CAPITOLO 3

CREDERE NELL'INFINITO[1]

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

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

1. Aritmetizzazione ed infinito attuale
Una volta che abbiamo definiti i numeri reali possiamo definire la geometria come viene attualmente studiata, cioè come capitolo dell'algebra lineare. Infatti vale il seguente teorema.

Teorema 1. Sia R l'insieme dei numeri reali, chiamiamo *piano euclideo* il prodotto cartesiano $R\times R$, e chiamiamo *punti* i suoi elementi. Inoltre chiamiamo *retta* un insieme di punti che verifichi una equazione lineare del tipo $ax+by+c = 0$. Allora la struttura ottenuta in tale modo verifica tutti gli assiomi della geometria euclidea.

Dim. Proviamo ad esempio che per due punti distinti $(\underline{x}_0,\underline{y}_0)$ e $(\underline{x}_1,\underline{y}_1)$ passa una ed una sola retta. Tale problema si traduce in quello di trovare a, b, c (non tutti nulli) tali che
$a\underline{x}_0+b\underline{y}_0 +c = 0$
$a\underline{x}_1+b\underline{y}_1 +c = 0$
Si tratta di un sistema omogeneo di due equazioni nelle incognite a, b e c e dalla teoria dei sistemi lineari si sa che tale sistema ammette infinite soluzioni e che due diverse soluzioni sono proporzionali tra loro. Ne segue che tutte queste soluzioni rappresentano una stessa retta e ciò prova l'esistenza e l'unicità della retta per $(\underline{x}_0,\underline{y}_0)$ e $(\underline{x}_1,\underline{y}_1)$.
I rimanenti assiomi si dimostrano in modo simile.

In definitiva, a partire dai numeri naturali (tanto cari alla scuola pitagorica) si è riusciti a costruire la classe dei numeri reali e con questi, tramite la geometria analitica, l'intera geometria. Un processo di aritmetizzazione simile è stato poi fatto per quanto riguarda l'analisi matematica. Infatti nascono le attuali definizioni di limite, derivata, funzione continua che fino alla prima metà dell'ottocento si basavano sulla intuizione del continuo geometrico. Appare di nuovo attuale l'antica idea della scuola Pitagorica per cui tutto è riconducibile ai numeri interi. Tuttavia il prezzo da pagare per attuare un tale processo di aritmetizzazione è l'accettazione dell'infinito attuale. Infatti se si utilizza, ad esempio, il metodo delle sezioni, allora

<u>ogni numero reale è un oggetto infinito,</u>

essendo una sezione costituita da due insiemi infiniti di razionali. La stessa affermazione la possiamo fare se ci riferiamo al metodo delle successioni di Cauchy. Infatti ciascuna successione di Cauchy è un oggetto infinito ed a maggiore ragione una classe completa di equivalenza di successioni di Cauchy è un oggetto infinito.
Naturalmente anche l'insieme dei numeri naturali, dei numeri relativi e dei numeri razionali sono infiniti. Tuttavia accettare tali numeri coinvolge solo l'infinito potenziale perché

<u>ciascun numero naturale, relativo o razionale è un oggetto finito</u>

ed i matematici operano solo su tali oggetti finiti. Infatti, nel caso della costruzione degli interi relativi, pur essendo ogni classe di equivalenza di coppie un oggetto infinito, noi potremmo benissimo fissare in ogni classe un particolare elemento rappresentativo, che chiamiamo in *forma normale*, e poi lavorare con tali elementi invece che con le classi.

[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 (ingenua) verso l'accettazione di insiemi infiniti.

Definizione 2. Chiamiamo in *forma normale* ogni coppia di numeri naturali del tipo $(p,0)$, che possiamo indicare con $+p$ oppure del tipo $(0,p)$, che possiamo indicare con $-p$.

Ogni intero relativo (m,n) si può ridurre in forma normale poiché è equivalente ad $(m-n,0)$ se $m \geq n$ ed a $(0,n-m)$ se $m<n$. Pertanto potremmo definire l'anello degli interi relativi al modo seguente:

Definizione 3. Chiamiamo *numero relativo* ogni coppia di numeri naturali in forma normale,
- chiamiamo *somma* di due numeri relativi la riduzione a forma normale della somma come è stata definita ne capitolo 2,
- chiamiamo *prodotto* di due numeri relativi la riduzione a forma normale del prodotto come è stato definito nel capitolo 2.

Lo stesso discorso può essere fatto per i numeri razionali. Infatti ogni classe $[(p,q)]$ in Q può essere rappresentata in un solo modo da una coppia (p,q) con p e q primi tra loro.

Definizione 4. Chiamiamo in *forma normale* una coppia (p,q) di interi relativi con p e q primi tra loro.

Ogni coppia può essere ridotta in forma normale in modo ovvio.

Definizione 5. Chiamiamo *numero razionale* ogni coppia di numeri relativi in forma normale. Inoltre, dati due razionali (p,q) ed (a,b),
- chiamiamo *somma* $(p,q)+(a,b)$ la riduzione a forma normale della coppia $(pb+qa,qb)$
- chiamiamo *prodotto* $(p,q)\cdot(a,b)$ la riduzione a forma normale della coppia (pa,qb)[2].

2. Ma questi insiemi sono poi veramente una novità ?

La teoria degli insiemi è stata proposta da Cantor alla fine del ottocento in stretto collegamento con i sui studi di analisi matematica. Cantor non è certo stato il primo ad utilizzare concetti come quelli di insieme, classe, collezione, concetti questi che 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",
etc. . . . .

Nelle scienze naturali si trovano numerosi esempi di un tale uso del concetto di classe. Ma allora:
- perché si dice che Cantor fu l'inventore della teoria degli insiemi ?
- in che cosa consiste la novità della sua proposta ?

Una adeguata risposta a tali domande è importante anche per comprendere il significato che ha l'introduzione (eventuale) della teoria degli insiemi nelle scuole. Per cercare di capire come vanno le cose, consideriamo alcune frasi del linguaggio comune. Ad esempio consideriamo 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*.

---

[2] Questo modo di procedere è molto generale ed in un certo senso può sostituire la nozione di quoziente di una struttura algebrica modulo una data congruenza. Infatti, data una congruenza (ma è sufficiente anche una qualunque equivalenza) in una data struttura algebrica, invece di lavorare sulle classi di equivalenza definendo su tali classi le relative operazioni, è possibile:
- individuare all'interno di ogni classe un particolare elemento che viene detto *in forma normale*
- effettuare l'operazione sulle forme normali e poi ridurre in forma normale il risultato.

Un tale modo di vedere i numeri razionali ed i numeri relativi viene adottato da sistemi di calcolo simbolico come Mathematica.

La prima frase è del tipo usuale, vi è un soggetto (la rosa che è nel vaso) ed un predicato (essere rosso). Essa 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. 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 i 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 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:

<u>non ha senso affermare che ciascuna rosa del vaso è *"dodici"*.</u>

Il predicato *"avere dodici elementi"* si riferisce all'intero insieme delle rose che pertanto viene ad essere il vero soggetto della frase c). 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 invece gli insiemi saranno visti come nuovi enti matematici e la c) sarà una asserzione matematica come le altre[3].

Concludiamo questo paragrafo osservando che, in definitiva, vi sono due modi di coinvolgere una collezione di elementi in un discorso scientifico.
1. Il primo si ha quando ci si riferisce a ciascun elemento della collezione stessa.
2. 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. 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 la teoria della classi, o, per meglio dire, il linguaggio delle classi.

Esempio: 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 ed l'insieme dei divisori di m". A me sembra un modo inutilmente complicato di dare la definizione! Il linguaggio

[3] 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"*.

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.

Esempio: A volte, per illustrare la nozione di intersezione, si dice che la balena è un elemento di intersezione tra gli insieme degli animali acquatici e l'insieme dei mammiferi invece di dire semplicemente che è un mammifero acquatico. Anche in questo caso sembra più semplice dire che la balena è un mammifero che vive nell'acqua senza disturbare l'operazione di intersezione.

Si fa' 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 numeri reali con il metodo delle sezioni o con un qualunque altro metodo.

3. I paradossi di Galileo.

La teoria degli insiemi è strettamente legata alla questione dell'infinito in matematica. Una delle prime domande che un matematico si pone riguarda la grandezza degli enti matematici che si propone di studiare. 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 conseguenti a tale possibilità.

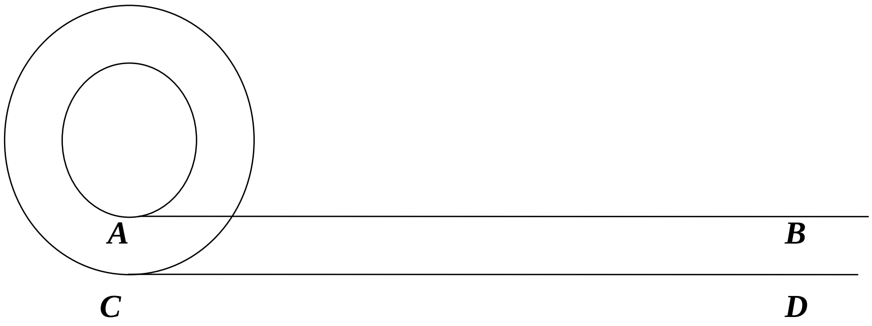
Il paradosso dei quadrati perfetti. Galileo confrontò l'insieme N degli interi e l'insieme QP dei quadrati perfetti e giunse alla paradossale conclusione che tali insiemi hanno lo stesso numero di elementi. Infatti egli osservò che ad ogni intero n è possibile associare il quadrato perfetto n^2 ottenendo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

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

Naturalmente in tale modo ad elementi 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 ma anche contradddittoria. 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.

