cohen; 152
di Completezza; 190
di Gödel (primo); 192
di Gödel (secondo); 195
di Hartogs; 13

di punto fisso per operatori compatti e monotoni; 230
teoremi limitativi
indecidibilità dell'aritmetica; 191
teoria
categorica; 153
consistente; 154
di Zermelo-Fraenkel; 144
indipendente; 155
teoria
completa; 156
teoria delle classi; 142
Terne di Peano
assiomi del primo ordine; 191
assiomi del secondo ordine (si veda il primo volume); 191
unione disgiunta; 96
verità di una formula; 189

BIBLIOGRAFIA.

Per i fondamenti e la storia della matematica

- Benci Vieri, Paolo Freguglia, La matematica e l'infinito, Carocci editore, Studi Superiori.
- Biacino Loredana*: Le funzioni elementari: un approccio storico*, Ed. CompoMat, 2009.
- Bottazzini-Freguglia-Rigatelli, *Fonti per la storia della matematica*, Sansoni, 1992.
- D'Amore B., M. Matteuzzi, *Gli interessi matematici*, Marsilio.
- Kline Morris, *La matematica nella cultura occidentale*, Feltrinelli.
- Kline Morris, *Storia del pensiero matematico*, vol I e II, Einaudi, 1972.
- Lolli G., *Da Euclide a Goedel*, Il Mulino, 2004.
- Lolli G., *Guida alla teoria degli insiemi*, Springer-Verlag Italia 2008.
- Paolini E., *Il paradosso di Banach-Tarski*.
- Radice L. L., *L'infinito*, Editori Riuniti.
- Zanardi A., *Note sugli insiemi*.
- Freguglia P. , La matematica e l'infinito, Carocci editore, 2019.
- Giusti E., Piccola storia dell calcolo infinitesimale dall'antichità al novecento, Il Giardino di Archimede, Istituti Editoriali e Poligrafici Internazionali, 2007.
- Maracchia S.,Storia dell'Algebra, Liguori editore, 2005.

Per quanto riguarda i fondamenti della geometria.

- Agazzi E., D. Palladino, *Le geometrie non euclidee*, Mondadori.
- Hilbert D., *Fondamenti della geometria*, Feltrinelli, 1970.
- Odifreddi P. O., *Divertimento geometrico*: Le origini geometriche della logica da Euclide a Hilbert, Boringhieri, 2003.
- Trudeau R., *La rivoluzione euclidea*, Boringhieri, 1991.

Per chi ha interessi verso la filosofia della matematica.

- Cellucci C., *La filosofia della matematica del Novecento*, Laterza, 2007.
- Casari G., *Questioni di filosofia della matematica*, Feltrinelli.
- Lolli G., *Filosofia della matematica*: *L'eredità del Novecento*.
- Geymonat L., *Storia del pensiero filosofico e scientifico*, Garzanti.
- Wang Hao, *Dalla matematica alla filosofia*, Boringhieri, 1984.
- Hofstadter D. R., Goedel, Escher, *Bach: un' eterna Ghirlanda Brillante*. Il Mulino, 2002.

Per chi ha interesse al rapporto tra matematica e letteratura

Toffalori C., L'aritmetica di cupido, Guanda Editore 2011.

Per una semplice e rigorosa introduzione dei sistemi numerici.

- Enea M. R., D. Saeli, *Sistemi Numerici*, ARACNE editrice 2009.

Per una rivisitazione del campo dei reali dal punto di vista della teoria della computabilità

- Mayoh B. H., « Unsolvable problems in the theory of computable numbers » in: *Formal Systems and Recursive Functions*, edited by Crossley-Dummett (North-Holland, Amsterdam 1965).