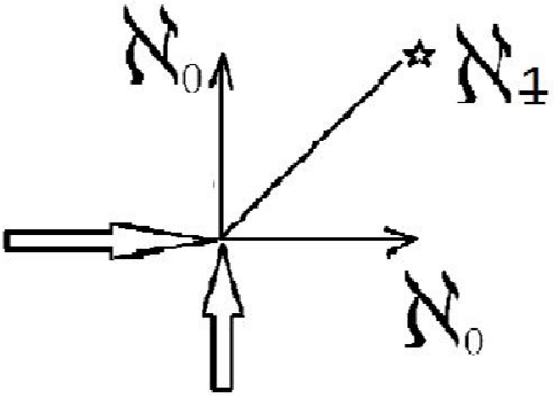
Omaggio a Umberto Cibien

(*mio amico fraterno*)
(PARTE PRIMA)

Voglio ricordarti così, come quando eravamo giovani e forti, quando le nostre menti viaggiavano alla velocità della luce su teorie delle quali solo in poche persone al mondo sono state in grado di compiere le nostre evoluzioni! Come acrobati eravamo in grado di far compiere alle nostre intelligenze dei voli sui più complicati concetti, come anime gemelle giocavamo sui campi della conoscenza! Adesso hai calcolato con estrema precisione l'integrale della gaussiana della parte concernete la tua permanenza su questo pianeta, lo hai fatto per liberarti in una geodetica esistenziale dove neanche i limiti della libertà saranno in grado di contenere il tuo spirito. Sarai sempre con me, nella mia mente e nel mio cuore. Adesso è grande il mio dolore, ma lo saprò superare! Torneremo ancora a giocare!
Ciao Umberto Cibien!



Hai scritto con lucida determinazione l'ultima equazione, lo hai fatto con un processo mentale di logica estrema, e con una facilità disarmante, applicando quanto espresso dalla "novacula Occami", facendo esattamente ciò che tutti si aspettavano che tu facessi, per dimostrare concretamente ciò che tu sapevi benissimo era assurdo fare!
Hai applicato alla lettera, nella realtà della vita quanto asserito dalla logica dialeteica del "***Paradosso del diniego***".
Hai accettato una imposizione: «Accettazione. Un soggetto dovrebbe accettare qualcosa se c'è una buona evidenza della sua verità.
Hai rifiutato al contempo l'imposizione stessa «Rifiuto(U): un soggetto dovrebbe rifiutare qualcosa se c'è una buona evidenza della sua non-verità, a meno che ci sia anche una buona evidenza della sua verità»
Hai voluto dimostrare l'incosnistenza delle verità scientifiche sbandierate dalla logica del potere.
Hai preso la locomotiva, quella che aveva costruito tuo padre, perfettamente funzionante anche se in miniatura, e la hai lanciata con con forza cieca di baleno su quel binario che ti avrebbe condotto a far superare ogni possibilità di interpretazione, sin anco all'ineffabilità di una possibile giustificazione degli eventi! E magari lo hai fatto cantando quella nostra canzone di tanti anni fa.
Io sono ancora qui, a cantare "L'avvelenata" mentre cerco di capire cosa ancora mi resta da fare!
Di sicuro, ancora una volta, mi hai fatto meditare e lo hai fatto come solo tu

sapevi fare, plasmando la realtà con la teoria, come se fosse qualcosa di modellabile, come facevi con le tue creazioni, con gli "oggetti a cui davi forma! Così sono andato a rispolverare testi antichi e testi moderni, per cercare di capire il senso della poesia racchiusa nell'esistenza e ho trovato le equazioni, quelle che ti hanno portato a questa decisione!

"Nella storia della filosofia troviamo numerose teorie secondo le quali esistono cose aldilà della nostra abilità di descrivere e concettualizzare; cose che sono ineffabili".

Tuttavia, anche solo dire che ci sono cose di questo tipo è un modo di descriverle/concettualizzarle; è un modo di parlarne. Dunque, si cade nella contraddizione.

Heidegger ritiene che l'Essere sia coinvolto negli aspetti più fondamentali della nostra vita quotidiana, tanto da affermare poeticamente che «L'essere è l'etere in cui l'uomo respira» (M. Heidegger, Schelling: Il trattato del 1809 sull'essenza della libertà umana).

L'Essere è sia interpretabile come oggettività fisica che metafisica, quindi non solo come interpretazione di "stato": il concetto di Essere (met) è semplicemente "l'essere un'entità" di un'entità.

Usando «oggetto» come sinonimo di «entità», possiamo dire che l'Essere (met) è l'oggettualità di un oggetto.

Quest'idea è stata interpretata a sua volta in due modi.

Nel primo caso, l'Essere (met) viene concepito in termini di dipendenza metafisica: gli oggetti sono oggetti a causa dell'Essere (met).

In altre parole, "l'essere un'entità" di ciascuna entità è fondato nell'Essere (met) o, in maniera equivalente, è metafisicamente dipendente dall'Essere (met) dove «**y** è fondato in **x**» – o «**x** dipende metafisicamente da **y**» – significa «**x** fa di/rende **y** un'entità».

Nel secondo caso, invece, l'Essere met viene spiegato facendo ricorso ad un'analogia con Meinong.

In particolare, Priest sostiene che, come per l'Aussersein di Meinong, l'Essere (met) di Heidegger è "l'essere un'entità" di un'entità, a prescindere dal suo statuto ontologico.

Allargando ulteriormente questa analogia, Priest sostiene che l'Essere (met) equivale all'avere Sosein, ovvero, nei termini di Meinong, a possedere delle proprietà.

Dato che qualcosa ha Essere (met) se e solo se è un oggetto e dato che, almeno nella prospettiva di Meinong, qualcosa è un oggetto se e solo se ha delle proprietà, allora qualcosa ha Essere (met) se e solo se possiede delle proprietà.

Seguendo McDaniel (2016, 2017), il senso generico in cui tutte le entità hanno Essere (met) può essere espresso da una quantificazione non ristretta, mentre uno specifico modo dell'Essere met corrisponde ad una quantificazione ristretta il cui dominio è una sottoclasse propria del dominio della quantificazione non ristretta. Inoltre, ogni quantificatore ristretto varia su tutte e sole quelle entità che condividono lo stesso modo dell'Essere (met).
Secondo Moore (2012)., la metafisica è da intendersi come il tentativo più generale di dare senso alle cose, e l'Essere (met) di Heidegger è esattamente ciò che ci permette di farlo.
Inoltre, è importante specificare che, secondo Moore, quella di "**senso**" è una nozione vaga che può stare per «il significato di qualcosa, lo scopo di qualcosa, o la spiegazione di qualcosa» (A. Moore, The Evolution of Modern Metaphysics: Making Sense of Things, Cambridge University Press, 2012, p. 5).
Infatti, quando l'Essere (met) viene inteso come intelligibilità, esso dà senso al fatto che le entità sono intelligibili.
Quando l'Essere met è inteso come l'oggettualità di un oggetto, esso dà senso al fatto che gli oggetti sono oggetti. Infine, quando l'Essere (met) è inteso come modi dell'essere, esso dà senso al fatto che le entità sono in modi differenti.
Dunque, qualsiasi cosa sia l'Essere (met) , esso non è un'entità.
Secondo questa visione, anche conosciuta come tesi della "differenza ontologica", l'Essere (met) non può essere una sedia, una stella, un numero o una qualsiasi altra entità, poiché esso è puramente trascendente: l'Essere (met) trascende il reame antico, ovvero l'insieme di tutte le entità.
Quindi "L'essere", in quanto tema fondamentale della filosofia, non è un genere dell'ente, e tuttavia riguarda ogni ente.
La sua «universalità» è da ricercarsi più in alto.
L'essere e la struttura dell'essere si trovano al di sopra di ogni ente e di ogni determinazione possibile di un ente.
L'essere è il "***Transcendens***" puro e semplice. (Heidegger, Essere e tempo, cit., p. 54).
Egli però ritiene che un'asserzione trasmetta contenuto solo quando è in grado di indicare le caratteristiche dell'entità di cui parla.
Ora, il modo con cui abbiamo a che fare con le entità quando ne parliamo tramite asserzioni è molto astratto, basti pensare ai concetti di "Entità trascendentali".
Il parlare, che è un atto intenzionale, è sempre diretto verso un'entità perché tutte le attività intenzionali sono dirette verso entità, ovvero verso gli oggetti

dell'intenzione.
L'Essere (met) non è un'entità e, siccome parlare è sempre parlare di un'entità, allora non è possibile parlare dell'Essere (met).
Tuttavia, noi ne parliamo, pertanto, l'Essere (met) deve essere un'entità.
La situazione che si ottiene è rappresentata in modo chiaro dal seguente argomento:
[1] L'Essere met non è un'entità
[2] Tutto ciò di cui parliamo è un'entità
[3] Noi parliamo dell'Essere met
[C] L'Essere met non è un'entità e l'Essere met è un'entità.
La premessa [1] corrisponde alla tesi della differenza ontologica.
La premessa [2] cattura l'idea di Heidegger secondo cui ogni volta che parliamo di qualcosa parliamo di un'entità.
La premessa [3] esprime l'evidenza fenomenologica che di fatto noi parliamo dell'Essere met .
Infine, da queste tre premesse segue correttamente che l'Essere (met) non è un'entità e che, allo stesso tempo, lo è. Questa conclusione, [**C**], può essere chiamata il "paradosso dell'Essere met ".
Non ha più senso parlare di "Essere (met)", con le accezzioni del linguaggio comune! In quanto stato temporale, Umberto è stato, Umberto è, umberto sarà!
In altre parole, la proposizione «Essere (met) » anche in questo caso è indeterminata (non ha alcuna determinazione) ed è determinata (possiede almeno una determinazione)! **Umberto è stato, è, e sarà!**
L'evento, quello che Heidegger chiama (Ereignis) e questo evento in particolare, è profondamente connesso alla questione del "**Seyn**", poiché è «la prima risposta alla domanda dell'essere»
Heidegger scrive che «***l'estrema decisione [riguarda la] verità dell'Essere*** [**Seyn**]» (Heidegger, Contributi alla filosofia, cit., §45).
Questa "***decisione cruciale"*** è esattamente quella che determina l'essere essenziale del Seyn, collegando l'evento e il Da-sein.
Ma, allora, cosa riguarda questa scelta? Tra quali opzioni l'essere umano dovrebbe decidere? L'idea più immediata è che la decisione sia tra uno dei due congiunti della conclusione contraddittoria [**C**].
Per vedere perché, ricordiamo che, secondo la conclusione [**C**], il Seyn non è un'entità (primo congiunto) ed è un'entità (secondo congiunto).
Se adottiamo ***PNC*** (Principio di Non Contraddizione), la conclusione [**C**] è inaccettabile.
Quindi, sarebbe naturale pensare che, per evitare la contraddizione, l'essere

umano debba decidere tra una della due opzioni seguenti: o il Seyn non è un'entità, o il Seyn è un'entità.
In questo caso, «**l'essenza della decisione**» è intesa come la scelta tra «l'essere oppure [in modo esclusivo] il non-essere» dello stesso Seyn (Heidegger, Contributi alla filosofia, cit., §20).
L'essenza della decisione – essere o non essere – si può determinare solo partendo dal suo presentarsi essenziale.
Decisione è decisione nell'orizzonte di un aut-aut.
Ma con ciò si anticipa il tratto che caratterizza la decisione come tale.
E' vero che niente e nessuno ci forza a compiere questa scelta.
L'essere umano, come esercizio radicale di libertà, può semplicemente decidere di non decidere.
Heidegger suggerisce che decidere di non decidere significa sostenere entrambi i congiunti contraddittori della conclusione [**C**].
In altre parole, secondo questo nuovo radicale inizio della filosofia, il Seyn diventa accessibile come risultato della decisione umana di accettare la sua natura inconsistente.
Nell'evento, ed in particolare in questo evento, il Seyn è e non è; è un'entità e non è un'entità.
Il dialeteismo è una visione certamente eterodossa ma che, se sviluppata sulla base delle risorse della **moderna logica paraconsistente**, diventa coerente e razionale, soprattutto nel caso venga applicata a situazioni come questa!
Proprio per quanto sopra esposto anche in questo caso niente è, e niente potrebbe essere, letteralmente sia vero che falso!
Popper osservò, (1969) nella propria critica alla "**logica dialettica**" di Hegel e Marx, che argomentare contro chi accetta contraddizioni è metodologicamente complicato.
Aristotele aveva sostenuto nella "**Metafisica**" che, quando qualcuno dice cose come «Per qualche **A**, **A** e **non-A** sono **entrambe vere**» (il cattivo era, in quel caso, Eraclito), dovremmo chiederci se pensa veramente ciò che dice.
Anche i seguaci contemporanei di Aristotele si chiedono se, quando dice cose simili, il dialeteista – così oggi chiamiamo chi accetta contraddizioni: cf. Berto (2007), Berto e Priest (2013) stia truccando il significato di «non», o quello di «vero»:
Quando i filosofi dibattono sul contenuto di concetti fondamentali, la discussione, com'è noto, va incontro a difficoltà metodologiche.
Possiamo approcciare la questione mediante quel che è stato chiamato il

"problema dell'esclusione" per il dialeteista.
In bocca al dialeteista, **~A** può non escludere **A**, dato che per lui sia **A** che **~A** possono esser veri.
Anche «**A è falso**» o «**A non è vero**» non sono di grande aiuto: **potrebbero non escludere che A sia vero**.
Priest ha proposto un approccio pragmatico: ***il dialeteista può escludere cose "rifiutandole".***
Io prospetto la possibilità che il dialettista sia anche in grado di accettare cose denegabili!
Prendiamo comunque il rifiuto come lo stato che un soggetto, **k**, può avere verso un enunciato – o piuttosto, verso la proposizione espressa.
Il rifiuto è l'opposto dell'accettazione o credenza (o, di un grado di credenza al di sopra di un certo valore): che **k** rifiuti qualcosa vuol dire che **k** rigetta senz'altro la credenza corrispondente.
Gli atti linguistici che manifestano accettazione e rifiuto sono, rispettivamente, l'asserzione e il diniego.
La coppia mentale e quella linguistica possono divergere in aspetti importanti, ma possiamo considerarle insieme per i nostri scopi. Prendiamo gli operatori pragmatici «$\vdash$ **k** » e «$\dashv$ **k** » («**k** accetta/asserisce (che)», «**k** rigetta/è in diniego (che)»).
Ora, il rifiuto/diniego vien spesso inteso come riducibile all'accettazione/asserzione della negazione via la cosiddetta riduzione di Frege-Geach:

(FG) $\dashv$ k A = df $\vdash$ k ~A.

FG esprime la posizione dominante sulla connessione fra accettazione/asserzione, rifiuto/diniego, e negazione:
Negare un enunciato è affermarne un altro, noto come la negazione o il contraddittorio del primo.
Dopotutto, il diniego è semplicemente la credenza nella negazione di una proposizione

Supponiamo però che A sia una dialeteia.
È un principio fondamentale della razionalità che noi si debba accettare qualcosa quando abbiamo buona evidenza che sia vero.
Allora dobbiamo accettare **~A** senza per questo rigettare **A**: se ci sono dialeteie, ***FG fallisce.***
Ciò rende difficile condurre ed esprimere le nostre discussioni su cosa si dovrebbe o non si dovrebbe escludere: rifiuto e diniego non ci consentono di

dire tutto quel che ci occorre dire.
Se il rifiuto non precludesse l'accettazione, ossia se **k** potesse accettare e rifiutare lo stesso enunciato, *simul, sub eodem*, saremmo al punto di partenza:
Si suppone, a rigor di logica, che chi rifiuta A non può accettarlo allo stesso tempo più di quanto una persona possa simultaneamente prendere e perdere un autobus, o vincere e perdere una partita a scacchi.
Un altro strumento a volte proposto come dispositivo per esprimere l'esclusione è ***arrow-falsum***, $\rightarrow \bot$, dove $\rightarrow$ è un condizionale che supporta il modus ponens e $\bot$ è o implica qualcosa di inaccettabile anche per il dialeteista.
Sia **Tr** un predicato di verità trasparente per il linguaggio in questione, ossia tale che per ogni **A**, **Tr** ⟨**A**⟩ e **A** (dove ⟨**A**⟩ è il nome di **A**) sono sostituibili in tutti i contesti (non opachi).
Secondo la teoria di Beall (2009) (chiamata **BXTT** = Teoria della verità Trasparenteed in particolare nella semantica della **logica paraconsistente**-dialeteica di base **LP**, arricchita con un $\rightarrow$ che supporta il modus ponens, possiamo prendere **Tr** come governato dalle regole di introduzione ed eliminazione:

(T-In) A ⊨ Tr ⟨A⟩

(T-Out) Tr ⟨A⟩ ⊨ A.

Ora, supponiamo che $\bot$ = **(∀)xTr(x).**
Il dialeteista potrebbe tentare di escludere A asserendo "A $\rightarrow \bot$", A va rigettato), perché l'affermazione trivialista che tutto è vero è troppo anche per lui (anche se magari non è troppo per "chiunque": il trivialismo è stato in effetti difeso, in modo interessante, in letteratura: cf. Kabay (2010)).
Per il dialeteista, essere non vero non è avere una caratteristica incompatibile con la verità.
Abbiamo la nostra vecchia contraddizione, che coinvolge la negazione.
Ma non abbiamo la corrispondente contraddizione assoluta, o istanza dell'inaccettabile **AC**, ossia **Tr** ⟨**L**⟩ **& Tr** ⟨**L**⟩ .
L'esclusione va presa come una nozione primitiva, di portata metafisica generale.
Un'ipotesi di esclusione è, semplicemente, sempre ritirata quando vien refutata.

Supponiamo che **«•»** stia per la nostra relazione di esclusione primitiva, che possiamo interpretare su coppie di caratteristiche o proprietà: «**P • Q**» va letto come «le proprietà **P** e **Q** sono incompatibili», o «Avere **P** esclude avere **Q**», o «Esser **P** esclude esser **Q**».
Per il dialeteista, in generale,

Tr ⟨~A⟩ ⊭ Tr ⟨A⟩

~Tr ⟨A⟩ ⊭ Tr ⟨A⟩ .

Ossia: falsità e non-verità non appartengono a **{P| P • Truth}**.
Questo ragionamento apre dunque le porte ad un concetto: "**il paradosso del diniego**".
Il diniego è un vero e proprio atto linguistico e il rifiuto, invece, un atteggiamento proposizionale (o stato cognitivo).
Al diniego corrisponde come atto linguistico duale quello dell'asserzione; al rifiuto corrisponde come atteggiamento proposizionale duale quello dell'accettazione (o credenza).
Ora, è ampiamente riconosciuto che questi atteggiamenti proposizionali siano strettamente collegati agli atti di diniego e asserzione, secondo questa relazione: accettazione e rifiuto sono, rispettivamente, atteggiamenti necessari agli atti di asserzione e diniego: ***si pensa che non sia possibile denegare (asserire) A senza averlo rifiutato (accettato).***
Tanto basti per la relazione tra diniego (asserzione) e rifiuto (accettazione).
Ma, chiediamoci: in che rapporto stanno questi con la negazione?
Diniego e rifiuto vengono, definiti sulla base della negazione (e dei loro duali), che viene ad assumere un ruolo prioritario rispetto ad essi.
Tale posizione, tuttavia, è stata messa in discussione.
Tra i suoi detrattori, una delle voci più importanti è quella dialeteista.
Per comprendere le ragioni dell'opposizione dialeteista alla denial equivalence bisogna partire da un'importante critica mossa al dialeteismo, che riguarda l'esclusività della negazione.
La negazione (per come viene classicamente intesa) è esclusiva nel senso che la verità di **A** esclude la verità di **¬A**, e viceversa: un enunciato e la sua negazione sono pertanto incompatibili.
Tuttavia, nella concezione dialeteista esistono contraddizioni vere: dunque, un enunciato e la sua negazione sono compatibili.
Per questa ragione, la negazione adottata dal dialeteista non è esclusiva.
Ora, però, se si ammette che l'uso della negazione logica nel linguaggio na-

turale tolleri la verità di qualche contraddizione, la stessa critica dialeteista del Principio di Non Contraddizione **(PNC)** sembra non riesca ad esprimere quel che vorrebbe.

Dal momento che l'asserzione e il diniego sono gli atti che esprimono questi atteggiamenti, ereditano anch'essi l'esclusività: ***non è possibile asserire e denegare contemporaneamente uno stesso enunciato. (ammenoché non vi sia una terza ragione occulta, un atto dimostrativo, qualcosa di controintuitivo che sfata ogni possibilità di analisi logica, ivi compresa quella dialeteica, quello che forse voleva dimostrare nei fatti Umberto!)***

Dunque, il diniego dialeteista, così come anche quello teorizzato dalla visione ortodossa, è esclusivo.
Per riassumere: secondo Priest è possibile asserire un enunciato e la sua negazione, ma non è possibile asserire e denegare lo stesso enunciato.
Un esempio grafico forse rende meglio l'idea:

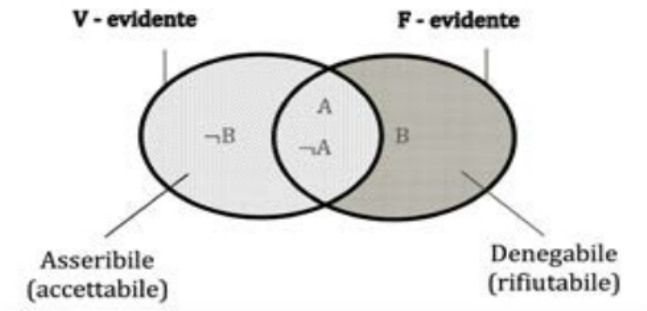


Fig. 1: rappresentazione della posizione di Priest.
Secondo il dialeteismo, ci sono enunciati che sono sia veri che falsi.
Dunque, ci sono enunciati, ad esempio A, che sono sia V-evidenti (vi è un'evidenza a favore della loro verità) che
F-evidenti (vi è un'evidenza a favore della loro falsità).
Tali enunciati — i.e. dialeteie — sono asseribili, ma non denegabili, e lo stesso vale per quegli enunciati che sono solo
V-evidenti, ad esempio ¬B. Invece, gli enunciati che sono denegabili sono quelli solo F-evidenti, come B.

A titolo esemplificativo, si può rifiutare/denegare enunciati come «Il trivialismo è una tesi filosofica corretta» o «Necessariamente, la consistenza è una proprietà desiderabile per ogni teoria logica», mentre si possono accettare-asserire enunciati come «L'enunciato del mentitore è vero», «L'enunciato del mentitore è falso» e «Ogni contraddizione è falsa».
Si può dunque esprimere un enunciato: il diniego di **A** esprime il fatto che **A** è assunto come solo falso, mentre il diniego di ¬**A** esprime che **A** è assunto come solo vero.
Questo uso del diniego suggerisce una teoria della deduzione naturale in cui venga incorporata l'esclusività negli atti linguistici dell'assumere e del concludere, in modo che risulti estranea al significato del connettivo logico della negazione.
Questi atti possono essere intesi in un duplice modo: quello ordinario e quello esclusivo. Assumere un enunciato in un modo ordinario corrisponde a supporlo almeno vero, mentre assumerlo in modo esclusivo corrisponde a ritenerlo solo vero.
Similmente, provare un enunciato in modo ordinario significa provare che è (sotto certe assunzioni) almeno vero, mentre provarlo in modo esclusivo significa provare che è solo vero.
Ne segue che le prove di **A** e ¬**A** in modo esclusivo sono incompatibili, nel senso che, in principio, conducono inevitabilmente alla refutazione di qualche assunzione da cui dipendono.
Il dialeteista ritiene esista almeno una coppia di enunciati **A** e ¬**A** entrambi asseribili, **A** risulta contemporaneamente asseribile e denegabile.
Dunque, il dialeteista che intenda fare ricorso alla nozione esclusiva di diniego non può definirla in funzione della negazione, e deve assumerla come primitiva, sostenendo come questi concetti — i.e. negazione e diniego — siano indipendenti.
In sintesi, un enunciato **A** è (almeno) vero se $\mathbf{1} \in \mathbf{v(A)}$, è (almeno) falso se $\mathbf{0} \in \mathbf{v(A)}$; **A** è solo vero se $\mathbf{0} \notin \mathbf{v(A)}$, è solo falso se $\mathbf{1} \notin \mathbf{v(A)}$.
Questa semantica viene successivamente estesa in modo analogo alla semantica di **FOL** = (First Order Logic).
Per semplicità, assumiamo che in **L** ci sia un nome per ogni oggetto del dominio di quantificazione, **D**.
La funzione di valutazione **v** assegna a ogni costante individuale un membro di D e a ogni predicato unario P due sottoinsiemi di **D:** l'estensione $\mathbf{P+}$ e l'anti-estensione $\mathbf{P-}$. $\mathbf{P+}$ e $\mathbf{P-}$ possono avere intersezione non-vuota
e sono tali che $\mathbf{P+} \cup \mathbf{P-} = \mathbf{D}$. Allora:
$\mathbf{v(Pa)} = \mathbf{\{1\}}$ **se a** $\in \mathbf{P+} - \mathbf{P-}$

v(Pa) = {0} se a $\in$ P – – P +
v(Pa) = {0,1} se a $\in$ P + $\cap$ P –

Per i predicati con arietà >1 l'estensione è simile. Per l'identità abbiamo:
(=) + = {(a,a): a $\in$ D}
mentre **(=) –** è arbitrario, col solo vincolo che **(=) +** $\cup$ **(=) + = D.**
Le clausole per i quantificatori universale ed esistenziale sono analoghe, rispettivamente, a quelle della congiunzione e della disgiunzione.
Infine, estendiamo la semantica di **LP** introducendo una nuova nozione di modello e, con essa, la relazione di conseguenza semantica.
Sia **S** un insieme di formule di **L**, alcune delle quali stellate (i.e. segnate dalla stella $*$).
Un modello **M** di **S** è una interpretazione in **LP** in cui tutte le formule di **S** sono vere e quelle stellate sono solo vere.
Una formula **A** (una formula stellata **A** $*$) è conseguenza semantica di un insieme **S** di formule potenzialmente stellate, in simboli **S $\models$ A($*$)**, se è vera (solo vera) in ogni modello di **S**.
Siano **A, B, C**, … formule del linguaggio **L**, e sia **Γ** un insieme finito di formule potenzialmente stellate.
Un **sequente** è un'espressione che possiede la forma seguente:

Γ $\vdash$ C($*$)
Da leggersi: «Dalle assunzioni in **Γ** si inferisce la conclusione **C** (in modo ordinario o esclusivo)».
Le formule non stellate appartenenti a **Γ** sono assunte in modo ordinario (sono assunte come almeno vere), mentre quelle stellate sono assunte in modo esclusivo (sono assunte come solo vere).
In modo analogo, anche la conclusione **C** può essere derivata in modo ordinario o esclusivo.

Si r*imanda l'approfondimento alle regole d'inferenza fondamentali di DLEAC (Logica Dialeteista con Assunzioni e Conclusioni Esclusive).*

Il diniego dialeteista di **A** è più forte dell'asserzione di ¬**A**: denegare A non corrisponde ad asserire ¬**A**, poiché A e ¬**A** possono essere entrambi correttamente asseribili e, volendo mantenere l'esclusività del diniego, **A** non può essere sia asserito che denegato.
Per questa ragione, come osservato in Littmann e Simmons (2004), dal momento che il dialeteista adotta una relazione non-standard tra asseribilità e

diniego, deve fornire una teoria che non solo descriva in modo soddisfacente queste nozioni, ma che sia anche capace di far fronte ad eventuali paradossi che sono generati a partire da esse.
Dalla nozione dialeteista di diniego non si possono generare paradossi semantici.
Il piano semantico va considerato come prioritario rispetto a quello pragmatico.
Più chiaramente: le nozioni pragmatiche, come gli atti di diniego e asserzione, o gli atteggiamenti proposizionali di accettazione e rifiuto, dipendono dalle (sono definiti in termini delle) nozioni semantiche di verità e falsità, ma non vale il contrario.
D'altronde, un enunciato è vero (falso) a prescindere dal fatto che sia accettabile (rifiutabile) o asseribile (denegabile), mentre che un enunciato sia accettabile (rifiutabile) e asseribile (denegabile) dipende proprio dalla (evidenza della) sua verità (falsità).
Per un dialeteista, un enunciato potrebbe essere asseribile anche nel caso ci siano evidenze della sua falsità.
Infatti, questo enunciato potrebbe essere una dialeteia, e dunque anche vero (oltre che falso).
Allora, se ci fossero evidenze anche in favore della sua verità, ovvero se ci fossero evidenze a sostegno del fatto che l'enunciato sia una dialeteia, nel quadro dialeteista l'enunciato risulterebbe asseribile.
Una dimostrazione matematica o una prova empirica rappresentino due esempi di buone evidenze per la verità (o la falsità) di un enunciato. Tuttavia, questa nozione rimane abbastanza vaga e per lo più basata su una sua comprensione intuitiva. (**Ma è quello che ha probabilmente messo in pratica Umberto!**)
Ora, una proposta piuttosto semplice e naturale è quella di definire accettazione e rifiuto nel modo seguente:
Accettare. Un soggetto dovrebbe accettare **p** se c'è un'evidenza della sua verità migliore rispetto all'evidenza della sua non-verità.
Rifiutare. Un soggetto dovrebbe rifiutare **p** se c'è un'evidenza della sua non-verità migliore rispetto all'evidenza della sua verità.
Adottando questa strategia, l'esclusività di accettazione e rifiuto dipende dalla possibilità di confrontare le evidenze e di stabilirne un ordine stretto: ovvero, che date due evidenze sia sempre possibile individuarne una migliore – di maggior valore.
A questo punto, allora, la questione si sposta sui criteri di valutazione di un'evidenza, e diventano importanti domande come: esistono tali criteri?

Ammesso che esistano, sono essi in grado di determinare la superiorità di un'evidenza rispetto ad un'altra in qualsiasi comparazione di evidenze si faccia?
Riassumendo: se si chiarisse la nozione di buona evidenza, riuscendo a fornirne una teoria che stabilisca un metodo per ordinare strettamente le evidenze in funzione del loro valore (della loro bontà), assumendo Accettare* e Rifiutare* si otterrebbe nuovamente l'esclusività delle nozioni di accettazione e rifiuto (e di asserzione e diniego), col vantaggio di non incorrere in un'asimmetria difficilmente giustificabile.
Che questo si riesca a fare, però, è molto discutibile.
Pensiamo, infatti, che per quanto sia talvolta possibile stabilire quali evidenze contano più di altre, ci siano casi vaghi (in cui il confronto non conduce a nessun esito) e casi di pareggio.
Il fatto che l'esito di questa nuova strategia sia la sospensione del giudizio può sembrare positivo per un dialeteista.
Per certi versi, la sospensione del giudizio si presenta come una reazione spontanea e pre-teoricamente attraente.
Il problema è che accettare questo approccio ha conseguenze gravi per il dialeteismo.
Infatti, simili casi di pareggio delle evidenze si hanno tipicamente proprio nelle dialeteie, che risulterebbero così non più asseribili.
Ne seguirebbe che le dialeteie, pur essendo sia vere che false, non andrebbero comunque asserite.
In questo modo uno dei tratti più tipici del dialeteismo si perderebbe.
Per ovviare a questo esito radicale, il dialeteista potrebbe proporre di emendare ulteriormente la norma che regola il rifiuto in questo modo: Rifiutare.
Un soggetto dovrebbe rifiutare **p** se c'è evidenza della sola non-verità di **p**.
La differenza con Rifiutare* è che Rifiutare chiede che vi sia evidenza che **p** sia solo non vera.
Il ché significa che l'evidenza che **p** sia non vera non sarebbe sufficiente a legittimare il rifiuto di **p**.
Affinché p sia rifiutabile, dovrebbe esserci evidenza che p sia solo non vera.
Più in generale, in un dilemma ci sono due enunciati **α** e **β**, tali che:
ø¬(α ∧ β), Oα e Oβ.
In particolare, un dilemma è detto razionale quando nella situazione appena descritta l'obbligo non è di natura etica, o di altro tipo, bensì è imposto dalla razionalità.
Ora, un punto importante da sottolineare è che «**[a]** *dilemma is not a contradiction, of the form* ***Ø*** *and* ***¬Ø***» (Priest, 2002, p. 11).

Priest fa l'esempio del paradosso dell'irrazionalità, che classifica proprio come dilemma razionale.
Sia ρ l'enunciato:(**ρ**) È irrazionale accettare **ρ**
È possibile dimostrare che **ρ** dà luogo ad un dilemma razionale.
Dimostrazione:
Sia **B** l'operatore di credenza «Credere (accettare) che» e si rappresenti «È irrazionale che» con **I**.
L'enunciato **ρ** diventa **IBρ**. Si assume lo schema:
(**P**): **IB(α ∧ IBα)** per ogni **α**.
A questo punto, si procede nel modo seguente:

$$\frac{IB\ (\rho \wedge IB\rho)}{\frac{IB\ (\rho \wedge \rho)}{\frac{IB(\rho)}{\rho}}}$$

Assumendo che **IBα ⊢ O¬Bα** e che **se ⊢ α allora ⊢ OBα**, otteniamo **O¬Bρ e OBρ**, che insieme a **O¬(Bρ ∧ ¬Bρ)** danno luogo al dilemma.

Nel caso di ρ, la razionalità richiederebbe di fare una cosa impossibile.
Nessuno (tantomeno un dialeteista) può escludere a priori l'esistenza di tali dilemmi:
Chiediamoci: il paradosso del diniego è un caso di dilemma razionale?
L'enunciato D consente di costruire un tale dilemma.
Indichiamo con $\mathscr{A}$ l'operatore di asserzione, che sta per «**Asserire che**», e con $\mathscr{D}$ l'operatore di diniego, che sta per «**Denegare che**».
Ora, secondo la visione di Priest, l'asserzione e il diniego sono necessariamente esclusivi, ovvero **Ø** ¬($\mathscr{A}$**D** ∧ $\mathscr{D}$**D**).
Tuttavia, abbiamo dimostrato che **D** è sia asseribile che denegabile.
In quanto asseribile, la razionalità ci impone di asserire **D**, ovvero **Ø** $\mathscr{A}$**D**.
In quanto denegabile, la razionalità ci impone di denegare D, ovvero **Ø** $\mathscr{D}$**D**.
Dunque, il dilemma è servito.
Tuttavia, questo argomento e il paradosso del diniego sono due cose distinte.

Certo, si può sostenere a rigor di logica che Il paradosso del diniego non sia un dilemma: è un argomento che conduce ad una contraddizione tout court, e non un argomento che conduce a fare qualcosa di impossibile.
Dunque, mentre il dilemma razionale derivabile da **D** può essere accettato da Priest come «***fact of life***», lo stesso non può dirsi per il paradosso del diniego, che esige una risposta differente dal dialeteista: è possibile formulare dei casi paradossali che minacciano la legittimità del dialeteismo.
Rispetto a questa situazione, il dialeteista può tentare almeno due contromosse: raffinare le nozioni pragmatiche di cui fa uso, oppure ammettere l'esistenza di dilemmi razionali, mostrando che il paradosso del diniego è proprio un caso dilemmatico.
Nel primo caso, se si sceglie il raffinamento suggerito da Priest, la conseguenza è un'asimmetria delle nozioni di asserzione e diniego (di accettazione e rifiuto) che riteniamo inaccettabile sulla base della nostra pratica ordinaria della razionalità.
Se, invece, si va nella direzione di un raffinamento della nozione di buona evidenza, bisogna mostrare che sia sempre possibile ordinare strettamente le evidenze in funzione del loro valore: un'opzione difficilmente sostenibile, come mostrato dall'esempio del mentitore rinforzato.
Nel secondo caso, la nozione di dilemma razionale definita da Priest non si applica al paradosso del diniego, la cui conclusione è una contraddizione e non una richiesta di svolgere un'azione impossibile.
In conclusione, se il dialeteista vuole insistere nel difendere la sua posizione sembra sia chiamato a fornire una risposta più convincente rispetto a quelle sin qui esaminate.

L'esposizione adottata è stata presa in prestito dal testo del libro sul dialeteismo, che forse è l'unico sistema inferenziale che può essere adottato per cercare di capire le dinamiche di scelte paradossali.

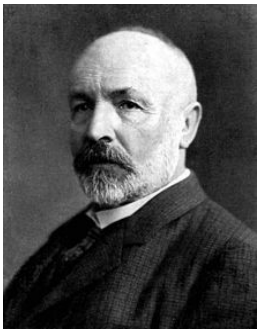
note di redazione:
Per il dialeteismo ci sono contraddizioni vere.
Questa concezione filosofica ha assunto una forma chiara e definita a partire dal lavoro del filosofo e logico Graham Priest – uno dei suoi padri fondatori, nonché uno dei suoi più strenui difensori.

Sono andato a farmi un giro sin nei meandri più nascosti dei tuoi computer, per cercare di trovare qualche piccolo gioiello da condividere con chi non ti ha conosciuto ed ho trovato dei frammenti di luce!

Gli infiniti di Cantor

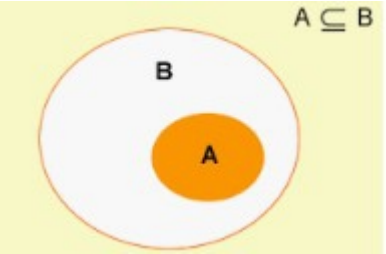
Parte prima: gli Insiemi

Già nell'antica Grecia era noto il concetto di infinito , Galileo aveva già compreso a quali paradossi può portare, ma la formulazione matematica rigorosa è dei tempi moderni (circa nel 1878) ed è dovuta a Georg Cantor.
Il grande matematico David Hilbert disse di lui:
« Nessuno riuscirà a cacciarci dal Paradiso che Cantor ha creato per noi. »
Per arrivare nel Paradiso di Cantor, dobbiamo prima introdurre due concetti fondamentali della matematica moderna; gli insiemi e le corrispondenze. In questo articolo ci occuperemo degli insiemi. Non voglio farlo in modo formale, ma intuitivo.


Georg Cantor

Tutti sappiamo intuitivamente cosa intendiamo dire per "insieme"; possiamo parlare di una collezione di oggetti di vario tipo, che possono essere lettere, numeri, parole, ecc. Basta dare una regola per determinare gli elementi di un insieme.
Ad esempio se definisco come A l'insieme delle capitali Europee, sono in grado di rappresentare A per elencazione, ovvero: A={Roma,Parigi, Berlino,Atene,…}
Gli oggetti di un insieme si dicono elementi dell'insieme.
La notazione formale per indicare l'appartenenza di un elemento a all'insieme A è $a \in A$.
L'insieme vuoto (che si indica con $\emptyset$) è un particolare insieme che si introduce così: "l'insieme che non ha nessun elemento".
Un insieme **A** è sottoinsieme di un altro insieme **B** quando tutti gli elementi di **A** appartengono anche a **B**.
Possiamo rappresentare gli insiemi con i diagrammi detti di Eulero-Venn.

Nelle figura sotto vediamo come A sia sottoinsieme di B.



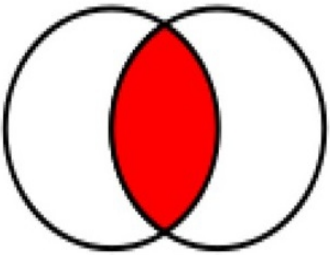
Se A è l'insieme delle capitali Europee, chiaramente A è un sottoinsieme delle città Europee B. Affermiamo poi che l'insieme vuoto è sottoinsieme di qualsiasi insieme (e lo giustifichiamo più avanti quando parleremo di unione fra insiemi). Bisogna però distinguere due casi di sottoinsiemi di un insieme B: i sottoinsiemi propri e quelli impropri. A è un sottoinsieme proprio se ci sono elementi di B che non appartengono ad A (come nell'esempio). Mentre invece A è sottoinsieme di se stesso (qualsiasi sia A), ma in tal caso è un sottoinsieme improprio.

L'inclusione propria di A in B si indica con $A \subset B$
L'inclusione impropria di A in B si indica con $A \subseteq B$

Operazioni fra insiemi.

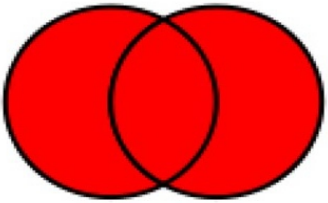
Intersezione fra insiemi:

l'insieme intersezione di A con B (che si indica con $A \cap B$) è un terzo insieme C costituito dagli elementi che sono sia in A che In B.(esempio: se A={a,b,c,d} e B={a,b,e,f} l'intersezione $A \cap B$ è l'insieme C= {a,b}. Se non hanno elementi in comune, gli insiemi si dicono disgiunti. In tal caso l'intersezione è l'insieme vuoto.



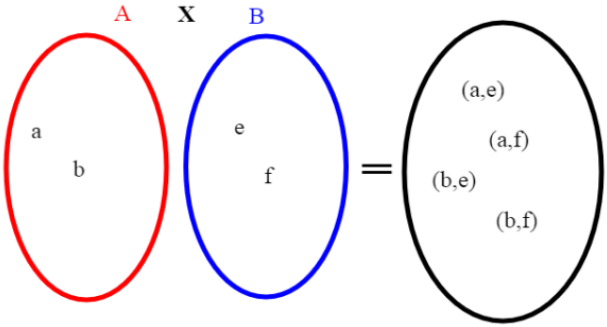
Unione di due insiemi:

l'insieme unione di A con B (che si indica con) $A \cup B$ è l'insieme formato da tutti gli elementi di A e B presi una sola volta; se A e B sono quelli dell'esempio sopra, $A \cup B$ ={a,b,c,d,e,f}.
Notiamo che $A \subset A \cup B$ qualsiasi sia A; in particolare se $A = \emptyset$ (insieme vuoto) allora $\emptyset \subset \emptyset \cup B \subset B$.



Quindi abbiamo dimostrato l'affermazione sopra, cioè che l'insieme vuoto è sottoinsieme di qualsiasi insieme.

L'insieme prodotto:
Un particolare insieme che ci servirà è l'insieme prodotto. Definiamo insieme prodotto di A con B (e lo indichiamo con A x B) l'insieme delle coppie che si ottengono prendendo un elemento da A e uno da B in tutti i modi possibili. Se A e B sono A={a,b} e B={e,f}, l'insieme prodotto è costituito dai seguenti elementi:



A x B = {(a,e),(a,f),(b,e),(b,f)}. Notiamo che se **A** ha **n** elementi e **B, m** elementi l'insieme prodotto ha **n *m** elementi.

Cardinalità di un insieme:
Fino ad ora abbiamo considerato esempi di insiemi finiti (ossia di insiemi di cui è possibile contare il numero di elementi.
La cardinalità di un insieme **A** (che si indica con **|A|**) è semplicemente il numero dei suoi elementi.