Il Paradosso delle ruote concentriche:

Questo paradosso, descritto da Galileo, sembra risalire ad Aristotele. Consideriamo due ruote concentriche, di raggi r e $2r$ *e* supponiamo di far fare alla più grande un giro completo in modo che rotolando tracci un segmento CD. Nel frattempo la ruota più piccola avrà fatto un giro completo ed avrà tracciato un segmento AB della stessa lunghezza.



Ma questo è assurdo perché i due segmenti rappresentano lo "srotolamento" di due circonferenze di lunghezza diversa. 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 capacita 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.

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 quanto una loro parte propria[4]. E' da notare che le motivazioni filosofiche di Cantor erano strettamente intrecciate a quelle religiose[5]. Ad esempio in una lettera del 1890 a padre Thomas Esser egli scrive tra l'altro.

---

[4] 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.

[5] D'altra parte le motivazioni religiose stanno 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, 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 "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)

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.

4. Confrontare le grandezze degli insiemi.

La possibilità di confrontare le grandezze di insiemi non necessariamente finiti è alla base della teoria degli insiemi.

Definizione 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. 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.

In altri termini A ed 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 ed ogni elemento di B si può ottenere in questo modo. Nel caso della corrispondenza proposta da Galileo tra N e l'insieme QP 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 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 $A \equiv C$.

Pertanto, in un certo senso, la relazione di equipotenza è una relazione di equivalenza[6] .

Dim. 1. Sia A un qualunque insieme, 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.

[6] In realtà non è completamente corretto parlare di relazione di equivalenza. Infatti l'insieme in cui tale relazione dovrebbe essere considerata dovrebbe essere la classe di tutti gli insiemi. Purtroppo, come vedremo nel prossimo capitolo, tale classe crea molti problemi. Analoga considerazione deve essere fatta per la relazione "avere meno potenza di" che viene trattata nel teorema successivo. Insomma le cose sono sempre più complicate di come si pensa.

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.

Teorema 3. La relazione $\leqq$ "avere meno potenza di" è una relazione di pre-ordine comunque si scelgano gli insiemi A, B e C :
1. $A \leqq A$
2. Se $A \leqq B$ e $B \leqq C$ implica $A \leqq C$.
Inoltre la relazione di equivalenza associata a tale relazione coincide con l'equipotenza. In altri termini;
3. $A \leqq B$ e $B \leqq A$ implica $A \equiv B$.

Dim. Per le proprietà 1 e 2 si procede allo stesso modo che nel teorema 2. Per la proprietà 3 si veda l'appendice 2.

La proprietà 3 va sotto il nome di Teorema di Cantor-Bernstein.

Proposizione 4. Sia A un insieme e $\equiv$ una relazione di equivalenza in A, allora il quoziente $A/\equiv$ ha potenza minore o uguale ad A.

Dim. Sia $f : A/\equiv \to A$ una funzione che associ ad ogni classe di equivalenza z un elemento $f(z) \in z$ (come vedremo una tale funzione esiste se si ammette l'assioma della scelta). Tale funzione è iniettiva perché se $f(z) = f(z')$ allora le due classi z e z' hanno un elemento in comune e quindi coincidono.

Proposizione 5. Se esiste una funzione suriettiva $f : A \to B$ di A in B allora B ha potenza minore o uguale ad A. Infatti se $\equiv$ è il nucleo di f, allora B è equipotente a $A/\equiv$.

Dim. Sia $f : A \to B$ una funzione suriettiva, allora il suo nucleo $\equiv$ ripartisce A in classi di equivalenza. La funzione $g : A/\equiv \to B$ definita ponendo $g([x]) = f(x)$ è ben definita perché il suo valore non dipende dall'elemento rappresentativo in $[x]$. Inoltre, poichè

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

la funzione g è iniettiva. Ciò prova che $A/\equiv$ è equipotente a B.

Il paradosso di Galileo di un insieme equipotente ad una sua parte propria sfrutta il fatto che i numeri naturali sono un insieme infinito. Come abbiamo già osservato in una nota, questo fenomeno può essere utilizzato proprio per dare una definizione di insieme infinito.

Definizione 6. Un insieme che risulta equipotente ad una propria parte propria viene detto *infinito*, altrimenti viene detto *finito.*

Proposizione 7. L'insieme N dei numeri naturali è infinito. Inoltre un insieme è infinito se e solo se ha potenza maggiore o uguale ad N.

Dim. Che N sia infinito deriva dall'osservazione di Galileo per cui N è equipotente all'insieme QP dei quadrati perfetti che costituiscono una parte propria di N. D'altra parte ogni terna di Peano è infinita perché la funzione successore è iniettiva per definizione e non è suriettiva in quanto il primo elemento non è successore di nessun altro elemento.

Sia S infinito, allora abbiamo già visto che contiene una terna di Peano e quindi ha potenza maggiore di N. Viceversa se S ha potenza maggiore o uguale al numerabile allora esiste una funzione iniettiva $f : N \to S$. Consideriamo la funzione $g : S \to S$ definita ponendo $g(x) = x$ se $x \notin f(S)$ e $g(f(n)) = f(n+1)$: in altri termini tale funzione sposta di un passo gli elementi della successione $f(n)$ e lascia immutati gli altri elementi di S. Ne segue che, poiché g non può assumere il valore $f(0)$, g è una funzione biettiva di S in una sua parte propria. Ciò prova che S è infinito.

Esercizio. Tenendo conto che un uomo non può avere più di 200.000 capelli dire se a Salerno esistono due uomini con lo stesso numero di capelli (si suggerisce di considerare la funzione che associa ad ogni salernitano il numero dei suoi capelli.

5. Insiemi numerabili

Gli insiemi equipotenti ad N vengono detti *numerabili*, gli insiemi che hanno potenza minore od uguale ad N vengono chiamati *enumerabili* o *codificabili*[7]. Pertanto un insieme A è numerabile se esiste una funzione $f : A \to N$ biettiva. A è enumerabile se esiste una funzione $f : A \to N$ iniettiva. Se si tiene conto della proposizione 5 del paragrafo precedente abbiamo la seguente ovvia proposizione.

Proposizione 1. Le seguenti asserzioni sono equivalenti:
a) A è enumerabile
b) A è vuoto, finito o numerabile
c) A è vuoto oppure esiste una funzione $f : N \to A$ suriettiva (che viene chiamata *funzione enumerante*).

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). Nel caso in cui in tale enumerazione non viene mai ripetuto due volte lo stesso elemento la f è anche iniettiva e quindi A è numerabile. La parola *codificabile* viene usata a volte in informatica poiché la funzione iniettiva $f : A \to N$ viene interpretata come un modo di assegnare ad ogni oggetto a in A un *numero di codice* $f(a)$ di a.

Proposizione 2. L'unione di due insiemi enumerabili è un insieme enumerabile. L'unione di un insieme finito ed uno numerabile è un insieme numerabile. L'unione di due insiemi numerabili è un insieme numerabile[8].

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

[7] In realtà il concetto di insieme enumerabile non sembra essere usato nei libri di matematica italiani. Nei libri in lingua inglese invece viene trattato sotto il nome di *countable set*. Invece sia in Italia che fuori Italia nei libri di informatica si parla di *effettivamente enumerabile* (in inglese *effectively enumerable*) per indicare un insieme che sia enumerato tramite una funzione per la quale esiste un opportuno programma capace di computarla.
[8] Alla fine di questo capitolo tale teorema viene illustrato tramite il raccontino degli "alberghi di Hilbert".

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

Tale funzione è suriettiva e quindi h rappresenta una funzione enumerante $A \cup B$.

Sia $A = \{a_1,...,a_n\}$ un insieme finito e B un insieme numerabile. Sia $f : N \to B$ una funzione biettiva enumerante B, allora una numerazione di $A \cup B$ sia ottiene al modo seguente:

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

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

$h(1) = a_1, h(2) = a_2,...,h(n) = a_n, h(n+1) = f(1), ..., h(n+m) = f(m), ...$

E' evidente che h è una funzione biettiva enumerante $A \cup B$.

Siano A e B numerabili, allora nel caso nel caso in cui A e B siano disgiunti la funzione h ora definita è biettiva. Invece nel caso $A \cap B \neq \emptyset$ h non è iniettiva in quanto un elemento dell'intersezione viene enumerato due volte. Intuitivamente basta che nella enumerazione

$f(1), g(1), f(2), g(2), . . .$

gli elementi già comparsi non siano ripetuti. Un modo più rigoroso ma meno costruttivo di procedere è quello di osservare che, essendo h suriettiva $A \cup B$ ha potenza minore o uguale a quella di N. Poiché è evidente che $A \cup B$ ha potenza maggiore o uguale a quella di N, $A \cup B$ è equipotente ad N. Tale modo di ragionare non fornisce però concretamente la funzione enumerante.

Esempio. Sia $A = \{5,3,7\}$ e sia QP l'insieme dei quadrati perfetti. L'insieme QP è numerabile perché la funzione $f(n) = n^2$ è una biezione di N in QP, cioè è una funzione enumerante QP. Allora possiamo enumerare al modo seguente gli elementi di $A \cup QP$:

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

Più precisamente una funzione $h : N \to A \cup QP$ enumerante $A \cup QP$ si ottiene 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 3. L'insieme degli interi relativi Z 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. Più precisamente una enumerazione degli elementi di Z si ottiene al modo seguente

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

cioè tramite la funzione $h : N \to Z$ definita al modo seguente

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

□

Cantor si pose poi il problema se N e l'insieme Q dei razionali fossero equipotenti. La risposta fu affermativa:

anche Q che appariva tanto più grande di N, aveva tanti elementi quanti ne aveva N !

Proposizione 4. L'insieme Q dei numeri razionali è numerabile.

Dim. Cominciamo col provare che l'insieme dei razionali positivi Q^+ è numerabile. Una dimostrazione intuitiva di tale numerabilità si ottiene disponendo i numeri razionali nella seguente matrice infinita

1/1 1/2 1/3 1/4 1/5 . . .

2/1 2/2 2/3 2/4 2/5 . . .

3/1 3/2 3/3 3/4 . . .

4/1 4/2 4/3 . . .

5/1 . . .

. . .

in cui il numeratore rappresenta la riga di appartenenza ed il denominatore la posizione all'interno della riga di un razionale. Ovviamente un 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).

E' possibile seguire la strategia indicata dalle frecce avendo cura di *saltare* i numeri razionali che già si sono incontrati

E' possibile precisare una tale strategia osservando che si è cominciato a "contare" gli elementi dell'insieme $Q_2 =\{1/1\}$, poi si sono contati gli elementi dell'insieme $Q_3 =\{1/2,2/1\}$, poi gli elementi dell'insieme $Q_4 = \{3/1, 2/2, 1/3\}$ ... Ciascuno di tali insiemi si può caratterizzare dal fatto che la somma del numeratore e del denominatore è rispettivamente 2, 3, ... Indichiamo 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 ottiene 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 Q^- è ancora numerabile e quindi che $Q = Q^+\cup Q^-\cup\{0\}$ è numerabile. □

Proposizione 4. Il prodotto cartesiano di un numero finito di insiemi numerabili è un insieme numerabile.

Dim. Proviamo la proposizione per induzione sul numero n di insiemi numerabili. Per $n = 2$ si procede esattamente con la stessa tecnica della dimostrazione precedente. Infatti se A e B sono due insiemi numerabili allora i loro elementi si possono ordinare 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 come abbiamo contato gli elementi di Q.

$$\begin{array}{lllll}
(a_1,b_1) & (a_1,b_2) & (a_1,b_3) & (a_1,b_4) & (a_1,b_5)\ \ldots \\
(a_2,b_1) & (a_2,b_2) & (a_2,b_3) & (a_2,b_4)\ \ldots & \\
(a_3,b_1) & (a_3,b_2) & (a_3,b_3)\ \ldots & & \\
(a_4,b_1) & (a_4,b_2)\ \ldots & & & \\
(a_5,b_1)\ \ldots & & & &
\end{array}$$

Supponiamo che la proposizione sia vera per n 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.

In particolare abbiamo che N^n è numerabile[9]. Un modo più diretto per provare che $N \times N$ è numerabile è il seguente. Indichiamo con $h : N \times N \to N$ la funzione definita dal porre $h(n,m) = 2^n \cdot (2 \cdot m+1)$. Tale funzione è biettiva perché ogni numero può essere scomposto in uno ed un solo modo come prodotto del tipo $2^n \cdot (2 \cdot m+1)$.

Proposizione 5. L'unione di una successione di insiemi numerabili è ancora un insieme numerabile.

Dim. Il procedimento è il solito. Se $(A_n)_{n \in N}$ è una successione di insiemi numerabili possiamo indicare con $a(i,j)$ l'elemento di A_i che occupa il posto j nella enumerazione di A_i. In questo modo si viene a definire una matrice infinita i cui elementi possono essere enumerati con la solita strategia

$$\begin{array}{lllll}
a(1,1) & a(1,2) & a(1,3) & a(1,4) & a(1,5)\ \ldots \\
a(2,1) & a(2,2) & a(2,3) & a(2,4)\ \ldots & \\
a(3,1) & a(3,2) & a(3,3)\ \ldots & & \\
a(4,1) & a(4,2)\ \ldots & & & \\
a(5,1)\ \ldots & & & &
\end{array}$$

6. Numerabilità e codifica.

Diamo ora un approccio alla questione della numerabilità che è più legato al punto di vista informatico ed alla teoria dei linguaggi formali. A tale scopo introduciamo la nozione di

[9] Un modo più diretto per provare che $N \times N$ è numerabile è il seguente. Indichiamo con $h : N \times N \to N$ la funzione definita dal porre $h(n,m) = 2^n \cdot (2 \cdot m+1)$. Tale funzione è biettiva perché ogni numero può essere scomposto in uno ed un solo modo come prodotto del tipo $2^n \cdot (2 \cdot m+1)$.

"parola". Intuitivamente una parola è una successione di lettere dell'alfabeto come ad esempio "cane", "canne", "cena", "acne", "accanne". Da notare che due parole come "cane" e "cena" che pur avendo le stesse lettere le hanno in posizione diversa vengono considerate diverse. Sono pure considerate diverse due parole come "cane" e "canne" in cui le lettere coincidono ma appaiono un numero diverso di volte. Invece due insiemi sono considerati uguali se hanno gli stessi elementi e quindi 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. Per potere rappresentare in modo insiemistico la nozione di parola si usa la nozione di n-pla che permette appunto di tenere conto di tali fattori (si veda anche l'appendice 1).

Definizione 1. Sia A un insieme finito (che chiamiamo *alfabeto*). Allora gli elementi di A^n vengono anche detti *parole di lunghezza n* nell'alfabeto A. Inoltre indichiamo con A^+ l'insieme $\cup_{n\in N}A^n$ di tutte le possibile parole.

Usualmente si preferisce indicare una parola come $(a_1,a_2,...,a_n)$ con $a_1,a_2,...,a_n$. Ad esempio la parola (c,a,n,e) si scriverà *cane*. 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 vuoto" che corrisponde al lasciare uno spazio vuoto tra due lettere. In questo caso si chiama parola anche quella che è per noi una sequenza di parole separate da spazi vuoti. Ad esempio gli appunti di questo libro possono essere considerate una parola nell'alfabeto che si ottiene usando i soliti caratteri della tastiera più un "carattere" per denotare lo spazio vuoto.

Proposizione 2. L'insieme A^+ delle parole su un alfabeto finito è numerabile.

Dim. Se A è non vuoto ed $a \in A$ 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 ovviamente una funzione iniettiva di N in a. Quindi A^+ ha potenza maggiore o uguale del numerabile. Rimane da provare che A^+ ha anche potenza minore o uguale al numerabile, cioè è necessario trovare una codifica di A^+ Esistono diversi modi per fare questo (cioè diversi modi per codificare un linguaggio). Ad esempio sia p_1, p_2, ... la successione infinita di numeri primi scritta in ordine crescente. Inoltre associamo ad ogni lettera in A un numero intero, cioè consideriamo una funzione iniettiva c : $A \to N$. Allora possiamo associare ad ogni parola $a(1)a(2)...a(n)$ il numero $p_1^{c(a(1))}\cdot p_2^{c(a(2))}\cdot...\cdot p_n^{c(a(n))}$. Tale corrispondenza è iniettiva (anche se non suriettiva).

Un modo più "informatico" di procedere è il seguente. Sia $c : A \to \{0,1\}^+$ una funzione iniettiva che associa 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. In tale modo abbiamo definito una funzione iniettiva di A^+ in N. Ad esempio supponiamo che il nostro alfabeto si riduca alle sole quattro lettere a, e, c, a. Allora possiamo porre $c(a) = 1111$, $c(e) = 1110$, $c(c) = 1000$, $c(n) = 1010$. In questo modo associamo ad una parola come "cane" il numero $c(c)c(a)c(n)c(e) = 1000111110101110$ scritto in base 2.

La tecnica che ora abbiamo utilizzato per dimostrare la proposizione corrisponde al modo concreto di utilizzo 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 alle lettere scritte (ma anche agli spazi vuoti).

Corollario 3 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.

Dalla proposizione 2 segue il seguente criterio per verificare che un insieme è numerabile.

CRITERIO DELLA DESCRIVIBILITA'. Sia X un insieme i cui elementi siano "descrivibili" in un linguaggio formale. Allora X è enumerabile (cioè finito o numerabile).

Naturalmente per essere più precisi si dovrebbe specificare che si intende per "descrizione". Tale criterio vale in quanto qualunque cosa si intenda per "descrizione" deve potersi identificare con una sequenza di lettere dell'alfabeto e di spazi vuoti cioè con un elemento di A^+. Consideriamo la funzione che associa ad ogni elemento in X la sua descrizione in A^+. Si ottiene una funzione di X in un insieme numerabile e questo prova che X è enumerabile.

Ad esempio applicando tale criterio possiamo dimostrare la seguente proposizione.

Proposizione 4. L'insieme $\mathcal{P}_f(N)$ delle parti finite di N è numerabile.

Dim. Basta osservare che ogni insieme finito di numeri interi può essere descritto al modo seguente $\{n_1,...,n_p\}$ cioè può essere descritto usando un linguaggio nell'alfabeto costituito dalle due parentesi {, }, dalle cifre 0,1, 2, 3, 4, 5, 6, 7, 8, 9 e dalla virgola. Allora, ad esempio, all'insieme finito {3,2,5,17} corrisponde un numero che è il numero immagazzinato, sotto la forma di una sequenza di 0 e di 1, nel mio computer quando ho scritto la parola {3,2,5,17}.

Usualmente tale proposizione viene dimostrata considerando un procedimento che consiste, dato un sottoinsieme finito X di N

1) nell'ordinare gli elementi di X in un ordine crescente $a(1) < a(2) <...< a(n)$

2) nell'associare ad X il numero $p(1)^{a(1)}\cdot p(2)^{a(2)}\cdot...\cdot p(n)^{a(n)}$

dove $p(1), p(2),...,p(n)$ sono i primi n numeri primi. Ad esempio all'insieme {4,2,8} associamo il numero $2^2\cdot 3^4\cdot 5^8$. In tale modo si definisce una funzione iniettiva di $\mathcal{P}_f(N)$ in N e ciò mostra che la potenza di $\mathcal{P}_f(N)$ è minore di quella di N. D'altra parte la funzione che ad ogni $n\in N$ associa l'insieme finito $\{n\}$ è una funzione iniettiva di N in $\mathcal{P}_f(N)$ e ciò mostra che la potenza di N è minore di quella di $\mathcal{P}(N)$. □

E' possibile anche ridimostrare in modo più semplice alcune delle proposizioni provate nel paragrafo precedente.