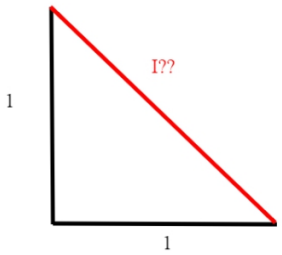
Insiemi numerici:
Particolari insiemi che i serviranno sono gli insiemi numerici, che tutti conosciamo. A parte la descrizione, vogliamo brevemente ricordare come gli insiemi numerici si siano evoluti per soddisfare delle esigenze di calcolo e di risoluzione di problemi.
L'insieme N dei numeri naturali:
(*quelli che servono per contare, e tutti conosciamo fin da bambini*)
N={0,1,2,3,4,…..}
Nell'evoluzione della matematica, ci si accorse che i numeri non servono solo per contare, ma anche per le operazioni di somma, sottrazione e divisione.

L'insieme Z dei numeri relativi:
(quelli che servono per contare, e tutti conosciamo fin da ragazzini)
Z={…,-5,-4.-3,-2,-1,0,1,2,3,4,5,…}
sono un estensione dei numeri naturali, che nasce dalla necessità di ampliare

le sottrazioni **a-b** con **b** maggiore di **a** (che non dà risultato positivo), oltre che ad esprime quantità fisiche come la temperatura o l'altitudine al di sotto di uno zero fissato.

L'insieme Q dei numeri razionali, è l'insieme di tutte le frazioni **p/q**, con **p, q** numeri relativi e $q \neq 0$.
I numeri razionali sono una estensione dei numeri relativi e servono per risolvere le equazioni del tipo **3x=2**, in quanto **2/3** non è un intero, quindi la soluzione non esiste nell'insieme dei relativi.

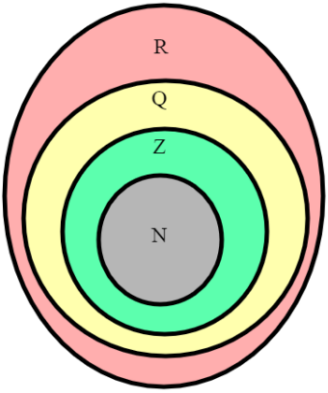
L'insieme R dei numeri Reali:
Nemmeno i numeri razionali bastano per risolvere certi problemi; $\sqrt{2}$ non è un numero razionale (che per il teorema di Pitagora non è altro che l'ipotenusa di un triangolo rettangolo di cateti **1,1**).
Infatti per il teorema di Pitagora: $\mathbf{I^2 = 1^2+1^2 = 2}$ per risolvere dobbiamo trovare il numero che elevato al quadrato dà **2**; ma questa è proprio la definizione di $\sqrt{2}$.



Radice di 2 non è un numero razionale:
Infatti se fosse un numero razionale, potremmo prendere la frazione che lo rappresenta (**p/q**) con **p** e **q** primi fra loro.
Ma se allora elevando al quadrato $\mathbf{p^2 = 2 * q^2}$ …1)
ma allora $\mathbf{p^2}$ è un numero pari; ma allora anche **p** è pari (perchè il quadrato di un numero dispari è dispari, basta fare il quadrato del binomio **2n+1** per rendersene conto), quindi posso scrivere **p=2k**; sostituendo nella 1) ottengo: $\mathbf{4 * k^2 = 2 * q^2}$; dividendo ambo i membri per 2: $\mathbf{2*k^2 = q^2}$
quindi anche **q** è pari ma questo contraddice l'affermazione che **p** e **q** siano primi fra loro.

Da qui la necessità di introdurre un nuovo insieme numerico, quello dei numeri reali, che contiene anche i numeri detti "***irrazionali***".

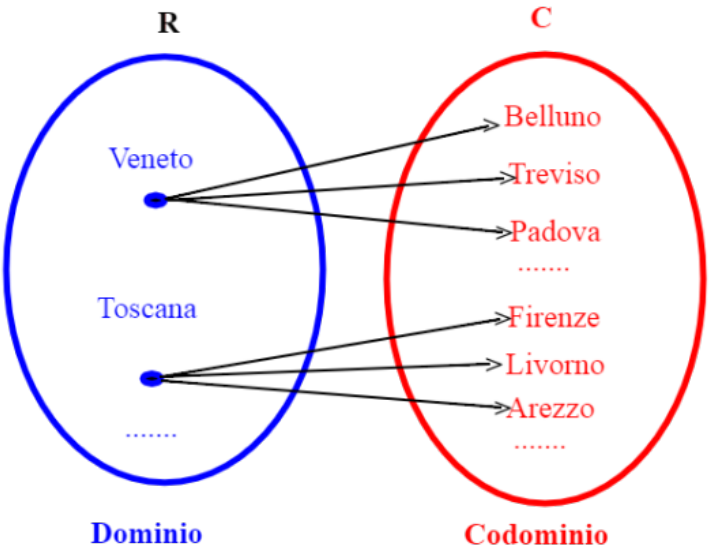
Esistono le seguenti inclusioni: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ (come è logico, essendo ciascun insieme una estensione dell'altro).



A differenza degli esempi precedenti, questi insiemi non sono finiti, ovvero non riusciamo a contare il numero degli elementi, quindi a definirne la cardinalità. Vedremo come superare questo ostacolo.
Quello che è stato trattato sugli insiemi è sufficiente per proseguire nel viaggio verso il ***Paradiso di Cantor***.

Parte seconda: corrispondenze e funzioni.

Adesso che abbiamo introdotto il concetto di insieme, vediamo come legare fra loro due insiemi. Introduciamo il concetto di corrispondenza fra due insiemi con un esempio.
Chiamo **R** l'insieme delle regioni italiane e **C** l'insieme delle città italiane.
Definisco una corrispondenza fra **R** e **C** in questo modo: associo ad ogni regione le proprie città:

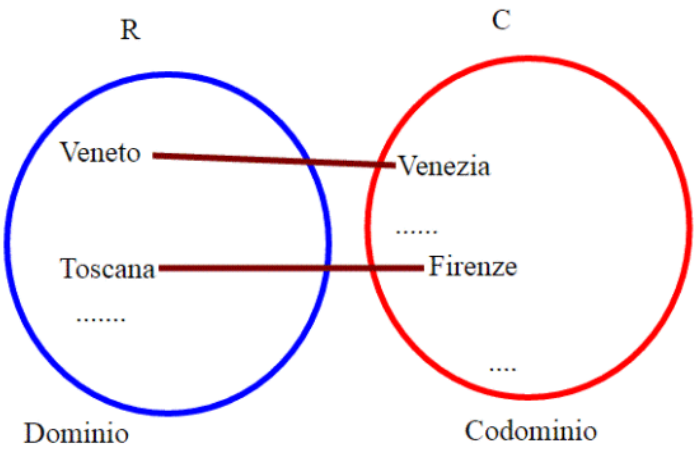


Si ha una corrispondenza quando sono assegnati un insieme di partenza, detto dominio, un insieme di arrivo, detto codominio, e un insieme di collegament (che possiamo pensare come delle frecce) che uniscono elementi del dominio con elementi del codominio.
In questo esempio abbiamo visto che ad un elemento del dominio possono anche corrispondere più elementi del codominio. Si dice anche che la corrispondenza non è univoca.

Le corrispondenze univoche, sono invece quelle corrispondenze in cui ad ogni elemento del dominio viene associato al più un elemento del codominio.
Una corrispondenza univoca è anche detta **funzione.**
Si dice funzione di **A** in **B** una corrispondenza univoca f tra gli insiemi A e B, cioè una corrispondenza che associ ad ogni elemento di **A** un solo elemento di **B**.

Le funzioni si indicano di solito in questo modo: **f: A—> B**

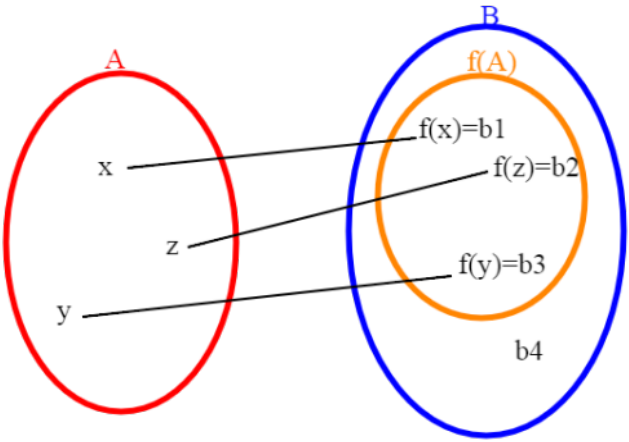
Nell'esempio precedente, se restringiamo l'insieme C delle città a quello dei capoluoghi di regione, otteniamo una corrispondenza univoca (ovvero uno funzione):



Partendo dalle corrispondenze, abbiamo ottenuto un altro oggetto matematico che è la funzione. Andiamo ad analizzare due importanti proprietà delle funzioni. In generale una funzione manda un elemento del dominio in un solo elemento del codominio.

Immagine di un elemento del dominio.

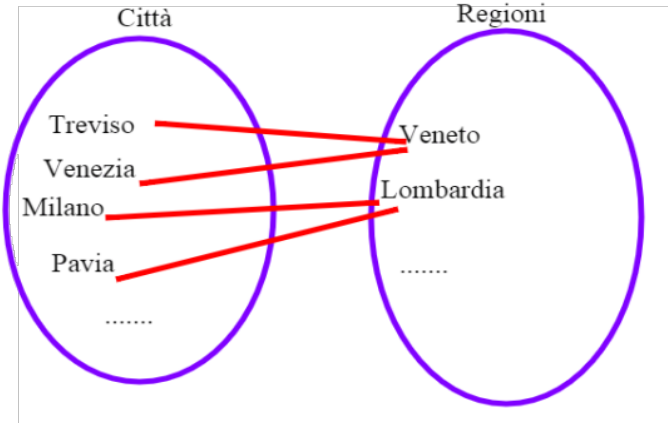
Data una funzione **f : A—> B**, chiamiamo immagine di un elemento **x** del dominio **A** l'elemento **f(x)** che appartiene al codominio **B**. Chiamiamo invece immagine di **A** e lo indichiamo con **f(A)** l'insieme costituito da tutti gli **f(x)**, con **x** che appartiene ad **A**.



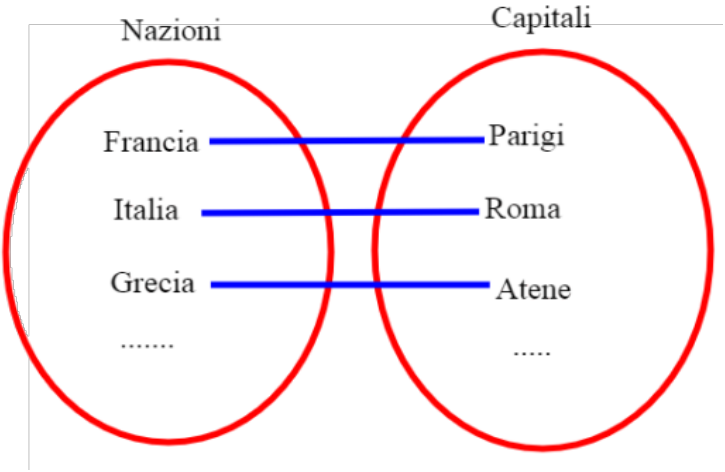
A={x,y,z} , **B={b1,b2,b3,b4}**; **f(x)=b1** (l'immagine di **x** è **b1**) **f(y)=b3** (l'immagine di **y** è **b3**) **f(z)=b2** (l'immagine di **z** è **b2**).
f(A) (immagine dell'insieme **A**) è **f(A)={f(x),f(y),f(z)}={b1,b3,b2}**

Funzione iniettiva.

Una funzione è iniettiva quando manda elementi distinti del dominio in elementi distinti del codominio.
Procediamo con degli esempi. Consideriamo le città e le regioni, ed associamo ad ogni città la propria regione.

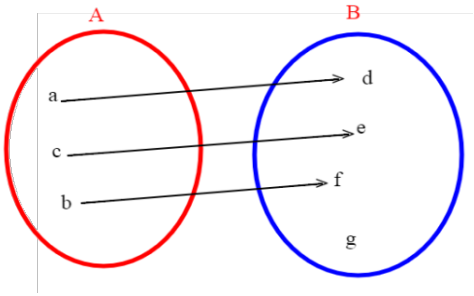


questa non è una funzione iniettiva, in quanto una regione ha più città. Mentre se associamo uno stato con la sua capitale abbiamo una funzione iniettiva, in quanto per stati diversi abbiamo capitali diverse.

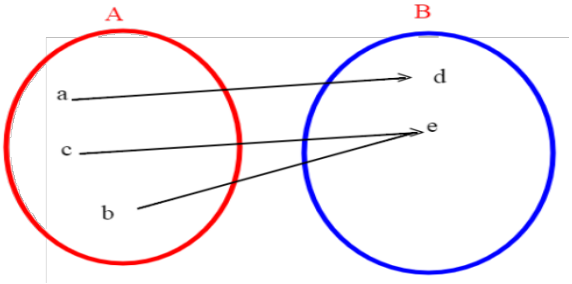


Funzione suriettiva.

Come sappiamo, per definire una funzione, a parte la legge di corrispondenza, servono due insiemi **A** e **B**, detti dominio e codominio.
La funzione **f : A–>B** si dice suriettiva se tutti gli elementi di **B** sono immagine di qualche elemento di **A**.
In parole povere **f** copre tutto **B**.
Questa non è una funzione suriettiva.



Questa sopra **NON è** una funzione suriettiva, in quanto l'elemento **g** di **B** non è immagine di alcun elemento di **A**.
Questa funzione invece è **suriettiva** in quanto copre tutto **B** (anche se non è iniettiva):



Questa invece è una funzione suriettiva.
Ricordando la definizione di immagine di un insieme tramite una funzione **f**, si può anche dire che **f** è suriettiva se **f(A)** coincide con il codominio **B**.

Funzioni biettive.

Una funzione si dice biettiva se è iniettiva e anche suriettiva: possiamo anche dire che in tal caso esiste una corrispondenza biunivoca fra dominio e codominio. L'esempio di Nazioni e Capitali è una corrispondenza biunivoca.
Una corrispondenza biunivoca è fondamentale per definire la cardinalità di un insieme (o meglio, definire quando due insiemi hanno lo stesso numero di elementi).
Infatti possiamo dire che due insiemi hanno lo stesso numero di elementi (senza preoccuparci quale sia tale numero) se possono essere messi in corrispondenza biunivoca.

Esempi di corrispondenze biunivoche con insiemi numerici.

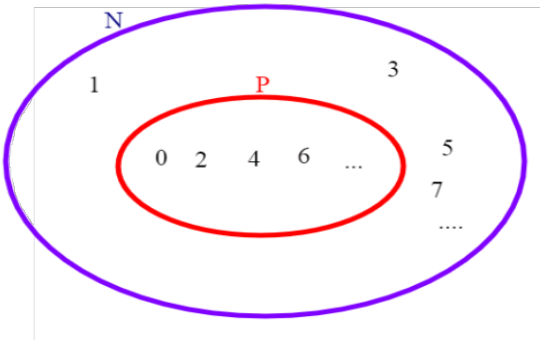
Se consideriamo l'insieme dei numeri naturali **N={0,1,2,3,4,5,….}**
e l'insieme dei numeri pari **P={0,2,4,6,8,10….}**
consideriamo la funzione **f: N—> P** così definita:
f(n)=2 n :dimostriamo che è una funzione **iniettiva**.

Infatti se $n1 \neq n2$ e moltiplico a destra e sinistra per 2 ottengo $2 \cdot n1 \neq 2 \cdot n2$ ma :
$2 \cdot n1 = f(n1), 2 \cdot n2 = f(n2)$ (sono le rispettive immagini di **n1 ,n2** quindi $f(n1) \neq f(n2)$ quindi la funzione manda elementi distinti in elementi distinti.

La funzione è anche **suriettiva**: infatti dato un qualsiasi numero pari **p**, esso è divisibile per **2**, quindi **p** si può scrivere come **p=2*n**, ma allora **p=f(n)**.

Quindi **f** è biettiva, ovvero è una corrispondenza biunivoca.

Notiamo una cosa importante; i due insiemi **N**, **P** sono degli insiemi infiniti (non riusciamo infatti a contare gli elementi dei due insiemi) e addirittura **P** è contenuto strettamente in **N** , però riusciamo a metterli in corrispondenza biunivoca.



I numeri pari sono un sottoinsieme proprio dei naturali!
Galileo aveva notato questo fatto, usando però due insiemi diversi, l'insieme dei quadrati perfetti e l'insieme **N** dei naturali:

1	2	3	4	5	6	7	8
1	4	9	16	25	36	49	64

Anche i quadrati perfetti sono ugualmente numerosi a tutti i numeri naturali, basta associarli alle loro radici quadrate.
Nei prossimi paragrafi chiariremo meglio questo fatto assai strano, che è caratteristica degli insiemi infiniti.

Parte terza: Gli insiemi numerabili.

Cardinalità di un insieme finito.

Affermiamo intanto che un insieme è finito se riusciamo a contare il numero dei suoi elementi. Tale numero è proprio la cardinalità dell'insieme.
Nell'articolo sulle corrispondenze, abbiamo visto come è possibile decidere in altro modo se due insiemi hanno lo stesso numero di elementi: basta che possano essere messi in corrispondenza biunivoca.

corrispondenza biunivoca fra nazioni e capitali
In questo esempio risulta chiaro che nazioni e capitali hanno lo stesso numero di elementi.

Cardinalità di un insieme infinito.

Nel caso di insiemi finiti, per decidere se hanno lo stesso numero di elementi ho dunque due possibilità:
1) contare il numeri rispettivi di elementi e vedere se sono uguali
2) vedere se possono essere messi in corrispondenza biunivoca.
Nel caso degli insiemi infiniti, non posso usare l'opzione 1), in quanto non

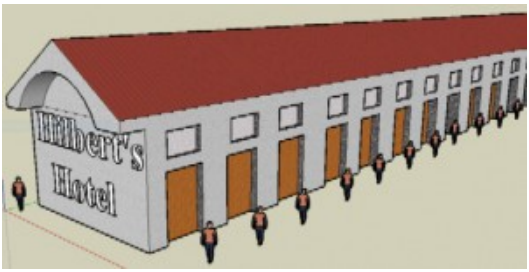
so cosa voglia dire contare gli elementi di un insieme infinito(conta e conta non finirei ma i di contare).
Nulla mi vieta di usare però la seconda opzione: (dovuta a Cantor nel 1878).

Due insiemi infiniti sono ugualmente numerosi se esiste una corrispondenza biunivoca tra di essi.

Qui però pur sapendo che due insiemi sono ugualmente numerosi, non sappiamo quale sia la cardinalità di un insieme infinito.
Possiamo provare a dare una prima risposta alla domanda di cosa sia il numero di elementi di un insieme **A**, che viene anche detto numero cardinale o cardinalità di **A**.
Esso non è altro che ciò che hanno in comune tutti gli insiemi ugualmente numerosi ad **A**, ossia che possono essere messi in corrispondenza biunivoca con **A**. Tale cardinalità si indica con **|A|**.

L'Albergo di Hilbert.

Un prima caratteristica di un insieme infinito è che è possibile aggiungere un elemento all'insieme senza modificare la sua cardinalità. Vediamolo con un esempio dovuto ad Hilbert.



L'albergo ha **infinite stanze** che sono numerate come i numeri naturali (**0,1,2,3,…**).
L'albergo è pieno, quindi i clienti sono tanti come i numeri naturali. Arriva un nuovo cliente; cosa si può fare? Si sposta ogni cliente presente nella camera successiva (quello della **0** nella **1**, quello della **1** nella **2** e così via).
Si mette il nuovo cliente nella camera **0** che si è liberata.

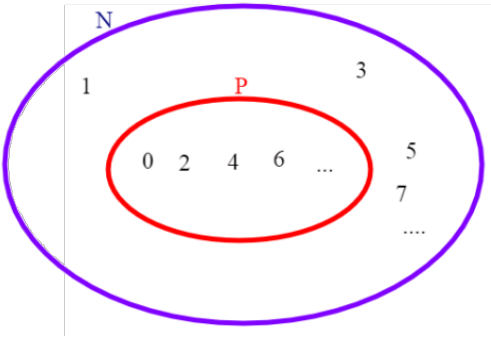
Alla fine il numero dei clienti non è cambiato anche se ne ho aggiunto uno, in quanto è sempre uguale al numero delle camere. Se le camere fossero state in numero finito, non sarebbe stato possibile effettuare questa operazione; se si riflette sul concetto di infinito come a qualcosa di dinamico, non si entra in nessuna contraddizione.

Gli insiemi numerabili

Cominciamo con degli esempi, consideriamo l'insieme dei numeri naturali **N** e l'insieme dei *Numeri Pari* **P**.
La funzione che a un numero naturale **n** associa **2n** è una corrispondenza biunivoca fra **N** e **P**.

0	1	2	3
0	1	4	6

Per ogni numero pari c'è uno e un solo numero naturale che lo genera.
Ma i numeri pari sono **strettamente** contenuti nei numeri naturali.



Gli insiemi che possono essere messi in corrispondenza con i numeri naturali si dicono anche insiemi **numerabili**.

Anche l'insieme dei numeri dispari è numerabile; basta associare ad ogni numero naturale il numero **2 n +1**.

0	1	2
1	3	5

Ma anche l'insieme dei numeri dispari è **strettamente** contenuto nei numeri naturali.
Possiamo concludere che:
La parte non sempre è minore del tutto.

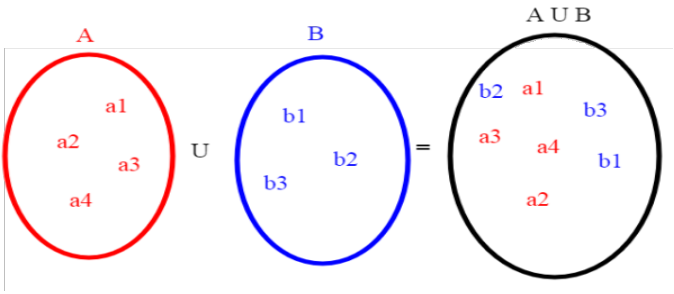
L'affermazione di Euclide "il tutto è maggiore di una qualsiasi sua parte" non è valida nel caso di insiemi infiniti.
Anzi Dedekind prende da qui la sua definizione di insieme infinito:
si dice che un insieme X è infinito se esiste una corrispondenza biunivoca tra X ed un suo sottoinsieme proprio.

La cardinalità dell'insieme unione.

Dati due insiemi **A** ,**B** sappiamo cos'è l' insieme **C** definito come unione di **A** con **B**:

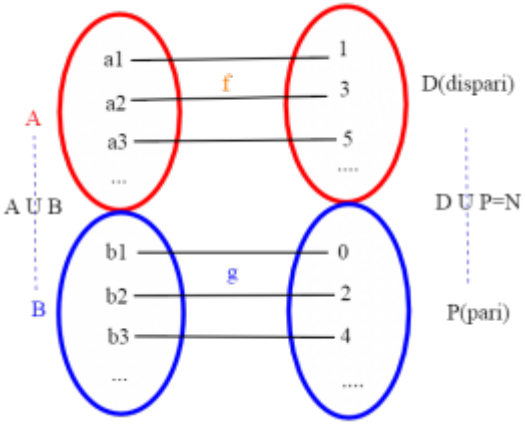
$$C = A \cup B$$

prendendo semplicemente per **C** tutti gli elementi che sono in **A** o in **B**.



Supponiamo che **A** e **B** siano numerabili e che **A** e **B** siano disgiunti ovvero senza elementi in comune.
Allora **A** può essere messo in corrispondenza biunivoca con i numeri dispari e **B** con i numeri pari, essendo entrambi numerabili.

Ma i numeri pari più i numeri dispari danno tutti i numeri naturali; In tal modo abbiamo stabilito una corrispondenza biunivoca tra l'unione di **A** e **B** e **N**; quindi **L'unione di due insiemi numerabili è numerabile.**



Vediamo di spiegare meglio questo fatto.
Se A può essere messo in corrispondenza biunivoca con **D** (numeri dispari) chiamiamo **f** tale corrispondenza (**f: A–>D**).
Allo stesso modo se **B** può essere messo in corrispondenza biunivoca con **P** (numeri pari) chiamiamo **g** tale corrispondenza (**g: B–>P**).
A e **B** sono disgiunti (questo è fondamentale).
Costruiamo un corrispondenza **e(x)** da **A U B** in **N** (pari più dispari) in tal modo:

e(x)=f(x) se x appartiene ad A
e(x)=g(x) se x appartiene a B

Essendo **f,g** biunivoche, anche **e** è biunivoca.

La cardinalità dell'insieme Z dei numeri relativi.

Perché abbiamo ricavato questo risultato? Vogliamo andare a vedere "quanti" elementi ha **Z**, insieme dei numeri relativi (che abbiamo visto nell'articolo sugli insiemi).

Pensiamo a **Z** come unione di due insiemi **A**,**B**

A={0,1,2,3,4,…} B={-1,-2,-3,-4,…}

A non è altro che **N** ;
Indichiamo con **N+={1,2,3,4,…} N** privato dello zero, che è ancora numerabile, perché se associamo a **n->n+1** abbiamo una corrispondenza biunivoca fra **N** e **N+.**
B può essere messo in corrispondenza biunivoca con **N+** con la seguente funzione: **-n** .

Allora abbiamo che **Z** è l'unione di due insiemi numerabili, quindi per quanto visto prima **Z è numerabile.**

Aleph0 ($\aleph(0)$) è il simbolo usato per indicare la cardinalità del numerabile.
Esso deriva dalla lettera dell'alfabeto ebraico ***aleph***, che è la prima lettera dell'alfabeto.
Riassumendo: se indichiamo con **|X|** la cardinalità di un insieme infinito **X**, con **P** l'insieme dei numeri pari, **D** l'insieme dei numeri dispari, abbiamo che :

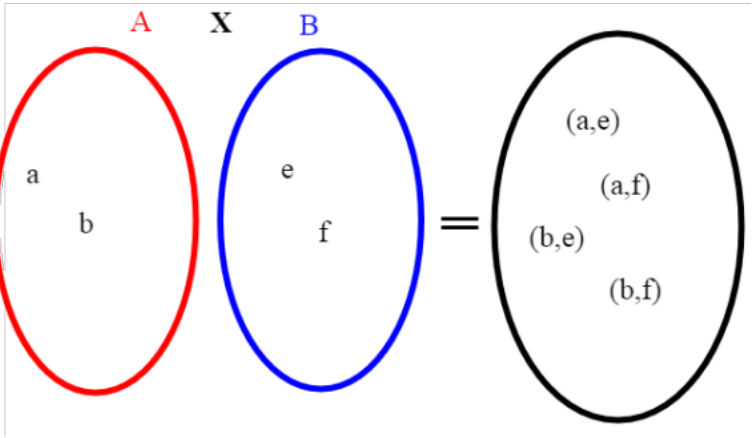
|N|= |P| =|D|=|Z|=($\aleph(0)$).

Quindi gli insiemi che abbiamo trattato finora hanno tutti lo stesso ordine di infinito.

La prossima volta ci occuperemo della cardinalità di un altro insieme numerico famoso: **Q** (***insieme dei numeri razionali***).

Parte quarta: L’albergo di Cantor.

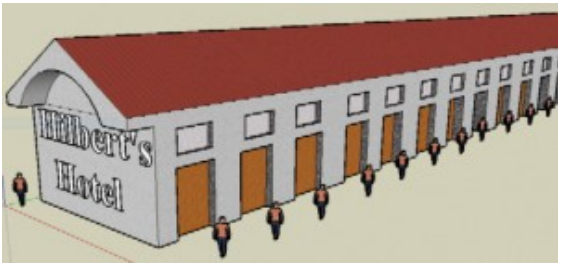
Nell’articolo sugli insiemi abbiamo visto chi è l’insieme prodotto di due insiemi **A** e **B**.
Abbiamo definito l’ insieme prodotto di **A** con **B** (e lo indichiamo con **A x B**) l’insieme delle coppie che si ottengono prendendo un elemento da **A** e uno da **B** in tutti i modi possibili.
Se **A** e **B** sono **A=(a,b,)** e **B=(e,f)**, l’insieme prodotto è costituito dai seguenti elementi:
A X B = ((a,e),(a,f),(b,e),(b,f)).
Notiamo che se **A** ha **n** elementi e **B, m** elementi l’insieme prodotto ha **n *m** elementi.



L’insieme prodotto di due insiemi in questo caso l’insieme ha **2 * 2=4** elementi
Quindi nel caso di insiemi finiti l’insieme prodotto è più numeroso dei singoli insiemi.
Ma nel caso di insiemi infiniti? Vogliamo analizzare la cardinalità dell’insieme **N x N**, ove **N** è l’insieme dei numeri naturali.

L'Albergo di Hilbert (N)

Riprendiamo un esempio che avevamo espresso nell'articolo precedente.

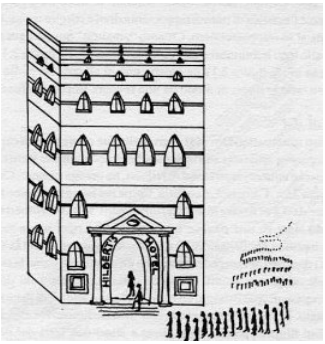


L'albergo di Hilbert

L'albergo di Hilbert ha infinite stanze che sono numerate come i numeri naturali (0,1,2,3,…). Le camere occupabili sono tante e quante i numeri naturali.

L'albergo di Cantor (N x N)

L'albergo di Cantor è molto più grande dell'albergo di Hilbert ; oltre ad avere infinite camere ha anche infiniti piani.



L'albergo di Cantor

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

La camera (**1, 2**) sarà la camera **1** del piano **2**.
Se **n, m** sono numeri naturali la camera **(n,m)** sarà la camera **n** del piano **m**.
A causa di un principio di incendio, l'albergo di Cantor deve essere evacuato.
Si pensa di traferire i clienti nell'albergo di Hilbert.

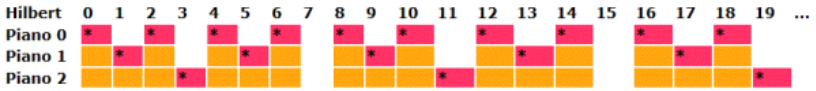
*(Se camere e piani fossero in numero finito, il problema avrebbe soluzione solo se il prodotto **piani x camere** dell'albergo di Cantor fosse minore o uguale al numero di camere dell'albergo di Hilbert.)*

Ma come è possibile? Le stanze dell'albergo di Cantor sembrano molte di più di quelle dell'albergo di Hilbert.
L'albergatore, che è lontano parente di Cantor, lo chiama e gli chiede come può fare.
Cantor gli dice di trasferire ordinatamente i clienti procedendo per piano, senza mandare tutti i clienti del piano zero dell'albergo di Cantor direttamente nell'albergo di Hilbert, altrimenti lo occuperebbero tutto .
Gli dice: manda i clienti del piano zero ad occupare una camera si e una no dell'albergo di Hilbert.
In pratica il piano zero va ad occupare le camere pari dell'albergo di Hilbert.

Passiamo al piano 1 dell'albergo di Cantor.
Ho a disposizione tutti i numeri dispari, ma occupo lo stesso una camera si e una no, per lasciare spazio ai clienti del piano 2:

e così via ; lascio sempre libera una camera si e una no:

In questo modo ogni cliente trova prima o poi la sua camera corrispondente. Da questo segue che l'albergo di Cantor ha lo stesso numero di camere di quello di Hilbert.
Ma l'albergo di Cantor non è altro che **N x N** (insieme prodotto di **N**).
Quindi **N x N** è numeroso quanto **N**.



schema riassuntivo

Ma i clienti sono un po' spaventati, c'è rischio che si comportino in modo non ordinato, andando ad occupare le camere in modo casuale.
Allora l'albergatore chiama di nuovo Cantor, e gli chiede: come posso dire al cliente della camera (**x,y**) , ad esempio camera **3** del piano **2**, che camera andrà ad occupare nell'albergo di Hilbert? Cantor gli risponde: digli che vada ad occupare la camera $2^y \cdot (2x+1)-1$
partiamo dal piano **0**. la formula diventa $2^0 \cdot (2x+1)-1 = 2x$ che sono proprio i numeri pari.

Piano 1: $2^1 \cdot (2x+1)-1 = 4x+2-1 = 4x+1$

dando ad **x** i valori **0,1,2,3,4,5..** ottengo la successione **1,5,9,13,17,21,25...**

Piano 2: $2^2 \cdot (2x+1) - 1 = 8x + 4 - 1 = 4x + 3$
dando ad x i valori 0,1,2,3,4,5.. ottengo la successione 3,11,19,27,35,43,..

Hilbert	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	...
Piano 2	*		*		*		*		*		*		*		*		*		

Grazie a questa formula possiamo dare una dimostrazione rigorosa del fatto che **N x N** è numerabile.
La funzione f: N x N–>N (x,y)—> $2^y \cdot (2x+1) - 1$ **é bunivoca.**
Possiamo limitarci a studiare la funzione $2^y \cdot (2x+1)$ (il **-1** serve solo per far saltar fuori lo 0 con **x=0**, **y=0**).

Nota: "y" è il numero di piano!

La funzione f è suriettiva.

Partiamo dall'osservazione che ogni numero naturale positivo può essere dato dal prodotto di una potenza di **2** con un numero dispari.
Infatti un numero o è pari o è dispari; se è pari possiamo senz'altro esprimerlo per una potenza di **2** moltiplicata per un numero dispari ; se è dispari (**n=2x+1**), ricordando che $2^0 = 1$, moltiplichiamo il numero stesso e per 1.
***ndr**: ricordo che si dimostra intuitivamente che 2^0 = **(**x^n / $x^m = x^{n-m}$**)**, ponendo **n**=**m**. E allora, indichiamo come **num/num=1**.*

La funzione f è iniettiva.

si vede poi subito che coppie diverse (**x,y**) danno valori diversi, quindi è iniettiva;
Quindi essendo iniettiva e suriettiva allora è **una corrispondenza biunivoca fra N x N e N.**
Quindi anche N x N è numerabile.

Parte quinta: l'induzione matematica.

(intermezzo)

Il metodo di induzione matematica si applica nel contesto dei numeri naturali e consiste nel dimostrare che se una certa proprietà vale per un certo numero naturale n_0,e supponendo che sia valida per n si dimostra che è valida per n+1 allora vale per tutti i numeri naturali $n \geq n_0$.
Definiamo formalmente Il principio di induzione:
Sia **P(n)** è una certa proprietà che dipende da **n** se:

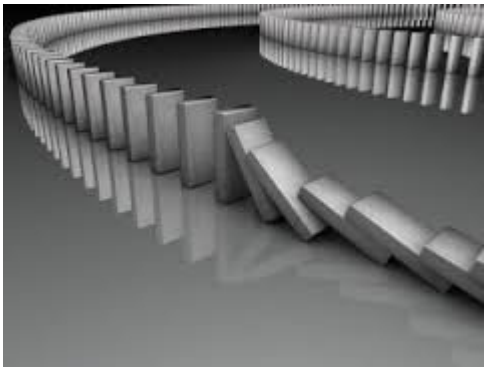
1. **P(n)** è vera per un certo numero naturale n_0 (cioè $P(n_0)$) è vera
2. Qualsiasi sia $n \geq n_0$ **P(n)** vera implica anche **P(n + 1)** vera,

allora P(n) `e vera per ogni $n \geq n_0$**.**

Il punto 1) viene detto anche base dell'induzione, il punto 2) passo induttivo.
Una giustificazione intuitiva di tale principio, può essere la seguente:
se sappiamo che **P(0)** è vera, per il passo induttivo è vera anche **P(1)**, ma allora anche **P(2)** e così via.
Dato un n qualsiasi, con un numero finito di passaggi riusciamo a dimostrare che è vera anche **P(n)** :

P(0)–>P(1)—>P(2)—> ……—> P(n).

Non possiamo dimostrare il principio di induzione; esso fa parte della teoria assiomatica dei numeri naturali del matematico Italiano ***Giuseppe Peano****.*
Notiamo però che è fortemente intuitivo, e il suo funzionamento si chiarisce meglio con degli esempi.



Metaforicamente l'induzione matematica può essere rappresentata con l'effetto domino esteso all'infinito!

1) **La somma dei primi n numeri natural**i .

Vogliamo dimostrare che:

$$S_n = 1 + 2 + 3 + 4 + ...n = \frac{n(n+1)}{2}$$

(*questa è la proprietà **P(n)** da dimostrare)* per ogni $n \geq 1$
sappiamo che per **n=1** è vera: infatti:

$S_1 = \frac{1 \cdot (1+1)}{2} = 1$ quindi il caso base **P(1)** è vero.

Passo induttivo: supponiamo

$S_n = \frac{n(n+1)}{2}$ cioè se ammettiamo che è vera **P(n)** (passo induttivo)

dobbiamo dimostrare che è vera **P(n+1)**, ovvero:

$$S_{n+1} = \frac{(n+1)(n+2)}{2}$$

(al posto di **n** devo mettere **n+1**, e al posto di **n+1, n+1+1=n+2**)
ma:

$$S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2}$$

quindi , raccogliendo (**n+1**):

$$Sn + 1 = \frac{(n+1)(n+2)}{2}$$

quindi **P(n+1)** è vera.

Ma allora è vera per ogni $n \geq 1$.

2) **Somma dei termini di una progressione geometrica.**

Vogliamo dimostrare che, per ogni $n \geq 0$

$$1 + a + a^2 + a^3 + \ldots a^n = \sum_{k=0} a^k = \frac{1 - a^{n+1}}{1 - a}$$

(ricordiamo che $a^0 = 1$)

Caso base, n=0

$$\sum_{k=0}^{0} a^k = a^0 = 1 = \frac{1 - a^1}{1 - a}$$

quindi **P(0)** è vera.

assumiamo **P(n)** vera (ipotesi induttiva):

$$\sum_{k=0}^{n+1} a^k = \sum_{k=0}^{n} a^k + a^{n+1} = \frac{1 - a^{n+1}}{1 - a} + a^{n+1} = \frac{1 - a^{n+1} + a^{n+1} - a^{n+2}}{1 - a}$$

quindi $\sum_{k=0}^{n+1} a^k = \frac{1 - a^{n+2}}{1 - a}$

cioè **P(n+1)** è vera.
Ma allora è vera per ogni $n \geq 0$

Notiamo un fatto; il principio di induzione ci permette di dimostrare in modo rigoroso la validità di una formula, ma solo l'intuito ci permette di ipotizzare il risultato.
Vorrei che qualcuno provasse a dimostrare questa formula:

$$\sum_{k=1}^{n}(2k-1) = n^2 \text{ per ogni } n \geq 1$$

Funzioni definite con il metodo di induzione:le funzioni ricorsive.
Il metodo induttivo si può applicare anche per definire una funzione sui numeri naturali dando il suo valore per 0 (o per un altro numero naturale iniziale), e fornendo la regola per passare da n ad n + 1.
Tali funzioni si chiamano ricorsive; una funzione è ricorsiva quando chiama se stessa.
L'esempio più noto è quello della funzione n! (n fattoriale) che altro non è che il prodotto dei primi n numeri interi :$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ...n$
Possiamo considerare il fattoriale come una funzione di f:N—>N che associa ad n f(n)=n!
si definisce il suo valore per 0: 0! = 1 (per convenzione)
Poi si passa a (n + 1)! =n! (n + 1)
Vediamo subito che la definizione corrisponde proprio al fattoriale.
Infatti $(n+1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \cdot (n+1)$;
ma $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$, quindi $(n+1)! = n! \cdot (n+1)$
La chiamata a n! chiede alla funzione di risolvere un calcolo più semplice di quello iniziale (il valore è più basso), ma è sempre lo stesso problema.
La funzione continua a chiamare se stessa fino a raggiungere il valore 1! (o O!) che sa risolvere immediatamente.

$$5! = 5 \cdot 4! = 20 \cdot 3! = 60 \cdot 2! = 120 \cdot 1! = 120$$

La successione di Fibonacci
l'esempio del fattoriale però non mostra completamente l'importanza delle funzioni definite per ricorrenza. Infatti possiamo calcolare il fattoriale come abbiamo sempre fatto, moltiplicando i primi n numeri interi.
Nel caso seguente invece la definizione può essere data solo in modo ricorsivo.
Ricordiamo che una successione di numeri naturali altro non è che una funzione di N–>N
La successione di Fibonacci, (che indichiamo con F: N–>N) è una succes-

sione di numeri interi positivi in cui ciascun numero è la somma dei due precedenti. Chiaramente riusciamo a fare questo se n>=3
Poniamo:

F(1)=1, F(2)=1

$F_n = F_{n-1} + F_{n-2}$ per n>=3

Per calcolare un termine della successione è necessario procedere in modo iterativo, calcolando prima i precedenti, non possiamo farlo in modo diretto. Per esempio vogliamo calcolare F(6):

F(6)=F(5) + F(4)
F(5)=F(4) +F(3)
F(4)=F(3) + F(2)
F(3)=F(2) + F(1)

quindi: F(3)=2, F(4)=2+1=3, F(5)=3+2=5, F(6)=5+3=8
I primi termini della successione di Fibonacci sono:
1,1,2,3,5,8,13,21,34,55,89,144 …

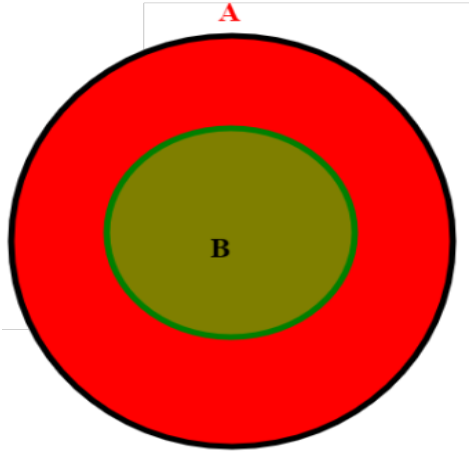
Parte sesta: Il minimo ordine di infinito.

(Aleph(0))

Abbiamo visto che un insieme numerabile contiene dei sottoinsiemi propri, che sono anch'essi numerabili.
L'esempio era stato quello dei numeri pari e dei numeri dispari, che possono essere messi in corrispondenza biunivoca con l'intero insieme **N**.
Consideriamo adesso un qualsiasi sottoinsieme proprio infinito **X** di **N**. Quale sarà sarà la sua cardinalità? Di sicuro **X** non potrà essere più numeroso di **N**, in quanto ha meno elementi (l'inclusione è propria).
Vogliamo dimostrare che la sua cardinalità è ancora **Aleph(0)**, che è la cardinalità di **N**.
Prima di iniziare devo ricordare qualche nozione sugli insiemi e su i numeri naturali.

Insieme complementare.

Dato un insieme **A** e un suo sottoinsieme **B**, definiamo insieme complementare, l'insieme costituito dagli elementi di **A** che non appartengano anche a **B**.



Nel caso evidenziato dalla figura, la parte rossa è l'insieme complementare di **B** in **A**.
Indichiamo Con **A-B** il complementare di **B** in **A**.
Notiamo che un elemento **x** o sta in **A** o sta nel complementare **A-B**.

Minimo di un insieme di numeri naturali.