Proposizione 5. 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. Basta osservare che l'usuale rappresentazione in base 10 permette di rappresentare gli interi relativi in un linguaggio il cui alfabeto consiste nelle cifre 0,1,2,3,4,5,6,7,8,9 e nei simboli +,-. Inoltre se a tale alfabeto si aggiunge il carattere /, allora possiamo rappresentare anche tutti i razionali. Infine per rappresentare l'insieme di tutte le possibili n-ple di numeri razionali è sufficiente aggiungere le parentesi (,) e la virgola.

Ricordiamo che un numero reale si dice *algebrico* se è radice di un polinomio a coefficienti razionali. 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 6. L'insieme *Al* dei numeri reali algebrici è numerabile. L'insieme delle funzioni computabili tramite un linguaggio di programmazione è numerabile.

Dim. Sia *Pol* l'insieme dei polinomi a coefficienti interi. Tale insieme essendo un insieme di parole su di un linguaggio finito è numerabile. Consideriamo una corrispondenza $h : Al \to Pol$ che associa ad ogni numero algebrico uno dei polinomi a coefficienti interi di cui è radice. Questa corrispondenza, che non è in generale iniettiva in quanto due numeri diversi possono essere radici dello stesso polinomio, mostra che la cardinalità di *Al* è minore o uguale alla cardinalità di *Pol*. Quindi *Al* ha potenza minore o uguale al numerabile. Più precisamente, poiché *Al* contiene tutti i razionali siamo sicuri che *Al* è numerabile.

7. La potenza del continuo

Cantor era giunto ad un punto morto: aveva confrontato *P* ed *N* ed aveva visto che avevano lo stesso numero di elementi, aveva confrontato *Q* ed *N* ed era arrivato alla stessa conclusione.
E se tutti gli insiemi infiniti fossero numerabili, cioè se tutti gli insiemi infiniti avessero lo stesso numero di elementi?

In tale caso una teoria che si occupa delle grandezze degli insiemi infiniti 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 questo il convincimento di Galileo che 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 il coraggio di negare validità all'assioma euclideo "il tutto è maggiore della parte" e di accettare l'esistenza dell'infinito attuale. Egli riuscì a trovare due insiemi infiniti di diversa grandezza; precisamente riuscì a provare che l'insieme dei numeri reali R ha potenza maggiore di quella di *N* e che quindi esistono almeno due ordini di infinito. Cominciamo con il dimostrare la non numerabilità dell'intervallo aperto (0,1).

Proposizione 1. L'insieme (0,1) non è numerabile (è più grande di *N*).

Dim. 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

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

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, 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. Ci proponiamo ora di costruire un numero reale $r = 0.c_1 c_2 c_3...$ 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

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

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. □

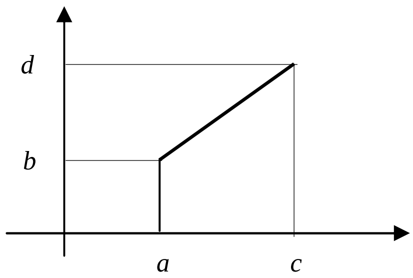
Problema. Dire perché il numero r definito all'interno della dimostrazione della proposizione 1 non coincide con $f(5)$.

Proposizione 2. Tutti gli intervalli aperti sono equipotenti tra loro. Tutti gli intervalli chiusi sono equipotenti tra loro.

Dim. Dati gli intervalli aperti (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

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

E' immediato che tale funzione è una corrispondenza biettiva tra (a,c) e e (b,d).



La stessa funzione f può essere vista come una corrispondenza biettiva tra $[a,c]$ e $[b,d]$.

Proposizione 3. Se S è infinito ed A è finito o numerabile allora S ed $S \cup A$ sono equipotenti.

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. Infatti essendo S infinito la potenza di S è maggiore o uguale al numerabile. Pertanto esiste una funzione iniettiva $f : N \rightarrow S$. Sia $A = \{a_1,...,a_n\}$, allora possiamo definire la corrispondenza $h : S \cup A \rightarrow S$ ponendo

$h(a_1) = f(1)$, $h(a_2) = f(2)$, ..., $h(a_n) = f(n)$

$h(f(i)) = f(i+n)$

$h(x) = x$ se x non appartiene ad $f(N)$ e non appartiene ad A.

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

Nel caso A numerabile, supponiamo che $g : N \rightarrow A$ 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 ad $f(N)$ e non appartiene a $g(N)$.

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. Si utilizzano i posti liberati per inserire gli elementi di A.

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

Corollario 4. Tutti gli intervalli (aperti o chiusi) sono equipotenti tra loro.

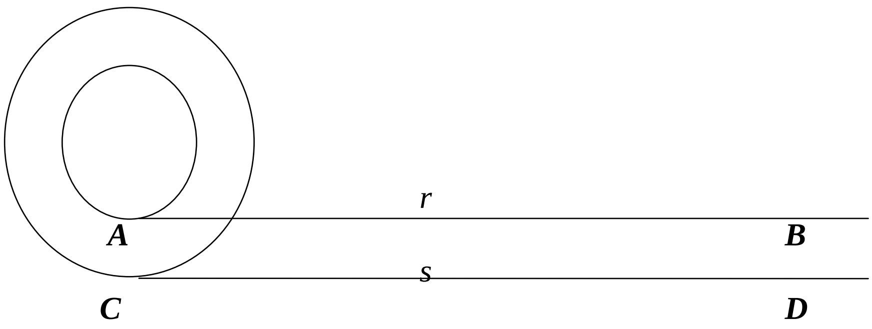
Dim. Ogni intervallo aperto (a,b) e' infinito, pertanto poiché $[a,b] = (a,b)\cup\{a,b\}$, per la proposizione precedente (a,b) è equipotente a $[a,b]$. □

Esempio: Supponiamo di volere costruire una corrispondenza iniettiva f tra [0,1] e (0,1). Allora basta

- fissare una qualunque funzione iniettiva $h : N\rightarrow (0,1)$ ad esempio la funzione $h(n) = 1/(n+1)$
- definire $f : [0,1] \rightarrow (0,1)$ 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 $x \neq 1/n$.

Il paradosso delle ruote concentriche. Torniamo al paradosso di Galileo sulle ruote concentriche



in cui sono coinvolte le due linee r ed s su cui scorrono i punti A e C delle due circonferenze. E' vero che possiamo considerare la corrispondenza che 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 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. Equivalentemente, le due circonferenze sono equipotenti tra loro, come è ovvio, ma questo non vuol dire che abbiano la stessa lunghezza.

Problema. Provare il corollario 4 osservando che ogni intervallo aperto è contenuto in un intervallo chiuso ed ogni intervallo chiuso è contenuto in un intervallo aperto. Pertanto ....

Per quanto riguarda l'insieme R dei numeri reali, vale la seguente proposizione.

Proposizione 5. L'insieme R dei numeri reali è equipotente all'intervallo aperto (-1,1).

Dim. La funzione $f(x) = x/(x^2-1)$ porta l'intervallo (-1,+1) nell'insieme R dei numeri reali in modo biettivo (studiare il grafico della funzione per rendersene conto). □

Definizione 6. Diciamo che un insieme ha la *potenza del continuo* se è equipotente ad R.

Naturalmente tutti gli intervalli, che siano aperti o chiusi, hanno la potenza del continuo. Tutte le circonferenze hanno la potenza del continuo e così via.

8. Superare la potenza del continuo

Abbiamo visto che R è un insieme la cui cardinalità è più grande di quella di N. Si pone allora il problema di vedere se esistono insiemi che abbiano cardinalità più grande di quella di R. L'impresa non è semplice come mostrano le seguenti due proposizioni.

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

Dim. Proviamo prima che $\{0,1\}^N$ è equipotente a (0,1) e quindi ha la potenza del continuo. Infatti possiamo associare ad ogni elemento $c : N \rightarrow \{0,1\}$ 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 $c : N \rightarrow \{0,1\}$ 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.

Per provare che $P(N)$ è equipotente a $\{0,1\}^N$, consideriamo la funzione $H : P(N) \rightarrow \{0,1\}^N$ che associa ad ogni sottoinsieme X di N la sua funzione caratteristica $c_X : N \rightarrow \{0,1\}$ definita dal porre:

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

□

Proposizione 2. L'insieme N^N delle funzioni di N in N ha la potenza del continuo.

Dim. Sappiamo che $N \times N$ è numerabile e quindi che $P(N \times N)$ ha la potenza del continuo. D'altra parte $N^N \subseteq P(N \times N)$ in quanto 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.

Ora tutti gli insiemi di cui abbiamo parlato fino ad ora sono del tipo "lineare" ed abbiamo visto che tutti hanno la potenza del continuo. Allora nella nostra ricerca di insiemi più grandi appare naturale rivolgerci ad insiemi di dimensione maggiore, ad esempio ai quadrati. Ebbene, una scoperta sconcertante dei matematici contemporanei a Cantor fu che anche l'insieme dei punti interni ad un quadrato ha la potenza del continuo !

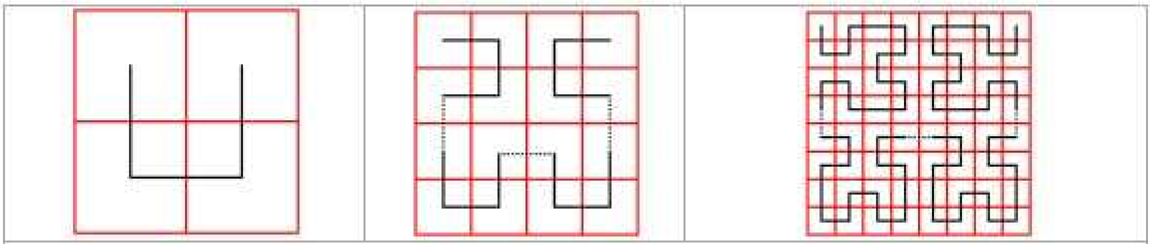
Teorema 3. L'insieme dei punti interni ad un quadrato è equipotente all'insieme dei punti interni ad un suo lato. Pertanto tale insieme ha la potenza del continuo.