Tutti sappiamo come fare il confronto fra due numeri naturali **distinti "**a" e "b" per dire chi è il più grande; risulta o a < b, oppure b> a.
Definiamo minimo di un insieme **X** il numero naturale più piccolo appartenente all'insieme, ovvero il numero **m<=x** per qualunque **x** appartenente ad **X**.
Ad esempio dato **X={5,2,3,4,7}** se indichiamo con **min(X)** il minimo di **X**; in questo caso è **2**.
Sembrerebbe così semplice stabilire il minimo di un insieme, ed è anche in-

tuitivo farlo, nell'esempio vediamo subito che **2** è più piccolo di qualsiasi altro elemento di **X**.
Ma nel caso **X** non si possa elencare così esplicitamente, oppure sia infinito? In questo caso ci soccorre il **Principio del buon ordinamento:** ogni insieme non vuoto di numeri naturali ha un elemento minimo.
Questo principio fa parte della base assiomatica data da ***Peano*** per i numeri naturali, come il principio di induzione che abbiamo trattato nell'articolo precedente; in realtà basta uno dei due principi, perché si dimostra che sono equivalenti.
Dato per vero Il principio di induzione, che abbiamo visto nell'articolo precedente, possiamo dimostrare il **principio del minimo ordinamento**, che riscriviamo :
Per qualsiasi sottoinsieme non vuoto $X \subseteq N$, esiste un elemento minimo, cioè esiste m tale che $m \leq x$, per ogni x appartenente ad X.
Sia **A** un sottoinsieme dei naturali *che non ha* un elemento minimo: mostriamo che è vuoto dimostrando per induzione che il suo complementare **N–*A*** coincide con tutto l'insieme **N** dei naturali.

Base dell'induzione.

Lo 0 appartiene a **N-A**; se così non fosse dovrebbe appartenere ad **A**, e avremmo che **A** ha un elemento minimo (infatti **0** è il più piccolo numero naturale) contro l'ipotesi.

Passo induttivo.

Supponiamo che **N-A** contenga i numeri naturali da **0** a **n**:
{**0,…,n**} $\subseteq N - A$;
ma allora **N-A** deve contenere anche **n+1**; altrimenti **n+1** dovrebbe appartenere al suo complementare **A**; quindi **A** conterebbe **n+1**, ma non **0**,**..n** che sono tutti minori di esso, quindi **A** avrebbe come minimo **n+1**, contro l'ipotesi.
Quindi {**0,…,n,n+1**} $\subseteq N - A$;
ma allora, per il principio di induzione {**0,…,n**} $\subseteq N - A$ è vera qualsiasi sia il numero naturale **n**.

Dunque N-*A* coincide con N e quindi A è vuoto.

Funzioni crescenti.

Consideriamo una funzione **f: N–>N**; diremo che tale funzione è crescente se **n<m** implica **f(n)<f(m)**.
Notiamo che **una funzione crescente è iniettiva**; infatti se supponiamo che **n<>m** allora **f(n)<>f(m)** (se **n,m** sono diversi, uno dei due è maggiore dell'altro, quindi questo vale anche per le immagini, che quindi sono diverse).

Sottoinsiemi infiniti di N.

Fra i sottoinsiemi infiniti di **N**, c'è n'è uno molto noto: l'insieme **X** dei numeri primi, **X={2,3,5,7,11,13,17,…}**.
Vogliamo dimostrare che questo insieme (come del resto ogni sottoinsieme infinito di **N**) può essere messo in corrispondenza biunivoca con **N**.
Prendiamo **X** come esempio, ma vogliamo arrivare ad una dimostrazione generica.
Come possiamo creare questa corrispondenza? L'idea è quella di enumerare gli elementi di **X** in ordine crescente:

N	0	1	2	3	4	5	6
X	2	3	5	7	11	13	17

Senza rendercene conto abbiamo costruito una corrispondenza biunivoca fra **N** e l'insieme **X**, che associa a **0–>2,1–>3, 2–>5, 3–>7, 4–>11** ecc. qualsiasi sia **n**, possiamo sempre trovare ***l'n-esimo*** numero primo, visto che i numeri primi sono infiniti.
Ma nel caso generico, come possiamo fare questa operazione? Dobbiamo ordinare l'insieme **X** in modo crescente ma dobbiamo dare una funzione, una regola, un algoritmo che ci permetta di trovare per ogni numero naturale **n** il corrispondente nell'insieme **X**.
Nell'articolo precedente, abbiamo definito le funzioni definite per ricorrenza, o ricorsive.
L'idea è quella di trovare dapprima il primo elemento dell'insieme **X**, poi di togliere tale elemento dall'insieme e trovare quindi il secondo elemento e così via.
Dato un sottoinsieme proprio infinito **X** di **N**, definiamo la seguente funzione ricorsiva **(F: N—>X)** in tal modo:

F(0)=min X

F(n+1)=min X-{F(1),F(2),F(3),…F(n)}

(togliamo ogni volta ad **X** tutti i valori calcolati precedentemente, poi facciamo il minimo.
Per quanto visto sopra sul principio del minimo ordinamento tale minimo esiste sempre, in quanto l'insieme **X** è infinito, quindi si desume che **X-{F(1),F(2),F(3),…F(n)}** non è mai vuoto.

Questa definizione può spaventare! In realtà se la illustriamo con un esempio diventa molto più comprensibile. Prendiamo come X il sottoinsieme infinito di N dei numeri primi: **X={2,3,5,7,11,13,17,..}**

F(0)=min X=2
F(1)=min{2,3,5,7,11,13,17,..}-{F(0)}=
min{3,5,7,11,13,17,..}-{2}=min{3,5,7,11,13,17,..}=3
F(2)=min{5,7,11,13,17,..}-{F(0),
F(2)}=min{2,3,5,7,11,13,17,..}-{2,3}=min{5,7,11,13,17,..}=5

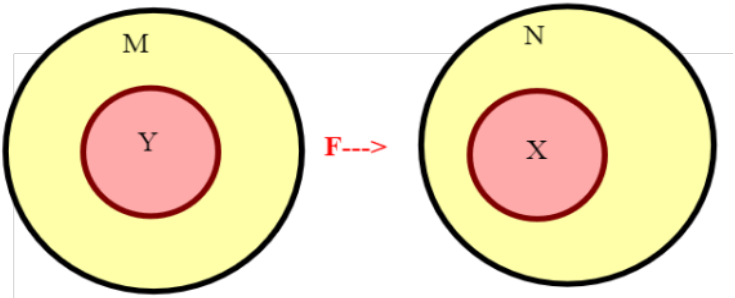
Visto in altro modo, in forma tabellare, possiamo costruire la sequenza:

n	**F(0)**	**F(1)**	**F(2)**	**F(3)**	**F(4)**
0	**2**	**3**	**5**	**7**	**11**
1		**3**	**5**	**7**	**11**
2			**5**	**7**	**11**
3				**7**	**11**
4					**11**

Osserviamo che otteniamo proprio quello che volevamo, ossia dei valori crescenti per **F(n)** cioè **F(n+1)>F(n**) ;questa è una conseguenza di come è costruita, come si vede dall'esempio *(più precisamente: parto da zero e trovo il minimo di X, al passo successivo prima tolgo il minimo a X, poi calcolo il nuovo minimo, che senz'altro è più grande del passo precedente, poi tolgo a X i due valori trovati e ricalcolo il minimo, ottengo ancora un valo-*

re più grande..e così via).
F è una funzione biunivoca di N in X; quindi X è numerabile.
(Ho messo la dimostrazione alla fine dell'articolo per non appesantire troppo l'esposizione; è abbastanza tecnica.
Comunque non è necessaria per comprendere i concetti che seguono.)

Ogni sottoinsieme infinito di un insieme numerabile è numerabile:
Per **N** lo abbiamo dimostrato; prendiamo adesso come **M** un qualsiasi insieme numerabile, e sia **Y** un suo sottoinsieme proprio infinito.
Se **M** è numerabile, esiste una funzione **F: M—> N** biunivoca.



Tale funzione manda il sottoinsieme Y di M in X=F(Y), e la funzione F ristretta ad Y è una applicazione biunivoca di Y—>X=F(Y), sottoinsieme di N; ma sappiamo che X è numerabile (è un sottoinsieme infinito di N), quindi anche Y lo è.

*(Ricordo che **F: Y–>F(Y)=X** è una funzione suriettiva, infatti copro tutto **F(Y)** per la definizione stessa di immagine)*

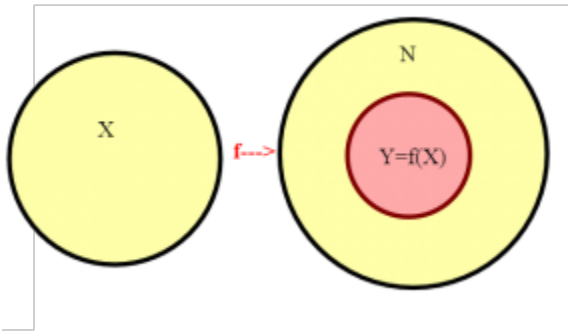
Confrontare la cardinalità di due insiemi:

Fino ad ora siamo riusciti a dire che due insiemi (infiniti) hanno la stessa cardinalità se esiste un corrispondenza biunivoca fra di essi.
Ma se ciò non si verifica? Vogliamo cioè definire quando la cardinalità di un

insieme **X** sia minore di quella di un insieme **Y**.
Diremo che **|X|<=|Y|** se esiste una funzione iniettiva **f** di **X** in **Y: f: X—>Y** (e sottolineiamo che una funzione iniettiva di **X** in **Y** è una corrispondenza biunivoca di **X** in un sottoinsieme di **Y**, che non è altro che l'immagine di **X**, **f(X))**.
Diremo invece che **|X|<|Y|** se esiste una applicazione iniettiva **f** di **X** in **Y**, ma tale applicazione non è suriettiva.
*In parole povere non copre tutti gli elementi di **Y**.*

Il minimo ordine di infinito:Aleph(0)

Esistono ordini di infinito minori di quello dei naturali? Sia **X** un insieme infinito con cardinalità **|X|<=|N|**.
Per quanto visto sopra sul confronto fra numeri cardinali, esiste una funzione iniettiva:

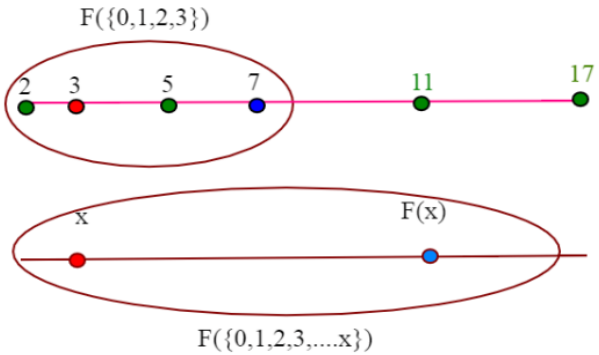


f:X–>N ; chiamiamo **Y** l'immagine di **X ,Y=f(X)**.
Ma allora la funzione **f–>Y=f(X)** è anche suriettiva, quindi è biunivoca.
Ma allora **|X|=|Y|**.
Ma **Y** è un sottoinsieme infinito di **N**, quindi è numerabile.
Ma allora **|X|=|Y|=|N|.**
Dunque **X** è numerabile, quindi **Aleph(0)** è il minimo numero cardinale.

Appendice

La funzione ricorsiva:

F(0)=min X
F(n+1)=min X-{F(1),F(2),F(3),…F(n)} dove X è un sottoinsieme infinito di N
E' una funzione biunivoca di **N—> X**
Abbiamo visto che **F è crescente, ma allora è iniettiva**, per quanto visto prima sulle funzioni crescenti.
Notiamo poi che **F(n)>=n** ; questo fatto si può dimostrare per induzione.
Infatti è vera per **0**; **F(0)=min X >=0** .
Supponiamo sia vera per **n**, dimostriamola per **n+1**.
F(n+1)>F(n); per ipotesi induttiva, **F(n)>=n**, allora **F(n+1)>F(n)>=n**, quindi **F(n+1)>n**, ma questo vuol dire **F(n+1)>=n +1**.
Quindi F(n)>=n qualsiasi sia n.
Sfruttiamo questo fatto per dimostrare che F è anche **suriettiva**.
Dato un qualsiasi **x** appartenente ad **X**, vogliamo dimostrare che **x** appartiene all'immagine di **F({0,1,…,x})**. Ma **F({0,1,…,x})={F(0),F(1),.. F(x)}**
(in pratica se prendiamo un insieme abbastanza grande, la sua immagine andrà a contenere **x**).



Ma **F** è crescente! Quindi l'immagine di **F({0,1,…,x})** è costituita dagli m appartenenti ad **X**, tali che **m<=F(x)**.
Ma sappiamo che **x<=F(x)**, quindi **x** appartiene all'immagine **F({0,1,…,x})**.

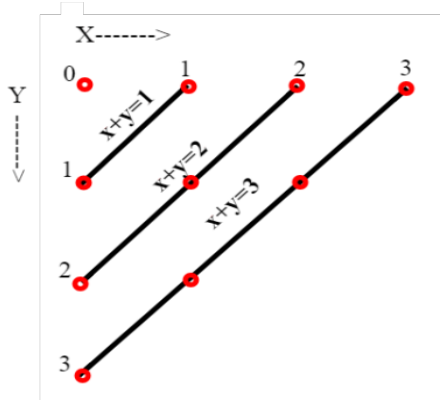
Parte settima: la cardinalitàdi Q.

(e le diagonali di Cantor)

Abbiamo già dimostrato che N x N è numerabile (nella quarta parte, l'albergo di Cantor.
Lo abbiamo fatto però in un modo un po' diverso rispetto al lavoro originale del grande matematico.
Non sarei completamente soddisfatto se non lo esponessi, per dovere soprattutto storico, anche se lo giudico abbastanza complesso.

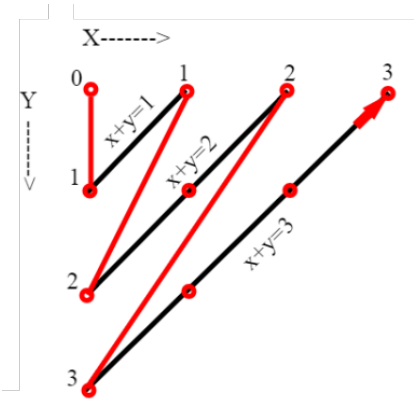
Il metodo diagonale di Cantor.

Vogliamo costruire un funzione **f: N x N —> N** che sia biunivoca.
Nell'articolo precedente abbiamo usato il principio del minimo per ordinare i sottoinsiemi infiniti di **N**.
Poi una volta ordinati è stato semplice metterli in corrispondenza biunivoca con **N**.
In **N x N** non abbiamo a disposizione un ordinamento, pertanto cerchiamo di crearne uno.
Per contare gli elementi di un insieme, è più facile metterli in ordine.
Pensate a quanto sia facile contare le tacche di separazione dei binari della ferrovia, rispetto a quanto sia difficile contare un gruppo di bambini che si muovono in continuazione; se in qualche modo non riusciamo a raggrupparli in delle file, risulta quasi impossibile.
Consideriamo le coppie (**x,y**) che hanno una somma costante uguale ad un certo numero naturale **n**, cioè **x+y=n.**

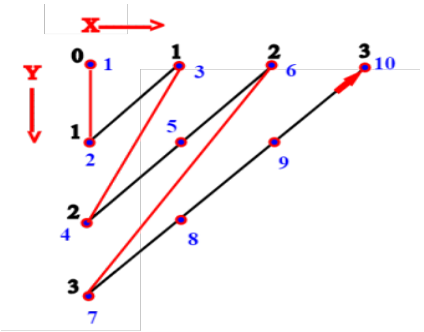


Se **n=0** ho solo la coppia (**0,0**)
Se **n=1** ho le due coppie (**0,1**) e (**1,0**)
Se **n=2** ho tre coppie (**0,2**),(**1,1**),(**2,0**)

Facendo scorrere **n** da **0** a infinito copro tutte le coppie di **N x N**; notiamo poi che all'interno del gruppo con **x+y=n**, metto prima le coppie con **x** più piccolo.
Così facendo sono anche riuscito ad ordinare le coppie.



Procedendo per valori crescenti di **x** percorro le diagonali in modo ordinato
Per ogni **n** ho dei gruppi (**x,y**) con somma uguale a **n**.
Come creare una corrispondenza biunivoca con **N**? Semplicemente contando questi punti.
Ricordiamo che contare stabilisce un applicazione biunivoca fra un insieme e **N**.
Per **n=0 (0,0)** ne ho solo uno e lo associo a **1**.
per **n=1** ne ho due (**0,1**) (**1,0**);
per **n=2** (**0,2**) (**1,0**) (**2,0**) (**n=2**) ne ho tre.
Per **n=3** (**0,3**) (**1,2**), (**2,1**) (**3,0**) ne ho quattro.
(notiamo che per ogni **n** ho **n+1** punti (**x,y)** con somma uguale ad **n**)
quindi fino alla diagonale **n=3** ne ho contati **1+2+3 +4=10**.
In pratica scorriamo diagonale per diagonale (le diagonali considerate sono quelle nere); se esauriamo completamente le diagonali fino a **n**, ho **1+2+3+4+…n** punti; ma questa formula altro non è che la somma dei primi **n** numeri interi; abbiamo visto in vari modi che tale somma è **n(n+1)/2**.



I valori della funzione sono indicati in blu e altro non sono che il conteggio degli elementi.
Questo è valido se esaurisco completamente la diagonale , corrispondente ad un certo **n**.
Ma se (**x,y**) sono generici e voglio avere il valore della funzione, ovvero del conteggio ?
Consideriamo il caso **n=3**:
ho le coppie: (**0,3**) (**1,2**), (**2,1**) (**3,0**) con **x+y=3** e **0<=x<=3**.
Supponiamo di voler vedere dove va la coppia (**1,2**).
Considero la diagonale precedente che ho esaurito, quindi sono arrivato a

contare fino a **1+2+3=4*3/2=6**.
Quindi devo sommare **2** per arrivare a (**1,2**), che occupa la seconda posizione.
Quindi **(1,2)–>8**.
Dati (**x,y**) qualsiasi (ma con il vincolo che la somma sia un certo **n**), sappiamo dunque che **x+y=n** per un certo **n**; ma allora per ottenere i valori successivi prima contiamo i precedenti **1+2+3+…n=n(n+1) /2**, poi facciamo variare la **x** da **0<=x<=n**; tenendo conto che **n=x+y e n+1=x+y+1.**

1+2+3+….n=n(n+1)/2=(x+y)(x+y+1)/2

Per contare i punti successivi basta sommare a questa somma **x +1** (naturalmente con **0<=x<=n**).
Arriviamo allora a scrivere la formula, valida per qualsiasi **x,y**:

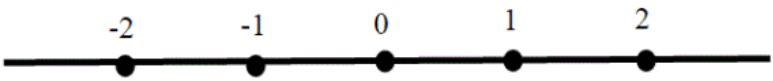
(x,y)—> (x+y) (x+y+1)/2 +x +1

Per come è costruita, la funzione è crescente, parte da **1** e incrementa di **1** ad ogni passo quindi è biunivoca fra **N x N –>N+** (copre tutti i numeri naturali maggiori di **0**).

Ma **N+** è anch'esso numerabile (basti pensare all'albero di Hilbert, o al fatto che è un sottoinsieme infinito di un insieme numerabile, quindi è numerabile), quindi **N x N** è numerabile.

Osservazioni su interi e razionali.

Disporre i numeri interi e i razionali sulla retta.



Possiamo disporre i numeri interi su una retta fissando una origine **O** e stabilendo una unità di misura (un segmento unitario, ad esempio **1 cm**), e un verso, che andrà da sinistra verso destra.
I punti corrispondenti ai numeri staranno a destra o sinistra di **O** a seconda

che siano positivi o negativi, e la loro distanza dall'origine sarà un multiplo fra il numero e l'unità di misura fissata.
Otteniamo in questo modo una corrispondenza fra i numeri interi e i punti della retta.
Per ogni numero intero ne esiste un altro che immediatamente lo precede nella successione ordinata dei numeri interi ed un altro che immediatamente lo segue.
Notiamo però per esempio, che tra **0** e **2** (***in Z***) esiste il numero **1**, ma tra **0** e **1** non troviamo alcun numero intero.
L'insieme dei razionali è denso.

Facciamo la stessa cosa per i razionali, per disporre un numero razionale **m/n** sulla retta, dobbiamo dividere l'unità di misura in **n** parti, e poi prendere **m** di queste parti, sempre partendo dall'origine , nel verso indicato dal segno del numero.
Ricordiamo che se **a/b** , **m/n** sono due razionali, diciamo che **a/b<m/n** se:
a *n < m*b (che equivale a moltiplicare ambo i membri per **b*n**);
Per i razionali, osserviamo però che fra due numeri ce n'é sempre un terzo; infatti se **a/b < m/n**, basta considerare la frazione: **(a+m)/(b+n)** ; dimostriamo che **a/b<(a+m)/(b+n)<m/n:**

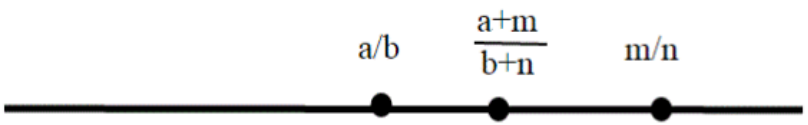
a/b<m/n, an<mb,

an+ab<mb+ab (ho sommato ad ambo i membri ab)

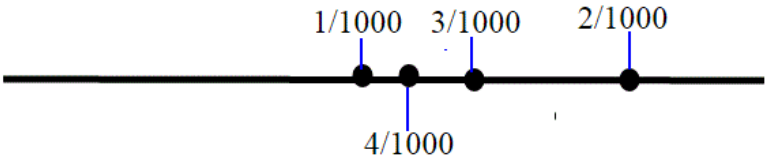
a(b+n)<b(a+m) (raccolgo a,b a destra e sinistra

a/b<(a+m)/(b+n)).

Lo stesso si dimostra per l'altra diseguaglianza.



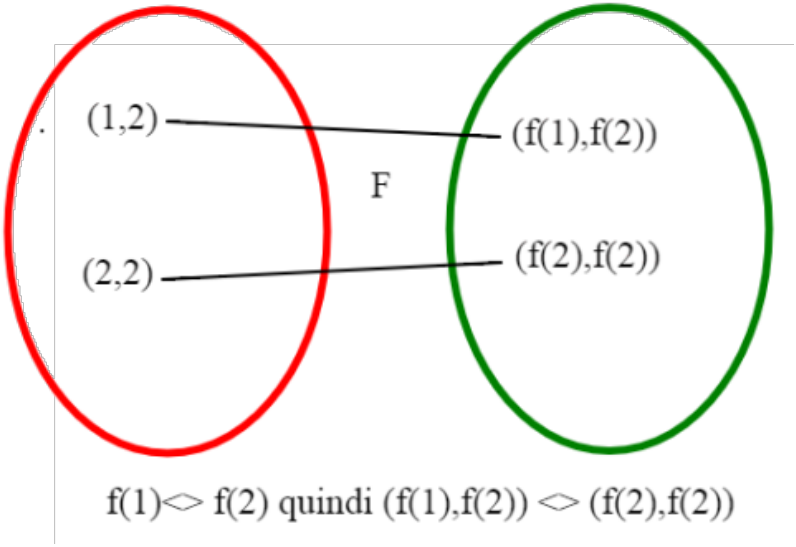
Chiaramente questo calcolo si può iterare; metto al posto di **m/n(a+m)/(b+n)** e riapplico la formula; trovo un punto ancora più vicino a **a/b**, e così via.
Se all'inizio **a/b=1/1000**, **m/n=2/1000**, applicando la formula trovo un punto uguale a **3/1000**; riapplicando con **m/n=3/1000** trovo **4/1000** e così via.



Alla fine trovo infiniti punti che si avvicinano ad a/b.
Per esprimere questo fatto, diciamo **che Q è denso sulla retta** *(anche se non copre tutti i punti sulla retta; lo abbiamo dimostrato nell'articolo sugli insiemi con l'irrazionalità di* $\sqrt{2}$*).*
Questo fatto potrebbe far pensare che i numeri razionali siano molti di più dei relativi; invece vedremo che non è vero.
Il fatto che sembrino tanti è per come sono disposti sulla retta; non riusciamo ad ordinarli come gli interi in una successione crescente, come non possiamo farlo per le coppie di numeri interi.
Ma sopra (metodo delle diagonali di Cantor) abbiamo visto come fare per aggirare l'ostacolo.
Z x Z è numerabile.

Abbiamo visto nell'articolo precedente che N x N è numerabile.
Ma allora anche **Z x Z è numerabile**, in quanto se possiamo mettere in corrispondenza biunivoca **N** con **Z** la stessa cosa possiamo fare con le coppie .
Infatti se sappiamo che esiste una funzione biunivoca **f: N–> Z** che a **n–>z=f(n)**, e consideriamo una **F : N x N –> Z x Z** così definita:
(n,m)–>(f(n),f(m)) allora **F** è biunivoca.
Infatti se la coppia $(n_1, m_1) \neq (n_2, m_2)$ allora almeno uno dei due elementi della prima coppia è diverso da uno dei due elementi della seconda; supponiamo sia $n_1 \neq n_2$; essendo f iniettiva $f(n_1) \neq f(n_2)$, ma allora $(f(n_1), f(m_1) \neq (f(n_2), f(m_2))$.

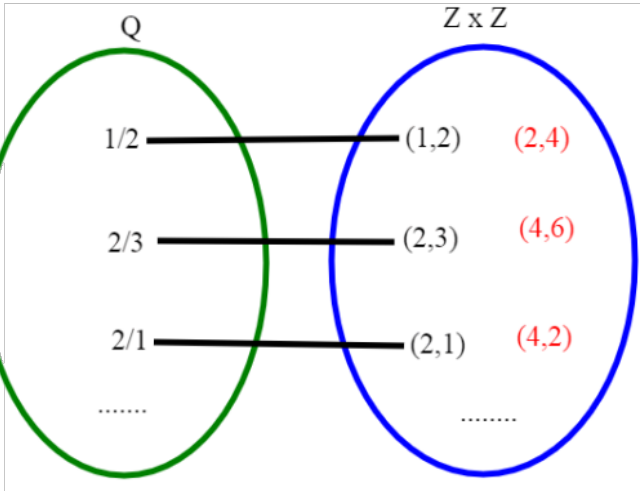
La stessa cosa se supponiamo $m_1 \neq m_2$.
(per esempio, la coppia $(1,2) \neq (2,2)$ *pur avendo il secondo elemento uguale).*



Quindi F è iniettiva.
Inoltre dati (**x,y**) qualsiasi in **Z x Z** , essendo **f** suriettiva esistono **n,m** tali che **f(n)=x, f(m)=y**
quindi **F** è anche **suriettiva.**

L'insieme Q è numerabile

Consideriamo adesso l'insieme **Q** dei razionali e costruiamo una funzione in questo modo: dato un numero razionale **x** (una frazione ridotta ai minimi termini, con numeratore e denominatore primi fra loro) sia **x=m/n**.
Associamo ad **x** la coppia (**m,n**): otteniamo un funzione di **Q–>Z x Z.**



Gli elementi in rosso non hanno immagine.

La funzione è iniettiva. Infatti se **m1/n1<> m2/n2**, le coppie associate sono diverse. Infatti o **m1<>m2** oppure **n1<>n2**.
Non è però suriettiva. Per esempio:
x=1/2–>(1,2)
La coppia (**2,4**) di **ZxZ** resta scoperta ; questo perchè **2/4=1/2**, ma noi abbiamo scelto una rappresentazione in cui **m** ed **n** sono primi fra loro. E così tante altre ancora, tutte le frazioni equivalenti (anche tutte le coppie (**m,0**) perché non esiste un **x** razionale con denominatore uguale a zero).
Chiaramente non copriamo tutto **ZxZ**, ma abbiamo solo una corrispondenza biunivoca fra **Q** e un **sottoinsieme** (infinito) di **ZxZ**.
Questo però non deve preoccuparci affatto; per quanto visto nell'articolo precedente, un sottoinsieme di un insieme infinito è numerabile.
Quindi Q è numerabile.

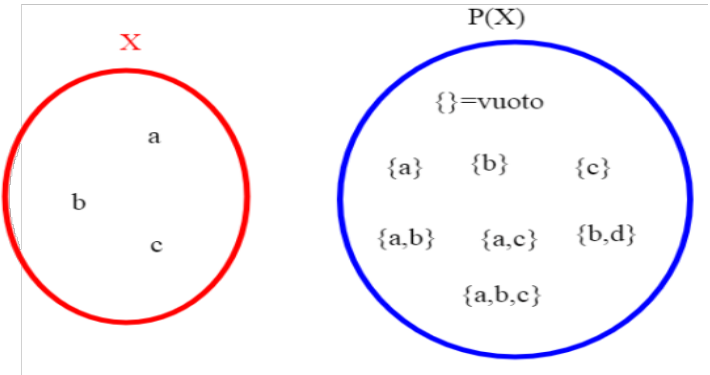
Parte ottava: l'insieme delle parti.

(e il teorema di Cantor)

Nell'articolo precedente abbiamo visto che anche **Q** è numerabile.
Questa è una conseguenza del fatto che **N x N** e quindi anche **Z x Z** sono numerabili.
Ci proponiamo adesso di trovare un insieme non numerabile.

L'insieme delle parti.

Dato un qualsiasi insieme **X**, consideriamo tutti i suoi sottoinsiemi.
L'insieme delle parti non è altro che l'insieme formato da tutti i sottoinsiemi di **X**, e si indica con **P(X)**.
Cominciamo con un esempio; sia **X={a,b,c}**.
Elenchiamo i sottoinsiemi di **X**.
C'è l'insieme **{}** (insieme vuoto) , poi i sottoinsiemi con un elemento **{a}**, **{b},{c}**, quelli con due elementi **{a,b}, {a,c},{b,c}**, e tutto l'insieme **{a,b,c}**.

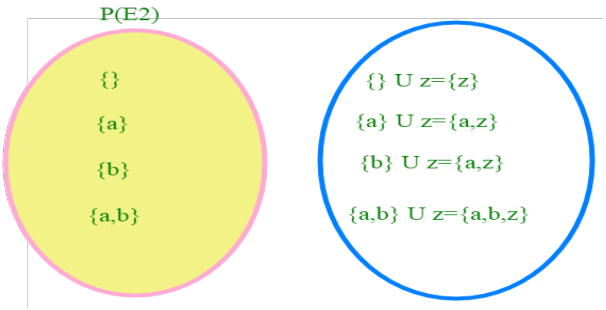


In tutto abbiamo otto sottoinsiemi.
In generale, se abbiamo un insieme con un numero finito di elementi **n** quanti saranno i suoi sottoinsiemi?
Osserviamo che possiamo elencare i sottoinsiemi in questo modo (caso in cui **n=3**), usando una combinazione di tre elementi **xyz** dove **x,y,z** valgono **0**

o **1**; facciamo corrispondere al sottoinsieme una sequenza di **0,1** che ci dicono se l'elemento è presente o no. Ad esempio:
101

1	**0**	**1**
a	**b**	**c**

Corrisponde al sottoinsieme **{a,c}**.
Così otteniamo tutti i sottoinsiemi di **X**.
In pratica abbiamo creato una corrispondenza biunivoca fra le sequenze di **0,1** di lunghezza **3** e i sottoinsiemi di **X**.
Quante sono le sequenze possibili? Il primo elemento lo posso scegliere in **2** modi diversi, e così pure il secondo e il terzo.
Quindi sono $2 \cdot 2 \cdot 2 = 2^3$.
Nel caso generale sono uguali a due moltiplicato n volte per se stesso, quindi $2 \cdot 2 \cdot 2 \ldots\ldots 2 = 2^n$.
Per chi non fosse convinto, possiamo fare una dimostrazione formale usando il principio di induzione.
Base dell'induzione: **n=1**, allora ho un solo elemento **a** e due sottoinsiemi: **{}** (vuoto), **{a}**
Supponiamo ora che E_n (insieme di **n+1** elementi dobbiamo aggiungere un certo elemento **z,** che non appartiene a E_n**.**
Sia quindi $E_{n+1} = E_n \bigcup z$.
Dividiamo i sottoinsiemi di questo insieme in due tipi; quelli che non contengono **z** quelli che lo contengono.



Esempio con **n=2**; aggiungendo l'elemento **z** ai sottoinsiemi di **E2** ottengo tutti i sottoinsiemi di **E3** con tre elementi; unendo poi questi due insiemi ottengo **P(E3)**, ovvero l'insieme delle parti di **E3.**
Il primo tipo è costituito da tutti i sottoinsiemi di E_n, che sono 2^n; il secondo si ottiene aggiungendo **z** a ciascuno dei sottoinsiemi di E_n.
Sono ancora 2^n sottoinsiemi. in tutto sono $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

Un concetto difficile.

Quando si parla di insieme delle parti abbiamo a che fare con degli elementi di un insieme che sono in realtà degli insiemi essi stessi.
Questo comporta uno sforzo di astrazione notevole; dobbiamo pensare agli elementi di **P(x)** proprio come degli elementi, però non dimenticandoci che sono essi stessi degli insiemi.
Riporto ora la definizione di confronto fra i numeri cardinali, anche se è già stata vista in un articolo precedente.

Confrontare la cardinalità di due insiemi.

Fino ad ora siamo riusciti a dire che due insiemi (infiniti) hanno la stessa cardinalità se esiste un corrispondenza biunivoca fra di essi.
Ma se ciò non si verifica? Vogliamo cioè definire quando la cardinalità di un insieme **X** sia minore di quella di un insieme **Y**.
Diremo che **|X|<=|Y|** se esiste una funzione iniettiva **f** di **X** in **Y: f: X—>Y** (e sottolineiamo che una funzione iniettiva di **X** in **Y** è una corrispondenza biunivoca di **X** in un sottoinsieme di **Y**, che non è altro che l'immagine di **X**, **f(X)**).
Diremo invece che **|X|<|Y|** se esiste una applicazione iniettiva **f** di **X** in **Y**, ma tale applicazione non è suriettiva.
In parole povere non copre tutti gli elementi di **Y**.

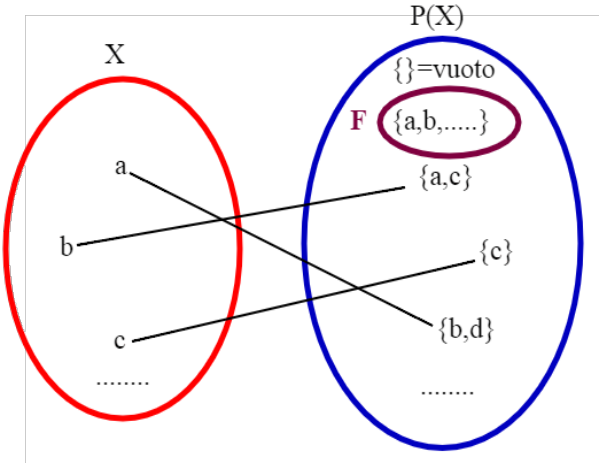
La cardinalità dell'insieme delle parti .

Abbiamo visto quanti sono gli elementi di **P(X)** nel caso **X** sia un insieme di n elementi: 2^n.
Ma quando **X** è infinito?
Può esistere un f biunivoca fra **X** e l'insieme dei sottoinsiemi di **X**? Nel caso

che **X** sia finito no di certo, perchè **X** ha n elementi, mentre **P(X)** ne ha 2^n.
Sappiamo però che le stranezze avvengono nel caso degli insiemi infiniti.

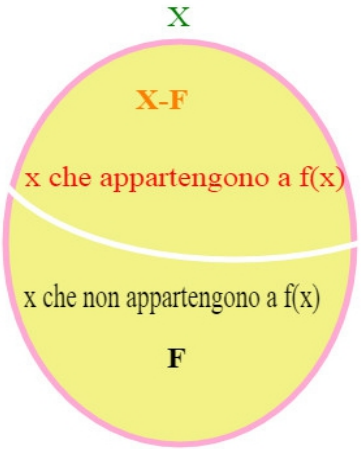
X non può essere messo in corrispondenza biunivoca con P(X).

Esiste sempre una funzione iniettiva **f: X–>P(X)**; è quella che ad **x** associa **{x}**.
Quindi **|X|<=|P(X)|**.
Dobbiamo dimostrare che **f non può essere suriettiva.**
Per dimostrare questa affermazione bastano poche righe (come vedremo) ma uno sforzo di astrazione notevole.
La difficoltà di questa dimostrazione sta nel considerare alternativamente un oggetto sia come insieme che come elemento.
Definiamo un insieme **F** come il sottoinsieme di **X costituito dagli x che non appartengono a f(x)**.

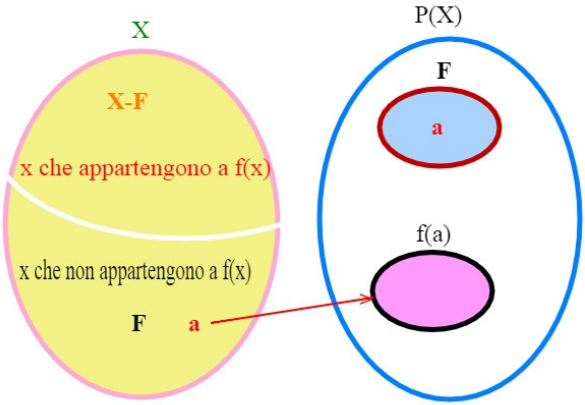


Facciamo un esempio:
F={a,b,….} infatti a non appartiene ad **f(a)={b,d}** e nemmeno **b**, in quanto **f(b)={a,c}**.
Invece c non appartiene ad **F**, in quanto c appartiene all'immagine **f(c)={c}**.
Questo è solo un esempio di come è definito **F** .
Dobbiamo ora ragionare più in generale.

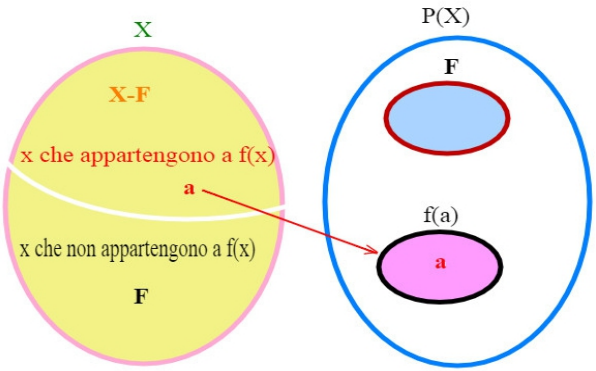
Abbiamo detto che **F={x}** appartenenti a **X** tali che x non appartiene a f(x)}.
Questo F è un certo sottoinsieme di X.
Questa definizione divide l'insieme **X** in **due parti complementari:**



Un elemento a o appartiene a **F** o a **X-F**



F e **f(a)** sono due insiemi visti in **X**, ma visti a destra sono due elementi di **P(X)**.
Per dimostrare che sono diversi, basta dimostrare che un certo elemento non sta in entrambi gli insiemi.
Comunque si scelga **a** appartenente a **X**, il sottoinsieme **F** di **X** non è uguale a **f(a)**.
Infatti, se **a** appartiene a F, allora a non appartiene a **f(a)** per la definizione di **F**.
Ma **F** e **F(a)** sono due insiemi; se non hanno in comune **a** allora sono diversi.

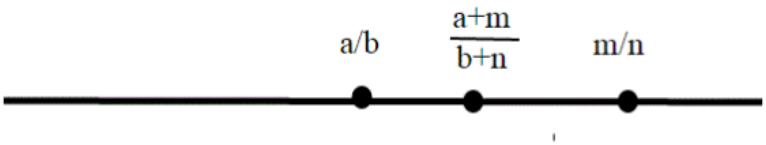


Allo stesso modo, se **a** non appartiene a **F**, allora **a** appartiene a **f(a)**.
Quindi in entrambi i casi **a** appartiene solo ad uno dei due insiemi **F** ed **f(a)**, ma non all' altro.
Ma **F** e **f(a)** sono due insiemi; se non hanno in comune **a** allora **F** e **f(a)** sono diversi (due insiemi sono uguali solo se contengono tutti gli stessi elementi).
Abbiamo dimostrato che **F** è diverso da **f(a)** per ogni **a** appartenente a **X**, e quindi che **F** non appartiene all'immagine di **f**.
In altre parole, **f** non è suriettiva.
Quindi, per come abbiamo definito il confronto fra la cardinalità di due insiemi,
|X|<|P(X)|
Teorema di Cantor: non esiste un insieme di cardinalità maggiore di ogni altro insieme.

La cardinalità dell'insieme delle parti di **P(X)** è maggiore di **X**.
P(X) è esso stesso un insieme, chiamiamolo **A=P(X)**. **|P(A)|>|A|**.
Possiamo ripetere questo procedimento all'infinito. Non esiste un numero cardinale più grande di tutti.
Nel caso che **X** sia **N**, l'insieme dei naturali, per analogia con il caso finito, **|P(N)|** si indica con $2^{\aleph_0}$, quindi $\aleph_0 < 2^{\aleph_0}$.
Quindi in particolare abbiamo trovato un insieme confrontabile con **N** che non è numerabile.

Parte nona. La continuità dei numeri reali.

Cercare di analizzare la cardinalità di **R** senza prima parlare della continuità che lo caratterizza è assurdo; le dimostrazioni infatti si appoggiano appunto sulla continuità dei numeri reali.
E' per questo che l'ordine di infinito di **R** è diverso (come vedremo) da quello degli insiemi numerabili: a causa della continuità.
Lo stesso Cantor per primo, fece una costruzione dei numeri reali per raggiungere lo scopo, noi considereremo però la costruzione di Dedekind.
Nell'articolo precedente, abbiamo disposto i numeri razionali sulla retta, usando una certa unità di misura, e visto che i razionali sono un insieme denso.



Pur essendo **Q** denso (ovvero fra qualsiasi coppia di razionali ne troviamo sempre un altro) Q non copre tutta la retta . Infatti $\sqrt{2}$ non è un numero razionale.
Lo abbiamo visto nel primo articolo sugli insiemi.
Da qui la necessità di introdurre un nuovo insieme numerico, quello dei numeri reali, che contiene anche i numeri detti "irrazionali".

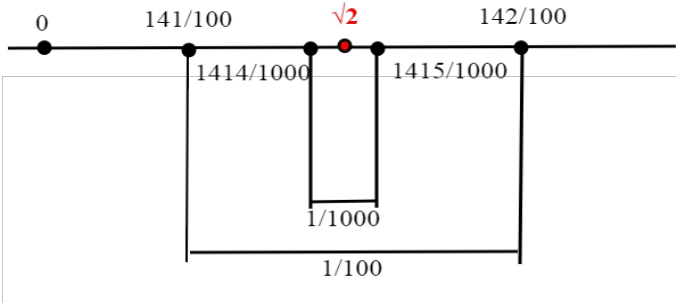
Approssimare $\sqrt{2}$

Tutti pensiamo di saper calcolare $\sqrt{2}$; basta prendere una calcolatrice per ottenere un risultato di questo tipo, a seconda della calcolatrice:

1,4142

(prima della calcolatrice esistevano vari algoritmi per il calcolo, già dai tempi dei Persiani e dei Babilonesi) in realtà questo numero non è radice di due, ma solo una sua approssimazione usando i decimali. Però senza ombra di dubbio, considerando solo le prime due cifre dopo la virgola, sappiamo che $\sqrt{2}$ è un numero compreso fra **1,41** e **1,42** che scritto in frazioni decimali porta alla seguente disuguaglianza:
1+4/10+1/100<$\sqrt{2}$**<1+4/10+2/100** ovvero:

141/100<$\sqrt{2}$**<142/100.**



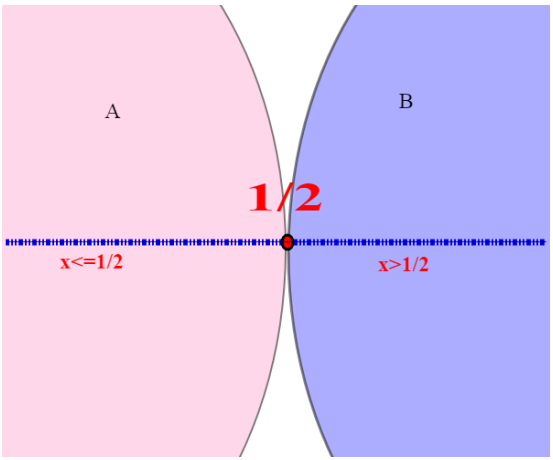
che si può verificare semplicemente elevando al quadrato il primo, il secondo e il terzo membro (se **x** è positivo, $x^2<2$ è equivalente a dire **x**<$\sqrt{2}$, $x^2>2$ è equivalente a dire **x**>$\sqrt{2}$).
Notare che la lunghezza di questo intervallo è **1/100**; se consideriamo **1,414 , 1+4/10+1/100 + 4/1000**<$\sqrt{2}$<**1,414** , **1+4/10+1/100 + 5/1000** ovvero **1414/1000**<$\sqrt{2}$<**1415/1000** otteniamo una stima maggiore, e $\sqrt{2}$ risulta confinata in un intervallo di larghezza **1/1000**.
Aumentando sempre di più la precisione da una parte ottengo dei numeri razionali il cui quadrato è minore di 2 (le approssimazioni per difetto), dall'altra quelli il cui quadrato è maggiore di 2 (le approssimazioni per eccesso).

La costruzione di Dedekind

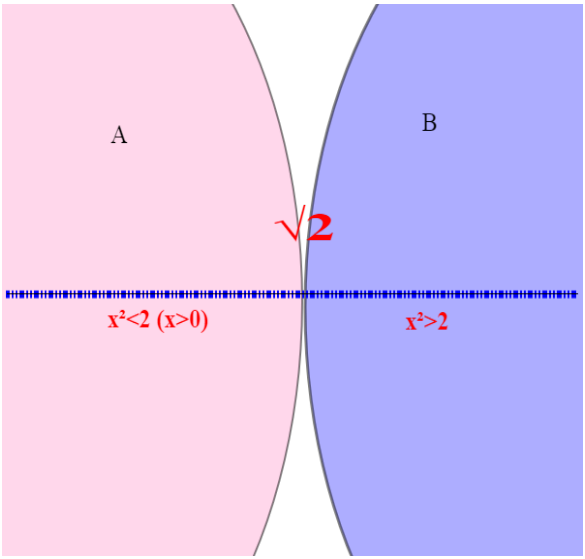
Anche se è un impresa ardua, vorrei dare una giustificazione della continuità dei reali.
Richard Dedekind (1831–1916) riuscì a definire i numeri reali come estensione dei numeri razionali.
Fece cioè una costruzione, definendo un numero reale partendo dai razionali: lo scopo principale era quello di risolvere tutte le equazioni del tipo $x^n = a$ che non sempre hanno soluzione razionale.
Egli diede innanzitutto una definizione: chiamiamo sezione di **Q** ogni coppia di insiemi **A , B** che soddisfino le seguenti proprietà:

1. **A** e **B** siano non vuoti,
2. **A** e **B** non abbiano elementi in comune e la loro unione dia:
   A U B=Q.
3. Qualsiasi elemento di **A** è minore di qualsiasi elemento di **B**.

Vediamo due esempi di sezione.
L'eventuale elemento **x** di **Q** che sta in mezzo ai due insiemi **(A,B)**
a<=x<= b si dice elemento separatore.
Facciamo due esempi:
A={a<=1/2}, B={b>1/2} questa è una sezione di **Q**; l'elemento separatore è **1/2**.
La sezione si dice di prima specie.



Consideriamo ora la seguente sezione di **Q**:
A={q <=0, q appartenente a Q} U {q>0, $q^2<2$, q appartenente a Q}
B={$q^2>2$, q appartenente a Q}; questi insiemi sono disgiunti, la loro unione dà **Q** e ogni elemento di **A** è minore di ogni elemento di **B**.
Altro non sono che le approssimazioni per difetto e per eccesso di $\sqrt{2}$.



Però non esiste alcun elemento in mezzo alle due sezioni ($\sqrt{2}$ non è razionale!); la sezione si dice di seconda specie.
Per dirla con le parole di **Dedekind**:
*…Ora, in ogni caso in cui c'è una sezione (A, B) che non è prodotta da un numero razionale, allora noi creiamo un nuovo numero irrazionale **a** che riteniamo completamente definito da questa sezione; diremo che questo numero **a** corrisponde a questa sezione oppure che produce questa sezione.*
In questo modo definisce i numeri reali come **sezioni** di numeri razionali, riempendo i buchi con le sezioni di seconda specie.
Ma un numero reale è un numero, come può essere definito come un coppia (A,B) di insiemi con certe caratteristiche? Basta definire opportunamente le operazioni e verificare poi le proprietà formali *(non spaventatevi sul termine proprietà formali; non sono che altro che le proprietà che abbiamo sem-*

pre applicato nelle espressioni algebriche studiate alle superiori).
La verifica di tutte le proprietà formali è una cosa lunga e noiosa.
Noi le prenderemo per buone.
La cosa più importante per noi è l'assioma di completezza, che in realtà non è un assioma, ma un teorema dimostrato partendo dalla definizione di numero reale come sezione.
Dedekind estende per similitudine le sezioni anche nel campo dei numeri reali, e dimostra che nei reali ogni sezione di numeri è di prima specie, ovvero (a differenza dei razionali) esiste sempre un numero reale che le separa.
In pratica l'assioma di completezza è una conseguenza del fatto che ogni sezione di numeri reali è di prima specie.
Prima di enunciare l'assioma di completezza di R, abbiamo bisogno di alcune definizioni che riguardano **R**, in quanto insieme totalmente ordinato. Cosa vuol dire? Un insieme in cui sia presente un ordinamento, ovvero in parole povere dotato di un confronto fra qualsiasi coppia di elementi che gli appartengono.
Sappiamo cioè decidere dati a, b diversi, se **a<b**, o **a>b**, qualsiasi siano **a** e **b**.
Questo ordinamento ci permette poi di definire:

Gli Intervalli in R.

Intervalli limitati.
Premetto che la scrittura **a<=b** significa semplicemente che a è minore o uguale a **b**.
Analogamente per **a>=b**.
Siano **a** e **b** due numeri reali tali che **a < b**.
L' intervallo aperto di estremi a e b è l'insieme **(a, b)** = {x appartenente ad **R** tale che **a < x < b**}; **a** è il primo estremo, **b** il secondo estremo.
L'intervallo chiuso di estremi a e b è l'insieme **[a, b]** = {**x** appartiene ad **R** tale che **a<= x<= b**}.
In maniera analoga si definiscono l'intervallo semiaperto a destra **[a, b)** e l'intervallo semiaperto a sinistra **(a, b]** mediante le disuguaglianze **a< x =< b** e **a< x<=b**.
In ciascuno dei casi si definisce lunghezza dell'intervallo la differenza fra gli estremi **l=b-a**.

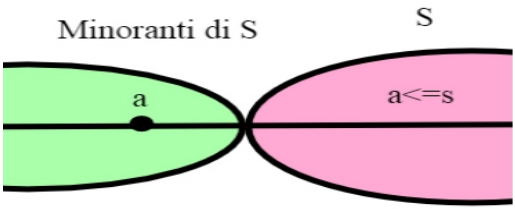
intervalli illimitati:

[**a**,$+\infty$)={**x** appartiene ad **R : a<= x**}
(**a**,$+\infty$)={**x** appartiene ad **R : a< x**}
($-\infty$, **a**)={**x** appartiene ad **R : x<a**}
($-\infty$, **a**]={**x** appartiene ad **R : x<=a**}

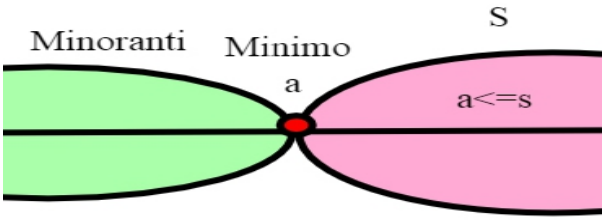
la notazione include i simboli $+\infty$,$-\infty$; è puramente simbolica, praticamente ci dice che possiamo andare a destra e sinistra sulla retta reale quanto vogliamo; $+\infty$, $-\infty$ **non sono numeri reali,** non potremmo in ogni caso definire somme e prodotti che li contengono.

Minoranti di un un sottoinsieme di R

Sia **S** un sottoinsieme non vuoto di **R**.
Diremo che un elemento **a** di **R** é un minorante di **S** se **a<= s** per ogni **s** appartenente a **S**.



Un insieme **S** si dice inferiormente limitato se esiste almeno un minorante di **S**.
Un minorante di **S** che appartiene a **S** si dice minimo di **S**.
Un insieme può avere al più un minimo, e lo indichiamo con **min** S.

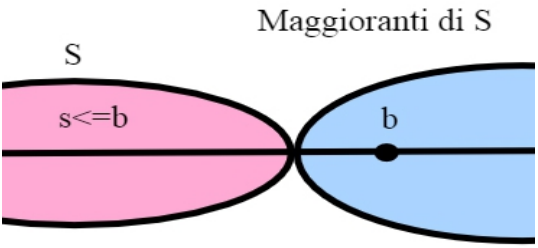


Unicità del minimo

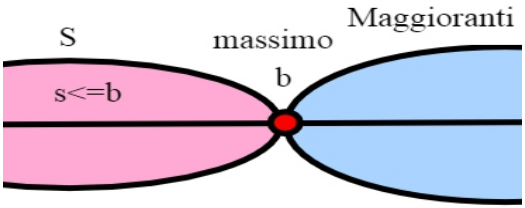
Infatti, se a e a_0 sono minoranti di **S** e appartengono entrambi a **S**, si ha **a**<=a_0 **e** a_0<=**a** quindi **a**=a_0.

Maggioranti di un un sottoinsieme di R

Analogamente diremo che elemento **b** di **R** è un maggiorante di **S** se **s**<=**b** per ogni **x** appartenente a **S**.
S è inferiormente illimitato se l'insieme dei minoranti di **S** è vuoto.



Un insieme si dice superiormente limitato se se esiste almeno un maggiorante di **S**, superiormente illimitato se l'insieme dei maggioranti è vuoto.
Un maggiorante di **S** che appartiene a **S** si dice massimo di **S**, e lo indichiamo con **maxS**.



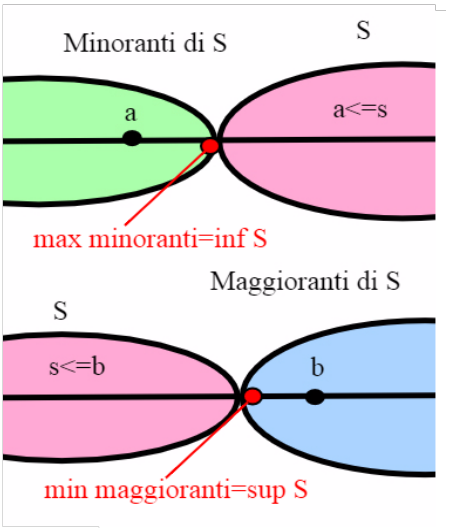
Unicità del massimo

Infatti, se **a** e a_0 sono maggioranti di **S** e appartengono entrambi a **S**, si ha **a**>=a_0 e a_0>=**a** quindi **a**=a_0.

<u>Un insieme si dice limitato se è superiormente e inferiormente limitato.</u>

Estremo superiore e estremo inferiore

Se l'insieme dei minoranti di **S** ha massimo **a** si dice che **a** è l'estremo inferiore di **S**.
Analogamente, se l'insieme dei maggioranti di **S** ha minimo **b** si dice che **b** e l'estremo superiore di S.
L'estremo inferiore e l'estremo superiore di un insieme, se esistono, sono necessariamente unici (essendo definiti come minimo e massimo di un insieme; abbiamo visto che sono unici).
Essi si denotano rispettivamente con **inf S** e **sup S**.
Si noti che se **S** ha minimo esso coincide con l'estremo inferiore.
Se S ha massimo, esso coincide con l'estremo superiore.



Esempi in R

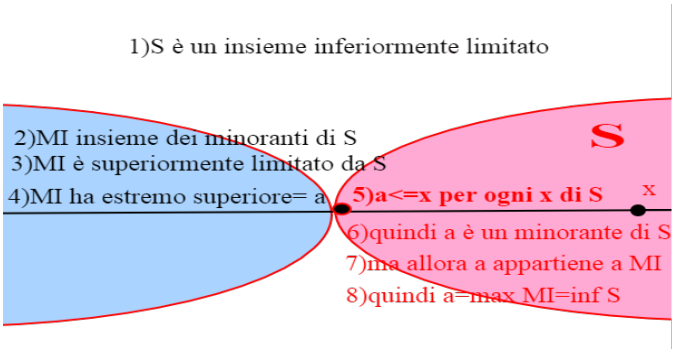
Consideriamo l'intervallo **S=[0,1)** (chiuso a sinistra e aperto a destra).L'insieme dei minoranti è l'intervallo $(-\infty,0]$. infatti per definizione di insieme di minoranti, sono gli x<=0. Ma questa è proprio la definizione dell'intervallo illimitato che abbiamo dato sopra. L'estremo inferiore di S è il massimo di $(-\infty,0]$, che è 0 che vi appartiene. Anche il minimo di S è zero, perchè zero appartiene a S. L'insieme dei maggioranti è invece l'intervallo $[1,+\infty)$ (gli x>=1). Il minimo dei maggioranti è 1; quindi sup S=1; notiamo invece che S pur avendo estremo superiore, non ha massimo, perchè 1 non appartiene ad S. In generale, anche se un insieme è limitato , non è detto che abbia massimo o minimo. Sembra però diversa la questione per l'estremo superiore e quello inferiore. Infatti è proprio quello che ci assicura l'assioma di completezza:

Assioma di completezza o continuità.

L'assioma si può esprimere in due modi:

1. Ogni sottoinsieme non vuoto superiormente limitato di **R** ha estremo superiore.
2. Ogni sottoinsieme non vuoto e inferiormente limitato di **R** ha estremo inferiore.

Le due definizioni sono equivalenti, ovvero la 1) implica la 2) e viceversa.
Facciamo vedere che 1) implica 2), ovvero che ogni sottoinsieme non vuoto e inferiormente limitato di **R** ha estremo inferiore.
(*La dimostrazione è tutta scritta nel disegno, penso che così si possa visualizzarla meglio*).



Osservazione su Q e R

Qualcuno sarebbe tentato di dire ; ma **Q** è denso, possiamo trovare quanti razionali vogliamo in un piccolo intervallo, quindi l'assioma di completezza potrebbe valere anche per **Q**, che è un insieme totalmente ordinato. **NO!** Consideriamo in **Q** l'insieme:

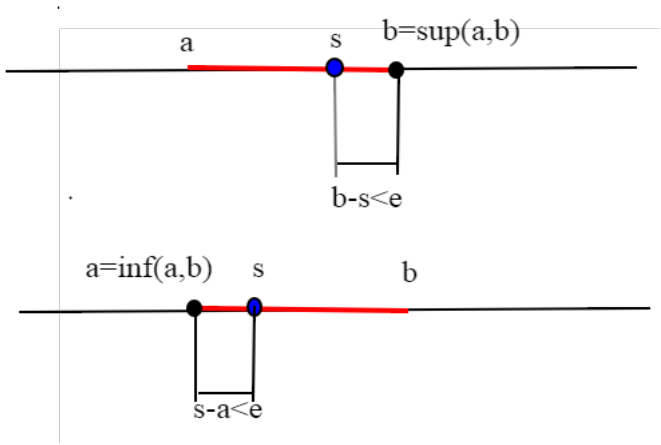
S={ q appartenenti a Q, q>o , $q^2 < 2$**}** ; questo insieme non è vuoto ($1^2 < 2$), è superiormente limitato (lo stesso numero 2 è un maggiorante, in quanto il quadrato di **2** è **4** e quindi ***2 non appartiene ad S***) , **ma non ha estremo superiore in Q**.

Intuitivamente possiamo dire questo: per l'assioma di continuità in **R** l'estremo superiore esiste ed è $\sqrt{2}$ (andrebbe dimostrato formalmente, ma senz'altro $\sqrt{2}$ è il primo candidato), ma sappiamo che $\sqrt{2}$ non appartiene a **Q** (non è un numero razionale).

Quindi in **Q** l'insieme **S** non ha estremo inferiore.

Conseguenze dell'assioma.

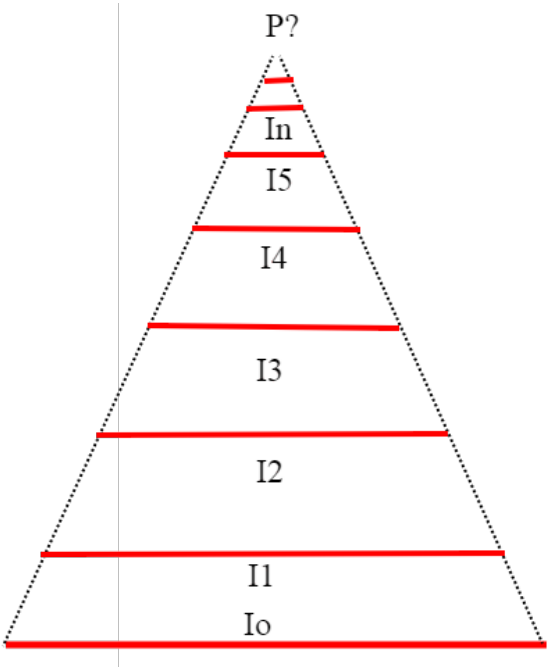
Una prima conseguenza dell'assioma, è che se **b** è l'estremo superiore di un insieme **S**, allora esistono elementi di **S, arbitrariamente vicini** a **b=sup S**.



Allo stesso modo se **a=inf S**, esistono punti di **S**, **arbitrariamente vicini** ad **a=inf S.**
Vediamolo nel primo caso di **b=sup S**; comunque prendiamo un qualsiasi numero **e>0**, dobbiamo dimostrare che esiste un elemento **s** appartenente ad **S**, tale che **b-s<e**; se esistesse un numero e per cui non è vera l'affermazione, vorrebbe dire che per ogni **s** appartenente ad **S, b-s>=e**, ovvero **s<=b-e**; allora **b-e** sarebbe un maggiorante di **S** minore di **b=sup S**, contrariamente all'ipotesi che **b** sia il minimo dei maggioranti.
Questa è una prima conseguenza dell'assioma di completezza; nel prossimo articolo ne vedremo delle altre che ci permetteranno di analizzare la cardinalità dell'insieme **R** .

Parte decima: Conseguenze della continuità di R

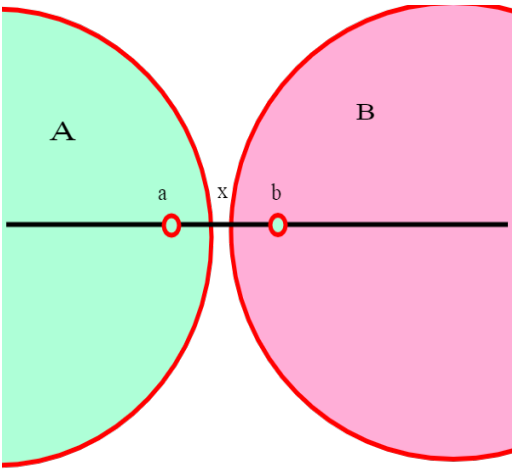
Siamo quasi pronti per dimostrare la non numerabilità dell'insieme dei numeri reali.
Purtroppo senza alcune proprietà della continuità di **R**, non è possibile darne un dimostrazione convincente.
Di solito si fa in quattro righe sfruttando la notazione decimale dei numeri reali e il secondo metodo diagonale di Cantor; a parte il fatto che la notazione decimale comporta alcuni problemi di non univocità , essa non è una delle cose più semplici da giustificare a fondo e inoltre deriva sempre dalle costruzioni di Dedekind e quindi dall'assioma di continuità.
Vi chiedo quindi ancora un po' di pazienza.
L'idea che ebbe Cantor può essere illustrata in un altro modo, che non è poi diversa da quella che usa la notazione decimale dei numeri reali, e fu quella di suddividere un intervallo dei numeri reali con un procedimento ricorsivo in intervalli tali che ogni intervallo contenga il successivo, ed escludendo dei numeri naturali, appartenenti a certe successioni.
Vi premetto questo per cercare di convincervi che non stiamo faticando a vuoto.
Adesso che abbiamo a disposizione l'assioma di completezza, possiamo dimostrare un fatto importante ed anche simpatico riguardo a tali intervalli, che ci permetterà di dimostrare la non numerabilità di R in modo quasi immediato.
Prendiamo in considerazione una successione infinita di intervalli chiusi $I_{n+1} \subseteq I_n$ per ogni n e di lunghezza sempre più piccola (l'estremo inferiore delle lunghezze è uguale a zero, ovvero esistono intervalli di larghezza minore a **e** e qualsiasi sia **e>0**)



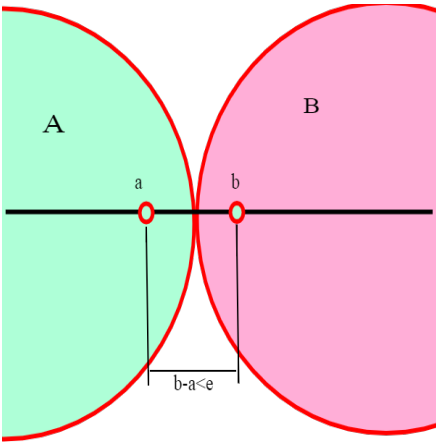
Si ha quindi $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots I_n \supseteq I_{n+1}$;
cosa sarà intuitivamente l'intersezione di tutti questi intervalli ? Un solo punto.
Scopo di questo articolo sarà dimostrare proprio questo partendo dall'assioma di continuità.
Prima però, una definizione e un teorema.

Coppie separate

Una coppia (**A,B**) di sottoinsiemi non vuoti di **R** si dice separata se per ogni **a** in **A** e **b** in **B** si ha **a<= b**.
Un numero reale **x** si dice un elemento di separazione della coppia (**A,B**) se **a<=x<= b** per ogni **a** in **A** e **b** in **B**.



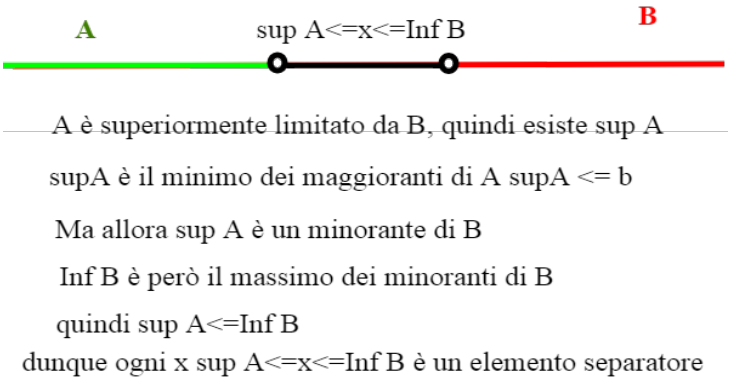
Una coppia separata si dice contigua se per ogni numero reale **e > 0** esistono due elementi **a** in **A** e **b** in **B** tali che **b − a <e** .



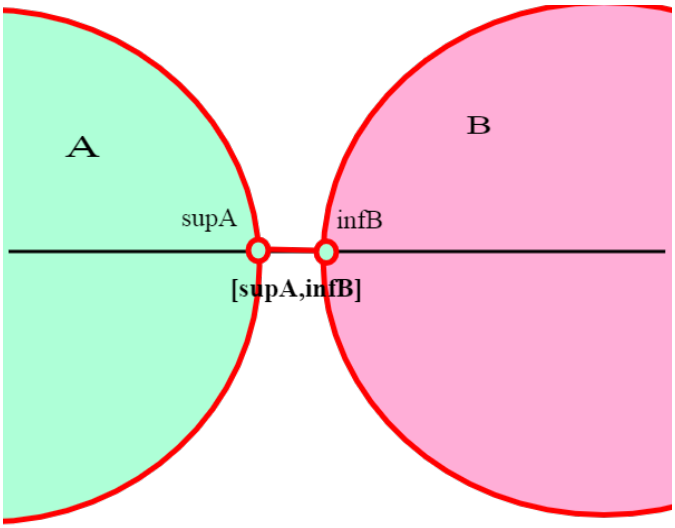
Ma esisterà sempre un elemento separatore che sta in mezzo? Si! Grazie all'assioma di continuità.

Se (A,B) è una coppia separata di sottoinsiemi non vuoti di R esiste almeno un elemento di separazione.
Se la coppia è contigua l'elemento di separazione è unico.

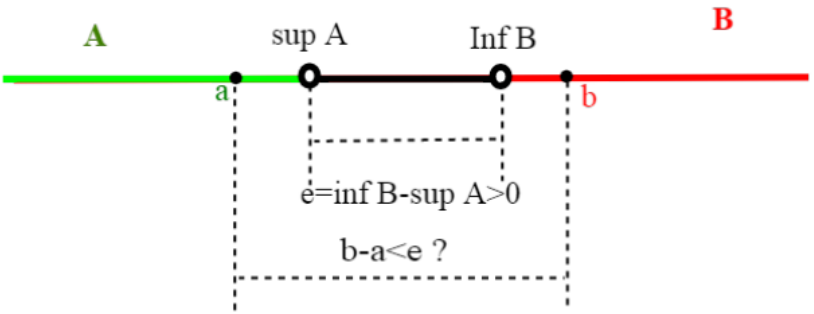
Ogni elemento di **B** è un maggiorante di **A**.
Quindi **A** è superiormente limitato e, per l'assioma di completezza, esiste **supA**.
Poichè **supA** è il minimo dei maggioranti di **A**, si ha **supA<= b** per ogni **b** appartenente a **B**.
Quindi **supA** è un minorante di **B** e pertanto **supA<= inf B** essendo **inf B** il massimo dei minoranti.
Tutti gli elementi dell'intervallo **[supA, inf B**] sono elementi di separazione della coppia **(A,B)** per la definizione di intervallo.



Prendiamo come esempio **A={a<1/2}** , **{b>1}**, **a** e **b** appartenenti ad **R**.
Ogni elemento di **a** è minore di ogni elemento di **b** ; **supA=1/2**, **inf B=1**, tutti gli **x** appartenenti all'intervallo **[1/2,1]** sono elementi separatori.

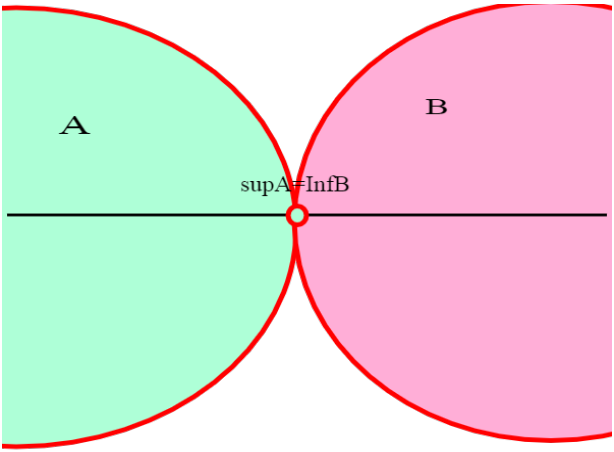


Supponiamo ora che **(A,B)** sia contigua.
Osserviamo che se **x** è un elemento di separazione allora deve essere **supA<=x<=inf B**.
Per dimostrare che l'elemento di separazione è unico, basta provare che :
supA = inf B.



non può essere **b-a<e**; **a** e **b** sono esterni a **sup A** e **inf B**.

Guardiamo il disegno sopra: se **supA<inf B**, allora la differenza è maggiore di zero: posto **e = inf B−supA**, per la definizione di contiguità dovrebbero esistere due elementi **a**, **b** il primo in **A** e il secondo in **B** con differenza **b-a<e**; ma questo non è possibile, come si vede dal disegno.
Infatti: **a<=sup A<=inf B<=b**, pertanto **b-a>inf B-sup A**.
Quindi **sup A** non può essere strettamente minore di **inf B**.
Ma allora **supA = inf B**.
Le dimostrazioni per assurdo lasciano sempre un po' di amaro in bocca, e io cerco di evitarle, perché a volte possono generare confusione.
Possiamo anche pensarla in altro modo; se fra **supA** e **inf B** ci sono degli elementi di **R**, non tutti appartengono ad A o B.
Si genera in tal modo un ostruzione alla contiguità; non posso avvicinarmi indefinitamente alle due classi separate.



Se le classi sono contigue, allora **supA=inf B** e l'elemento di separazione è unico.
Esempio: **A={a<=0, a numero reale}**, **B={1/n , n numero naturale ,n>0**}.
Ogni elemento di **a** è minore di ogni elemento di **b**; **A** e **B** sono contigue;
infatti qualsiasi sia **e>0**, troviamo **a=0** , **b=1/n** con **n>1/e**; **a** è in **A** e **B** è in **B** ma allora **sup A=0**, **Inf B=0**
Ma chi mi assicura che qualsiasi sia **e**, riusciamo a trovare un **n** abbastanza grande affinché **n>1/e** ? **L'assioma di Archimede!** (quindi pensate quanti

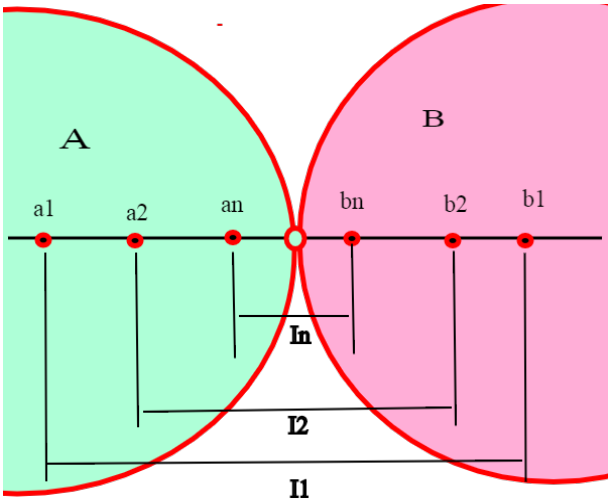
anni ha l'assioma).
Al tempo, quando **Archimede** per primo lo formulò era un assioma, oggi possiamo giustificarlo con quello che abbiamo visto su **R**.

Comunque si scelgano due numeri **e**, **a** positivi: esiste un numero naturale tale che **n*e>a**.
(nel nostro esempio **a=1**).
Giustifichiamolo inizialmente così: se ad esempio **a=1**, **e=0,00000003**
1/e=33333333,333333333333333333333333..
basta prendere **n > 33333333 +1**
(ho considerato la parte intera di **1/e**, e ho aggiunto **1**.
La dimostrazione rigorosa l'ho messa in appendice a questo articolo, per chi vuole approfondire.

Gli intervalli incapsulati

Torniamo ora agli intervalli di cui abbiamo parlato all'inizio.
Una successione di intervalli (**In**) si dice incapsulata se:
In $I_{n+1} \subseteq I_n$ per ogni **n.**
Si ha quindi $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots I_n \supseteq I_{n+1}$
L'intersezione di una successione incapsulata di intervalli chiusi e limitati non è mai vuota.
Se (In) è una successione di intervalli chiusi e limitati incapsulati esiste un elemento comune a tutti gli intervalli.

Tale elemento è unico se l'estremo inferiore delle lunghezze degli intervalli è 0.
(*per chi conosce l'analisi matematica si può anche dire che* $lim_{n\to\infty} l(I_n) = 0$*)*
Sia **In = [an, bn]:** la lunghezza di **In** è allora ***l*(In) = bn −an** .
Consideriamo gli insiemi **A = {an : n in N} e B = {bn : n in N}**.
Dimostriamo che la coppia (**A,B**) è separata.
Si ha che **an<= bn** per ogni **n**, perchè **an** e **bn** sono, rispettivamente, primo e secondo estremo dello stesso intervallo.
Questo però non ci basta, dobbiamo dimostrare che qualsiasi sia **h,k ak<=bh** (qualsiasi a in **A** deve essere minore uguale di qualsiasi **b** in **B**).



Sia **n<=m**; allora poichè **Im** è contenuto in **In** si ha che **an<=am** e **bm<=bn** .
Guardiamo il disegno: **1<2**, **I2** è contenuto in **I1**, **a1<a2**, **b1>b2**.
Siano ora a_k un generico elemento di **A** e b_h un generico elemento di **B** (facciamo variare cioè gli indici **h,k** in tutti i modi possibili)
Ci sono due possibilità:
se **k <=h** si ha $a_k <= a_h <= b_h$
se **h<=k** si ha $a_h <= a_k <= b_k$
In ogni caso $a_k <= b_h$ e, quindi, (**A,B**) è separata.
Ma abbiamo visto sopra che:
Se (A,B) è una coppia separata di sottoinsiemi non vuoti di R esiste almeno un elemento di separazione.
esiste quindi un numero reale **x** tale che **an<= x<=bn** per ogni **n**.
Pertanto **x** appartiene a **In** per ogni **n**.
Sappiamo ora che l'estremo inferiore delle lunghezze egli intervalli è zero: **inf{*l*(In) :n in N} = 0**; se ricordiamo quanto detto nell'articolo precedente, questo significa che qualsiasi sai **e>0**, troviamo un **n** tale che ***l*(In)<e**.
Ma ***l*(In)=bn-an**, quindi per un certo **n**, abbiamo due elementi, **an** e **bn** in **A** e **B** tali che **bn-an<e**; ma questa è la definizione di classe contigua.
Se la coppia è contigua l'elemento di separazione è unico.

Riassumendo: esiste un numero reale **x** tale che **an<= x <=bn** per ogni **n**, quindi **x** appartiene ad ogni **In**, e quindi alla'intersezione $\bigcap_n I_n$, in più **x** è unico.

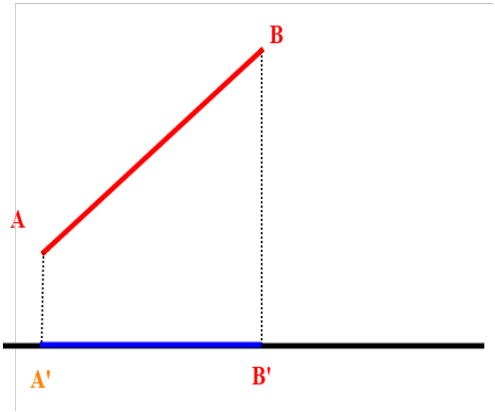
Appendice

L'assioma di Archimede:
Comunque si scelgano due numeri **e**, **a** reali positivi esiste un numero naturale **n** tale che **n*e>a**.
Supponiamo che questo non sia vero; allora dati e, a **n*e<a** per ogni numero naturale **n**; ma allora a è un maggiorante dell'insieme **A={n*e, n appartenente a N}**, quindi **a** è superiormente limitato.
Per l'assioma di continuità, esiste l'estremo superiore **sup A**.
Quindi **n*e<=sup A** qualsiasi sia **n**.
Prendiamo **m=n+1**;
m*e<=a, (n+1)*e<a, n*e <=sup a-e che quindi diventa un maggiorante di **A**; ma **sup A-e <sup A** contrariamente al fatto che **sup A** sia il minimo dei maggioranti.

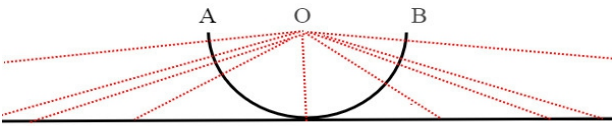
Parte undicesima:la potenza del continuo

L'insieme R dei numeri reali non è numerabile.

Premettiamo che una caratteristica particolare di **R** è che può essere messo in corrispondenza biunivoca con un suo qualsiasi intervallo.
Già Galileo aveva osservato che si possono mettere in corrispondenza biunivoca segmenti di lunghezza diversa, proiettandoli uno sull'altro.



Se poi prendiamo un segmento di una certa lunghezza finita e lo incurviamo fino ad ottenere una semicirconferenza, e proiettiamo la semicirconferenza dal suo centro su una retta, otteniamo tutta la retta reale.



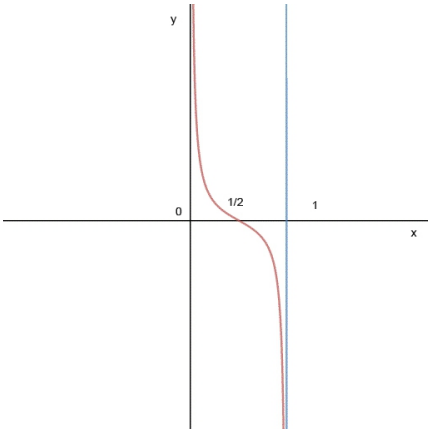
Queste sono cose intuitive, ma non si prestano molto a delle dimostrazioni rigorose.
Vediamole nel caso di un intervallo aperto.
In particolare vogliamo mettere **R** in corrispondenza biunivoca con **[0,1]** (che è quello che ha fatto Cantor).
Consideriamo la funzione:

f:(0,1)—> R definita da: **f(x)=**$\frac{1}{x}+\frac{1}{x-1}$

f(x) è una funzione ovunque definita in **(0,1)** dove è continua e derivabile;
f(x)= 0 per x=1/2; infatti

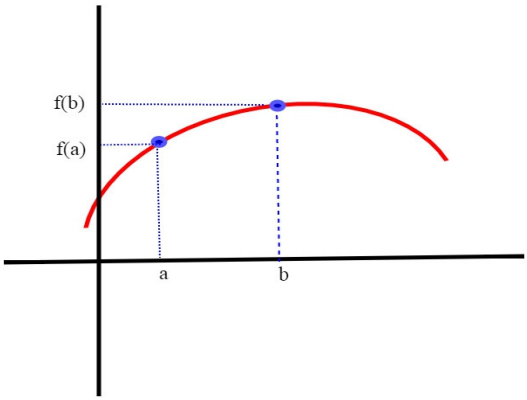
$$\frac{1}{x}+\frac{1}{x-1}=\frac{x-1+x}{x(x-1)}=\frac{2x-1}{x(x-1)}$$

la funzione si azzera pertanto in **2x-1=0**, quindi **x=1/2**
il numeratore è positivo per **x>1/2**; essendo **x** sempre maggiore di **0**, il denominatore è sempre negativo in **(0,1)**, quindi per **0<x<1/2** la funzione è positiva, per **1/2<x<1** la funzione è negativa.
Consideriamo poi i due limiti negli estremi:
$lim_{n\to 0+}\frac{1}{x}+\frac{1}{x-1}=+\infty$; se **x** tende a zero (dalla parte destra) **1/x-1** tende a **1**, mentre sappiamo che **1/x** tende a $+\infty$.

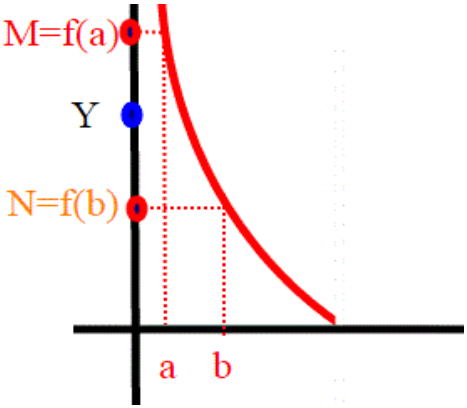


$lim_{n\to 1^-} \frac{1}{x} + \frac{1}{x-1}$; se **x** tende a **1**, dalla parte sinistra, **1/x** tende a **1**, mentre **1/x-1** tende a $-\infty$ quindi la funzione ha due asintoti verticali; l'asse delle **y (x=0)** e la retta **x=1**.
(il segno dei due limiti si vede dal fatto che per **x<1/2** la funzione è positiva, per **x>1/2** invece è negativa).
La funzione (in **(0,1)**) è sempre strettamente decrescente; infatti la derivata prima $-\frac{1}{x^2} - \frac{1}{(x-1)^2} < 0$ è sempre negativa (è la somma di due numeri al quadrato cambiati di segno) quindi **f** è iniettiva (**x1<x2 implica f(x1)>f(x2)** , quindi **f(x1)<>f(x2)**.
Ma **f** non è né inferiormente né superiormente limitata, per quanto visto dai suoi due limiti negli estremi.
Studiando graficamente la funzione,vediamo quindi che assume tutti i valori fra $(-\infty,+\infty)$, e quindi è suriettiva.
Quindi l'intervallo **(0,1)** ha la stessa cardinalità di **R**.
Ma è così immediato dire che f assume tutti i valori reali? In realtà no, non è affatto banale.
E' una conseguenza di un importante teorema sulle funzione continue che riporto di seguito:

Il teorema dei valori intermedi.



Il teorema afferma che se una funzione è continua in un intervallo chiuso **[a.b]**, supposto **f(a)<f(b)**, allora assume tutti i valori dell'intervallo **[f(a),f(b)]**.
Analogamente se **f(a)>f(b)**, assume tutti i valori dell'intervallo **[f(b),f(a)]**.
Ma qui non siamo in queste condizioni, **(0,1)** è un intervallo aperto, allora a cosa serve?



Consideriamo la figura: sia **Y** un qualsiasi numero reale.
Siccome **f** non è superiormente limitata , allora esiste un **a** tale che **M=f(a)** con **M>Y**; analogamente, essendo non inferiormente limitata, esiste un **b** tale che **N=f(b)<Y**.
Se consideriamo l'intervallo chiuso **[a,b]** siamo nelle condizioni del teorema; **f** assume tutti i valori fra **f(a)** e **f(b)**; in particolare anche il valore **Y**, visto che **f(b)<Y<f(a)**.
Quindi la nostra **f** assume tutti i valori reali.
Abbiamo preso per buono il teorema dei valori intermedi; per chi vuole approfondire ho messo una appendice.

Confronto fra segmenti aperti e chiusi.