Dim. In termini analitici 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. D'altra parte la corrispondenza che associa ad ogni $x\in(0,1)$ la coppia $(x,1/2)$ è una funzione iniettiva di $(0,1)$ in $(0,1)^2$ e quindi la potenza di $(0,1)$ è minore di quella di $(0,1)^2$. Pertanto per il teorema di Cantor-Bernstein possiamo concludere che $(0,1)$ è equipotente a $(0,1)^2$. □

Nota. 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.... e 0.9999... ma tale coppia non rappresenta un punto interno al quadrato).

Questo risultato ai tempi di Cantor appariva stupefacente perché stabiliva l'uguaglianza delle grandezze di due enti geometrici di differente dimensione. Un modo diverso per convincersi della possibilità di mettere in corrispondenza i punti di una retta ed i punti interni ad un 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

La curva di Peano è una funzione continua di $(0,1)$ in $(0,1)^2$. D'altra parte, stante la diversa dimensione di $(0,1)$ e $(0,1)^2$ non esiste nessuna funzione bicontinua (continua, invertibile e tale che la sua inversa sia continua) tra $(0,1)$ e $(0,1)^2$.

Problema. Dimostrare che un cubo nello spazio ha la potenza del continuo.

Teorema 4. L'insieme dei punti del piano ha la potenza del continuo. L'insieme dei punti dello spazio ha la potenza del continuo.

Dim. Poiché R è equipotente a $(0,1)$, $R\times R$ è equipotente a $(0,1)\times(0,1)$. D'altra parte abbiamo già dimostrato che tale insieme è equipotente a $(0,1)$ e quindi ha la potenza del continuo.
In modo analogo si dimostra che l'insieme dei punti dello spazio ha la potenza del continuo.

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 ?

Esercizio. Dimostrare che due circonferenze sono equipotenti (Una dimostrazione analitica si ottiene col considerare le equazioni parametriche. 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).

Proposizione 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.

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

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

Ancora una volta sembra difficile trovare qualche cosa di più grande del continuo. Il seguente teorema, dovuto a Cantor, mostra che:

<u>dato un insieme *S* esiste sempre un insieme più grande di *S*.</u>

Teorema 6. (Teorema di Cantor) Dato un insieme S, risulta che $P(S)$ ha potenza strettamente maggiore di quella di S. In particolare, $P(R)$ ha potenza strettamente maggiore di R.

Dim. Supponiamo per assurdo che esista una funzione biettiva f di S in $P(S)$ e consideriamo l'insieme $T = \{x\in S \mid x\notin f(x)\}$. Siccome f è suriettiva esisterà $x_o\in S$ tale che $f(x_o) = T$. Allora:
- se $x_o \in T$ avremo x_o verifica la proprietà caratteristica di T e quindi $x_o\notin f(x_o)$ e pertanto $x_o\notin T$
- se $x_o\notin T$ allora x_o non verifica la proprietà caratteristica di T e quindi $x_o\in f(x_o)$ e $x_o\in T$.
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. □

In definitiva se indichiamo con n un insieme finito con un numero n di elementi, abbiamo visto che esiste una successione
1, 2, 3, 4, 5, ...N, $P(N)$, $P(P(N))$, . . .
di insiemi che è crescente rispetto alla relazione di "avere potenza minore di".

9. Numeri che non possono essere definiti e funzioni che non possono essere computate

Una semplice ma sorprendente conseguenza del fatto che R non è numerabile è il seguente teorema.

Teorema 1. Comunque si fissi un linguaggio, esisteranno sempre infiniti numeri reali che non possono essere in nessun modo descritti in tale linguaggio. Precisamente l'insieme dei numeri reali che non sono descrivibili ha potenza maggiore del numerabile.

Dim. Basta osservare che se si fissa un alfabeto finito allora l'insieme D dei numeri reali descrivibili con parole in tale alfabeto ha la potenza del numerabile. Se l'insieme *Ind* dei numeri indescrivibili avesse la potenza del numerabile allora $R = D\cup Ind$ sarebbe numerabile mentre sappiamo che non lo è.

Un discorso simile può essere fatto per i numeri trascendenti dove chiamiamo *trascendente* un numero reale che non sia algebrico.

Teorema 2. Esistono infiniti numeri trascendenti. Infatti l'insieme dei numeri trascendenti ha la potenza maggiore del numerabile.

Dim. Abbiamo già provato che l'insieme *Al* dei numeri algebrici è numerabile. Se indichiamo con *Trasc* l'insieme dei numeri trascendenti, allora $R = Al\cup Trasc$. Pertanto se

Trasc fosse numerabile avremmo che R avrebbe la potenza del numerabile in contrasto con quanto provato nel paragrafo precedente.

Possiamo provare anche la seguente sorprendente conseguenza in ambito informatico dei teoremi ora dimostrati.

Teorema 3. Esistono sottoinsiemi X di N talmente complicati che nessun computer potrà mai essere programmato in modo da dirci, dato un intero n, se n appartiene ad X oppure no (insiemi indecidibili). Esistono funzioni f di N in N talmente complicate che nessun computer sarà mai in grado di computarle (funzioni non computabili).

Dim. Chiamiamo *decidibile* un sottoinsieme X di N per il quale esista un programma, scritto in un qualunque linguaggio di programmazione prefissato, in grado di dirci se n appartiene ad X oppure no. Ad esempio tutti gli insiemi finiti sono decidibili. L’insieme dei numeri primi è decidibile (non è difficile scrivere un programma capace di verificare se un numero è primo oppure no). Allora possiamo associare ad ogni insieme decidibile uno dei programmi che abbiamo supposto esistere (ad esempio il più corto). Ma un programma non è altro che una parola in un alfabeto finito e quindi l’insieme dei programmi è numerabile. Quindi la classe dei sottoinsiemi decidibile ha potenza uguale al numerabile. In conclusione la classe degli insiemi indecidibili ha potenza maggiore del numerabile.

Una dimostrazione analoga viene fatta per le funzioni computabili.

10. 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"*

Il modo migliore di formalizzare un tale processo di astrazione è quello di utilizzare la nozione di equipotenza nella classe di tutti gli insiemi e chiamare “numero cardinale” una classe completa di equivalenza. Tuttavia come mostreremo nel capitolo 4, <u>non è possibile riferirsi alla classe di tutti gli insiemi perché questo conduce ad una contraddizione.</u> Allora ci riferiamo ad una classe C più piccola che contenga solo tutti gli insiemi che si utilizzano usualmente in matematica ($\emptyset$, N, Z, Q, R,...). Inoltre supponiamo anche che C sia chiusa rispetto:

- al prendere un sottoinsieme
- all’unione,
- all’intersezione,
- al prodotto cartesiano
- all’operatore “insieme delle parti”
- alla operazione di X^Y di elevazione a potenza

Pertanto in C metteremo anche $R\times R$, $P(Q)$, ... In C consideriamo la relazione di preordine $\leqq$ “avere potenza minore o uguale a”. Dalla teoria generale delle relazioni di preordine sappiamo che $\leqq$ induce una relazione di equivalenza e che tale relazione coincide con l’equipotenza. Sappiamo anche che $\leqq$ induce una relazione d’ordine nel quoziente $C/\equiv$.

Definizione 1. Chiamiamo *insieme ordinato dei numeri cardinali* l’insieme ordinato $(C/\equiv, \leqq)$ e chiamiamo *numero cardinale* ogni elemento di $C/\equiv$, cioè ogni classe completa di equivalenza.

Allora un numero cardinale è una classe completa di equivalenza $[X]$. Inoltre viene posto

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

Ad esempio, l'insieme N dei numeri naturali 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. Ad esempio avremo il cardinale $[\{a\}]$, il cardinale $[\{a, b\}]$, il cardinale $[\{a,b,c\}]$, ... Naturalmente il cardinale più piccolo che possiamo trovare è $[\emptyset]$.
Un ulteriore passo è quello di introdurre opportune operazioni in $(C/\equiv, \leqq)$. Poiché vogliamo estendere le operazioni di somma e di prodotto definite in N, cerchiamo di individuare un significato insiemistico per tali operazioni.

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 la equipotenza è una relazione di congruenza rispetto a tale operazione.

Proposizione 2. Il prodotto cartesiano è una operazione in C compatibile con $\equiv$, cioè

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

Pertanto induce nel quoziente $C/\equiv$ un'operazione $\times$ che chiamiamo di *moltiplicazione di cardinali*.

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.

Proposizione 3. La moltiplicazione di cardinali è commutativa ed associativa. Se denoto con 1 il cardinale $[\{e\}]$ definito dai singoletti, allora vale l'equazione $x \cdot 1 = x$ e quindi 1 è l'elemento neutro. Se denoto con 0 il cardinale $[\emptyset]$ definito dall'insieme vuoto allora risulta che $x \cdot 0 = 0$.

Dim. Per provare che $x \cdot 1 = x$ osserviamo che se $\{e\}$ è un singoletto ed X un insieme allora $X \times \{e\}$ è equipotente ad X. Per provare che $x \cdot 0 = 0$ osserviamo che $X \times \emptyset = \emptyset$.

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

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

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 dovesse capitare che tali insiemi hanno qualche elemento in comune, dopo questo etichettamento ciò non può più avvenire.

Proposizione 5. L'operazione $\underline{\cup}$ è compatibile con $\equiv$. Pertanto induce nel quoziente $C/\equiv$ una operazione + che chiamiamo di *addizione di cardinali*

L'operazione di addizione è commutativa ed associativa. Si noti che vale l'equazione $x+0 = x$, cioè che 0 è elemento neutro rispetto a +. In definitiva, detto $\{e\}$ un qualunque singoletto, abbiamo provato che $\equiv$ è una congruenza nella struttura algebrica $(C, \times, \underline{\cup}, \emptyset, \{e\})$. E' possibile allora dare la seguente definizione.

Definizione 6. Chiamiamo *algebra dei numeri cardinali* la struttura algebrica $(C/\equiv, \times, +, 0,1)$ che si ottiene come quoziente della struttura $(C, \times, \underline{\cup}, \emptyset, \{e\})$ modulo la relazione di equipotenza.

Proposizione 7. L'algebra dei numeri cardinali $(C/\equiv, \times, +, 0,1)$ è una estensione dell'usuale algebra dei numeri naturali $(N, \times, +, 0, 1)$.

Dim. Indichiamo con F la classe di tutti i cardinali finiti e con $s : F \rightarrow F$ l'operazione ottenuta ponendo $s([X]) = s([X])+1$, cioè $[X\cup\{e\}] = s([X])$ dove x è un qualunque elemento non appartenente ad X. Allora la struttura $(F,s,0)$ è una terna di Peano in cui l'addizione e la moltiplicazione coincidono con quelle di addizione e moltiplicazione di cardinali che abbiamo ora definito.

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 $(C, \times, \underline{\cup}, \emptyset, \{e\})$ 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. 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 $P(S)$ può essere indicata con $2^{[S]}$.

In particolare la potenza del continuo può essere indicata con 2^{ω}. Il teorema di Cantor si esprime allora dicendo che:

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

11. Nuovi numeri: i numeri ordinali.
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 un ordine tra gli oggetti di un insieme. 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 basti pensare che in una lista 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.
Quando si utilizza un numero per denotare una quantità si parla di *numero cardinale* quando si utilizza per indicare una posizione all'interno di un ordinamento allora si parla di un *numero ordinale*. In italiano quando si parla di "primo", "secondo", ... in realtà si stanno utilizzando numeri ordinali.

Volendo definire una teoria degli ordinali dobbiamo ispirarci all'ordinamento dell'insieme dei numeri naturali. Abbiamo visto nel secondo capitolo che tale ordinamento è un buon ordinamento e che questo fatto permette di dimostrare il principio di induzione transfinita. Sembra allora naturale riferirsi solo agli insiemi ben ordinati. Ricordiamo la definizione di insieme ben ordinato.

Definizione 1. Una relazione di ordine $(S,\leq)$ è detta di *buon ordinamento* se ogni sottoinsieme non vuoto di S ammette minimo.

Abbiamo già osservato che l'ordine in N è un buon ordine. Per dare un esempio di relazione d'ordine che non è di buon ordine basta considerare una struttura del tipo $(P(S),\subseteq)$. Infatti vale la seguente proposizione.

Proposizione 2. Ogni insieme ben ordinato ha un elemento minimo. Inoltre ogni relazione di buon ordine è una relazione d'ordine totale.

Dim. La prima parte della proposizione è ovvia. Per provare che l'ordine è totale consideriamo due elementi x ed y. Allora poiché l'insieme $X = \{x,y\}$ per ipotesi è dotato di minimo e questo minimo o è x oppure y. Nel primo caso risulterà $x\leq y$, nel secondo caso $y\leq x$.

In generale l'elemento minimo di un insieme ben ordinato si denota con 0.

Invece l'ordine che usualmente si definisce nell'insieme Z degli interi relativi non è un buon ordine. Infatti l'insieme dei numeri negativi non ammette minimo. Per lo stesso motivo anche l'ordine definito usualmente in Q (ed in R) non è un buon ordine. Anche se ci restringiamo al solo insieme $Q^+ = \{x\in Q : x\geq 0\}$ dei numeri razionali non negativi l'ordinamento naturale non è un buon ordinamento. Infatti il sottoinsieme $\{1/n : n\in N\}$ di Q^+ non ammette minimo (pur ammettendo 0 come estremo inferiore).
Niente esclude peraltro che in Z ed in Q possano essere definiti dei buon ordinamenti. Infatti vale la seguente proposizione.

Proposizione 3. In ogni insieme numerabile è possibile definire un buon ordinamento isomorfo[10] a quello dei numeri naturali.

[10] Ricordiamo che un isomorfismo tra due strutture ordinate $(S,\leq)$ e $(S',\leq')$ è una funzione biettiva tale che $x\leq y$ se e solo se $f(x) \leq' f(y)$.

Dim. Supponiamo che X sia numerabile, allora esiste una funzione biettiva $f : N \to X$ e Z può essere visto come l'insieme degli elementi della successione $f(1)$, $f(2)$, . . . Definiamo in Z la relazione ≤' ponendo

$$f(n) \leq' f(m) \Leftrightarrow n \leq m^{11}.$$

Allora è evidente che $(X,\leq')$ è una struttura relazionale isomorfa ad $(N,\leq)$ e che f è un isomorfismo tra tali strutture. Ne segue che ≤' è una relazione di buon ordine in X.

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 in corrispondenza un buon ordinamento rappresentato 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. Infatti basta ordinare gli elementi di Z ponendo prima tutti i negativi e poi tutti i positivi al modo seguente:

$-1 <^* -2 <^* -3 <^* \ldots <^* 0 <^* 1 <^* 2 <^* 3 \ldots.$

Una tale relazione d'ordine, come vedremo, è quella dell'ordinale $\omega+\omega$. Vogliamo provare che non può esistere un isomorfismo f di N in tale ordinamento. Infatti sia $\underline{n}$ un intero tale che $f(\underline{n}) = 0$, allora poiché $\underline{n}-1<\underline{n}$ e tra $\underline{n}-1$ ed $\underline{n}$ non esistono elementi, allora $f(\underline{n}-1) < f(\underline{n})$ e tra $f(\underline{n}-1)$ ed $f(\underline{n})$ non potrebbero esistere elementi.

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

$0 < 1 < 1/2 < 2/1 < 1/3 < 3/1 < 1/4 < 4/1 < 2/3 < 3/2 < \ldots.$

Non è difficile trovare anche un buon ordinamento per Q intrecciando opportunamente razionali positivi e negativi.

Più complesso il discorso per R. Infatti la dimostrazione di esistenza di un buon ordine in R coinvolge l'assioma della scelta.

Principio di induzione transfinita. Diciamo che in un insieme ordinato $(S,\leq)$ vale il *principio di induzione transfinita* se, per ogni proprietà P definita in S, dalla asserzione

i) se P vale per ogni $x<y$ allora P vale per y

segue che

ii) P vale per ogni $x \in S$.

Con lo stesso tipo di dimostrazione che abbiamo dato per provare che una terna di Peano vale il principio di induzione transfinita, possiamo provare che:

Proposizione 4. In ogni insieme ben ordinato vale il principio di induzione transfinita.

Dim. Sia $S' = \{x \in S : x \text{ non verifica } P\}$. Allora se tale insiemi non fosse vuoto avrebbe un minimo elemento m. Allora, in quanto non appartenenti ad S', tutti gli elementi $y<x$ verificherebbero la proprietà P. Ciò, per *ii*) comporta l'assurdo per cui m verifica P.

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

[11] In altre parole, una volta fissata una strategia di enumerazione degli elementi di X diciamo che un elemento x è minore di un elemento y se in tale enumerazione in un certo senso x "viene prima" di y.

- $S \in C$
- $\leq$ è un *buon ordinamento*.

Inoltre indichiamo con $\equiv$ la relazione in C di isomorfismo tra strutture ordinate.

Definizione 5. 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 $[N]$ che viene denotato con ω. I numeri ordinali finiti sono le classi di equivalenza individuate da un *segmento* $\{0,1,2,...,n\}$ di interi.

Introduciamo ora opportune operazioni in O. Per prima cosa definiamo il prodotto di due insiemi ordinati $(S_1,\leq_1)$ e $(S_2,\leq_2)$. Si tratta di definire un ordinamento nell'insieme $S_1 \times S_2$ e per fare questo ci ispiriamo all'ordinamento 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*

Definizione 5. 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

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

Se ad esempio avessimo gli insiemi ordinati $\{0,1,2,3\}$ e $\{0,1,2\}$, allora nel prodotto cartesiano avremmo l'ordinamento seguente

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

Se rappresentiamo tali coppie in una matrice

(0,0) (0,1) (0,2)
(0,1) (1,1) (1,2)
(0,2) (2,1) (2,1)
(0,3) (3,1) (3,2)

allora l'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). Se volessimo moltiplicare $(N,\leq)$ per se stesso allora avremmo 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) . . .
. . .

allora l'ordinamento è ancora quello che si ottiene leggendo la matrice da sinistra a destra e poi dall'alto al basso[12].

Proposizione 6. Il prodotto di due insiemi ben ordinati è un insieme ben ordinato. Inoltre l'operazione $\times$ è compatibile con la relazione di isomorfismo.

Definiamo ora la somma di due insiemi ben ordinati e, come nel caso della somma di cardinali, riferiamoci alla unione. 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

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

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. Ad esempio se dovessi definire la somma di N con se stesso avrei dei problemi. 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. Ad esempio, se si osserva che {0} ed {1} sono insiemi ordinati, allora possiamo considerare $(S_1,\leq_1)\times\{0\}$ e $(S_2,\leq_2)\times\{1\}$ al posto di $(S_1,\leq_1)$ e $(S_2,\leq_2)$.

Definizione 7. Dati due insiemi ordinati $(S_0,\leq_0)$ e $(S_1,\leq_1)$, poniamo

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

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 8. La somma di due insiemi ben ordinati è un insieme ben ordinato. Inoltre l'operazione + è compatibile con la relazione di isomorfismo.

Si osservi che in maniera più sintetica potremmo porre $\leq\ = \ \leq_1\cup\leq_2\cup S_1\times S_2$.