Vogliamo dimostrare adesso (per essere pignoli) che l'intervallo aperto **(0,1)** ha tanti punti quanti l'intervallo chiuso **[0,1]**, e che quindi **R** ha tanti punti quanti l'intervallo chiuso **[0,1]**.
(0,1) è contenuto in **[0,1]**: possiamo definire una funzione iniettiva

I:(0,1)—>[0,1] che è semplicemente l'identità, ossia quella che ad **x** associa **x**.
Non è però suriettiva , **0** e **1** sono punti non coperti da **I**.
Esiste poi senz'altro una applicazione iniettiva **f: [0,1]—>(0,1)**; per esempio: **f(x)=x/3 (se x1<>x2, x1/3<>x2/3).**
Basandoci su queste due funzioni, vogliamo costruire un nuova funzione che chiamiamo **g:[0,1]—>(0,1)** in questo modo:

g(x)=x/3 se esiste **n** appartenente ad **N** tale che **x=**$\frac{1}{3^n}$.

g(x)=x altrove.

Questa definizione divide l'intervallo in due insiemi complementari.
g(x) è iniettiva; infatti ci sono tre casi:

1. x1 =$\frac{1}{3^n}$, x2<>$\frac{1}{3^n}$; in questo caso f(x1)=$\frac{1}{3^{n+1}}$, f(x2)=x2 che è diverso da $\frac{1}{3^n}$ qualsiasi sia **n .**
2. x1<>$\frac{1}{3^n}$, x2<>$\frac{1}{3^n}$, x1<>x2; in questo caso si applica sempre la **I**, e quindi **f(x1)<>f(x2)** .
3. x1<>$\frac{1}{3^n}$, x2=$\frac{1}{3^n}$ f(x2)=$\frac{1}{3^{n+1}}$. f(x1)=x1 che è diverso da $\frac{1}{3^n}$ qualsiasi sia **n .**

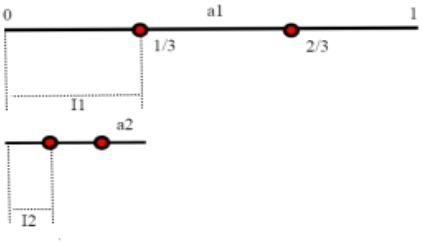
La funzione **f** è anche suriettiva; se **y** appartiene a **(0,1)** abbiamo due casi:

1. y=$\frac{1}{3^n}$ **per qualche n**; ma allora y=f($\frac{1}{3^{n-1}}$)=1/3 *$\frac{1}{3^{n-1}}$=$\frac{1}{3^n}$
2. y<> $\frac{1}{3^n}$ **qualsiasi sia n**, ma allora y=f(y)

Quindi **R** ha la stessa cardinalità di **[0,1].**

[0,1] non è numerabile.

Supponiamo che esista una corrispondenza biunivoca fra i Numeri naturali **N** e i numeri reali **R**.
Vogliamo dimostrare che non copre tutto **R**, qualsiasi essa sia.
Come sempre ci basiamo sul confronto fra cardinali, ci basta dimostrare che non esiste un funzione suriettiva di **N–>[0,1]**.
Infatti tale intervallo è un sottoinsieme di **R,[0; 1]** è equipotente a **R**.
Per farlo consideriamo una qualsiasi successione di numeri reali.
Cos'è una successione? è una funzione di **N–>R**, che in pratica etichetta i numeri reali con un certo numero naturale.
Indichiamo con **a1,a2,a3,…an** i termini di tale successione a valori in **R**.
Vogliamo dimostrare che è impossibile che ricopra tutto l'intervallo **[0,1]**.
Il metodo che adotto è differente dall'usuale metodo detto di diagonalizzazione di Cantor, che fa uso della notazione decimale di un un numero reale.
Ci basta trovare un numero reale che appartenga all'intervallo **[0,1]** , ma che non appartenga alla successione.
Costruiamo una successione di intervalli **I1,I2,I3,…In** (chiusi, ovvero anche gli estremi appartengono all'intervallo) in questo modo:
Parto dall'intervallo **[0,1]**, e lo divido in tre parti uguali; sia **a1** il primo termine della successione di numeri reali.
Considero come **I1** l'intervallo che non contiene **a1** .
Ce ne sono due di possibili, a patto che **a1** non coincida con gli estremi.
Abbiamo diviso l'intervallo in tre parti proprio per questo; nella peggiore delle ipotesi **a1** appartiene a due intervalli contigui, ma allora prendiamo il terzo intervallo.

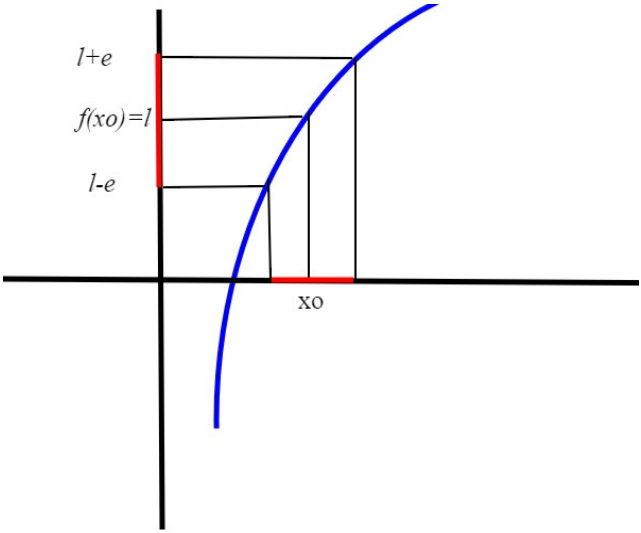


in un caso limite, **a1** potrebbe coincidere con **1/3**; ma in tal caso prenderemmo l'intervallo **[2/3,1]**
Analogamente costruisco **I2**; divido in tre parti **I1** e prendo uno degli intervalli che non contiene **a2**, che è il secondo termine della successione.
Notiamo che oltre ad **a2**, neanche **a1** può appartenere ad **I2**.
Chiaramente **I1** contiene **I2** per costruzione; Vado avanti così e costruisco **I3,..In**
Cosa hanno in comune tali intervalli? Sono in successione decrescente di inclusione; Il termine generico **In** non contiene nessuno dei termini **a1,a2,a3**, **… an** della successione.
La lunghezza dell'intervallo **In** non è altro che $\frac{1}{3^n}$ e ha come estremo inferiore **0**.
Intuitivamente l'intersezione di tutti gli **In** non è altro che un punto che chiamiamo **a** e che appartiene a **[0,1]**.
Ma questo lo abbiamo anche dimostrato rigorosamente nell'articolo precedente; gli **In** sono una successione di intervalli incapsulati e l'estremo inferiore delle lunghezze è zero.
Esiste dunque un punto **a** che appartiene a tutti gli intervalli.
Dunque **a** appartiene a tutti gli **In**, ma è diverso per costruzione da tutti gli **an**.
Quindi gli **an** non coprono tutti i numeri compresi in **[0,1]**.
Si usa indicare con **c** la cardinalità del continuo, quindi **aleph(0)<c**

PS: la costruzione che abbiamo visto, quella di suddivisione degli intervalli, in modo leggermente diverso porta alla costruzione di un un insieme chiamato **"insieme di Cantor"** o anche **"polvere di Cantor"**.
Lo vedremo in seguito in modo più approfondito

Appendice

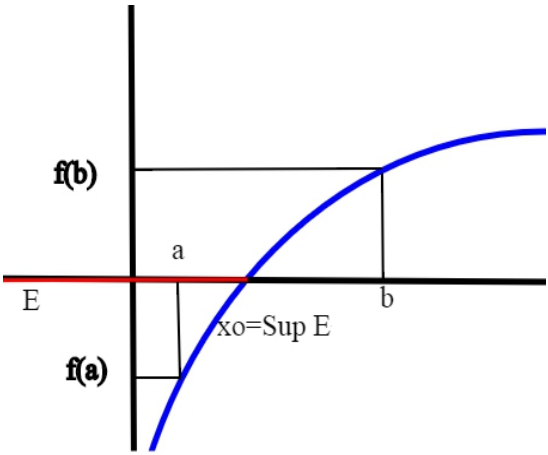
Premessa : una proprietà delle funzioni continue: la **permanenza del segno.**
Consideriamo una funzione **f** continua; essa avrà in un punto **xo** il valore del suo limite **l (per x–>xo).**
l=f(x0), vogliamo dimostrare che in un certo intervallo contenente **xo** la funzione assume lo stesso segno del suo limite, che essendo **f** continua coincide con **f(xo)**.
supponiamo **f** positiva (analogo discorso se negativa);



Per la definizione di limite, qualsiasi sia **e>0**, **f** sarà confinata fra i confini stabiliti da: **l-e<f(x)<l+e** in un certo intervallo contenente **xo**; se prendiamo **e=l/2**, abbiamo **l-e=l-l/2=l/2>0**, quindi **l/2<f(x)<l+l/2=3/2l**; quindi nell'intervallo la funzione assume tutti valori positivi, essendo **l=f(xo)>0.**
Per dimostrare il teorema dei valori intermedi, è necessario conoscere il teorema riportato di seguito.

Teorema degli zeri.

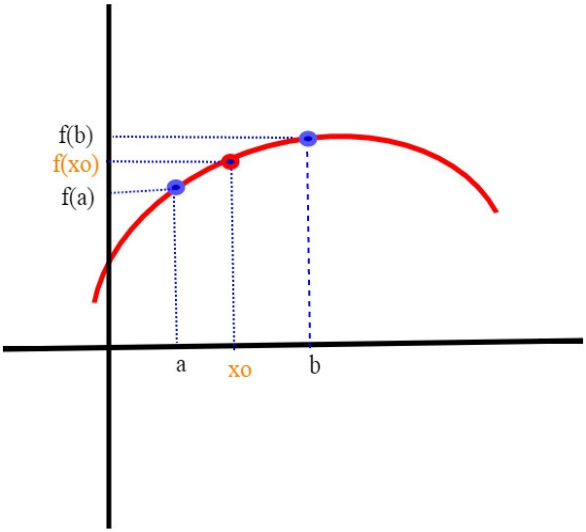
Se **f** è una funzione continua su **[a,b]** e si ha **f(a)<0<f(b)** allora esiste un punto in cui **f** si annulla.
Come vediamo l'enunciato è semplice, ed ha una forte valenza intuitiva. Noi abbiamo supposto **f(a)** negativo e **f(b)** positivo; la stessa cosa vale se **f(a)** è positivo, **f(b)** negativo.
Definiamo un insieme **E={x appartenenti ad [a,b] tali che f(x)<0}**
E, contiene almeno **a**, quindi non è vuoto; **E** è superiormente limitato da **b**, quindi per l'assioma di completezza esiste **xo=sup E<b.**
Supponiamo per assurdo che **f(x)** non si annulli mai in **[a,b]** allora in particolare anche **f(x0)** ***non si annulla*** ; ci sono allora due casi:



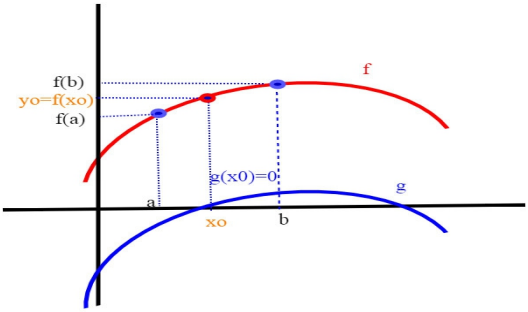
1. **f(xo)<0**; ma allora per la permanenza del segno della funzione continua **f** esiste un **d** tale che in **(xo,xo+d)** ⊆**(xo-d,xo+d)**⊆**[a,b]** sia **f(x)<0**; ma allora ci sarebbe un **x>x0** appartenente a **(xo,xo+d)** in cui **f(x)<0** contrariamente al fatto che **xo** è un maggiorante di **E**, cioè è ***più grande*** di tutti gli **x** per cui vale **f(x)<0**
2. Premettiamo che qualsiasi **x** in **[a,b]** in cui **f(x) >0** è un maggiorante di **E**.
   Supponiamo dunque **f(xo)>0**; sempre per la permanenza del segno allora esiste **d** tale che ogni **x** appartenente a **(xo-d,xo)**⊆**(xo-d,xo+d)**⊆**[a,b] f(x)>0**; quindi esisterebbe un **x** appartenente a **(xo-d,xo)** ***minore di*** **xo** che sarebbe maggiorante di **E** perché **f(x)>0**, contrariamente al fatto che **x0**, essendo **sup E** è il minimo dei maggioranti.

In entrambi i casi arriviamo a delle conclusioni false, ***perciò siamo partiti da un ipotesi sbagliata***.
Quindi **f(x)** si annulla in almeno un punto di **[a,b]**.
Da notare ancora una volta l'importanza dell'assioma di completezza, che da quanto visto è alla base anche dei teoremi fondamentali dell'analisi matematica.

Dimostrazione del teorema dei valori intermedi



Dobbiamo dimostrare che: comunque prendiamo un punto **y0** interno ad **[f(a),f(b)]** esiste un **xo** appartenente all'intervallo **[a,b]** tale che la sua immagine sia **yo**, ovvero **yo=f(x0)** (abbiamo supposto **f(a)<f(b)**; analogamente si procede nel caso contrario.
Sappiamo dunque che **f(a)<yo<f(b)**; definiamo una funzione **g(x)=f(x)-yo**; allora:



La funzione **f** viene traslata della quantità **yo** appositamente per poter applicare il teorema degli zeri:
g(a)=f(a)-yo<0
g(b)=f(b)-yo>0; **g** è una funzione continua, perchè **f** è continua, dunque per il teorema degli zeri esiste un punto **xo** in cui si annulla, cioè: **g(xo)=0=f(x0)-yo**; quindi **yo=f(xo)**

Parte dodicesima: Il teorema di Bernstein

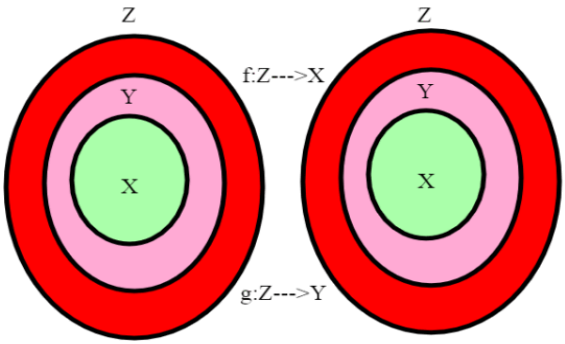
Stiamo affrontando un fase preparatoria ; dobbiamo introdurre uno strumento di confronto per semplificare alcune dimostrazioni sulla cardinalità degli insiemi.
Quando andremo a confrontare insiemi come "l'insieme delle parti di **N**" con **R**, oppure **R** (retta euclidea) con **R x R** (piano euclideo) non sarà così facile trovare un corrispondenza biunivoca fra i due.
La cosa più difficile in genere non è dimostrare che una corrispondenza sia iniettiva, ma dimostrarne la suriettività.
C'è un metodo più semplice, dovuto a Bernstein.
Riprendo prima una definizione usata precedentemente in altri articoli.

Confrontare la cardinalità di due insiemi.

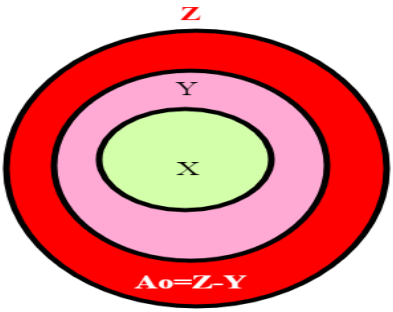
Vogliamo definire quando la cardinalità di un insieme **X** sia minore di quella di un insieme **Y**.
Diremo che **|X|<=|Y|** se esiste una funzione iniettiva **f** di **X** in **Y: f: X—>Y** .
Ma se fosse anche **|Y|<=|X|** ? Ovvero se esistesse una funzione iniettiva **g** di **X** in **Y**: **g: Y—>X**? Saremmo tentati di dire che **|X|=|Y|**, come faremmo con due numeri reali.
Nel caso di due insiemi finiti **A, B** è abbastanza ovvia; se **f:A–> B** è iniettiva, manda punti distinti in punti distinti, quindi se indichiamo con **a,b** il numero di punti di **A,B** allora **a<=b** ; per lo stesso motivo, se c'è una **g:B–> A** iniettiva, **b<=a**, quindi **a=b**.
Nel caso di insiemi infiniti invece la dimostrazione non è banale e prende il nome di **Teorema di Cantor-Bernstein ,** ed è stata realizzata da **Felix Bernestein,** che si dice sia stato allievo di Cantor e a cui Cantor affidò la dimostrazione del teorema, essendo probabilmente già certo della soluzione.

Lemma preparatorio

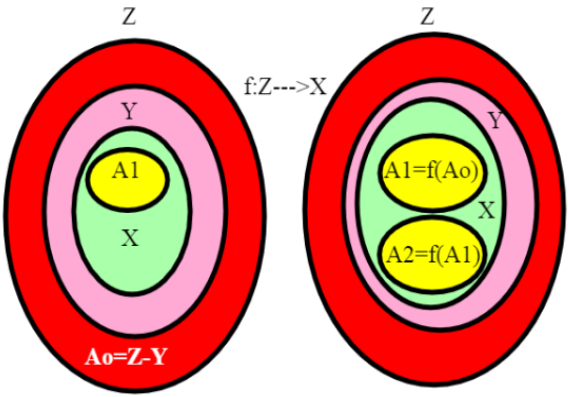
Sia $X \subseteq Y \subseteq Z$; supponiamo che esista una applicazione biunivoca **f: Z—>X**; allora esiste anche una applicazione biunivoca **g** di **g: Z—->Y.**



Osserviamo che questo è possibile solo se gli insiemi in gioco sono infiniti; infatti nel caso finito non può esistere una corrispondenza fra un insieme e un suo sottoinsieme proprio, ma nel caso infinito si (basta ricordare l'esempio di **N** e dei numeri pari).
Sappiamo poi che ciò è possibile nel caso dei tre insiemi **N,Z,Q**.
Vogliamo dimostrare che è vero nel caso generale di insiemi infiniti qualsiasi.
Dimostrazione del lemma preparatorio.
Poniamo **Ao=Z-Y**, ovvero la parte in rosso della figura qui sotto.



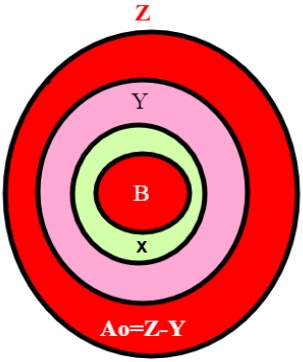
Definiamo una famiglia di insiemi in modo ricorsivo; **A0=Z-Y**:
A1=f(Ao);
A2=f(A1)…
An=f(An-1);
An+1=f(An).
(non lasciatevi spaventare da questa definizione: è stata generata dall'intuito di un grande matematico, vedremo in seguito a cosa serve).



Osserviamo che **A1,A2, ...An, An+1** sono sottoinsiemi di **X**, essendo **f** una applicazione di **Z–>X**
Chiamiamo $A = (\bigcup_n A_n)$ ovvero l'unione di tutti gli **An**; possiamo anche dire che $A = Ao \bigcup (\bigcup_{n>1} A_n)$ quindi , ponendo $B = \bigcup_{n>1} A_n$, $A = A_0 \cup B$ f(A) risulta contenuta in **X**.
(gli **Ai** sono tutti sottoinsiemi di **X**, quindi anche la loro unione è contenuta in **X**) e quindi anche in **Y**, essendo **X** sottoinsieme di **Y**;

$$f(A) \subseteq X \subseteq Y.$$

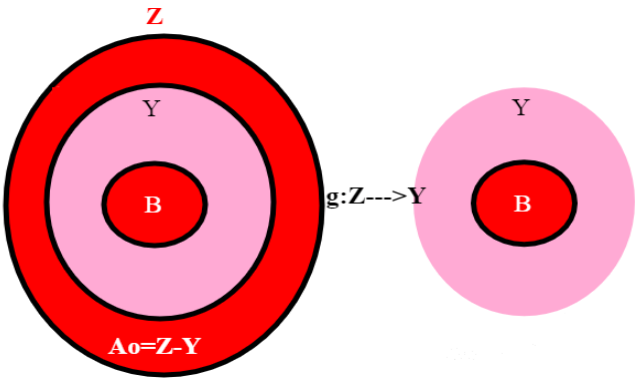
Notiamo poi che su $B = A \cap Y$ f è suriettiva; infatti comunque prendiamo un elemento in A, tale elemento apparterà a qualcuno degli Ai, ma ogni Ai è immagine di qualche altro elemento della famiglia di insiemi.
A questo serve la definizione ricorsiva di A.



la parte rossa del disegno individua **A=Ao U B**
Costruiamo adesso una funzione di **Z—> Y** in questo modo: (la funzione **f** è definita su tutto **Z** e ha valori in **X**; dobbiamo in qualche modo estenderla perchè **f** non ha valori in**Y**, ma solo in **X**)

$$g(z)=\begin{cases} f(z);z\in A \\ z;z\in Z-A \end{cases}$$

In questo modo riusciamo a coprire gli elementi della parte viola di **Y**.



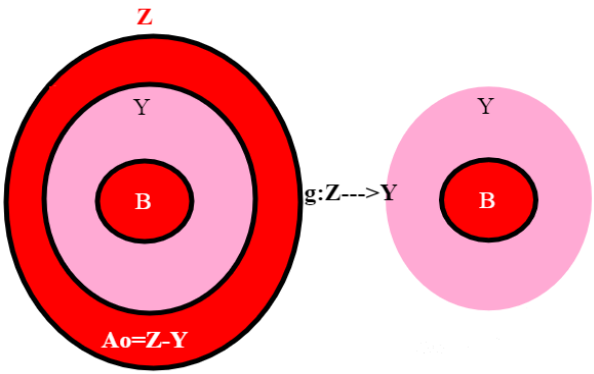
La parte rossa del disegno è **A**, quella viola **Z-A.**
Dimostriamo per prima cosa che **g** è iniettiva; possiamo distinguere tre casi:

1. z_1, z_2 appartengano ad A; ma essendo g definita in tal caso interamente da f, $z_1 \neq z_2$ implica
   $g(z_1) = f(z_1) \neq f(z_2) = g(z_2)$;
   quindi $g(z_1) \neq g(z_2)$
2. z_1, z_2 appartengono a **Z-A**, $z_1 \neq z_2$; ma allora la definizione della funzione è: $g(z_1) = z_1 \neq z_2 = g(z_2)$;
   quindi $g(z_1) \neq g(z_2)$
3. z_1 appartiene ad **A**, z_2 appartiene a **Z-A**;
   ma allora $g(z_1) = f(z_1)$ che appartiene ad **A**, essendo immagine di **f** di un elemento di **A**; $g(z_2) = z_2$ che appartiene a **Z-A.**

Ma allora $g(z_1) \neq g(z_2)$ perchè $g(z_1), g(z_2)$ appartengono ad insiemi complementari.

Suriettività di g:

Se **y** appartiene a **Y**, allora o appartiene a **Y-A**, oppure appartiene ad **A** :



B sostituisce **A** nella differenza, perché **Ao** è esterno a **Y**; la parte viola è **Y-A=Y-B**

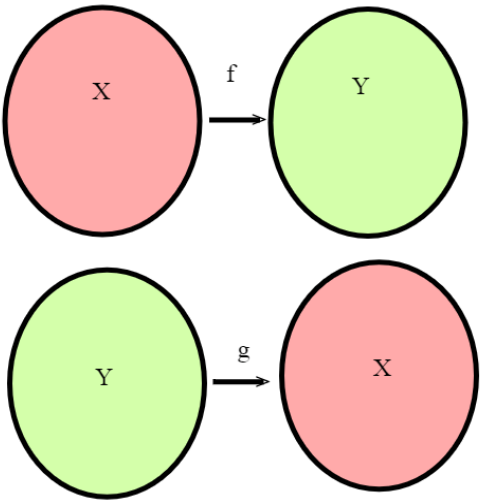
(ricordiamo la definizione di g: $g(z) = \begin{cases} f(z); z \in A \\ z; z \in Z - A \end{cases}$).

Supponiamo che **y** appartenga a **Y-A**; allora **g(y)=y** perché se non appartiene ad **A** sta in **Z-A**.

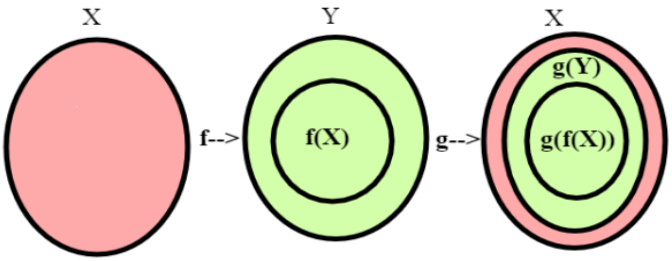
Se **y** appartiene Ad **A** (ovvero a **B**) allora essendo $B = \bigcup_n A_{n>1}$; questo vuol dire che esiste un certo i per cui **y** appartiene ad A_i; ma per come sono definiti gli A_i (anzi, sono stati definiti apposta così) esiste **z** appartenente ad A_{i-1} tale che **f(z)=y**. ma dato che **z** appartiene ad **A**, **g(z)=f(z)=y**.
(Osserviamo che essendo **n>1**, al limite per **i=0**, troviamo che **z** sta in **Ao**).

Il Teorema di Cantor-Bernstein.

Siano **X** e **Y** due insiemi e supponiamo che **f:X—>Y** e **g:Y–> X** siano due funzioni iniettive.
Detto con il linguaggio dei numeri cardinali, **|X|<=|Y|, |Y|<=|X|**;



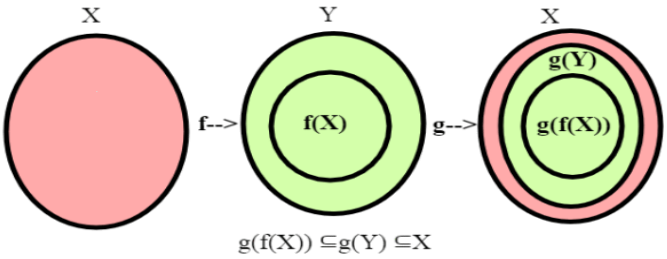
Allora esiste una funzione biettiva **h:X—> Y**, ovvero se **|X|<=|Y|, |Y|<=|X|** allora **|X|=|Y|**
Osserviamo che:



|X|=|f(X)| infatti f è iniettiva, ma anche suriettiva su f(X)
|f(X)=|g(f(X)|| infatti g è iniettiva, ed è anche suriettiva su g(f(X))
ma allora |X|=|f(X)|=|g(f(X)|

1. **|X|=|f(X)|,** infatti **f:X—>Y** è iniettiva, ma considerando come co-dominio **f(X)** è anche suriettiva, quindi è una corrispondenza biunivoca.
2. **|f(X)=|g(f(X)||** infatti **g** è iniettiva, ed è anche suriettiva su **g(f(X)).**

Dal confronto fra 1) e 2) segue allora **|X|=|f(X)|=|g(f(X)|**; il fatto che **|f(X)|=|g(f(X)|** implica che esiste una applicazione biunivoca fra **X** e **g(f(X),** essendo poi $g(f(X)) \subseteq g(Y) \subseteq X$.



g(f(X)) ⊆g(Y) ⊆X

Se **y** sta in **f(x)**, allora sta anche in **Y**, ma allora l'immagine **g** di **y** sta in **g(Y)**, quindi **g(y)=g(f(x))** sta in **g(Y)**; inutile poi dire che **g(y)** è un elemento di **x.**
Siamo nelle ipotesi del **Lemma preparatorio**; esiste una corrispondenza biunivoca fra **X** e **g(f(X))** ma allora esiste anche una corrispondenza biunivoca fra **X** e **g(Y)**.
Ma dato che **|g(Y)|=|Y| .**
(***g** è iniettiva ma anche suriettiva su **g(Y)***) allora |**X**|=|**g(Y)**)=|**Y**|**.**

Parte tredicesima: la polvere di Cantor.

Nel nostro percorso, abbiamo trovato due insiemi particolari, che non sono numerabili; l'insieme delle parti di **N**, e l'insieme **R** dei reali.
Indicheremo nel seguito con $2^{\aleph 0}$ la cardinalità delle parti di **N**, e con **c** la cardinalità di **R**.
Che relazione c'è fra $2^{\aleph 0}$, e **c**? Vedremo che sono uguali.
Non possiamo però arrivarci subito, ma dobbiamo farlo per gradi, sfruttando il teorema di Bernstein.
In questo articolo vogliamo dimostrare che la cardinalità dell'insieme delle parti è minore o uguale a **c**, ovvero $2^{\aleph 0}$<=**c**
Per far ciò useremo un insieme, detto insieme di Cantor, definito tramite un metodo iterativo.
Ancora una volta la ricorsione gioca un ruolo essenziale nell'ambito degli insiemi infiniti.
Prima però, due concetti importanti.

Successioni binarie e insieme delle parti.

Nell'articolo sull'insieme delle parti abbiamo dimostrato che il numero di sottoinsiemi di un certo insieme **X** contenente **n** elementi è 2^n.
Per farlo abbiamo usato una corrispondenza fra i sottoinsiemi di **X** e le sequenze di **0,1**
Ricordiamo che possiamo elencare i sottoinsiemi di **X** in questo modo (caso in cui **n=3,X={a,b,c}**), usando una combinazione di tre elementi **xyz** dove **x,y,z** valgono **0** o **1**; facciamo corrispondere al sottoinsieme una sequenza di **0,1** che ci dice se l'elemento è presente o no.

Ad esempio:
101

1	**0**	**1**
a	**b**	**c**

Corrisponde al sottoinsieme **{a,c}**.
Così otteniamo tutti i sottoinsiemi di **X**.
In pratica abbiamo creato una corrispondenza biunivoca fra le sequenze di **0,1** di lunghezza **3** e i sottoinsiemi di **X**.
Vogliamo adesso estendere questo fatto al caso in cui **X** sia infinito, in particolare **X=N**; in tal modo definiamo proprio delle successioni.
Estendiamo dunque al caso infinito; consideriamo delle sequenze **010101111….** infinite di **0,1**; esse sono in corrispondenza biunivoca con i sottoinsiemi di **N**, quindi con l'insieme delle parti di **N**.
Quindi tali successioni, non sono un un insieme numerabile, ma hanno la stessa cardinalità di **P(N)**.
Vediamolo più in dettaglio nel caso di **N :** indico con **h:**$\{0,1\}^n$ **—> P(N)** l'insieme di tutte le successioni binarie infinite, $a_1 a_2 a_3 \dots a_n \dots$

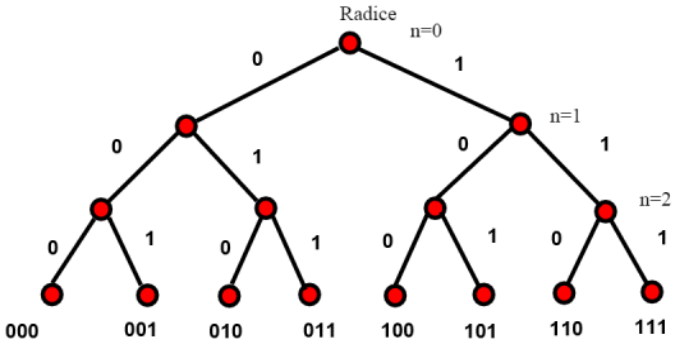
0	1	2	3	4	5	..	n	..	..
a1	a2	a3	a4	a5	a6	..	an	..	..

Gli ai possono valere o zero o uno a seconda che l'elemento ci sia o no e definisce un sottoinsieme di N;
l'applicazione **h:**$\{0,1\}^n$ **—> P(N)** sopra descritta è biunivoca; infatti successioni che differiscono per almeno un elemento generano sottoinsiemi diversi di **N**; **h** è anche suriettiva, perché dato un qualsiasi sottoinsieme di **N**, ad esempio **A={4,6,8,…}**, possiamo costruire la successione che ha per immagine **A**; partiamo dalla prima cifra della successione che sarà **0** perché zero non compare, e così pure la seconda perché **1** non compare e così via, otteniamo la successione **0000101010000…**

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**..**
0	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**..**

L’Albero binario completo

Cominciamo dalla definizione di albero che è intuitiva; non è altro che un albero vero e proprio, come quelli che esistono in natura.
Oppure si può pensare ad un albero genealogico, in cui la radice è il capostipite.
Per ramo intendiamo una successione di elementi, ognuno figlio del precedente, che parte dal capostipite.
Un nodo corrisponde alle biforcazioni di due rami.

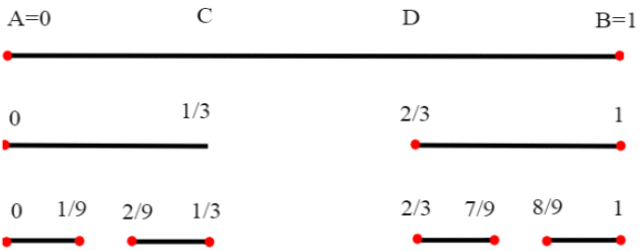


Albero binario: come si può vedere dalla figura i rami vengono identificati dalle sequenze di **0,1** sui percorsi destra-sinistra.
Un tipo particolare di albero è l’albero binario.
Un albero binario è caratterizzato dal fatto che ogni nodo può avere al massimo due figli.
Un albero binario è completo quando i figli sono esattamente sempre due.
Quante sono i rami terminali un albero binario completo? Dipende dalla profondità dell’albero, che chiamiamo n.
Partendo dalla radice, **n=0** , e procedendo ad ogni diramazione (nodo) abbiamo due nuovi rami , quindi **2*2…*2, n** volte, ovvero 2^n.
Vediamo questo fatto in altro modo; per ogni livello n possiamo pensare di percorrere l’albero andando a destra o sinistra in ogni nodo.
I possibili percorsi (rami) sono tanti quante le sequenze di **0,1** (poniamo **0** se andiamo a sinistra, **1** se andiamo a destra.

Nel caso **n=3** abbiamo le sequenze del disegno che identificano tutti i rami, sono sempre $2^3 = 8$.
Concentriamoci adesso su un albero binario infinito; quanti sono i rami (nel senso di cardinalità)? Come nell'esempio finito, partendo dalla radice, ogni volta ho due possibilità di scelta (andare a destra o a sinistra.
Ho delle sequenze di **0,1** ovvero delle sequenze binarie infinite visto che la profondità dell'albero è infinita.
Ma abbiamo visto che le successioni binarie sono tante quante l'insieme delle parti di **N**, **P(N)**.
Quindi la cardinalità di un albero binario completo infinito è $2^{\aleph_0}$.

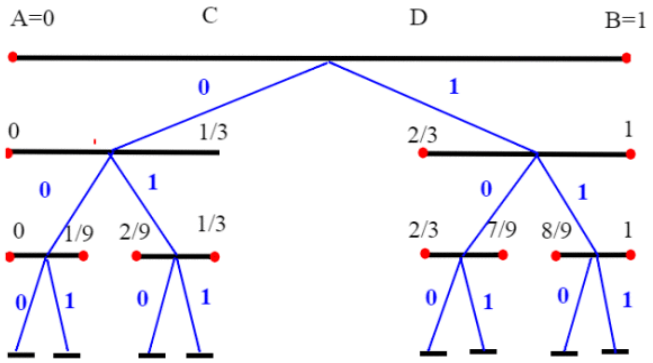
L'insieme di Cantor, un albero binario completo

Consideriamo un segmento chiuso **AB=[0,1]**; sappiamo che **AB** è equipotente a tutto **R**.
Dividiamo il segmento **AB** in tre parti uguali:

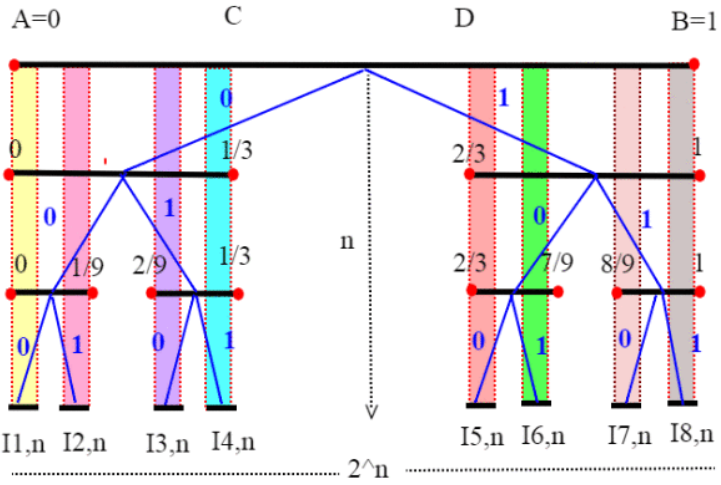


e togliamo dalla parte centrale il segmento aperto **(C,D)** otteniamo due segmenti chiusi, di lunghezza **1/3** di **AB**. Se ripetiamo il procedimento ai due segmenti rimasti, dividendoli sempre in tre parti otteniamo in tutto quattro segmenti, di lunghezza **1/9** di **AB**. Vogliamo estendere questo procedimento indefinitamente; cosa resta del segmento **AB=[0,1]** iniziale, dopo tutte le cancellazioni? L'insieme di Cantor. Osserviamo che non resta alcun segmento non degenere, infatti la lunghezza all'n-esima iterazione è $\frac{1}{3^n}$, che ha come estremo inferiore **0** ,o <(se preferite) limite zero.

Restano allora solo dei punti (da qui il termine suggestivo “polvere di Cantor”).
L’insieme senz’altro non è vuoto (gli estremi di un segmento non vengono mai cancellati,viene solo tolta la parte centrale).
Quanti sono questi punti?
Osserviamo che l’insieme di Cantor è un albero binario completo.



La sequenza **000** porta all’estremo di sinistra; quella **111** all’estremo di destra.
Ogni volta che dividiamo i segmenti successivi in tre parti e togliamo il segmento (aperto) centrale, abbiamo due scelte; prendere quello di sinistra, oppure quello di destra.
Gli intervalli che corrispondono ad un certo ramo sono tutti incapsulati; ovvero ogni precedente contiene i successivo;sono intervalli **chiusi** e la loro ampiezza tende a zero (è uguale a $\frac{1}{3^n}$); per quanto abbiamo visto su gli intervalli incapsulati, la loro intersezione è un unico punto).
Quindi per ogni ramo abbiamo nell’insieme di Cantor almeno un punto.

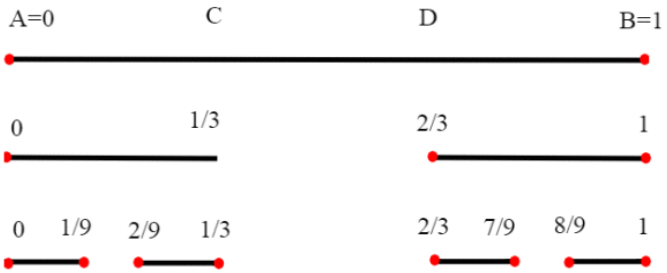


I rettangoli di vario colore evidenziano gli intervalli incapsulati; al passo n=3, abbiamo già **2^3=8** successioni distinte di intervalli incapsulati.
Osserviamo che gli intervalli **In** di una singola successione sono **n**, mentre le successioni che poi convergeranno ad un singolo punto sono **2^n**
Ma i rami dell'insieme di Cantor sono almeno tanti quanti le successioni binarie infinite, ovvero $2^{\aleph_0}$; vogliamo cioè dimostrare che $2^{\aleph_0}$<=**|C|.**
Per far questo basta provare che la funzione **h:**$\{0,1\}^n$ –>**|C|** che a una successione binaria associa quel punto che è l'intersezione dei relativi intervalli incapsulati, è iniettiva.
Se **a,b** sono due successioni di $\{0,1\}^n$, e $a \neq b$, allora esiste almeno un **n** tale che $a_n \neq b_n$. per comodità prendiamo il più piccolo n per cui questo si verifica.
Sappiamo che gli **an**, ovvero le successioni di **0,1** che determinano un ramo, individuano gli intervalli incapsulati; ma se in **n** $a_n \neq b_n$, vuol dire che ho scelto di andare in una successione a sinistra e nell'altra a destra (fino a **n-1** gli intervalli erano gli stessi); quindi vado a finire in due intervalli disgiunti, e l'intersezione finale di tutti gli intervalli non può essere la stessa.

Se indichiamo con **|C|** la cardinalità dell'insieme di Cantor, allora: |$2^{\aleph 0}$**<=|C|<=|[0,1]|=c.**
Infatti $2^{\aleph 0}$**<=|C|** perché come abbiamo visto la funzione **h** è iniettiva; del resto **C** è contenuto in **[0,1]**, quindi **C|<=|[0,1]**; sappiamo poi che la cardinalità di **[0,1]** è uguale a quella di **c.**
Il nostro scopo è stato raggiunto; la prossima volta dimostreremo la disuguaglianza opposta (c<=$2^{\aleph 0}$);
e potremmo concludere (grazie al teorema di Bernstein) che $2^{\aleph 0}$**=c**; per finire volevo illustrare delle proprietà di un insieme che si è dimostrato molto fertile.

Definizione formale

Per definire l'insieme di Cantor formalmente, chiamiamo **Co=[0,1]**, **C1** quello che resta dopo la prima cancellazione, **C1=[0,1/3] U [2/3,1]**
C2 = [0, 1/9] [[2/9, 1/3] [[2/3, 7/9] [[8/9, 1] quello che resta dopo la seconda cancellazione, ecc.
Allora insieme di Cantor: $C = \bigcap_n C_n$.



Non ho dato subito questa definizione , perchè poteva generare confusione. Ora che abbiamo visto come si estendono le successioni di intervalli su rami disgiunti, osserviamo che i **C0,C1,..Cn** sono tutti inclusi nel precedente,quindi la loro intersezione al passo iterativo n, non è altro che **Cn**, ovvero quello rimane all'n-esima cancellazione. Quindi quando il processo iterativo diventa infinito, **Cn** diventa proprio l'insieme di Cantor.

L’insieme di Cantor ha misura nulla.

Possiamo definire la misura di un intervallo, semplicemente facendo la differenza fra gli estremi.
Vogliamo vedere qual’è la misura totale delle cancellazioni che vengono eseguite partendo dall’intervallo **[0.1]**.
Alla prima iterazione tolgo un segmento di lunghezza **1/3**; alla seconda due segmenti di lunghezza **1/9**, ovvero **2/9**, alla terza **4** segmenti di lunghezza **1/27**, ovvero **4/27** e così via.
La somma **S** delle misure che tolgo è quindi **S=1/3 + 2/9 + 4/27 +** … $2^{n-1}/3^n$..
Quindi **S** è somma della serie:

$$S = \sum_{0}^{\infty} \frac{2^n}{3^{n+1}} = \frac{1}{3} \sum_{0}^{\infty} \frac{2^n}{3^n}$$

abbiamo dunque un serie geometrica di ragione 2/3; sappiamo che la somma di tale serie è $\frac{1}{1-\frac{2}{3}} = 3$,

S=3 *1/3

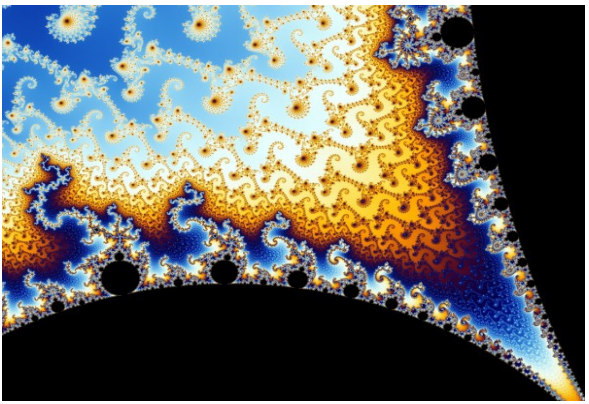
Quindi **S=1**.
Ma come definire la misura di un insieme di punti, come quello di Cantor? in questo caso possiamo farlo come differenza fra la misura di tutto l’intervallo e **S**.
Ma allora la misura dell’insieme di Cantor è ***l*([0,1])-S=1-1=0**
Questa è una cosa assai sconcertante, vi anticipo perchè. Abbiamo dimostrato che $2^{\aleph^0}$**<=|C|<=|[0,1]=c.**
Ma nel prossimo articolo, dimostreremo anche che $2^{\aleph^0}$**>=c,** quindi che:
$2^{\aleph^0}$**=c;** ma allora riprendendo la diseguaglianza sopra **c=**|$2^{\aleph^0}$**<=|C|<=|[0,1]=c,** quindi **|C|=c.**
L’insieme di Cantor ha addirittura la cardinalità della retta **R**, ma la sua misura è nulla (mentre la retta ha misura infinita!).

L'insieme di Cantor è un frattale

Se chiamiamo **C1,C2,C3,C4,..** i livelli della costruzione dell'insieme di Cantor, notiamo che i due blocchi in cui è diviso per ogni livello **Cn+1** sono copie esatte ridotte di **1/3** di **Cn**.
Questo fatto non deve sorprenderci; si può dimostrare che per come è definito, l'insieme di Cantor contiene infinite copie di se stesso, su scala diversa; questo è intuitivo, se cominciamo la costruzione da un qualsiasi pezzo dei **Cn** dove eravamo arrivati e prima lo riscaliamo, otteniamo ancora l'insieme di Cantor.
Esistono altre strutture geometriche, e non solo , ma anche in natura , che hanno questa proprietà (quella di contenere copie di se stesse ridotte di scala); basti pensare a un cavolfiore o alle coste frastagliate.
Se ingrandiamo le parti di questi oggetti, troviamo sempre che la parte ha una somiglianza con il tutto. Si dice che sono auto simili.
Fu **Mandelbrot**, l'inventore del termine "**frattale"**; riportiamo di seguito le sue parole originali:

<<Ho coniato la parola frattale dall'aggettivo latino "fractus" Il corrispondente verbo latino "frangere" che significa rompere per creare frammenti irregolari. e pertanto sensibile e quanto appropriato per le nostre necessità che, oltre a "frammentato" (come in frazione o in rifrazione), "fractus" dovrebbe anche significare "irregolare", con entrambi i significati preservati in frammento".
(The Fractal Geometry of Nature,)>>

Può aprirsi davanti a noi un altro magico mondo, quello dei frattali ,visualizzati tramite iterazioni al computer in colori che dipendono da certi parametri delle iterazioni, che ci portano ad immagini fantastiche come questa (insieme di Mandelbrot):



Un ingrandimento dell'insieme di Mandelbrot; non vi ricorda la superficie solare?
Pensate che il procedimento iterativo che conduce alla definizione è molto semplice; considero tutti i punti del piano complesso **C;** per ciascun punto definisco un successione ricorsiva in questo modo:

$$\begin{cases} z_0 = 0 \\ z_{n+1} = z_n^2 + c \end{cases}$$

se tale successione è convergente, allora il punto appartiene all'insieme di Mandelbrot, altrimenti no.
Si può dare colore nero se appartiene all'insieme, ma se poi si danno colori diversi a seconda della velocità di convergenza, allora si ottengono figure colorate come quella qui sopra.
Naturalmente i frattali (o più precisamente le loro immagini) sono diventati di dominio pubblico dopo l'avvento del computer; prima esistevano solo nella mente dei matematici.
Sembra che il primo frattale sia dovuto a Arthur Cayley, nel 1870, più un secolo prima della nascita della grafica al computer.

Parte quattordicesima: la cardinalità di R.

(è uguale a quella delle parti di N)

Nell'articolo precedente , servendoci dell'insieme di Cantor, abbiamo dimostrato che $2^{\aleph 0} \leq c$, ovvero che la cardinalità dell'insieme delle parti di **N** è minore o uguale a quella di **R**, ovvero **c ,** la potenza del continuo.
Vogliamo ora trovare la diseguaglianza opposta, ovvero $c \leq 2^{\aleph 0}$, per poter poi concludere, grazie al Teorema di Bernstein, che: $c = 2^{\aleph 0}$.
Prima un richiamo alle proprietà dei numeri reali, in particolar modo all'assioma di **Archimede**, che più che un assioma è una conseguenza della continuità dei numeri reali.
Abbiamo infatti dimostrato che comunque si scelgano due numeri e, a reali positivi esiste un numero naturale **n** tale che **n*e>a**.
Descriviamo l'assioma con un esempio: **a=1, e=0,00000003.**
1/e=33333333,33…. per avere **n*e>1** basta prendere **n>33333333+1**.
Possiamo anche dire che per l'assioma, dati due numeri reali qualsiasi, è sempre possibile trovare un multiplo dell'uno che sia maggiore dell'altro.
Vogliamo ora vedere una importante conseguenza di questo assioma; comunque scelga due numeri reali, esiste sempre un numero razionale che sta in mezzo ai due numeri.
Detto formalmente, per ogni **x,y** appartenenti ad **R**, con **x<y,** esiste un **q** appartenente a **Q**, tale che **x<q<y**.
Osserviamo che possiamo limitare la dimostrazione al caso in cui **0<x<y**; infatti ci sono altri due casi:

1. **x<0<y**; ma in questo caso il numero razionale lo abbiamo già trovato (o è un numero razionale)
2. **x<y<0**; ma allora **-x>-y>0**, ovvero **o<-y<-x**. Ci riduciamo al caso in cui i due numeri siano entrambi positivi; se riusciamo a dimostrare che **0<-y<q<-x**, allora **x<-q<y<0**.

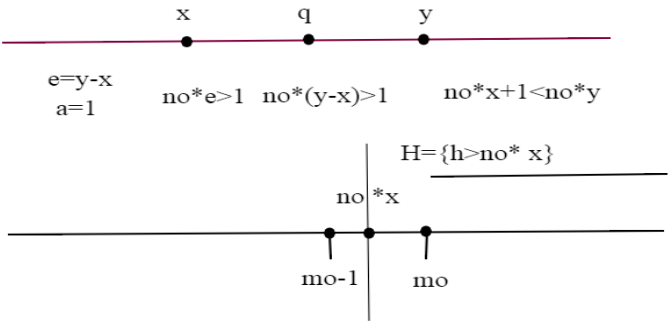
Dimostrazione

Siamo nel caso **0<x<y**, allora **y-x>0**; possiamo allora applicare l'assioma di Archimede; consideriamo **e=y-x**, **a=1**; allora esiste un numero naturale n_0 tale che $n_0 \cdot e > 1$, ossia $n_0 \cdot (y - x) > 1$,
$n_0 \cdot y - n_0 \cdot x > 1$, da cui:

1) $n_0 \cdot x + 1 < n_0 \cdot y$;

Consideriamo adesso il numero reale $n_0 \cdot x$ e l'insieme
H={h naturali tali che $h > n_0 \cdot x$**}**.

H non è vuoto; infatti sempre per l'assioma di Archimede, esiste h_1 tale che $h_1 > n_0 \cdot x$
Per il principio del buon ordinamento dei naturali, l'insieme H (come ogni altro insieme di numeri naturali) ammette minimo, chiamiamolo m_0; allora $m_0 > n_0 \cdot x$ mentre $m_0 - 1 \leq n_0 \cdot x$, perché $m_0 - 1$ non appartiene ad **H**, essendo m_0 il minimo di **H**.



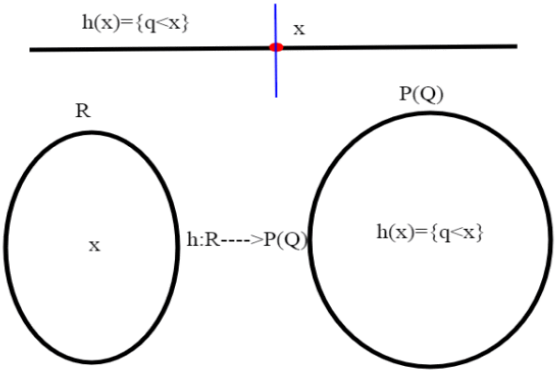
quindi:
$n_0 \cdot x < m_0$
$n_0 \cdot x > m_0 - 1 \Rightarrow n_0 \cdot x + 1 > m_0$
$n_0 \cdot x < m_0 < n_0 \cdot x + 1 < n_0 \cdot y$ dove abbiamo usato la 1), cioè $n_0 \cdot x + 1 < n_0 \cdot y$ nell'ultimo passaggio.
$n_0 \cdot x < m_0 < n_o \cdot y$; dividiamo adesso entrambi i membri per n_0:

$x < \frac{m_0}{n_0} < y$ ma $\frac{m_0}{n_0} = q$ essendo un rapporto fra numeri naturali è un numero razionale. Quindi per quanto siano vicini **x,y** esiste sempre un razionale che sta in mezzo ai due.

Dimostriamo ora che $c \leq 2^{\aleph 0}$

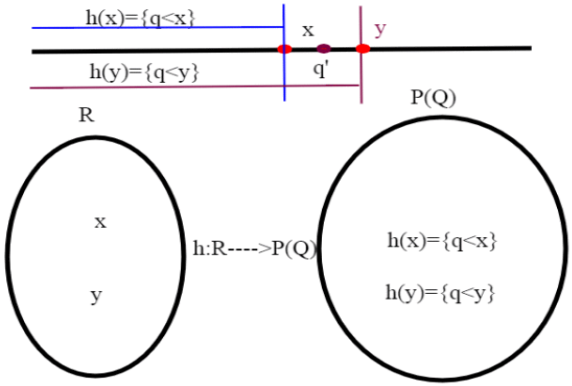
Dato un numero reale **x** qualsiasi, consideriamo tutti i sottoinsiemi di **Q**, per cui, per ogni elemento **q** che vi appartiene, **q<x**.

Questi sottoinsiemi sono un sottoinsieme delle parti di **Q** (e gli elementi di **P(Q)** sono tanti quanti $2^{\aleph 0}$, essendo **Q** numerabile, vedi appendice).



Chiamo quindi **h** l'applicazione che associa ad un numero reale **x** il sottoinsieme di **P(Q)** composto dai numeri razionali **q** tali che **q<x**, **h: R—>P(Q)**; mi basta dimostrare che **h** è iniettiva, se **x,y** sono due numeri reali diversi, possiamo supporre **x<y**; per quanto visto esiste **q'** tale che **x<q'<y**, quindi ho almeno un punto razionale che differisce negli insiemi di numeri razionali **q<x**, **q<y** che sono rispettivamente **h(x)** e **h(y)**, ovvero **h(x)<>h(y)**, quindi **h** è iniettiva, e $c \leq 2^{\aleph 0}$.

Ci basta questo per concludere, in base al **teorema di Bernstein**, e al risultato dell'articolo precedente, che $c = 2^{\aleph 0}$.



Appendice

L'insieme delle parti di **Q**, **P(Q)** ha la stessa cardinalità dell'insieme delle parti di **n**, **P(N)**, ossia **|P(Q)|=**$2^{\aleph 0}$.
Essendo **Q** numerabile, sappiamo che esiste una applicazione biunivoca , chiamiamola **h:N—>Q.**
Vogliamo costruire una applicazione **p:P(N)—>P(Q)**
se **N1** è un sottoinsieme di **N**, **N1={n1,n2…}** definiamo:
p(N1)={h(n1),h(n2)…}

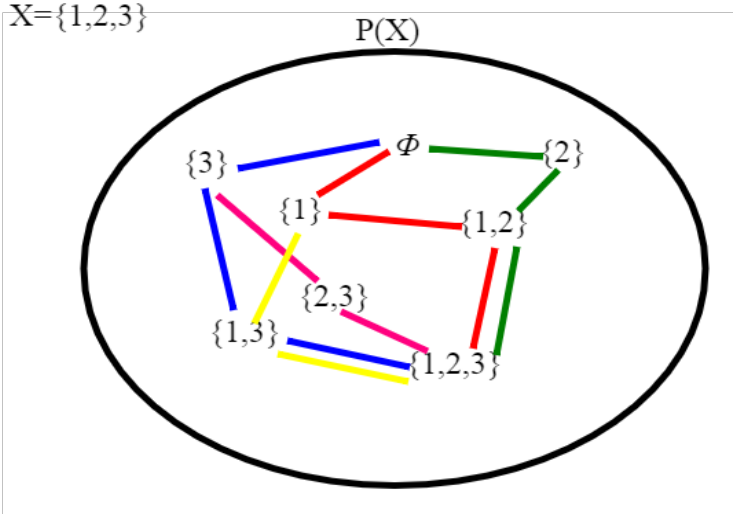
p è iniettiva.
Infatti, se consideriamo due sottoinsiemi di **N** diversi, chiamiamoli **N1** e **N2**, allora differiscono per almeno un elemento, sia **n**,che per esempio sta in **N1** ma non in **N2**.
Ma allora se mando questi due sottoinsiemi in **P(Q)** usando la **p**, ottengo due insiemi diversi, perché **h** è iniettiva, quindi **h(n)** sta in **h(N1)**, ma non in **h(N2)**.

p è suriettiva:
Se **{q1,q2,..}** è un sottoinsieme di **P(Q)**, esistono **n1,n2,..** tali che **h(n1)=q1**, **h(n2)=q2**.
Quindi l'immagine **p {n1,n2..}** è proprio **{q1,q2,..}**.

Parte quindicesima: l'assioma della scelta .

Insiemi ben ordinati.

Abbiamo già visto degli esempi di insiemi ben ordinati: i numeri naturali.
L'insieme dei numeri naturali è totalmente ordinato (un insieme è totalmente ordinato se presi comunque due elementi, posso sempre decidere se uno è maggiore dell'altro).
Genericamente, quando si parla di insiemi ordinati, non si è sicuri che questi insiemi siano totalmente ordinati, per cui in generale si dice che tali insiemi sono parzialmente ordinati.
Un esempio di insieme parzialmente ordinato è l'insieme delle parti di un insieme **X**, prendendo come ordine l'inclusione.
Se due sottoinsiemi di **X** non sono uno contenuto nell'altro, non sono confrontabili.



Nel caso **X={1,2,3}**, vediamo che a parte l'insieme vuoto, che è confrontabile con qualsiasi elemento, non tutti i sottoinsiemi sono confrontabili; ad esempio **{1,2}** non è confrontabile con **[1,3}**

Se oltre ad essere totalmente ordinati, tali insiemi soddisfano al principio del minimo (ovvero ogni sottoinsieme di **X** ha minimo), allora si dicono ben ordinati.
Perchè riprendiamo questi concetti? Per rispondere a questa domanda: *é sempre possibile confrontare la cardinalità di due insiemi?* Cantor pensava di si , a patto che ogni insieme si possa ben ordinare, anche se il nesso non è così immediato (vedremo che in due insiemi ben ordinati si può sempre definire una applicazione iniettiva di uno nell'altro).
Nel 1904 **Ernst Zermelo** ha dato una dimostrazione rigorosa del fatto che ogni insieme si può bene ordinare. Tale dimostrazione dipende sostanzialmente dall'accettazione dell'assioma della scelta, prima però dovremmo introdurre dei nuovi concetti sugli insiemi parzialmente ordinati, e considerare il fatto che l'assioma della scelta implica il lemma detto di Zorn.
Lo schema che seguiremo in questa serie di articoli, sarà questo:
Assioma della scelta $\Rightarrow$ Lemma di Zorn $\Rightarrow$ insiemi ben ordinati $\Rightarrow$ confronto fra cardinali.
Non ci resta che partire dall'assioma della scelta.

L'Assioma della scelta

Come già detto, Zermelo si occupo' di sistemare la teoria degli insiemi dal punto di vista assiomatico.
Questo perché la trattazione iniziale di Cantor (strettamente intuitiva) e detta anche "***teoria ingenua degli insiemi***", poteva dar adito a una serie di paradossi (quello più famoso quello di **B.Russel**).
Nacque perciò la necessità della costruzione di una base assiomatica in modo rigoroso.
Non tratteremo tutti gli assiomi di Zermelo , ma solo il più importante, che permette di risolvere (tramite una sua enunciazione equivalente, il lemma di Zorn) il problema di ben ordinare qualsiasi insieme.
Il lemma di Zorn ci servirà anche per trovare la cardinalità dell'insieme prodotto in caso di insiemi infiniti qualsiasi (noi lo abbiamo visto solo nel caso degli insiemi numerabili, ma dobbiamo ancora dimostrarlo per il piano euclideo, ovvero **R x R**).
L'assioma della scelta stabilisce che:

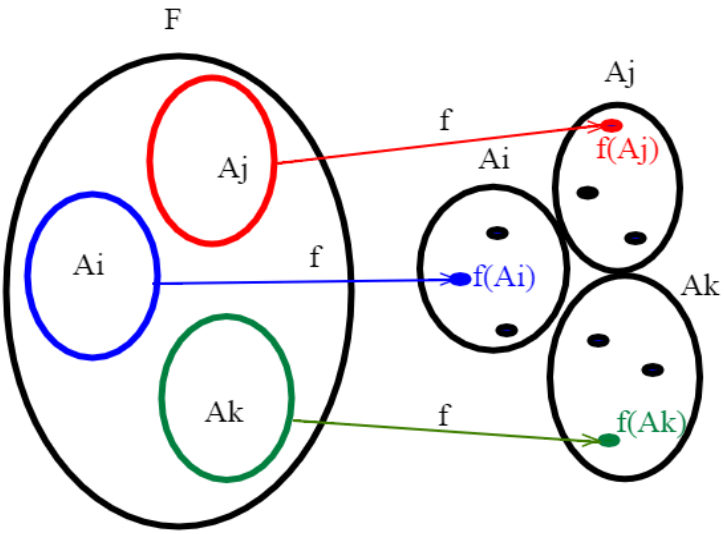
Data una famiglia non vuota di insiemi non vuoti esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento.

Informalmente, quando ci viene data una collezione di insiemi non vuoti possiamo costruire un nuovo insieme "scegliendo" un singolo elemento da ciascuno di quelli di partenza. Praticamene come posso procedere? Devo scegliere un elemento da uno degli insiemi, un altro elemento da un altro degli insiemi, e così via.
E' evidente che se gli insiemi sono infiniti, le scelte devono essere fatte una ad una, e non si termina mai; ma è altrettanto evidente che una scelta di un elemento da ogni insieme è sempre possibile.
Un tipico esempio (***dovuto a B. Russell:***) con cui si spiega il senso dell'assioma è il seguente:
"Per scegliere un calzino da ognuna di infinite paia di calzini serve l'assioma della scelta, mentre l'assioma non e necessario se si vuole scegliere una scarpa da ognuna di infinite paia di scarpe."
Supponiamo cioè di avere un numero infinito di paia di scarpe e di voler definire un insieme che contiene una (e una sola) scarpa di ogni paio; possiamo farlo senza problemi considerando ad esempio l'insieme delle scarpe destre.
I problemi nascono se abbiamo un numero infinito di paia di calzini (supponendo che il destro e il sinistro non siano distinguibili), e vogliamo considerare come prima un insieme che contenga un calzino per ognuno di essi: non possiamo più parlare dell'insieme dei "calzini destri" e non abbiamo in effetti nessun modo di distinguere i due elementi di un paio, cioè di avere una funzione di scelta che ci assicuri di poterne scegliere contemporaneamente uno da ogni insieme.
Per poter dire che un tale insieme comunque esiste dobbiamo invocare l'assioma della scelta.

Enunciato formale dell'assioma.

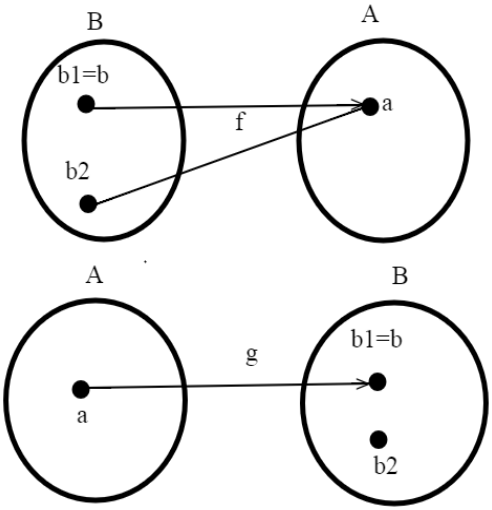
Definiamo prima cosa intendiamo per famiglia ***indiciata*** di insiemi; semplicemente una collezione di insiemi che abbiamo in qualche modo contrassegnato con un indice **i**; abbiamo già trattato collezioni di questo tipo (gli intervalli I_n incapsulati,con **n** numero naturale).
Qui in generale l'indice non è un numero naturale, ma appartiene ad un certo insieme **I**.
Di seguito useremo il simbolo $\in$ *per indicare l'appartenenza di un elemento ad un insieme, e i* ***":"****(due punti) per dire "tale che".*
Passiamo allora all'enunciato dell'assioma:

Data una famiglia $F = \{A_i : i \in I\}$ di insiemi non vuoti A_i, esiste una funzione **f** con dominio **F**, che manda ogni A_i in $f(A_i) \in A_i$.



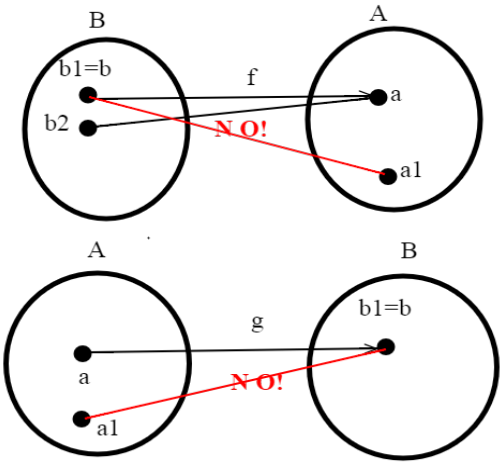
La funzione di scelta associa ad un insieme **Ai** (che possiamo considerare come un elemento della famiglia **F**), un suo elemento **f(Ai)**,considerando **Ai** come insieme.
L'importanza dell'assioma della scelta sta nel garantire l'esistenza di funzioni che potrebbero non essere definibili tramite una regola esplicita.
Cerchiamo di chiarire l'assioma con un esempio; supponiamo di considerare dei sottoinsiemi A_i di **R**, $A_i \subseteq \mathbb{R}$; per l'assioma della scelta, esiste una funzione che ad ogni A_i associa un elemento appartenente ad A_i, ma non sappiamo esprimere tale funzione esplicitamente; nel caso gli A_i siano sottoinsiemi di **N** invece che di **R**, riusciamo ad esplicitare una funzione di scelta in questo modo: **f(**A_i**)=min** A_i, minimo che sappiamo esistere qualsiasi sia il sottoinsieme A_i.
Notiamo che non possiamo applicare la stessa definizione di **f** al caso di sottoinsiemi **Ai** di **R**, in quanto un sottoinsieme di **R** (anche se limitato) non sempre ha minimo (si pensi ad un intervallo aperto).

L'esempio si limita a sottoinsiemi di numeri naturali; In realtà e valido per qualsiasi insieme ben ordinato: **se ogni insieme si può ben ordinare (teorema di Zermelo)**, allora vale l'assioma della scelta:
Consideriamo una famiglia $F = \{A_i : i \in I\}$ di insiemi non vuoti A_i, e l'insieme $\bigcup_{i \in I} A_i$ Se per ipotesi l'insieme $\bigcup_{i \in I} A_i$ è ben ordinato, vuol dire che ogni sottoinsieme **Ai** ha minimo.
Consideriamo la funzione **f** con dominio **F**, che manda ogni A_i nel minimo di **Ai**, $f(A_i) \in A_i$.
Questa è una funzione di scelta per la famiglia **Ai**.
(abbiamo così anticipato che il Teorema di Zermelo, la cui dimostrazione verrà data nei prossimi articoli, implica l'assioma della scelta).
Vediamo subito delle conseguenze dell'assioma della scelta.
Se esiste un funzione f suriettiva f: B–>A, allora esiste una funzione iniettiva g di g: A–>B



Dobbiamo definire una funzione **g: di A —>B**; preso un qualunque a appartenente ad **A**, sappiamo, essendo **f** suriettiva, che esistono uno o più b_i appartenenti a **B**, tali che $f(b_i) = a$; grazie all'assioma ne scegliamo uno e

lo chiamiamo **b** ; definiamo **g(a)=b** e abbiamo una funzione iniettiva (la funzione **g** è iniettiva perchè **f** è una funzione).



Il fatto che **f** sia una funzione ci assicura che lo stesso **b** non possa andare in **a** diversi, e quindi ribaltando dominio con codominio, che **a** diversi possano andare nella stesso **b**, ovvero che **g** non sia iniettiva.
NB: questo ci dice che per dimostrare che |A|<=|B, ovvero che la cardinalità di A è minore di quella di B, basta trovare una funzione suriettiva di |B | in |A|.
Approfitto aprendo una piccola parentesi, per applicare subito questo importante risultato (derivante dall'assioma della scelta) agli insiemi numerabili, abbiamo visto che l'unione di due insiemi numerabili è numerabile, usando il principio di induzione, si può dimostrare che l'unione finita di insiemi numerabili è numerabile(*per n=2* $A_1 \bigcup A_2$ *è vera, supposta vera per n,* $A_1 \bigcup A_2 .. \bigcup A_n$ *è allora numerabile, basta allora scrivere* $(A_1 \bigcup A_2 .. \bigcup A_n) \bigcup A_{n+1}$ *e ho ancora l'unione di due insiemi numerabili*); e se abbiamo una unione numerabile (quindi infinita) di insiemi numerabili?

L'unione di una famiglia numerabile di insiemi numerabili $\{A_n : n \in N\}$ è numerabile.

Essendo ogni **An** numerabile, esiste una corrispondenza biunivoca:
gn: N–>An per ogni n: $\{g_n : n \in N\}$.
Consideriamo adesso l'insieme **N x N** e costruiamo un funzione $f : N \times N \to \bigcup_n A_n$ ponendo $f(n,m) = g_n(m)$; **f è suriettiva**.
Infatti se $a \in \bigcup_n A_n$, allora $a \in A_n$ per qualche n; quindi (essendo g_n suriettiva) esiste m tale che $g_n(m) = a$
Essendo f suriettiva,per quanto visto sopra, esiste una funzione iniettiva $g : \bigcup_n A_n \to N \times N$, quindi $|\bigcup_n A_n| \leq |N \times N| = \aleph_0$
essendo **N x N** numerabile; ma allora $\bigcup_n A_n$ è numerabile, essendo $\aleph_0$ il minimo ordine di infinito.
Nel prossimo articolo, vedremo come l'assioma della scelta implichi qualcosa di molto importante, il lemma di Zorn.
Prima di arrivare alla formulazione del lemma, dovremo però acquisire delle importanti nozioni sugli insiemi ben ordinati.
Il lemma continua a sembrare qualcosa di misterioso,anche un po' per il nome; ma non è altro che una formulazione equivalente all'assioma della scelta, però di più facile applicazione in certe dimostrazioni.

Parte sedicesima: il lemma di ZORN 1/3

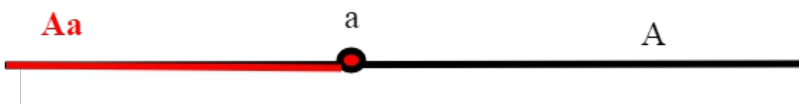
Questo è il primo di una miniserie di (tre) articoli dedicati unicamente al lemma di **Zorn**.
Per poter enunciare il lemma di Zorn, è necessario conoscere certe definizioni e certi risultati sugli insiemi ben ordinati.
Ricordo che gli insiemi ben ordinati sono insiemi totalmente ordinati (ovvero insiemi in cui è possibile il confronto fra due elementi qualsiasi) in cui ogni sottoinsieme non vuoto ammette minimo.
Ne abbiamo visto un esempio: i numeri naturali.
Invece gli insiemi **Z, Q, R** pur essendo totalmente ordinati non sono ben ordinati, in quanto non tutti i sottoinsiemi hanno un minimo.
Gli insiemi ben ordinati sono, per così dire, una "***estensione teorica***" dell'ordinamento dei numeri naturali.
Se nei naturali esistevano concetti come il successivo e l'induzione , in questi insiemi possiamo definire un successore e una sorta di induzione (***induzione transfinita***).
Notiamo che un insieme ben ordinato non è detto che sia numerabile.

Proprietà e definizioni sugli insiemi ben ordinati.

Maggioranti di un insieme.

Dato un insieme **A**, chiamiamo b maggiorante di **A** se **a<=b** qualsiasi sia **a** appartenente ad **A**.

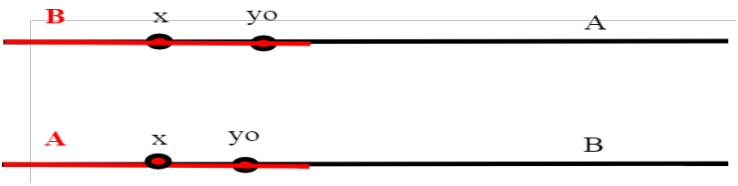
Segmenti iniziali
Dato un insieme ben ordinato **A**, definiamo segmento iniziale di **A** ogni sottoinsieme così definito:
$A_a = \{x \in A : x < a\}$ dove a è un elemento qualsiasi di **A**; essendo l'insieme A_a strettamente contenuto in **A** (a non appartiene ad A_a), il segmento iniziale ***si dice proprio***.



Quando in matematica si dà una definizione su un insieme (tipo quella di buon ordine) la prima cosa che si prova a fare è vedere se la definizione si conserva con le usuali operazioni, tipo l'unione.
Non è però vero che l'unione di buoni ordini sia in generale un buon ordine (vedi più sotto l'insieme delle parti, che non è totalmente ordinato ma può essere rappresentato come unione di insiemi totalmente ordinati) ma se aggiungiamo una condizione sui segmenti iniziali, allora si.

L'unione di un insieme (collezione,famiglia) di buoni ordini che sono uno un segmento iniziale dell'altro è ancora un buon ordine.

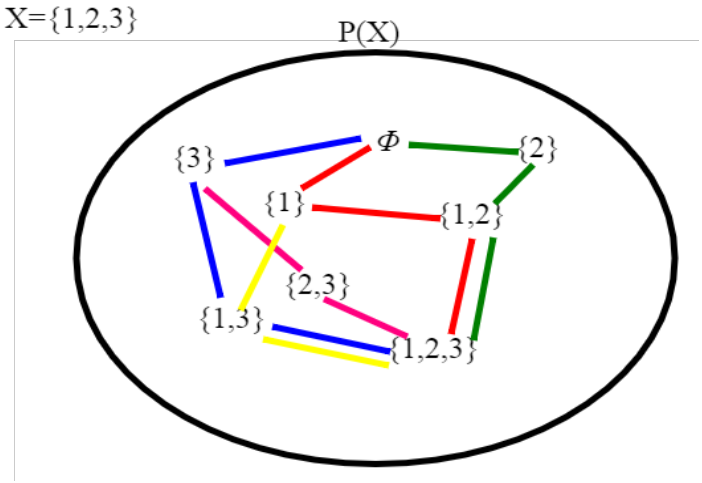
Supponiamo di avere una famiglia (collezione) **F** di insiemi ben ordinati. Consideriamo l'unione di tali insiemi, $X = \bigcup_{A \in F} A$. **X** è totalmente ordinato.
Dati **a; b** appartenenti a **X**, prendiamo **A;B** appartenenti a **F** tali che **a** appartenga ad **A** e **b** appartenga **B**.
Sappiamo che **A** è un segmento iniziale di **B** o viceversa; sia vero per **A**;
Allora **a,b** sono confrontabili in **B**, e quindi nell'unione **X**.
Per vedere se **X** è un buon ordine, verifichiamo che ogni sottoinsieme **Y** di **X** ha minimo.
Consideriamo $y_0 \in Y$; supponiamo che y_0 non sia il minimo di Y, altrimenti avremmo già finito; sia $A \in F$ tale che $y_0 \in A$; consideriamo adesso l'insieme degli $x < y_0$, che apparteranno a qualche **B** di **F** ($x \in B, B \in F$).
(In pratica ogni $x \in X$ apparterrà a qualche **B** della famiglia, essendo appunto **X** unione di questi insiemi).
Sappiamo che **A** è un segmento iniziale di **B** o viceversa.
In ogni caso **x** appartiene anche ad **A**.



$X_{y_0} = \{x \in X : x < y_0\} \subseteq A$ e quindi $Y' = \{y \in Y : y < y_0\} \subseteq A$
(se vale per ogni x in **X**, allora vale senz'altro per quelli in **Y**).
Ma **A** è un insieme ben ordinato, quindi **Y'** ammette minimo.
E il minimo di **Y** in **X** coincide con il minimo di **Y'** in **A** (i minoranti infatti stanno tutti in **A**, come visto, inoltre, il minimo è il massimo dei minoranti).

Insiemi parzialmente ordinati

Qualora non tutti gli elementi di un insieme siano confrontabili si parla di insiemi parzialmente ordinati.
Un esempio di insieme parzialmente ordinato è l'insieme delle parti con l'ordine di inclusione; non tutti gli elementi sono confrontabili.



esempio di insieme parzialmente ordinato.
Gli insiemi **{1,2}** e **{1,3}** non sono confrontabili!

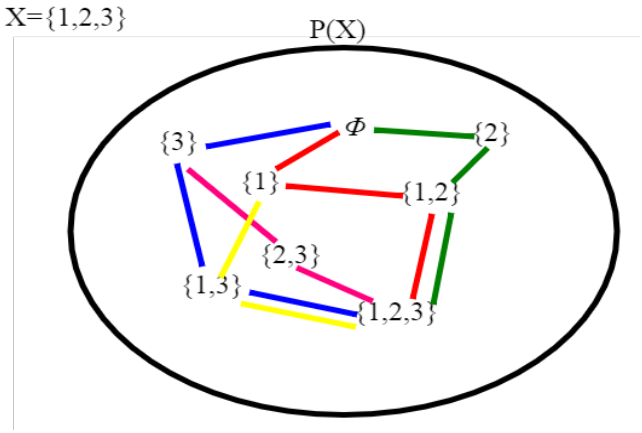
Elemento massimale

Un elemento m appartenente ad **A** si dice massimale se non esiste nessun elemento **a** appartenente ad ad **A** tale che **m < a**.

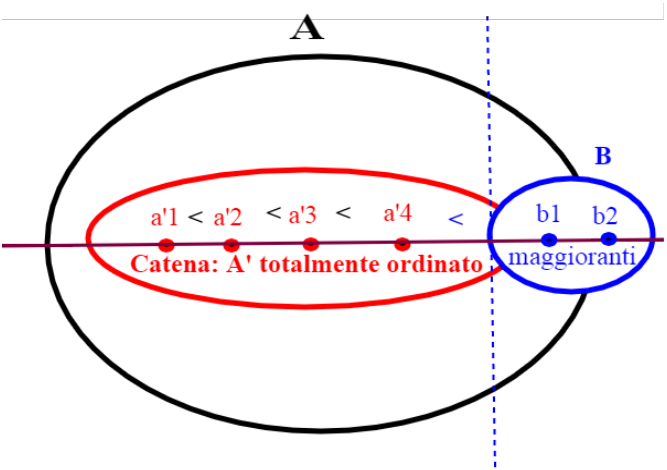
Per un insieme **A** totalmente ordinato, le nozioni di elemento massimo ed elemento massimale coincidono, e sappiamo che il massimo è unico.
Un insieme parzialmente ordinato può invece possedere più elementi massimali.
Nell'esempio sopra di **P({1,2,3})**, **X={1,2,3}** è evidentemente un massimo per **P(X)**; se consideriamo invece **P(X)\{1,2,3}**, ovvero togliamo **{1,2,3}**, abbiamo più elementi massimali, **{1,2,},{2,3},{1,3}**.

Catene negli insiemi parzialmente ordinati

Abbiamo visto che in generale in un insieme **X** parzialmente ordinato, non è detto che ogni elemento sia confrontabile con un altro elemento dell'insieme.
E' però possibile che certi sottoinsiemi di **X** siano totalmente ordinati.



Se come esempio se consideriamo l'insieme delle parti **X=P({1,2,3}** con l'ordine generato dall'inclusione, gli elementi di **Xϕ,{1} {1,2},{1,2,3}** costituiscono un sottoinsieme totalmente ordinato di **X.**
Tali sottoinsiemi prendono anche il nome suggestivo di **catene**.
Se un sottoinsieme **C** di **X** è una catena, un elemento **x** di **X** si dice maggiorante di **C** se per ogni **c** di **C**, **c<=x**.
L'elemento x può appartenere o no a C; nel caso non appartenga, x si dice maggiorante stretto.



Vi chiedo un po′ di pazienza; per arrivare al ***lemma di Zorn*** sono necessari i concetti espressi in questo articolo e nel prossimo.
Se un insieme è ben ordinato, si fa presto a trovare elementi minimi e massimi.
Se non lo è (e questo è il caso più generale) ,ma lo è solo parzialmente, dobbiamo esplorarlo sfruttando dei sottoinsiemi ordinati, che che abbiamo chiamato catene.
La prossima volta ci occuperemo di isomorfismi fra buoni ordini.
Dò solo la definizione di isomorfismo, quale introduzione al prossimo articolo.

Isomorfismi di buoni ordini

Siano dati due insiemi ordinati **A** e **B** una funzione **f : A—> B** crescente, ovvero **x < y** implica **f(x) < f(y)** per ogni **x; y** appartenente ad **A**. Se **f** e anche biunivoca diremo che **f** e un isomorfismo .
Ricordiamo che una funzione crescente è iniettiva.
Quindi basta che **f** sia suriettiva per essere biunivoca.
Non facciamoci spaventare da questa definizione:isomorfismo è una parola che deriva dal Greco, e significa in pratica che due cose hanno la stessa forma; per i matematici due insiemi isomorfi nell'ambito di certe strutture praticamente sono la stessa cosa

Parte sedicesima: il lemma di ZORN 2/3

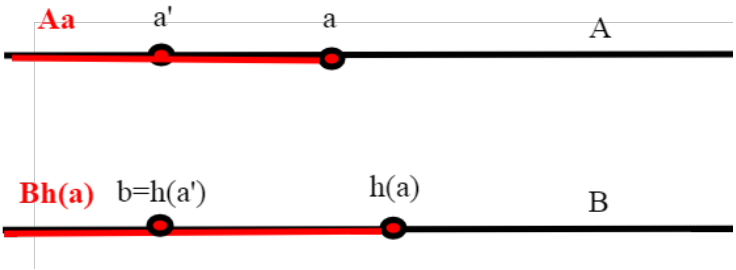
Riprendo la definizione di isomorfismo data alla fine dell'articolo precedente. Questo articolo sarà completamente dedicato alla dimostrazione di un importante teorema sugli isomorfismi, essenziale per la comprensione del lemma di Zorn.

Isomorfismi di buoni ordini

Siano dati due insiemi ordinati **A** e **B** e una funzione f **: A—> B** crescente, ovvero **x < y implica f(x) < f(y) per ogni x; y appartenente ad A**. Se **f** è anche biunivoca diremo che **f** e un isomorfismo .
Ricordiamo che una funzione crescente è iniettiva, quindi basta che f sia suriettiva per essere biunivoca e per essere un isomorfismo.
Non facciamoci spaventare da questa definizione:isomorfismo è una parola che deriva dal greco (ἴσος, isos, che significa uguale, e μορφή, morphé, che significa forma), e significa in pratica stessa forma; per i matematici due insiemi isomorfi nell'ambito di certe strutture praticamente sono la stessa cosa.
Esempio di isomorfismo: consideriamo i numeri naturali **N** e i numeri pari **P**; entrambi sono insiemi ben ordinati; l'applicazione **f: N–>P** che
a $n \to 2 \cdot n$ è una applicazione crescente e copre tutti i numeri pari (è suriettiva). Quindi è biunivoca.

Restrizione di un isomorfismo

Un prosizione molto importante, che ci servirà nel seguito,è la seguente:
Sia **h: A–>B** un isomorfismo.
Per ogni **a** appartenente ad **A**, consideriamo **la restrizione di h** ad A_a, $h_{|A_a} : A_a \to B_{h(a)}$; **h è un isomorfismo tra il segmento iniziale di A generato da a e il segmento iniziale di B generato da h(a).**
(la scrittura $h_{|A_a}$ indica appunto la restrizione di una funzione ad un sottoinsieme del dominio).



Proviamo che $h(A_a) = B_{h(a)}$, ovvero che l'immagine del segmento A_a è uguale a $B_{h(a)}$, ovvero che **h** è suriettiva su $B_{h(a)}$.
Basta dimostrare una doppia inclusione.
Cominciamo da $h(A_a) \subseteq B_{h(a)}$; essendo **h** crescente (**x<a, h(x)<h(a)**).
Proviamo l'altra inclusione $B_{h(a)} \subseteq h(A_a)$; prendiamo un **b<h(a)**; **h** è suriettiva (stiamo considerando tutta la funzione **h**, da **A–>B**), quindi esiste **a'** tale che **h(a')=b**, e **a'<a**, perchè **h** è crescente.
Quindi $a' \in A_a$.
Tre note preliminari, necessarie per la dimostrazione di un importante teorema sugli isomorfismi.

1) Se f: A–>A è un isomorfismo,(cioè se a<a' implica f(a)<f(a')), allora f(a) >=a per ogni $a \in A$?
Se per assurdo la tesi fosse falsa, esisterebbe:
$x = min\{a \in A : f(a) < a\}$
(che è un sottoinsieme di **A**, ma **A** è ben ordinato).
Ma allora f**(x)<x**, **f(f(x))<f(x)** quindi: $f(x) \in \{a \in A : f(a) < a\}$
contro il fatto che x è il minimo.

2) A non è isomorfo ad alcun suo segmento iniziale proprio.
Non possono esistere funzioni **f: A —> Aa** che rispettano l'ordine, perché si avrebbe $f(a) \in A_a$, cioè **f(a) < a**, contro la (1).