Proposizione 9. La relazione $\equiv$ è compatibile con le operazioni +, $\times$, pertanto è una congruenza della struttura algebrica $(O, +,\times,\emptyset,e)$.

Nel seguito porremo $0 = [\emptyset]$ e $1 = [\{e\}]$ dove $\{e\}$ è un qualunque insieme con un solo elemento e.

Definizione 10. Chiamiamo *algebra dei numeri ordinali* la struttura algebrica ordinata $(O/\equiv, \times, +, 0,1)$ che si ottiene come quoziente della struttura $(O, \times, +, \emptyset,\{e\})$ modulo $\equiv$.

Proposizione 11. L'algebra dei numeri ordinali è una estensione dell'usuale algebra dei numeri naturali $(N ,\times ,+ ,0 ,1)$.

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:

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

La definizione di una relazione d'ordine nell'insieme dei numeri ordinali presenta qualche difficoltà. Infatti se ponessimo, come sembrerebbe naturale,

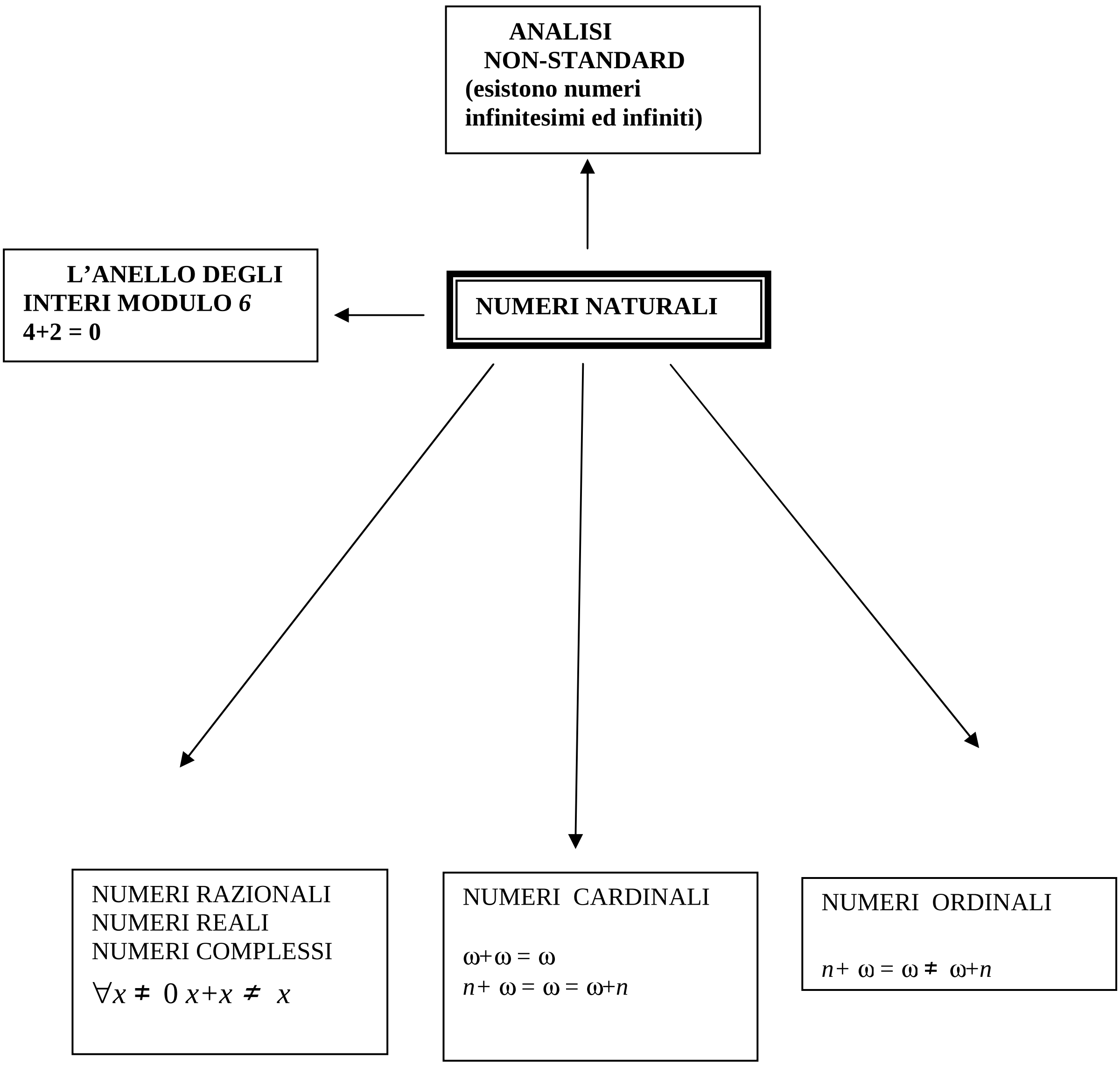
$$(S_0,\leq_0) \leq (S_1,\leq_1) \Leftrightarrow \text{esiste una immersione di } (S_0,\leq_0) \text{ in } (S_1,\leq_1),$$

allora la relazione indotta da $\leq$ nell'insieme dei numeri ordinali non sarebbe di ordinamento non verificando la proprietà asimmetrica. Infatti non vale per le strutture ordinate un analogo del teorema di Cantor-Bernstein, e può accadere che $(S_0,\leq_0)$ sia immerso in $(S_1,\leq_1)$ ed $(S_1,\leq_1)$ in $(S_0,\leq_0)$ senza che $(S_0,\leq_0)$ e $(S_1,\leq_1)$ siano isomorfi. Allora siamo costretti a dare la seguente relazione d'ordine tra insiemi ben ordinati.

Definizione 12. Indichiamo con $\leq$ la relazione binaria in O definita ponendo $(S_0,\leq_0) \leq (S_1,\leq_1)$ se $(S_0,\leq_0)$ è isomorfo ad un segmento iniziale di $(S_1,\leq_1)$ cioè se esiste $t \in S_1$ tale che $(S_0,\leq_0)$ sia isomorfo a $([0,t], \leq_1)$.

Proposizione 13. Le relazione $\leq$ è compatibile con la relazione di isomorfismo e definisce nell'insieme degli ordinali una relazione d'ordine totale.

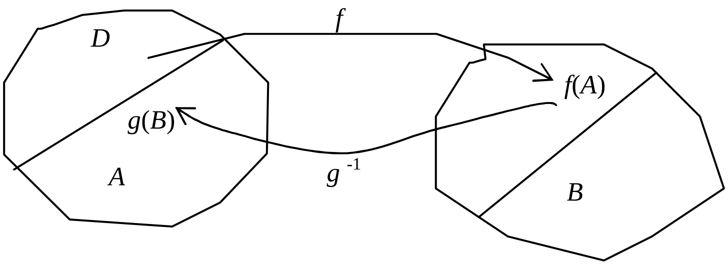
NOTA: Il punto di partenza di molte nostre costruzioni sono i numeri naturali. Naturalmente questo non è un caso poiché il processo di contare è quello più antico nella storia dell'umanità ed è presente in tutti i popoli ed in tutti i tempi. A partire dalla struttura algebrica di *N* siamo passati all'anello dei numeri relativi, poi al campo dei razionali, poi ai reali e poi ai numeri complessi. Sempre a partire dalla struttura algebrica di *N*, con l'introduzione del concetto di numero cardinale abbiamo esteso i naturali alla aritmetica dei transfiniti. Un'altra 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 non-standard in cui vengono introdotti numeri infiniti e numeri infinitesimi. Invece 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.* Possiamo rappresentare tale situazione tramite il seguente grafico:



APPENDICE
Cercare una dimostrazione del Teorema di Cantor Bernstein

Esiste una dimostrazione non troppo complicata del teorema di Cantor-Bernstein che è esposta in tutte le trattazioni elementari della teoria degli insiemi. Il limite di tali esposizioni è che non rendono l'idea di come si sia potuto pervenire ad "inventare" una tale dimostrazione. D'altra parte questo modo di procedere è presente in tutti i libri di matematica in cui, dato un teorema, ci si limita quasi sempre a riprodurre una delle dimostrazioni già note, possibilmente la più semplice e breve possibile. Insomma in generale nei testi non si considera la "dimostrazione" come qualcosa da trovare ma qualcosa già trovata da altri e da capire e ripetere.
In questa appendice tenterò invece di affrontare il teorema di Cantor Bernstein come se non ne esistesse ancora una dimostrazione e fosse nostro compito trovarla. Ricordiamo che il problema, non facile, da affrontare è il seguente:

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.



Il punto di partenza allora è che esistono due funzioni iniettive $f : A \to B$ e $g : B \to A$. Dobbiamo provare che esiste una funzione biettiva h di A in B. Se f fosse suriettiva potremmo porre semplicemente $h = f$. Se g fosse suriettiva potremmo invertire g e porre $h = g^{-1}$. In entrambi i casi il problema sarebbe risolto. Supponiamo pertanto che f e g non siano suriettive. L'idea che potremmo allora utilizzare per costruire una funzione biettiva $h : A\to B$ è quella di:

- fare operare in alcuni casi la funzione $f : A\to B$ (che è iniettiva ma non suriettiva)
- in altri casi fare operare la funzione $g^{-1} : A'\to B$, dove $A' = g(B)$, (che è suriettiva in A' 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

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

sia la funzione cercata. Si tratta ora di capire come dovrebbe essere un tale insieme perché il tutto funzioni e, naturalmente, cercare di dimostrare che tale insieme esiste.