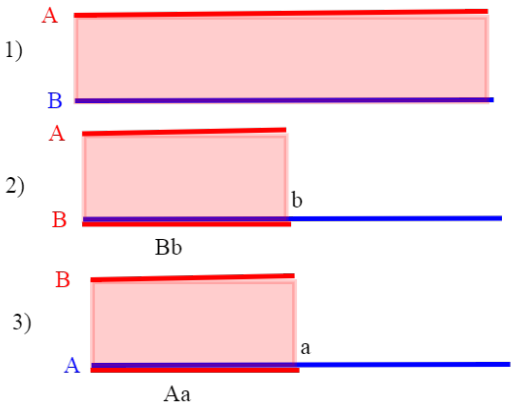
3) Segmenti iniziali propri diversi non sono isomorfi, cioè $a \neq a'$ implica $A_a \ncong A_{a'}$
se $a \neq a'$ allora per esempio **a' < a**; possiamo considerare $A_{a'}$ come un segmento iniziale dell'insieme (ben ordinato) A_a; che per la 2) non può essere isomorfo a $A_{a'}$.

Eccoci arrivati all'enunciato di un teorema molto importante sugli isomorfismi (anche detto **Tricotomia degli insiemi bene ordinati**).

Dati due buoni ordini A e B uno dei due è isomorfo ad un segmento iniziale dell'altro (non necessariamente proprio).

Indichiamo con $A \cong B$ due insiemi isomorfi.
L'enunciato equivale a dire, che dati due insiemi ben ordinati **A, B**, ci possono essere tre possibilità:

1. $A \ncong B$
2. $A \cong B_b$ (**A** è isomorfo ad un segmento iniziale di **B**)
3. $B \cong A_a$ (**B** è isomorfo ad un segmento iniziale di **A**)



Questo è un discorso molto simile a quello che vogliamo dimostrare sulla cardinalità degli insiemi; l'isomorfismo in fin dei conti è una applicazione biunivoca, che in più , nel caso di insiemi ordinati, conserva l'ordine.

Il segmento iniziale di un insieme però altro non è che un sottoinsieme; dire che esiste una applicazione biunivoca di **A** in un segmento iniziale di **B**, vuol anche dire che esiste una applicazione biunivoca di **A** in un sottoinsieme di **B** (e questo nel caso dei cardinali significa che **|A| <=|B|**); se come anticipato possiamo dimostrare che qualsiasi insieme si può ben ordinare, allora grazie a questo teorema avremo risolto il problema della confrontabilità dei cardinali.
Dobbiamo in qualche modo costruire una funzione da **A–>B** che sia biunivoca e conservi l'ordine.
Definiamo un sottoinsieme di A x B in questo modo:
(ricordiamo che a volte per dare una funzione basta definire qual'è il suo grafico)
Consideriamo una corrispondenza (un sottoinsieme di **A x B**) così definita:
$G = \left\{ (a,b) \in A \times B : A_a \cong B_b \right\}$
(i due elementi corrispondono se esiste un isomorfismo fra i sottoinsiemi iniziali che definiscono) questo è un sottoinsieme di **A x B**; vogliamo dimostrare che è il grafico di una funzione **F**, che sarà l'isomorfismo cercato.

Dimostriamo per prima cosa che **G è una funzione, ovvero che è univoca.**
Se **(a,b), (a,b')** appartengono a **G**, allora $A_a \cong B_b$ e $A_a \cong B_{b'}$, quindi $B_b \cong B_{b'}$ (se esiste una applicazione biunivoca **f** fra **A** e **B**, e una **g** fra **A** e **C**, ne esiste intanto una **h** fra **B** e **A**; allora componendo **h** con **g** otteniamo una applicazione biunivoca fra **b** e **C**).
Abbiamo due segmenti iniziali di **B** isomorfi, necessariamente **b=b'** per l'affermazione 3) delle note sopra; quindi **G** rappresenta proprio una funzione (è univoca, ovvero per un **a** abbiamo una sola immagine **b**).
Possiamo allora chiamare **F(a)** l'immagine **b** di **a**.

1) **Il dominio di F è un segmento iniziale di A.**
Se **b=F(a)**, allora $A_a \cong B_b \cong B_{F(a)}$; esiste allora un isomorfismo **h:**$A_a \to B_{F(a)}$; se **a'<a**, possiamo considerare la restrizione di **h** su $A_{a'} \to B_{h(a')}$ che è ancora un isomorfismo, (lo abbiamo visto sopra); perciò, oltre ad **a**, anche **a'** appartiene al dominio di **F**, **dom(F)**.
Quindi il dominio di **F,** chiamiamolo **A'=dom(A)** è un segmento iniziale di **A** (può anche essere tutto **A**, può infatti esistere un isomorfismo di **A–>B** per ogni elemento di **A**).
Inoltre **F(a')=h(a')<b=h(a)=F(a)** quindi **F è crescente**.

2) L'immagine di F è un segmento iniziale di B.
Consideriamo ancora l'isomorfismo **h:**$A_a \to B_b$; se **b'<b**,sia **a'** l'elemento di **A** tale che **h(a')=b'**: consideriamo la restrizione di
h:$A_{a'} \to B_{b'}$ che è ancora un isomorfismo.
F(a')=b', quindi anche l'immagine di **F** è un segmento iniziale, stavolta di **B**.
Chiamiamolo **B'=imm(F)** (che può essere tutto **B** per quello che ne sappiamo).
Quindi **F** è un isomorfismo fra **A'** e **B'** (il dominio infatti è **A'** per definizione; la funzione è iniettiva perché crescente, quindi è biunivoca sull'immagine **B'**).

3) A' e B' non possono essere entrambi segmenti propri.
La funzione **F** è un isomorfismo fra un segmento iniziale **A'** di **A** è un segmento iniziale **B'** di **B.**
Non può essere che **A',B'** siamo entrambi segmenti propri.
Avremmo, se ciò fosse vero, un isomorfismo $F : A_a \to B_b$, e quindi **(a,b)** apparterebbe a **G**, **a** apparterrebbe a $dom(F) = A_a$, **b** apparterrebbe a $imm(F) = B_b$, il che è assurdo.
(**a, b** non possono appartenere ai segmenti A_a, B_b, che sono rispettivamente gli **x<a, y<b**)
Restano perciò le tre possibilità dell'enunciato del teorema:

1. $A' = A, B' = B$; quindi $A \cong B$
2. $A' = A, B' = B_b$; quindi $A \cong B_b$ (**A** è isomorfo ad un segmento iniziale di **B**)
3. $A' = A_a, B' = B$; quindi $B \cong A_a$ (**B** è isomorfo ad un segmento iniziale di **A**)

Siamo ora pronti per affrontare il lemma di Zorn; nel prossimo articolo applicheremo questo importante risultato ad un tipo particolare di insiemi ben ordinati; le **f-catene**.

Parte sedicesima: il lemma di ZORN 3/3

Per dimostrare il lemma di **Zorn**, abbiamo bisogno di un nuovo oggetto, le **f-catene** che sono un particolare tipo di catene che si definiscono a partire da una funzione di scelta, la cui esistenza è assicurata dall'assioma della scelta.
Il nostro scopo finale è usare queste **f-catene** nel caso ammettano sempre almeno un maggiorante, per dimostrare che l'insieme che le contiene ha un elemento massimale.

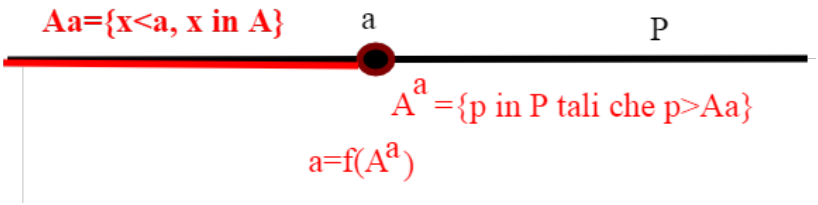
f-catene

Dato un insieme **P**, consideriamo l'insieme delle parti di **P**.
Sappiamo , grazie all'assioma della scelta, che esiste una funzione che associa ad ogni sottoinsieme di **P**, $X \subseteq P$ un suo elemento $f(X) \in X$.

Sappiamo che esiste almeno una f che fa questo; **fissiamone** una.

Consideriamo un sottoinsieme A di P; diremo che a è una f-catena se:

1. **A** è un insieme ben ordinato (è una catena).
2. Qualsiasi sia il segmento iniziale A_a di **A**, (quindi qualsiasi sia $a \in A$) consideriamo l'insieme A^a dei maggioranti **stretti** del segmento A_a**={x<a, x in A}**, cioè i **p** maggiori di qualsiasi elemento di A_a, A^a**={p in P tali che p>**A_a**}**. (1) Se **A** è una f-catena, deve valere la condizione **f(**A^a**)=a**.



(la scrittura p>A_a significa che i**p** sono maggiori di qualsiasi elemento di A_a).
Questa definizione di f-catena può sembrare un po' strampalata, e troppo formale .
Vediamo a cosa serve : ***quello che dobbiamo dimostrare è il lemma di Zorn:***

Se P è un insieme parzialmente ordinato e se ogni sottoinsieme totalmente ordinato (catena) di P ha maggiorante, allora P ha un elemento massimale.

L'idea alla base di tutto, visto che abbiamo un insieme che è solo parzialmente ordinato, è di costruire una catena (che altro non è che un insieme ben ordinato) il più lunga possibile; supponendo di avere dei maggioranti stretti come nelle ipotesi del lemma, ciò si ottiene aggiungendo un elemento alla volta, scelto (tramite la funzione di scelta) fra l'insieme dei maggioranti (è necessario l'assioma della scelta).
Otteniamo così una **f-catena** (f-catena perché dipende dalla funzione **f**).
Se **f** è una funzione di scelta, supponiamo di costruire una f-catena così; sia p_0**=f(P)**, ovvero l'immagine di tutto P; **A={**p_0**}** è una f-catena; infatti $A_{p_0} = \phi$ (abbiamo un solo $a = p_0 \in A$, ma nessun elemento di **A** è minore di p_0), e quindi **P** coincide con A^{p_0} (tutti gli elementi di **P** sono maggiori di quelli di $A_{p_0} = \phi$, visto che non ha elementi); ma $f(A^{p_0}) = f(P) = p_0$; se p_0 fosse un elemento massimale, non potremmo più andare avanti (però avremmo finito).
In caso contrario, per la catena {p_0} abbiamo dei maggioranti; consideriamo adesso i maggioranti di {p_0}, ovvero M= {$p \in P : p > p_0$} e sia p_1=f({$p \in P : p > p_0$}); p_1>p_0 e inoltre l'insieme {p_0,p_1} è ancora una f-catena; infatti la condizione 2) è verificata per a=p_0 (lo abbiamo visto sopra), per **a**=p_1, A_{p_1}**={po}**, A^{p_1}**={p>**p_0**}**, **f(**A^{p_1}**)=f({p>**p_0**})=**p_1.
Se p_1 è massimale, abbiamo finito; altrimenti possiamo andare avanti ancora nella costruzione, perché abbiamo dei maggioranti stretti (che non appartengono ad **A**) appartenenti a **P**.
In generale per iterare il procedimento possiamo fare così: **data la f-catena A**, la estendiamo con:
3) $p_\alpha = f(\{p \in P : p > A\})$;

passando a $A' = A \bigcup \{p_\alpha\}$; chiaramente vale la 1) (l'insieme **A'** è totalmente ordinato) dobbiamo verificare la 2) per ogni $a \in A'$; se $a \in A$ è vero perché **A** è una **f-catena**, ci resta da provarlo per p_α; ma il segmento iniziale $A'_{p_\alpha} = \{a \in A : a < p_\alpha\}$ coincide con **A** e l'insieme dei maggioranti di tale segmento è $A'^{p_\alpha} = \{p \in P : p > A\}$ quindi per la 3) $f(A'^{p_\alpha}) = f(\{p \in P : p > A\}) = p_\alpha$.

Quindi per iterazione costruiamo una catena **A={**$p_0, p_1, p_2, \cdots p_n, \cdot\cdot$**}**; continuiamo finché abbiamo dei maggioranti stretti, allungando al massimo la catena.
Quando non ci saranno più maggioranti stretti, p_α sarà un massimo per la **f-catena** , e un elemento massimale per **P**.
Abbiamo giustificato la definizione di **f-catena** e il suo utilizzo nel lemma di Zorn in modo informale; per chi vuole la dimostrazione rigorosa del lemma, la trova in appendice.

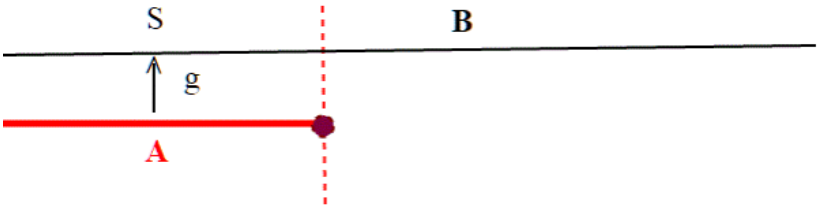
Osservazione sui massimali di un insieme

*Non è vero in generale che ogni insieme parzialmente ordinato debba contenere elementi massimali; basta pensare all' insieme **X** i cui elementi sono i sottoinsiemi finiti di **N**, ordinato rispetto all'inclusione.*
*Chiaramente nessun elemento di **X** è massimale, perché a ogni sottoinsieme finito di **N** posso aggiungere un elemento, ottenendo così un sottoinsieme che lo include, ma ancora finito.*
*Infatti **X** non soddisfa alle ipotesi del **lemma di Zorn**: **C = {{0}, {0, 1}, {0, 1, 2}, {0, 1, 2, 3}, . . . }** è una catena che non ammette alcun maggiorante in **X**. In effetti, un sottoinsieme di **N** che contenga tutti tali sottoinsiemi (che sono tutti finiti) dovrebbe essere **N** stesso, che non è un insieme finito, e quindi non è un elemento di **X**.*

Applicazioni del lemma di Zorn
Nel prossimo articolo dimostreremo che il lemma di Zorn implica che ogni insieme è ben ordinato,fatto noto come teorema di Zermelo; arriveremo così a dimostrare, grazie alla Tricotomia degli isomorfismi, che due numeri cardinali sono sempre confrontabili, che non dimentichiamo, è il nostro obiettivo primario.

Appendice:

DIMOSTRAZIONE RIGOROSA DEL LEMMA DI ZORN:
Due proprietà importanti delle ***f-catene****, che ci semplificheranno la dimostrazione del lemma.*
Se A e B sono due f-catene, allora una è un segmento iniziale dell'altra.
Visto che **A** e **B** sono buoni ordini, uno dei due è isomorfo ad un segmento iniziale dell'altro (per il teorema di Tricotomia degli insiemi ben ordinati, visto nell'articolo predente).
Ad esempio, supponiamo che **g: A –> S** sia un isomorfismo, dove **S** è un segmento iniziale (non necessariamente proprio) di **B**.
Vogliamo dimostrare che **g** è l'identità.



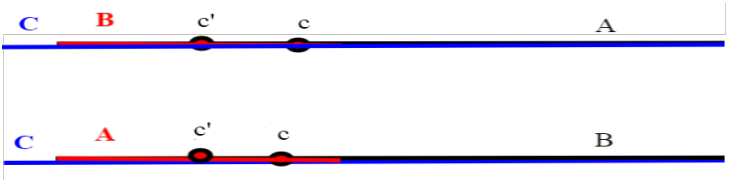
Se per assurdo **g** non è l'identità, allora non sempre i valori di **g(x)** sono uguali a **x**.
Sia $a = min\{x \in A : g(x) \neq x)\}$ ovvero il più piccolo elemento di **A** per cui questo succede(il minimo esiste perché **A** è ben ordinato).
Osserviamo due cose: $g(a) \neq a$, se **x<a g(x)=x**, quindi sul segmento di **A** $A' = A_a = \{x \in A : x < a\}$, **g(x)=x**; esistendo un isomorfismo che conserva l'ordine, se consideriamo l'insieme:
$B_{g(a)} = \{x \in B : x < g(a)\}$ che è un segmento iniziale di **B**, tale segmento coincide con A_a.
Osserviamo innanzitutto, che se x=g(x), allora x appartiene sia ad A che a B; dobbiamo poi provare una doppia inclusione;

Se $x \in A_a$, allora **x<a**; **x=g(x)<g(a)** essendo **g** isomorfismo.
Dunque $A_a \subseteq B_{g(a)}$;

se $x \in B_{g(a)}$, **x<g(a)**; ma allora esiste **a'** tale che **x=g(a')**; **a' <a** perché **g(a')<g(a)**; ma se **a'<a**, **g(a')=a'=x, x=a'<a**, quindi **x** appartiene ad **Aa,** $B_{g(a)} \subseteq A_a$.
Ma se tali segmenti sono uguali, anche i maggioranti lo sono; $A^a = B^{g(a)},\ a = f(A^a) = f(B^{g(a)}) = g(a)$, contrariamente al fatto che abbiamo supposto $g(a) \neq a$.

L'unione C di tutte le f-catene di un insieme P è una f-catena.

Essendo poi C unione di tutte le f-catene è l'**f-catena massima**.
Sappiamo che l'unione di un insieme di buoni ordini che sono un segmento iniziale dell'altro è ancora un buon ordine (vedi Zorn 1/3).
Abbiamo poi visto che date due **f-catene**, una è sempre segmento iniziale dell'altra (quindi sottoinsieme dell'altra) e quindi è ancora una f-catena.
Supponiamo quindi che $C = \bigcup_{A_i \in F} A_i$ sia l'unione di certi **Ai**, tutti f-catene.
Qualsiasi sia $c \in C$, preso un segmento iniziale **Cc** dobbiamo dimostrare che $c = f(\{p \in P : p > C_c\})$.
Se $c \in C$ allora $c \in A$ per qualche **A** che compone l'unione.
Sappiamo che **A** è una f-catena, quindi se **Ac** è il segmento iniziale corrispondente a c in A, $c = f(\{p \in P : p > A_c\})$.
Vogliamo provare che:
$\{p \in P : p > C_c\} = \{p \in P : p > A_c\}$ da cui seguirà $c = f(\{p \in P : p > C_c\})$; se per assurdo i due insiemi non sono uguali, essendo $A \subseteq C$, esisterà **c'<c** che sta in **C** ma non in **A**.



Tale **c'** dovrà appartenere a qualche **B** dell'unione, ma sappiamo che o **A** è segmento iniziale di **B** o viceversa; in entrambi i casi (vedi disegno) **c'** appartiene anche ad **A**.
(Ricordiamo la definizione di elemento massimale.
Un elemento **m** appartenente ad **S** si dice massimale se non esiste nessun elemento **a** appartenente ad ad **S** tale che **m < a**.)
Siamo pronti per dimostrare il lemma, di cui ripetiamo l'enunciato:

Lemma di Zorn: Se P è un insieme parzialmente ordinato e se ogni sottoinsieme totalmente ordinato (catena) di P ha maggiorante, allora P ha un elemento massimale.

Grazie ai risultati già elaborati sulle f-catene, la dimostrazione diventa relativamente immediata: sia **C** l'unione di tutte le **f-catene** di **S**.
Sappiamo che **C** è una **f-catena**, e quindi è la **f-catena massima**.
Non esistono maggioranti stretti di **C** (altrimenti la catena **C** potrebbe essere estesa).
Da questo segue che un elemento maggiorante della catena **C** (che deve sempre esistere) è necessariamente il massimo di **C**, ed è inoltre un elemento massimale per **P**. Infatti se **m** è tale **massimo**, se non fosse massimale per **P**, esisterebbe **n>m**, **n** appartenente a **P**.
Avremmo che l'insieme **M** dei maggioranti di **C** non è vuoto (contiene almeno **n**) e quindi la catena ottenuta estendendo (unendo) **C** con **f(M)** (che è ancora una **f-catena**) sarebbe più grande di **C**, mentre sappiamo che **C** è **l'unione di tutte le f-catene di P**.

Parte diciasettesima: il teorema di Zermelo.

(o del buon ordinamento)

Adesso che abbiamo a disposizione il lemma di Zorn, siamo in grado di dimostrare Il **teorema di Zermelo (o del buon ordinamento).**

*Ogni insieme **X** è ben ordinabile, ovvero è possibile trovare per **X** un ordinamento che sia totale, e per cui ogni sottoinsieme **Y** di **X** abbia minimo.*

Per dare un buon ordine, è necessario dare un insieme e un ordine fra i suoi elementi.
Se **B** è un sottoinsieme di **X**, indichiamo con la coppia $(B, \leq_B)$ un certo buon ordine.
Consideriamo adesso l'insieme di tutti questi buon ordini, e chiamiamolo BO; dunque:
$BO = \{(B, \leq_B)) : B \subseteq X, (B, \leq_B) : buonordine\}$; in pratica costruiamo un nuovo insieme, BO, i cui elementi sono dei *buoni ordini*.
Ci vuole un certo sforzo di astrazione per comprendere ciò.
L'insieme BO non è vuoto: infatti se consideriamo dei sottoinsiemi **B finiti** di **X**, essi sono ben ordinabili (1) (vedi nota in fondo alla pagina).
Stabiliamo adesso su BO un ordine in tal modo; diremo che $(B, \leq_B) \preceq (B', \leq_{B'})$ se **B** è un segmento iniziale di **B'**; questo equivale a richiedere tre cose:

1. $B \subseteq B'$
2. la relazione $\leq_{B'}$ ristretta a **B** coincida con $\leq_B$
3. se x$\leq_{B'}$, **b** con **b** appartenente a **B**, allora anche **x** appartiene a **B** (non basta essere sottoinsiemi per essere segmenti iniziali, ci vuole una condizione in più).

La relazione $\preceq$ è una relazione d'ordine (parziale) su BO.
Semplifichiamo un po' le notazioni; indichiamo con $A_<$ la coppia (A,$<_A$), $B_<$ la coppia (B,$<_B$), $C_<$ la coppia (C,$<_C$).

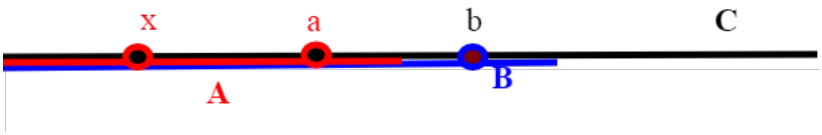
Dobbiamo verificare le tre proprietà:

1) simmetrica:
sia $A_<$ qualsiasi; chiaramente A è segmento iniziale (non proprio) di se stesso, quindi:
$A_< \preceq A_<$.

2) antiriflessiva:
dobbiamo dimostrare che se $A_< \preceq B_< \; B_< \preceq A_<$ allora $B_<$=$A_<$; ma se **A** è sottoinsieme di **B** e **B** sottoinsieme di **A** allora **A=B**.

3) transitiva:
dobbiamo provare che da $A_< \preceq B_<, B_< \preceq C_<$ segue $A_< \preceq C_<$.

- $A \subseteq B \subseteq C \Rightarrow A \subseteq C$
- La relazione $\leq_C$ ristretta a B coincide con$\leq_B$; anche la relazione $\leq_B$ ristretta su A coincide con $\leq_A$; ne segue che $\leq_C$ ristretta su A coincide con $\leq_A$.
- Se a appartiene ad **A** e **x<A**, anche **x** appartiene ad **A** (è segmento iniziale di **B**)



Consideriamo ora una qualsiasi catena **C** di elementi di BO:
$(B, \leq_B) \preceq (B', \leq_{B'}) \preceq (B'', \leq_{B''}) \preceq (B''', \leq_{B'''}) \ldots$;
sappiamo da un articolo precedente che l'unione di un insieme (collezione,famiglia) di buoni ordini che sono uno un segmento iniziale dell'altro è ancora un buon ordine , quindi un elemento di BO, e inoltre tale elemento è un maggiorante per la catena; siamo nelle ipotesi del lemma di

Zorn (per ogni catena esiste un maggiorante) quindi esiste un elemento massimale $(M, \leq_M) \in BO$.
Resta da dimostrare che **M=X**.
Se fosse $M \subset X$, possiamo prendere un elemento $\gamma \in$ **X\M**.
Notiamo che γ è un elemento per così dire "libero", in quanto non è in relazione con alcun elemento di **M**.
Consideriamo l'insieme (**sottoinsieme di X**) **D=M U {**γ**}**; definiamo un buon ordine in tal modo, (**M U {**γ**},**$\leq$) dove poniamo γ maggiore di tutti gli elementi di **M**.
In pratica, su **M** abbiamo l'ordine $\leq_M$ qualsiasi siamo **x,y** in **M**, mentre al più può succedere che uno dei due (o entrambi) siano uguali a γ.
Ma allora (**D,**$\leq$) sarebbe un buon ordine, e **M** segmento iniziale di **D**, generato da γ, quindi $(M, \leq_M) \preceq (D, \leq)$; ma allora:
$(M, \leq_M) \in BO$ non sarebbe più massimale.
Quindi **M=X**; ma allora $(X, \leq_X) \in BO$, quindi **X** è totalmente ordinato.

Conseguenza immediata del teorema di Zermelo è la confrontabilità dei numeri cardinali.
Riprendiamo un teorema sugli isomorfismi (dimostrato nella parte sedicesima 2/3) :
Dati due buoni ordini A e B uno dei due è isomorfo ad un segmento iniziale dell'altro (non necessariamente proprio).

Se consideriamo due insiemi (infiniti) **A** e **B** qualsiasi, possiamo applicare ad essi il teorema di Zermelo e ben ordinarli.
Siamo adesso nelle ipotesi del teorema sugli isomorfismi; l'isomorfismo in fin dei conti è una applicazione biunivoca, che in più , nel caso di insiemi ordinati, conserva l'ordine.
Il segmento iniziale di un insieme è anche un sottoinsieme; dire che esiste una applicazione biunivoca di **A** in un segmento iniziale di **B**, vuol anche dire che esiste una applicazione biunivoca di **A** in un sottoinsieme di **B** (e questo nel caso dei cardinali significa che |**A**| <=|**B**|).
Il fatto che il segmento iniziale possa non essere proprio si traduce con la possibilità che sia |**A**|=|**B**|.
La tricotomia dei numeri cardinali si esprime anche cosi:
Dati due insiemi **A,B** esistono tre possibilità:

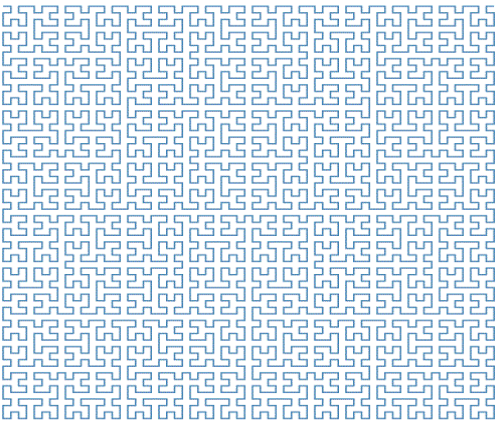
1. **|A|<|B|**
2. **|A|>|B|**
3. **!A|=|B|**

nota (1)
Sebbene non sia mai sottolineato , il fatto che **BO** non sia vuoto perché i sottoinsiemi **B** finiti di **X** sono ben ordinabili è un punto fondamentale della dimostrazione.
Finché siamo nel finito non ci sono problemi; possiamo dare un ordine in un insieme come vogliamo, mediante una relazione fra elementi di **B X B**; per trovare il minimo di un insieme finito , che senz'altro esiste, possiamo applicare l'algoritmo che meglio ci aggrada.

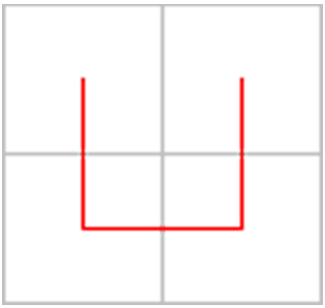
Parte diciottesima: La curva di Peano- Hilbert

Qual'è la cardinalità del piano? A occhio e croce ben di più di quella della retta, che ha cardinalità **c**, pari dunque a quella dei numeri reali.
Invece avremo una gran bella sorpresa: la cardinalità del piano è uguale a quella della retta.
Questo fatto è fortemente controintuitivo.
Lo stesso Cantor , in una lettera a Dedekind ,dove ne riporta la dimostrazione, scrive: "Lo vedo, ma non lo credo".
Premettiamo innanzitutto che possiamo limitarci a confrontare il segmento unitario con il quadrato di lato unitario.
Infatti abbiamo visto nell'articolo sulla Cardinalità di **R** che **[0,1]** ha la stessa cardinalità di **R**; se consideriamo adesso il quadrato **[0,1] x [0,1]** e la funzione biunivoca in **R x R** così definita: **(x,y)—> (f(x),f(y))** che è costruita quindi partendo dalla funzione biunivoca **f**.
essendo quindi **|R|=| [0,1]| e |R x R |=| [0,1] x [0,1]|** possiamo limitarci a confrontare il segmento unitario con il segmento unitario.
Ci sono più modi per fare questo confronto, noi cominceremo con **la curva di Peano-Hilbert**, per poi analizzarlo (nel prossimo articolo) in modo più generale usando **il lemma di Zorn**.
Lo facciamo anche per introdurre un argomento un po' curioso, quello delle **curve frattali**, che lo stesso Hilbert definì "**curve mostruose**".
Se pensiamo ad un coperchio di una scatola, e ad una corda con un certo spessore, possiamo piegare la corda in tanti tratti e occupare tutta la superficie del coperchio, con una certa lunghezza finita.
Questo perché la corda ha un certo spessore.
Ma possiamo farlo anche con una corda senza dimensione? **Si!**, anche se in questo caso la corda non avrà una lunghezza finita.
L'idea è quella di generare una curva che riesca a coprire tutti i punti del piano.
Tale curva è nota come curva di **Peano-Hilbert**, ed è una curva generata con un metodo ricorsivo.
Riporta entrambi i nomi dei due matematici, perché fu concepita da Peano e poi perfezionata da Hilbert.
Il nostro intento è quello di trovare un metodo per disegnare una curva (ovvero una linea continua) che copra tutti i punti del quadrato; non certo disegnarla perché è impossibile.
Ma fornire un algoritmo da dare in pasto a un calcolatore per ottenere im-

magini approssimanti come la seguente:

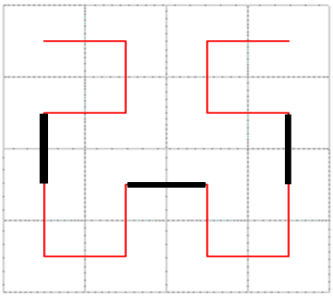


Ci sono diversi algoritmi per disegnare la curva di Peano; il modo più semplice a mio avviso per disegnare la curva è cominciare **dividere il quadrato iniziale di lato uno** in quattro quadratini di **lato 1/2**; dobbiamo riempire tutto il quadrato in modo ricorsivo; consideriamo i centri di questi quattro quadrati e uniamoli ottenendo l'elemento base:

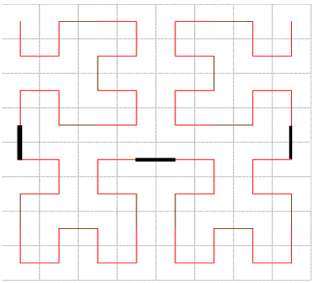


Passo1:In questo modo qualsiasi punto del quadrato dista dalla curva meno di ½.

Vogliamo adesso costruire il secondo passo; divido il quadrato in 16 quadratini; devo replicare partendo dall'elemento base, quindi disponendolo su i quattro quadrati più grandi;



Passo2: in questo caso qualsiasi punto del quadrato dista dalla curva meno di ¼.
Voi capite che questo equivale a congiungere i centri dei sottoquadratini; ma in che ordine? Dobbiamo costruire una poligonale; un modo può essere mantenere nei due quadrati inferiori lo stesso orientamento dell'elemento di base, e ruotare i superiori di 90° in modo opportuno.
Infatti poi dobbiamo connettere (segmenti neri) gli elementi per ottenere una poligonale; se ruotassimo per esempio di 90° a destra l'elemento del primo quadrante in alto, non riusciremmo a chiudere la poligonale.
Adesso che abbiamo a disposizione un elemento base un po' più grande, continuiamo con la costruzione; riportiamo la costruzione 2 (ridotta di un quarto) in una nuova suddivisione, ridotta sempre di un quarto, e mantenendo l'orientamento come nel caso precedente.



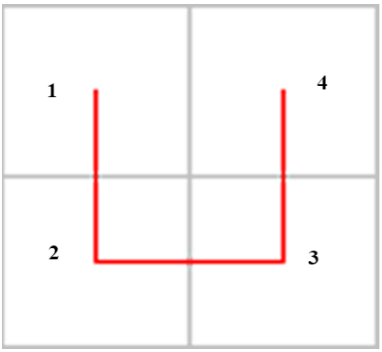
Passo3: in questo modo qualsiasi punto del quadrato dista dalla curva meno di 1/8.
Al passo uno abbiamo 4 suddivisioni; al due 16 e al tre 64.
Se indichiamo con n il passo della costruzione, le suddivisioni sono $2^n 2^n = 2^{2n}$, mentre la lunghezza del lato della suddivisione è $1/2^n$; la distanza di un punto qualsiasi del quadrato iniziale è minore o uguale a $1/2^n$; si intuisce che quando n va all'infinito, riusciamo a coprire tutto il quadrato.
Per adesso abbiamo fatto solo una costruzione geometrica; di seguito definiremo una curva vera e propria,con funzione parametrica, e dimostreremo che è suriettiva.

Curva parametrica piana

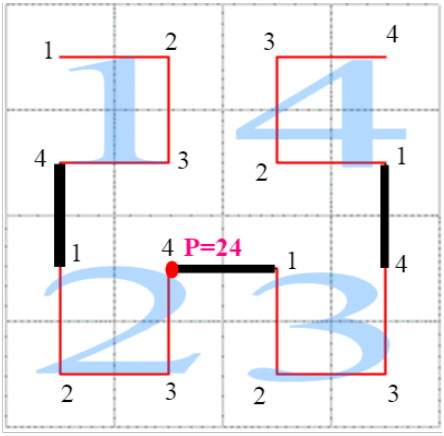
Una curva parametrica piana è una curva che giace interamente in un piano ed è identificabile da una funzione continua da un intervallo di **R** in un sottoinsieme **Q** di **R x R.**
h:[a,b] —->Q⊆ R x R; in pratica una funzione che associa ad un numero reale un punto nel piano **R x R, t—->(x(t),y(t))**; facciamo un esempio.
$h(t(\,) = (t,t^2)$ rappresenta una parabola.

Definizione della curva di Peano come curva parametrica

Dividiamo il quadrato iniziale in quattro quadratini di lato 1/2 , che numeriamo con i numeri 1,2,34.
L'ordine di numerazione è quello di percorrenza della prima curva approssimante:

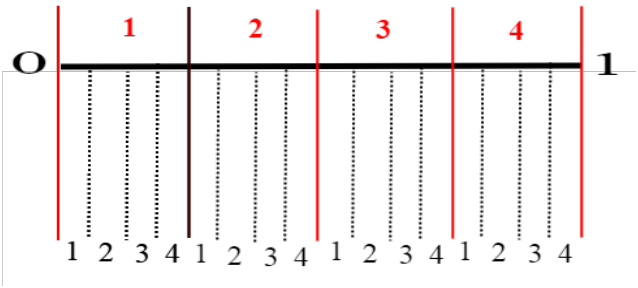


Dividiamo ora ciascuno dei quattro quadrati numerati in altri quattro quadratini, ottenendo in tutto 16 quadratini (di lato ¼).

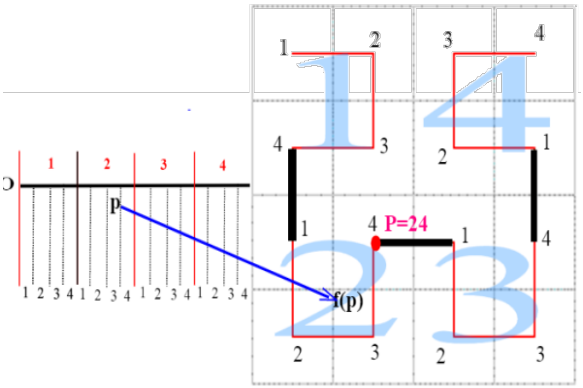


Il punto **P** del disegno che appartiene al centro di un quadratino potrà essere individuato dalla dalla successione di numeri **24**; **2** è il quadrato della prima suddivisione, **4** il quadratino della seconda suddivisione.
Chiaramente questo è un caso semplice; il punto appartiene al centro di uno dei quadratini.
Pensiamo al caso generale ; dato un punto qualsiasi appartenente al quadrato iniziale, come possiamo individuarlo con un procedimento iterativo? Ripetiamo la costruzione per ogni quadratino a cui il punto appartiene e la scriviamo ottenendo una successione di cifre (**da 1 a 4**).

Il centro della successione di quadratini inscatolati convergerà al punto dopo infinite iterazioni.
Il punto corrisponderà ad una successione infinita di cifre con valori compresi **fra 1 e 4**.
Avevamo promesso di dare una espressione parametrica per la curva di Peano Hilbert; cosa significa? Dobbiamo dare una funzione che associ ad un certo intervallo della retta una coppia di di valori nel piano, ovvero un punto del piano.
Consideriamo l'intervallo **[0,1]**;



Suddividiamo l'intervallo in 4 parti, che numeriamo da 1 a 4 da sinistra verso destra; ciascuno di questi intervalli lo dividiamo ancora in quattro parti (e li numeriamo da 1 a 4 da sinistra verso destra;; iteriamo poi questo procedimento ai 16 intervalli generati,all' infinito.
Dato un punto qualsiasi dell'intervallo **[0,1]**, consideriamo la successione infinita di intervalli incapsulati che lo contengono; la successione di cifre che corrisponde agli intervalli si ottiene prendendo come prima cifra l'intervallo di ordine uno. seconda cifra l'intervallo di ordine due, e così via.
Praticamente si procede così; data un punto **p** nel'intervallo **[0,1]** dividiamo l'intervallo in quattro parti; consideriamo l'intervallo che lo contiene (la sua posizione 1,2,3,4 ci dà la prima cifra della successione); dividiamo l'intervallo trovato ancora in quattro parti e prendiamo ancora l'intervallo che lo contiene.
Otteniamo una successione di intervalli incapsulati, che corrisponde anche ad una successione numerica (in genere) infinita di cifre che vanno da 1 a 4, ad esempio 23…



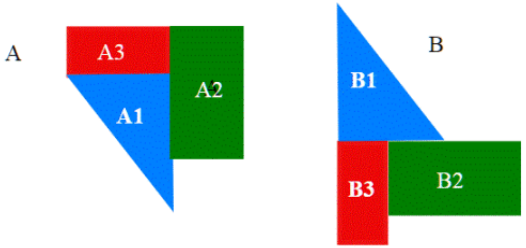
Il punto **f(p)** nel quadrato unitario è contenuto nei rispettivi quadrati 23… Viceversa, dato un qualsiasi punto del quadrato, esso sarà inscatolato in una successione di quadrati **xyz...** il numero corrispondente nell'intervallo **[0,1]** lo troviamo negli intervalli corrispondenti a **xyz...** dunque la funzione **f** (***curva di Peano***) è suriettiva.
Nell' articolo sull'assioma della scelta, abbiamo dimostrato che **Se esiste una funzione f suriettiva f: B–>A, allora esiste una funzione iniettiva g di g: A–>B**
Indichiamo con **Q** il quadrato unitario, e con **I l'intervallo [0,1].**
Sappiamo che **|I|<=|Q|** (Immersione, ovvero **I** è contenuto in **Q**).
Essendo **f:I–>Q** suriettiva, esiste una funzione iniettiva di **Q:—>I**, ovvero **|Q|<=|I|**.
Quindi **Q|=|I|**.

Parte diciannovesima: l'insieme di Vitali

Dopo una lunga pausa ho pensato di riprendere gli articoli sugli insiemi infiniti e sulle loro applicazioni a cose decisamente "strane".
Nella parte quindicesima, abbiamo visto la necessità di inserire nella teoria degli insiemi un assioma, detto "assioma della scelta" che ci permette di effettuare infinite scelte su famiglie di insiemi.
L'assioma della scelta è proprio un assioma, pur avendo una giustificazione intuitiva; c'è chi lo prende per buono e chi no.
Accettare l'assioma della scelta porta a situazioni paradossali, come ***l'insieme di Vitali e il paradosso di Banach***, che spero di riuscire a sviscerare.
Rinunciare a tale assioma comporta invece la perdita di importanti risultati sugli insiemi infiniti, quali ad esempio l'unione numerabile di insiemi numerabili, il **teorema di Zermelo** o l'equivalente **lemma di Zorn**.
Anticipiamo una nozione che ci servirà più volte nell'articolo:

Equidecomponibilità

Parliamo di insiemi.
Indichiamo con questo simbolo⊔ l'unione disgiunta di **C,D:** $C \sqcup D$**.**
E' semplicemente l'unione di due insiemi disgiunti, ossia tali che $C \cap D = \varnothing$.
Diciamo che due sottoinsiemi A, B sono equidecomponibili se è possibile trovare degli insiemi (disgiunti) **A1,..An** e dei movimenti rigidi Θ tali che
$A_1 \sqcup A_2 ..... \sqcup A_n = \Theta(A_1) \sqcup \Theta(A_2) ..... \sqcup \Theta(A_n)$.
Come al solito è più difficile dirlo che farlo: Vediamolo nel piano: nella figura A e B sono degli insiemi apparentemente molto diversi , ma sono equidecomponibili.



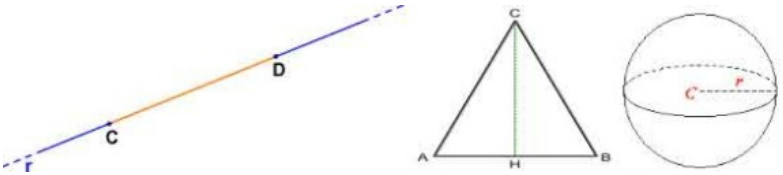
B1=θ1(A1) traslazione + rotazione 180

B2=θ2(A2) traslazione+rotazione 90°

B3=θ3(A3) traslazione+ rotazione 90°

Misurare gli insiemi

Ci proponiamo di definire cos'è la misura di un insieme.
Chiamiamo μ tale misura,che agisce sui sottoinsiemi di R^n.
Avremo quindi una applicazione definita su sottoinsiemi di R^n a valori in $[0, +\infty]$, ovvero sui numeri reali positivi o nulli .
La misura è dunque una funzione $\mu : P(R^n) \to [0, +\infty]$.
Misurare un segmento è facile, così pure altre semplici figure geometriche nel piano, o i solidi principali nello spazio; In ogni caso otteniamo tramite formule più o meno complesse una lunghezza, una superficie o un volume.



Tutti sappiamo calcolare la misura di questi tre oggetti geometrici.