1. Per prima cosa, perché la definizione abbia senso ogni elemento $x \notin D$ deve avere una anti-immagine $g^{-1}(x)$ e questo si ottiene solo se risulta

$$-D \subseteq g(B).$$

2. Inoltre, perché la funzione h sia iniettiva è sufficiente supporre che:

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

Infatti, essendo sia f che g^{-1} iniettive in D e $-D$, rispettivamente, la non iniettività di h si potrebbe realizzare solo se esistessero $x \in D$ ed $y \in -D$ tali che $h(x) = f(x) = g^{-1}(y) = h(y)$ e ciò comporterebbe che $h(x) \in f(D)\cap g^{-1}(-D)$.
3. Infine perché g sia suriettiva deve accadere che

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

Riassumendo, dobbiamo trovare un sottoinsieme D di A tale che:

1) $-D \subseteq g(B)$ 2) $f(D)\cap g^{-1}(-D) = \emptyset$ 3) $f(D)\cup g^{-1}(-D) = B$

cioè tale che

1. $D \supseteq -g(B)$; 2. $g^{-1}(-D) = -f(D)$

Dalla prima inclusione si ricava che $-g(B) \supseteq -D$ e quindi [13] $g(g^{-1}(-D)) = -D\cap g(B) = -D$. Pertanto, poiché dalla seconda equazione $g(g^{-1}(-D)) = g(-f(D))$ e passando al complemento, si ricava che

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

Viceversa, da (1) segue subito che $D \supseteq -g(B)$ e che $g^{-1}(-D) = g^{-1}(g(-f(D))) = -f(D)$ e quindi le due condizioni che vogliamo imporre a D equivalgono all'unica condizione (1). In definitiva, indicando con $k : P(A)\rightarrow P(A)$ la funzione definita ponendo

$$k(X) = -g(-f(X)), \tag{2}$$

dobbiamo provare che esiste un insieme D tale che

$$D = k(D).$$

Siamo allora giunti al seguente punto :

<u>la dimostrazione del teorema di Cantor-Bernstein si riconduce alla dimostrazione che l'equazione</u>

$$k(X) = X \tag{3}$$

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

Abbiamo 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. A questo punto dobbiamo andare a cercare in biblioteca se esiste qualche buon teorema di punto fisso. In Appendice vengono riportati alcuni teoremi di punto fisso. Se ci riferiamo al teorema 1 e consideriamo come reticolo completo la classe $P(A)$ dei sottoinsiemi di A, allora dobbiamo solo verificare che k è monotona. D'altra parte la cosa è ovvia perché al crescere di X:
- $f(X)$ cresce
- quindi $-f(X)$ decresce
- quindi $g(-f(X))$ decresce
- quindi $-g(-f(X))$ cresce.

In conclusione, il <u>teorema di Cantor-Bernstein è provato.</u> Inoltre se andiamo a vedere come si prova tale teorema, sappiamo anche che possiamo scegliere D uguale all'insieme $\bigcup\{X \subseteq A : X \subseteq -g(-f(X))\}$.

Per trovare in modo più "costruttivo" l'insieme D possiamo riferirci al teorema 2. In questo caso dobbiamo provare che

$$k(\cup_{n\in N} X_n) = \cup_{n\in N} k(X_n) \tag{4}$$

per ogni successione crescente $(X_n)_{n\in N}$ di sottoinsiemi di A. Ciò è vero poiché

[13] Se f è una funzione di S in T ed X è un sottoinsieme di S allora $f^{-1}(f(X)) = X$. Invece se Y un sottoinsieme di T allora $f(f^{-1}(Y))$ non coincide con Y. Infatti se y è un elemento di Y di cui non è possibile fare l'anti-immagine in quanto non appartiene ad $f(T)$, allora y "*scompare*" quando si calcola $f(f^{-1}(Y))$. In realtà vale l'equazione $f(f^{-1}(Y)) = Y\cap f(S)$.

$k(\cup_{n\in N}X_n) = -g(-f(\cup_{n\in N}X_n)) = -g(-\cup_{n\in N} f(X_n)) = -g(\cap_{n\in N} -f(X_n))$
$= -\cap_{n\in N} g(-f(X_n)) = \cup_{n\in N} -g(-f(X_n)) = \cup_{n\in N} k(X_n)$.

dove l'uguaglianza $g(\cap_{n\in N} -f(X_n)) = \cap_{n\in N} g(-f(X_n))$ è una conseguenza del fatto che g è iniettiva. In definitiva è possibile calcolare un punto fisso di k calcolando gli elementi della successione $k(\emptyset)$, $k^2(\emptyset)$, . . . , $k^n(\emptyset)$, … e poi l'unione $\cup_{n\in N} k^n(\emptyset)$. Questo significa che dobbiamo calcolare le due successioni A_0, A_1, A_2... e B_0, B_1,B_2... al modo seguente:

$A_1 = k(\emptyset) = -g(B)$; $B_1 = -f(A_1)$
$A_2 = k(k(\emptyset)) = -g(B_1)$; $B_2 = -f(A_2)$
. . . .
$A_n = k^{n+1}(\emptyset) = -g(B_n)$; $B_n = - f(A_n)$.
. . . .

e poi porre $D = \cup_{n\in N}A_n$.

Naturalmente è probabile che la strategia che abbiamo esposto in questa appendice per giungere alla dimostrazione del teorema non sia la stessa di Cantor Bernstein.

Nota: E' poi tanto ovvio che valga il teorema di Cantor-Bernstein ? Io credo di no poiché se si cambia la nozione di funzione non è detto che continui a valere. Ad esempio potremmo immaginare una comunità di matematici per cui solo le funzioni continue hanno il diritto di chiamarsi "funzioni"[14]. Per tali matematici il teorema di Cantor-Bernstein dovrebbe essere riformulato sostituendo alla nozione di equipotenza quella di *omeomorfismo* e quindi enunciata al modo seguente.

Dati due spazi topologici A e B se A è omeomorfo ad una parte di B e B è omeomorfo ad una parte di A allora A e B sono omeomorfi tra loro.

D'altra parte è facile mostrare con contro-esempi che tale teorema non vale. Ad esempio se poniamo $A = (-1,1)$ e $B = [-1,1]$ allora A è omeomorfo a se stesso e quindi ad una parte di B. Inoltre l'applicazione $f(x) = x/2$ è un omeomorfismo che porta $B = [-1,1]$ in $[-1/2,1/2]$ che è una parte propria di A. D'altra parte è evidente che A e B non sono omeomorfi.

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

[14] 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 accettate come funzioni solo quelle riconducibili a curve geometriche o algebriche. Anche attualmente esistono matematici che tendono a considerare come esistenti solo gli oggetti matematici che "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 costruttivismo in matematica. Ora risulta che tutte le definizioni proposte di funzione computabile di variabile reale verificano l'implicazione

$$\textit{computabile} \Rightarrow \textit{continua}.$$

Pertanto anche i costruttivisti accettano solo funzioni che sono continue.

LETTURE
(*Rudy Rucker – La mente e l'infinito – Editore Muzzio, pag. 85, 86.*)

L'Hotel di Hilbert

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 *Hotel 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' Hotel di Hilbert 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.

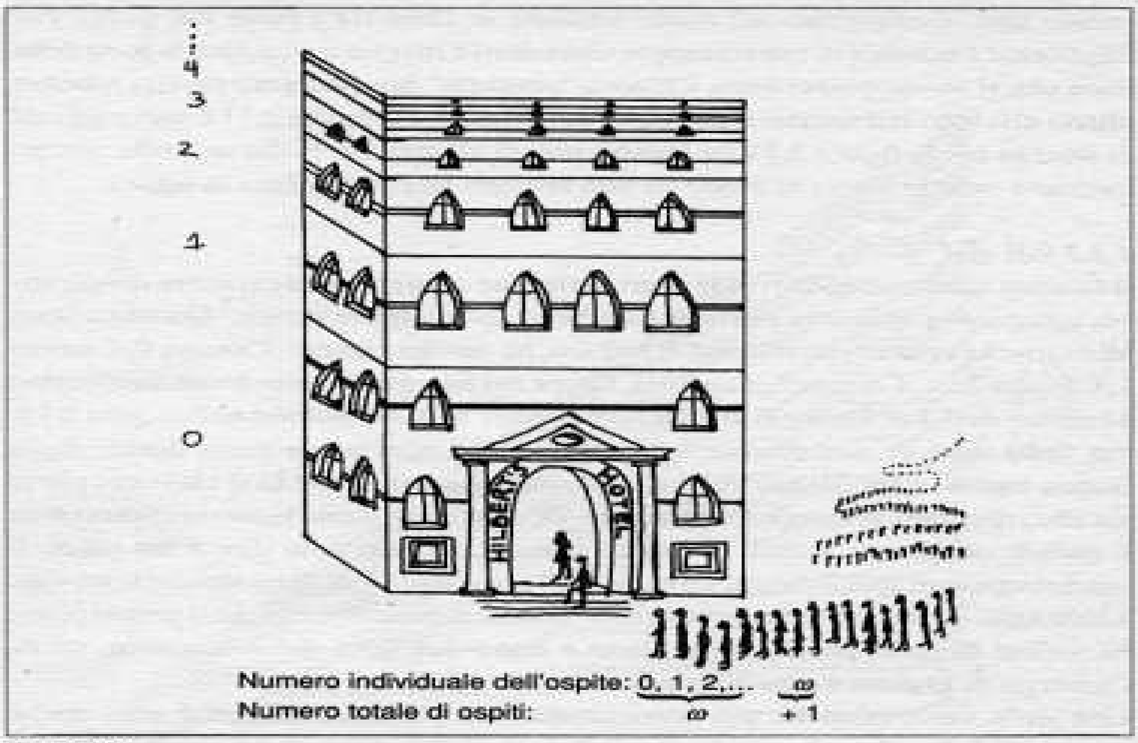


Fig. 2.13.

Una delle caratteristiche più sconcertanti dell'Hotel 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 pulmann di collocarsi in tali camere. Precisamente al prima turista che scende dal pulman si assegna la camera 1 = 2·1-1, al secondo turista la camera 3 = 2·2-1, ... al turista *n* la camera 2·*n*-1.