La stessa cosa non si può dire per un **insieme qualsiasi di punti**, che siano essi in R, R^2, R^3.
Non ci preoccupiamo però di come calcolare una tale misura, ossia quali tecniche usare. Ma quali proprietà deve avere una tale misura? Bè, ci fareb-

be comodo scomporre l'insieme che misuriamo in parti e poi sommare le misure delle varie parti.
Per applicare tale proprietà, abbiamo proprio introdotto la nozione intuitiva di equidecomponibilità; possiamo pensare di scomporre un insieme **A** in tanti pezzi **A1..An** che siano **disgiunti.**
Cosa ci aspettiamo da questa misura μ?
Che la somma delle misure dei singoli pezzi **A1..An** sia uguale alla misura dell'unione dei pezzi, e di conseguenza alla misura di **A**.
Scomponiamo **A** nell'unione di tanti pezzi disgiunti: in modo formale:
$A = \bigcup_{k}^{N} A_k$; questa scrittura significa che facciamo variare **k** nell'insieme **N**, che è l'insieme dei numeri naturali.
Si parla di unione numerabile.
La nostra misura deve avere perciò una "numerabile additività":

$$\mu(A) = \mu(\bigcup_{k}^{N} A_k) = \sum_{k}^{N} \mu(A_k)$$

Chiaramente il fatto che valga l'additività nel caso di unione numerabile, implica che valga anche quando parliamo di unioni finite.
Basta considerare infatti gli **Ai** tutti vuoti da un certo punto in poi.
Cos'altro deve avere la nostra misura per definirsi valida per i nostri scopi?
Se misuriamo un segmento, la sua misura deve chiaramente coincidere con la misura elementare.
Qual'è la misura elementare di **[0.1]**? E' chiaramente 1.
Quindi $\mu([0,1]) = 1$>0.
** In questo articolo avevamo accennato al gruppo delle isometrie piane, ossia ai movimenti rigidi.
Vogliamo anche che la nostra misura sia invariante per movimenti rigidi.
Detto in parole povere: se prendiamo un insieme e lo facciamo ruotare o traslare e lo misuriamo prima e dopo dobbiamo avere lo stesso risultato. In modo formale, indicando con Θ una isometria di $R^n \to R^n$:
$\mu(A) = \mu(\Theta(A))$.
Le proprietà che vogliamo dalla nostra misura, ovvero che ci farebbero comodo, sono quindi queste.
Sono cose abbastanza intuitive; non è invece intuitivo che se ci mettiamo in **R** e vogliamo trovare una tale misura, ci accorgiamo che non esiste.

Ed è qui che interviene Vitali con il suo insieme: tale insieme non è misurabile.
In genere la dimostrazione di questo fatto viene tralasciata perché ritenuta complessa, ma con quello che abbiamo fatto sugli infiniti di Cantor, possiamo provarci.

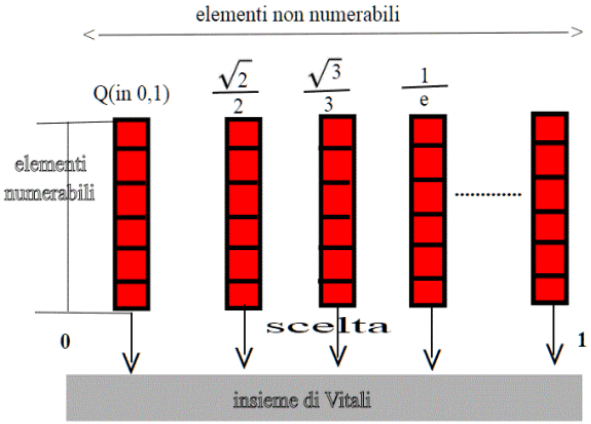
L'insieme di Vitali.

Mettiamoci sulla retta, che è pur sempre un caso di spazio R^n, con **n=1.**
Consideriamo l'intervallo **[0,1]**: in esso definiamo la relazione d'equivalenza:
$x \sim y$ se e solo se $x - y \in Q$.
Detto in parole povere, consideriamo nell'intervallo **[0,1]** coppie tali che la loro differenza sia razionale.
Riuscire a visualizzare quali siano le classi che origina tale definizione è impresa ardua; sta di fatto che però è una relazione di equivalenza.
Infatti:

- i) è riflessiva in quanto **x-x=0** è un numero razionale
- ii) è simmetrica: se **x-y=q, y-x=-q**
- iii) è transitiva: **(x-z)=(x-y)-(y-x)**; essendo le due differenze a secondo membro razionali, anche il primo membro è razionale.

Notiamo che se prendiamo una classe qualsiasi, essa è un insieme numerabile.
Una classe, per esempio, è costituita da numeri razionali in **[0,1]**.
Infatti presi qualsiasi due numeri razionali in **[0,1]**, la loro differenza è ancora un numero razionale.
Chiaramente l'insieme dei razionali in **[0,1]** è un insieme numerabile.
Preso un qualsiasi numero irrazionale in **[0,1]**, ad esempio $\frac{\sqrt{2}}{2}$, per avere tutti gli elementi della sua classe, basta sommargli un razionale **q**, ovvero i numeri equivalenti sono del tipo $\frac{\sqrt{2}}{2} + q$, con l'avvertenza di prendere i razionali per cui $0 \leq \frac{\sqrt{2}}{2} + q \leq 1$; anche qui abbiamo una infinità numerabile di razionali che soddisfano a tale richiesta.

Per chi non ne fosse convinto, prendiamo un **q** positivo e tale $\frac{\sqrt{2}}{2} + q \leq 1$; cioè $q \leq 1 - \frac{\sqrt{2}}{2}$=**0,292…**
quindi basta prendere un **0<q<0.29=29/100**; tutti i **q=29/n** con **n>100** vanno bene, e sono quindi una infinità numerabile.



Per quello che abbiamo visto sulle classi di equivalenza, esse formano una **partizione** dell'intervallo **[0,1]**.
Poiché ogni classe di equivalenza è un insieme numerabile, la famiglia delle classi di equivalenza ha la potenza del continuo.
Infatti se consideriamo l'insieme di tutte le classi di equivalenza indotte dalla relazione appena definita, queste devono essere una ***infinità non numerabile***, poiché se fossero un'infinità numerabile avremmo che l'insieme **[0,1]** stesso sarebbe numerabile (in quanto unione numerabile di insiemi numerabili).
Questo fatto (unione numerabile di insiemi numerabili) lo avevamo visto nella parte quindicesima a proposito dell'assioma della scelta.
Supponiamo adesso di scegliere un rappresentante per ogni classe di equivalenza.
Chiamiamo **V** tale insieme; che questa scelta si possa fare è garantito dall'assioma della scelta.
Quindi V altro non è che l'insieme quoziente della relazione $\sim$.

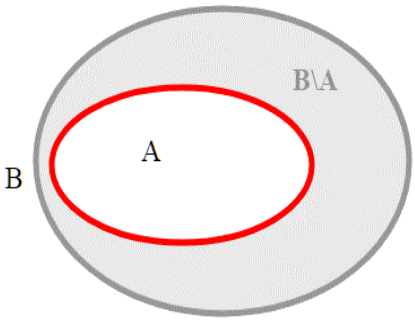
Dato adesso un razionale **x**, definiamo traslato dell'insieme **V**, e lo indichiamo con **V+x**, l'insieme :
V+x={x+y con y appartenente a V}.
Consideriamo adesso due numeri razionali **q1,q2**; vogliamo dimostrare che se **q1<>q2** allora i due insiemi traslati di **V**. **q1+V, q2+V** sono insiemi disgiunti, ovvero non hanno elementi in comune.
Supponiamo per assurdo che **x** appartenga all'intersezione.
Vogliamo dimostrare che **q1=q2**;
sappiamo che **x=q1+y1** con **y1** appartenente a **V**; allo stesso modo, **x=q2+y2**, con **y1** appartenente a **V**.
quindi:
x=q1+y1
x=q2+y2
sottraendo membro a membro otteniamo:
0=q1-q2+y1-y2;
y1-y2=q2-q1; ma **q2-q1** è un numero razionale, quindi **y1,y2** stanno nella stessa classe d'equivalenza.
Ma **V** ha un solo elemento per ogni classe di equivalenza, quindi **y1=y2**.
Di conseguenza **q1=q2**.
Trovandoci sulla retta quali isometrie sono possibili? Bè le traslazioni.
Perché abbiamo introdotto gli insiemi traslati? Perché vogliamo sfruttare l'invarianza della misura rispetto alle traslazioni.
Vogliamo adesso dimostrare il seguente fatto:
i traslati razionali di **V**, **r+V**, con **r** razionale appartenente a **[-1,1]** coprono con la loro unione l'intervallo **[0,1]** ed inoltre la loro unione è contenuta in **[-1,2].**
Dobbiamo per prima cosa dimostrare che:

$$[0,1] \subseteq \bigcup_{r \in Q, -1 \leq r \leq 1} (r+V)$$

Prendiamo un **x** appartenente a **[0,1]**; c'è un unico **y** appartenente a $V \subset [0,1]$ tale che **r=x-y**.
Poichè **x, y** sono in **[0,1]**, $-1 \leq r \leq 1$, quindi **x=r+y**, con **r** razionale, $-1 \leq r \leq 1$ e quindi **x** appartiene ad un insieme del tipo **r+V**.
Il fatto poi che $\bigcup_{r \in Q, -1 \leq r \leq 1} (r+V) \subseteq [-1,2]$ è banale; infatti il valore più piccolo di **r è-1**,quello di un elemento di **V è zero**, quindi **-1+o=-1**; analogamente **1+1=2.**

L'insieme di Vitali non è misurabile

Supponiamo che **V** sia misurabile.
Partiamo da lontano; nella definizione di misura, abbiamo detto che deve essere invariante per traslazione; se prendiamo il nostro insieme **V** anche il suo traslato **r+V** deve essere misurabile e inoltre $\mu(V) = \mu(V + r)$
forse non lo abbiamo detto esplicitamente, ma se μ è una misura, e $A \subseteq B$ allora $\mu(A) \leq \mu(B)$.
Infatti se $A \subset B$, possiamo scomporre B in una unione disgiunta: $B = A \sqcup (B - A)$.



B=A U B\A

A ∩ B\A=ϕ

se applichiamo l'additività della misura,
$\mu(B) = \mu(A \cup (B - A)) = \mu(A) + \mu(B - A)$,
quindi $\mu(B) \geq \mu(A)$.
quindi essendo $V \subseteq [0, 1]$,
$0 \leq \mu(V) \leq \mu([0, 1]) = 1$
Abbiamo poi parlato di unione numerabile; se abbiamo una famiglia **Ai** numerabile di insiemi misurabili, si deve avere:

$$\mu(A) = \mu(\bigcup_{k}^{N} A_k) = \sum_{k}^{N} \mu(A_k);$$

consideriamo adesso il nostro insieme $\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V)$

(**l*o abbiamo costruito così apposta!***).

Nel nostro caso gli **Ai** sono costituiti dagli **r + V**; non dimentichiamo infatti che i razionali compresi fra **-1** e **1** sono un insieme numerabile.

Applichiamo l'additività numerabile a questi insiemi, che come abbiamo dimostrato sopra sono disgiunti, e teniamo conto anche dell'invarianza per traslazione:

$(\mu(V)=\mu(V+r))$.

$$\mu(\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V))=\sum_{r\in Q,-1\leq r\leq 1}\mu(r+V)=\sum_{r\in Q,-1\leq r\leq 1}\mu(V)$$

l'ultimo membro dell'eguaglianza è una somma infinita di un termine costante.

Se **V** è misurabile possiamo avere due casi:

$\mu(V)=0$

$$\mu(\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V))=\sum_{r\in Q,-1\leq r\leq 1}\mu(V)=0$$

$\mu(V)\neq 0$:

$$\mu(\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V))=\sum_{r\in Q,-1\leq r\leq 1}\mu(V)=\infty$$

Abbiamo poi visto che:

$$[0,1]\subseteq\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V)\subseteq[-1,2]$$

$\mu([0,1]) \subseteq \mu(\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V))\mu(\subseteq [-1,2])$

$1 \leq \mu(\dot{\bigcup_{r\in Q,-1\leq r\leq 1}}(r+V)) \leq 3$; ma zero o infinito non sono compresi fra **1 e 3**.

Dobbiamo quindi concludere che V non è misurabile, perchè supporlo tale porta ad un assurdo.

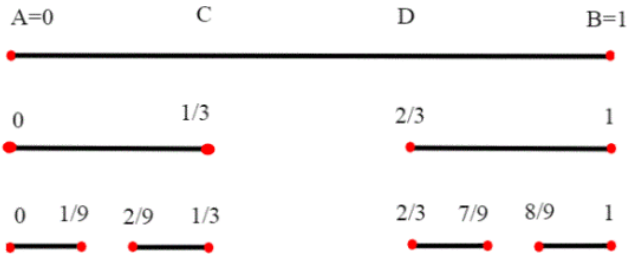
La scala del Diavolo

La scala del diavolo ,ovvero la funzione di Cantor- Vitali.

La scala del diavolo è una di quelle curve (come la curva di Peano e quella di Koch) che **Hilbert** definì "*curve mostruose*".
Mentre la curva di **Peano** è una curva che riempe tutti i punti di un quadrato, e quella di **Koch** una funzione non derivabile in nessun punto, quella di **Cantor-Vitali** merita davvero il nome di "*curva del diavolo*".
E' l'esempio di una curva debolmente crescente che ha derivata nulla in quasi tutti punti (chiariremo il significato di quel "quasi " più avanti).
La curva cresce dal valore 0 al valore 1 senza però essere mai strettamente crescente.
Nonostante questo non ha "*salti*" essendo una funzione continua.
Inoltre mappa un insieme di misura nulla in un intervallo!
Cercherò di introdurre questo argomento non proprio facile nel modo più intuitivo possibile.
Ci proponiamo di costruire una funzione sulla base di un insieme che abbiamo già conosciuto nella parte tredicesima: l'insieme di Cantor.
Penso che sia necessario riprendere le parti principali dell'articolo.

L'insieme di Cantor, costruzione.

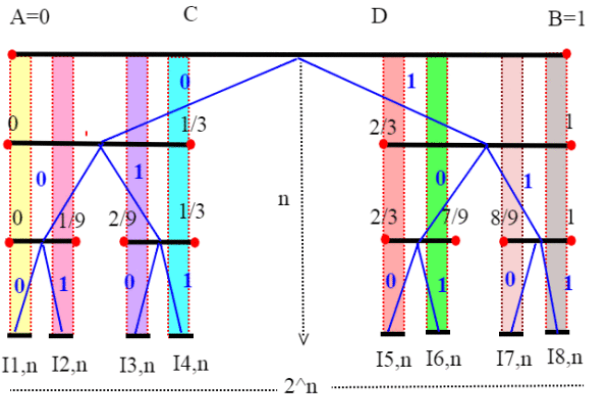
Consideriamo il segmento chiuso **AB=[0,1]**.
Dividiamo il segmento **AB** in tre parti uguali:



Togliamo dalla parte centrale il segmento aperto **(C,D)** otteniamo due segmenti chiusi, di lunghezza **1/3** di **AB**.
Se ripetiamo il procedimento ai due segmenti rimasti, dividendoli sempre in tre parti otteniamo in tutto quattro segmenti, di lunghezza **1/9** di **AB**.
Vogliamo estendere questo procedimento indefinitamente; cosa resta del segmento **AB=[0,1]** iniziale, dopo tutte le cancellazioni? *L'insieme di Cantor.*
Osserviamo che non resta alcun segmento non degenere, infatti la lunghezza all'n-esima iterazione è $\frac{1}{3^n}$, che ha come estremo inferiore 0 ,o (se preferite) limite zero.

Restano allora solo dei punti (da qui il termine suggestivo "*polvere di Cantor*").
L'insieme senz'altro non è vuoto (gli estremi di un segmento non vengono mai cancellati,viene solo tolta la parte centrale).
Ogni volta che dividiamo i segmenti successivi in tre parti e togliamo il segmento (aperto) centrale, abbiamo due scelte; prendere quello di sinistra, oppure quello di destra.

Gli intervalli che corrispondono ad un certo ramo sono tutti incapsulati; ovvero ogni precedente contiene i successivo; sono intervalli **chiusi** e la loro ampiezza tende a zero (è uguale a $\frac{1}{3^n}$); per quanto abbiamo visto su "*gli intervalli incapsulati*", la loro intersezione è un unico punto).
Quindi per ogni ramo abbiamo nell'insieme di Cantor almeno un punto!



I rettangoli di vario colore evidenziano gli intervalli incapsulati; al **passo n=3**, abbiamo già $2^3 = 8$ successioni distinte di intervalli incapsulati.
In generale , all'enn-esimo passo ne abbiamo 2^n!

La cardinalità dell'insieme di Cantor

Nello stesso articolo e, come vedremo nel seguente abbiamo, sfruttando le successioni binarie infinite, la cardinalità dell'insieme di Cantor è uguale a quella di **R**.
Detto in parole povere: ***l'insieme di Cantor ha tanti punti quanti quelli della retta reale.***

L'insieme di Cantor ha misura nulla.

Possiamo definire la misura di un intervallo, semplicemente facendo la differenza fra gli estremi.
Vogliamo vedere qual'è la misura totale delle cancellazioni che vengono eseguite partendo dall'intervallo **[0,1]**.
Alla prima iterazione tolgo un segmento di lunghezza 1/3; alla seconda due segmenti di lunghezza **1/9**, ovvero **2/9**, alla terza **4** segmenti di lunghezza **1/27**, ovvero **4/27** e così via.
La somma S delle misure che tolgo è quindi:
S=1/3 + 2/9 + 4/27 + …$2^{n-1}/3^n$**...**
Quindi **S** è somma della serie :

$$S = \sum_0^\infty \frac{2^n}{3^{n+1}} = \frac{1}{3}\sum_0^\infty \frac{2^n}{3^n}$$

abbiamo dunque un ***serie geometrica di ragione 2/3***; sappiamo che la somma di tale serie è $\frac{1}{1-\frac{2}{3}} = 3$,

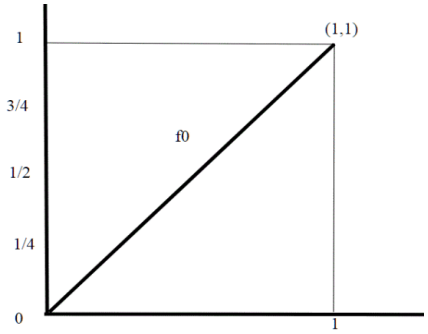
S=3 *1/3
Quindi S=1.

Ma come definire la misura di un insieme di punti, come quello di Cantor? In questo caso possiamo farlo come differenza fra la misura di tutto l'intervallo e **S**.
Ma allora, **la misura dell'insieme di Cantor è L(C) = *L*([0,1])-S=1-1=0**

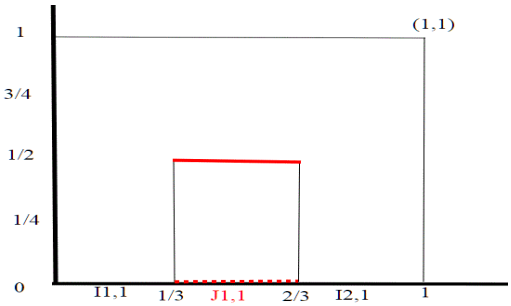
Costruzione grafico-intuitiva della funzione di Cantor-Vitali.

Vogliamo costruire una successione di funzioni che abbiano i***l valore 0 in 0 e il valore 1 in 1***, cioè:
fn(0)=0, fn(1)=1

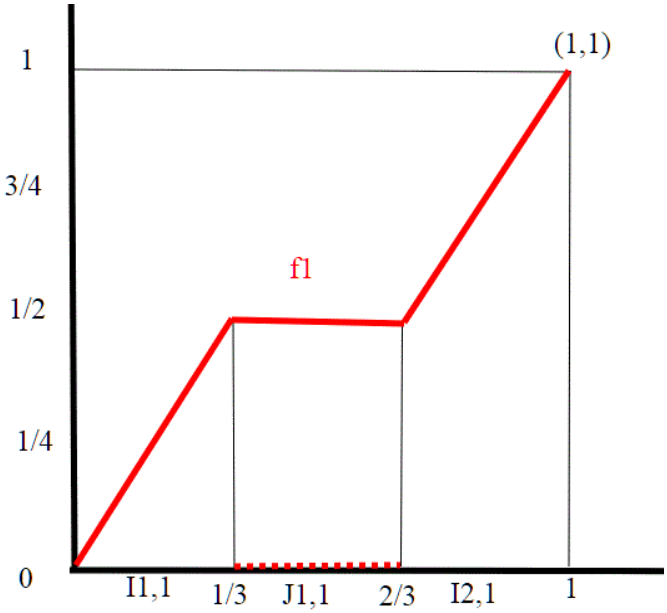
Tutte le **fn** devono essere debolmente crescenti.
Tutte le **fn** devono essere poi continue; le costruiremo con delle poligonali, che senz'altro sono delle funzioni continue.
Definiamo **f0(x)** il tratto obliquo che unisce **[0,0] a [1,1]**, che quindi è una retta, di equazione **y=x.**



Passiamo ora a f1.
Seguiamo sulle ascisse il metodo usato per generare l'insieme di Cantor.
Dividiamo l'intervallo **[0,1]**, che è il dominio della nostra funzione, inizialmente in tre parti uguali, come nella costruzione dell'insieme di Cantor. Nell'intervallo (**1/3,2/3**) che corrisponde ad uno degli intervalli tolti nel primo passo dell'insieme di Cantor, poniamo **f1** costantemente uguale ad **1/2**. Indichiamo con **J1,1** il primo tratto tolto (**n=1**), mentre con **I1,1,I2,1** gli intervalli che rimangono.
In pratica poniamo uguale a $\frac{k}{2^n}$ il valore della **fn** nell'intervallo **jk,n**.
($\frac{1}{2^1} = \frac{1}{2}$).

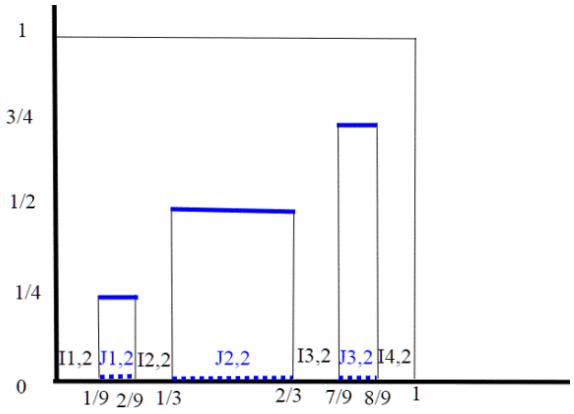


Uniamo ora l'estremo sinistro del tratto orizzontale con (0,0), e l'stremo destro con (1,1)

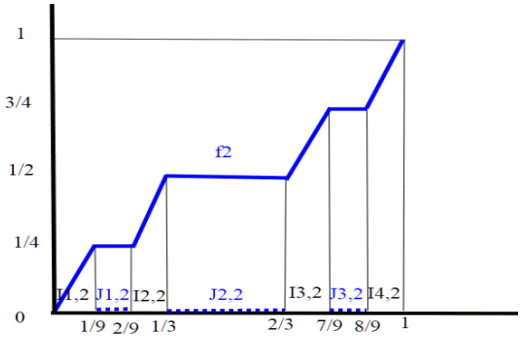


Le pendenze dei tratti obliqui sono ovviamente uguali e valgono **1/2/1/3=3/2**.
f1 risulta quindi definita su tutto [0,1].
Una osservazione importante; **I1,1** è un intervallo chiuso, mentre **J1,1** è un intervallo aperto, e in tutti i punti di questo intervallo **f1** ha valore uguale ha quello che ha nel punto **1/3**, che è un punto dell'insieme di Cantor.
I tratti obliqui sottendono un intervallo chiuso sull'asse delle x in cui gli estremi (non venendo mai cancellati) sono punti dell'insieme di Cantor C.

Passiamo a f2:



Continuiamo la nostra costruzione dell'insieme di Cantor sulle ascisse; gli intervalli tolti sono adesso 3 in totale, gli associamo secondo la regola di prima il valore $\frac{k}{2^n}$; in **J1,2** $\frac{1}{2^2} = 1/4$, in **j2,2** $\frac{2}{2^2} = 1/2$, in **j3,2** $\frac{3}{2^2} = 3/4$.



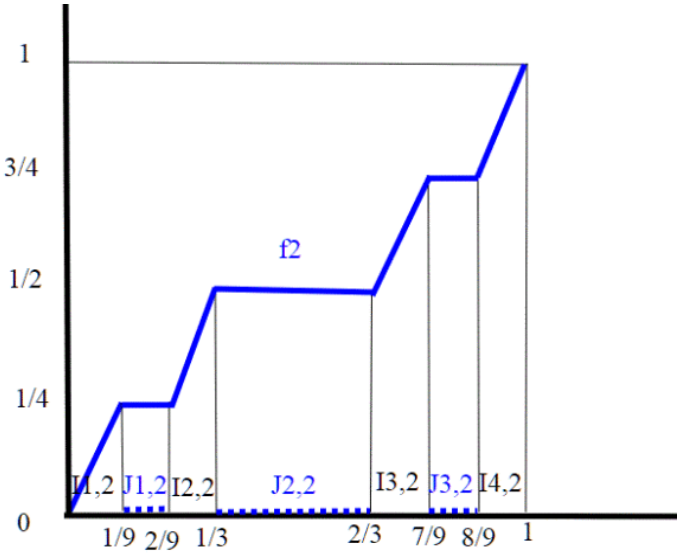
Come per **f1**, cominciamo da (**0,0)** con il primo tratto obliquo, dopo di che interpoliamo con dei tratti obliqui gli estremi destro-sinistro dei tratti orizzontali, fino ad arrivare in **(1,1).**
Notiamo che la pendenza dei tratti obliqui(sempre costante) è aumentata, ed è uguale a **1/4/1/9=**$(\frac{3}{3})^2$.
Chiaramente con questa costruzione possiamo andare avanti all'infinito. Abbiamo costruito una successione di funzioni.
Non ci resta che definire **funzione di Cantor, f(x), il limite di questa successione:**
$f(x) = lim_{n\to+\infty} f_n(x)$.

Che questa successione converga, è conseguenza di un criterio sulla convergenza uniforme di funzioni continue, ma questa volta dovete **credermi sulla parola**.
Inoltre, essendo limite di una successione di funzioni continue, è anch'essa una **funzione continua.**
Senza possedere queste importanti nozioni di convergenza, possiamo anche pensarla così: ad ogni iterazione affiniamo la nostra curva che diventa sempre più simile ad una gradinata.
Se ingrandiamo un qualsiasi tratto della curva, ritroviamo sempre una poligonale che quindi è continua per costruzione.
In pratica seguendo passo passo il procedimento ricorsivo della costruzione dell'insieme di Cantor, costruiamo anche la scala del Diavolo.
Nel disegno abbiamo messo in evidenza gli intervalli **In,k , Jn,k**.
Gli **I** sono gli intervalli che restano ad ogni divisione, gli **J** quelli che vengono tolti.
Notiamo che il valore costante che viene dato dentro gli **J** è proprio , se l'intervallo è **Jn,k , fn(x)=**$\frac{k}{2^n}$.
Infatti, nell'intervallo **J1,1** vale **1/2**, in **J1,2=1/4**, in **J3,2=3/4**.

Quanti tratti orizzontali ha fn? quanti tratti verticali?

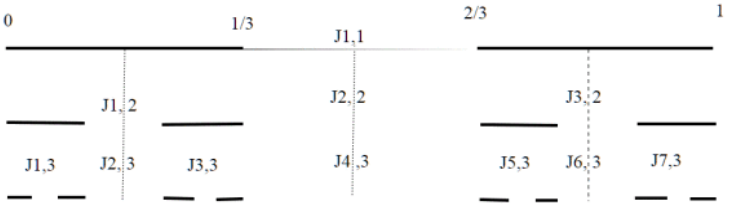
Sappiamo, per come la stiamo costruendo, che l'n-esima poligonale ha tanti tratti obliqui, quanti sono gli intervalli **I** della n-esima costruzione dell'insieme di Cantor, che sono 2^n, mentre i tratti orizzontali costanti sono tanti come gli intervalli **J** che togliamo ad ogni passo, cioè $2^n - 1$.

f0 ha infatti 1 tratto obliquo, $2^0 = 1$, e nessun tratto orizzontale $2^0 - 1 = 0$
f1 2 obliqui, 2^1 e 1 orizzontale, **2-1=1**
f2 quattro obliqui 2^2, e tre orizzontali, $2^2 - 1 = 3$
Perché associamo in **Jn,k** ,ad **f(x)** il valore $\frac{k}{2^n}$?
Riporto il disegno per capirci meglio.



Per una necessità di costruzione regolare, da tradurre analiticamente.
Abbiamo appena visto che i tratti orizzontali sono $2^n - 1$.
Ad essi dobbiamo associare un valore sulle ordinate; possiamo pensare di dividere in 2^n parti uguali l'intervallo [0,1].
Partendo da 0 e arrivando a 1 quanti punti ho generato?
2^n+1.
Ma se tolgo 0 e 1 i punti interni diventano 2^n+1-2=$2^n - 1$.
Quindi sono tanti come i tratti orizzontali.
Inoltre negli Jk,n , k<=$2^n - 1$, quindi $\frac{k}{2^n}$**<1**.

L'importante poi è che tale valore, a parità di intervallo **J**, non dipenda da **n**, ovvero dal passo della costruzione.
Con un po' di fatica e guardando il disegno sotto ci si rende conto che:
Jk,n-1=J2k,n, e quindi $\frac{k}{2^{n-1}} = 2 \cdot \frac{k}{2^n}$.

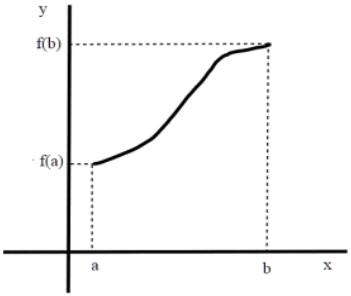


Quant'è la pendenza del lato obliquo? $(\frac{3}{2})^n$;
Infatti l'intervallo proiettato sull'ordinata del tratto obliquo misura $1/2^n$, il tratto orizzontale della proiezione $1/3^n$, quindi il rapporto $(\frac{3}{2})^n$.
se **n=0,1,2** come nei disegni, la pendenza vale rispettivamente **1, 3/2, 9/4**.

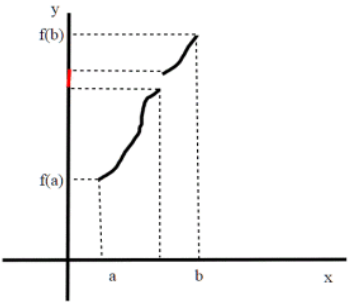
Notiamo che quando **n** diventa molto grande, la pendenza tende ad infinito, ovvero le spezzate tendono a dei gradini verticali, e sono sempre più corte. Da qui il nome di "***scala***" Il diavolo c'entra per vari motivi: uno è che pur avendo dei gradini, il grafico non ha nessun salto (*la funzione è continua!*).
Un altro modo in cui mette alla prova la nostra intuizione è che, pur crescendo dal valore **0** al valore **1**, non è strettamente crescente su alcun sottointervallo non degenere di **[0, 1]**.
Per giustificare questo fatto dobbiamo tener ben presente ***l'insieme di Cantor*** ricordandoci che su ogni sotto intervallo di **[0,1]** c'è sempre un segmento in cui la funzione risulta costante.
Supponiamo per esempio di prendere un intervallo in cui la funzione cresce strettamente (lato obliquo), questo è un intervallo che poi andrà diviso in tre parti, e conterrà una parte costante.

Iniettività e suriettività

La funzione non è iniettiva; sappiamo infatti che negli intervalli che non appartengono all'insieme di Cantor, la funzione è costante, quindi per valori di **x** diversi, dà lo stesso **f(x)**.



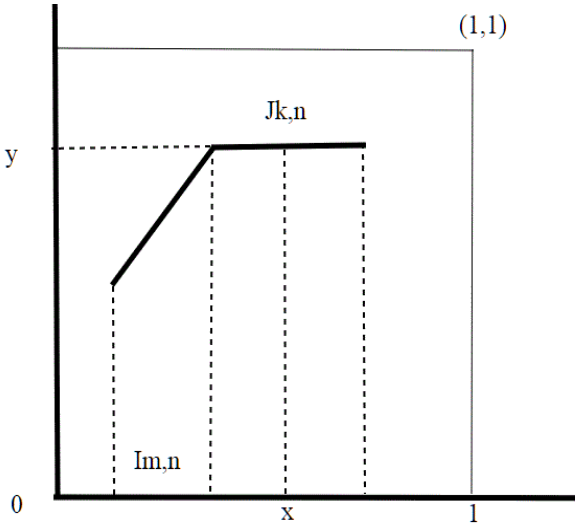
Funzione monotona continua



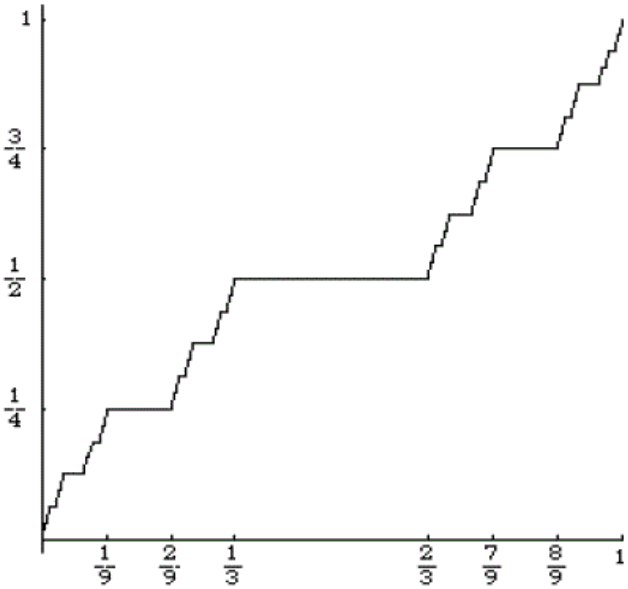
Funzione monotona discontinua

Il fatto che una funzione continua assuma tutti i valori fra **f(a)** e **f(b)** è giustificabile dal disegno; la f a destra non essendo continua perde i valori indicati in rosso.
E' però suriettiva, ovvero copre tutto **[0,1]**; essendo continua , debolmente crescente e inoltre **f(0)=0, f(1)=1**.
Quindi assume tutti i valori **fra 0 e 1**.
Un fatto eccezionale:
L'immagine dell'insieme **C** di Cantor è tutto l'intervallo, ovvero **f(C)=[0,1]**!
Questo significa che l'immagine di un insieme di misura nulla ha come immagine un intervallo!
Vediamo se riusciamo a giustificarlo.

Prendiamo un $y \in [0,1]$; essendo suriettiva,sappiamo che esiste un $x \in [0,1]$ tale che f(x)=y.



Se $x \in C$ abbiamo finito.
Se **x** non appartiene a **C**, allora appartiene ad uno degli intervalli che abbiamo tolto durante la costruzione, **Jk,n**.
Ma **f** è costante su **Jk,n**, quindi nell'estremo sinistro assume lo stesso valore dell'estremo destro di un intervallo in cui la funzione è obliqua.
Ma l'estremo, come sappiamo dalla costruzione dell'insieme di Cantor, appartiene a **C**.

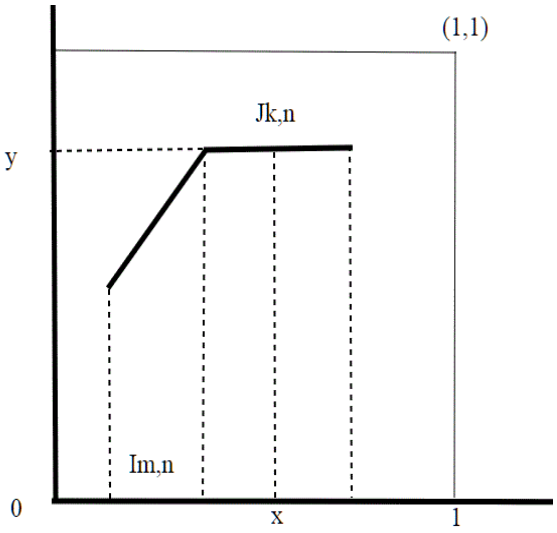


Il "quasi ovunque" della matematica.

Prima di continuare il discorso sulle strane proprietà della scala del diavolo, volevo introdurre i discorso del "***quasi ovunque***" in matematica.
Esso deriva sostanzialmente dalla necessità di estendere delle proprietà che non sono sempre vere in un insieme prendendole sempre per buone lo stesso, a parte il fatto che esse non si verifichino solo su insieme di misura nulla.
Riemann fu costretto a inventare una nuova definizione di integrale, affinché molte funzioni che fossero discontinue anche solo in un numero finito di punti, fossero lo stesso integrabili.
Ebbene, dimostrò che seguendo la sua definizione, ogni funzione continua **quasi ovunque** è integrabile.
Guarda caso, per costruire la scala del diavolo è stato preso un insieme infinito di misura nulla, l'insieme di Cantor, e che ha addirittura la stessa cardinalità del continuo.

La funzione di Cantor-Vitali è derivabile quasi ovunque.

Sappiamo infatti, che comunque prendiamo un segmento, dobbiamo tener ben presente l'insieme di Cantor ricordandoci che su ogni sotto intervallo di **[0,1]** c'è sempre un segmento in cui la funzione risulta costante.
Quindi al di fuori dell'insieme di Cantor, ovvero al di fuori di un **insieme di misura nulla**, la funzione è sempre derivabile, con derivata nulla.



Più in dettaglio: **Jk,n** non appartiene a **C** ed è un insieme aperto e in esso la derivata è nulla, mentre l'estremo destro di **Im,n** appartiene a **C**.
Tale estremo infatti non viene mai tolto, ma nello spigolo la derivata non esiste.

In quanti punti non è derivabile? Solo nei punti dell'insieme di Cantor!

Lunghezza della funzione di Cantor.

Nel quiz sul paradosso della scala e della formica**, avevamo concluso che la lunghezza della scala era la somma dei cateti, **a** e **b**.
Lì il discorso era però diverso; la scala partiva già con dei gradini verticali, e comunque si suddividessero ottenevamo come lunghezza sempre la somma delle proiezioni, che sono appunto **a. b**.
Se pensiamo adesso alla lunghezza dei nostri tratti orizzontali, sulla scala, e li proiettiamo sull'asse delle **x**, altro non otteniamo che la lunghezza del complementare dell'insieme di Cantor, che abbiamo già calcolato nella prima parte dell'articolo, ottenendo:

$$S = \sum_{0}^{\infty} \frac{2^n}{3^{n+1}} = \frac{1}{3} \sum_{0}^{\infty} \frac{2^n}{3^n} \textbf{=1}$$

Scheeffer (1884) ha mostrato che la lunghezza della scala del diavolo è 2; da ciò ne deriva che la parte "inclinata" ha lunghezza **1**, come intuitivamente si pensa tendendo i lati obliqui alla verticale.
Questo non ci può stupire più di tanto, in quanto la funzione di Cantor, come abbiamo visto, trasforma un insieme di punti **C,** nell'intervallo **[0,1]**.

Termino con questa osservazione, **dedicata unicamente a chi conosce l'integrale di Riemann.**
L'integrale della derivata della scala diabolica (quando essa è derivabile) non è la scala diabolica.
Chiamiamo come di consueto **C** l'insieme di Cantor.
Allora, indicando con **f '(x)** la derivata della funzione di Cantor, abbiamo:

$$f'(x) = \begin{cases} 0 & x \in [0,1] - C \\ nonesiste & x \in C \end{cases}$$

Definiamo adesso una funzione g(x):

$$g(x) = \begin{cases} 0 & x \in [0,1] - C \\ S & x \in C \end{cases}$$

dove **S** è un qualsiasi valore, ma non illimitato.

La funzione **g** è integrabile (***secondo Riemann***) perché vale quasi sempre

zero, a parte in un insieme di misura nulla, **C**.

$$h(x) = \int_0^x g(t)dt = 0$$

quindi :

$$h(x) \neq f(x)$$
$$0 = h(x) = \int_0^x g(t)dt = \int_0^x f'(t)dt \neq f(x)$$

Ne consegue che l'integrale della derivata della scala diabolica, non è la scala diabolica.
In pratica con la scala di Cantor svanisce il tentativo di estendere il teorema fondamentale del calcolo integrale.

Cantor e i numeri trascendenti. Parte prima.

Consideriamo l'insieme dei numeri reali.
Tutti hanno le idee chiare sulla differenza fra numeri razionali e irrazionali.
Meno evidente è invece il discorso dei numeri trascendenti.
Come si definiscono quest'ultimi? I numeri trascendenti sono numeri che non sono algebrici.
Ma chi sono i numeri algebrici? Sono i numeri che si ottengono come risultato di una equazione polinomiale, tipo ad esempio $ax^2 + bx + c = 0$ a coefficienti interi.
In generale come radici di un polinomio $a_n x^n + a_{n-1} x^{n-1} + ...a_0$ in cui i coefficienti **an,an-a,…a0** sono tutti interi.
Notare che la definizione di numero algebrico ingloba i numeri razionali, in quanto, per esempio **q=a/b** è soluzione dell'equazione di primo grado **bx=a**.
Attorno al 1850 **Joseph Liouville** (1809-1882) diede la prima dimostrazione della trascendenza di particolari numeri reali.
Per quanto riguarda i numeri reali che conosciamo meglio bisogna aspettare ancora qualche anno: nel 1873 **Charles Hermite** dimostra che il numero **e** è trascendente, mentre la trascendenza di π è stata dimostrata da **Ferdinand von Lindemann** nel 1882.
Come si inserisce Cantor in questo contesto? Se Liouville si dannò tanto per scoprire che esisteva almeno un numero reale trascendente, Cantor nel 1891 basandosi sui suoi infiniti dimostrò addirittura che i numeri trascendenti sono tanti quanti i reali stessi, ovvero l'insieme dei reali e l'insieme dei trascendenti hanno la stessa cardinalità, quella del continuo.
In pratica, abbiamo a che fare più che altro, con numeri trascendenti .
Passiamo ora a dimostrare quanto asserito; mi servirò dei risultati che potete trovare negli articoli precedenti inerenti Cantor.

Riassunto

Gli insiemi Z e Q sono numerabili.

Potete trovare nella parte terza, un articolo introduttivo sugli insiemi numerabili, e nella parte settima la dimostrazione della numerabilità di Q.
A) Il prodotto cartesiano $Z^n = ZxZxZ....xZ$ è numerabile.
Questo risultato non è stato visto; ci siamo limitati a dimostrare che: 1) **Z x**

Z è numerabile, quando abbiamo parlato della numerabilità di Q.
Ma ci viene in aiuto il principio di induzione: la proposizione è vera per **n=1** banalmente.
Supponiamo adesso che Z^n sia numerabile: scriviamo $Z^{n+1} = Z^{n-1} \times (Z \times Z)$; sappiamo per 1) che **Z x Z** è in corrispondenza biunivoca con Z, quindi anche sarà in corrispondenza biunivoca con $Z^{n-1} \times Z = Z^n$, quindi Z^{n+1} sarà in corrispondenza biunivoca con Z^n che è numerabile per ipotesi induttiva.

B) Se abbiamo una famiglia di insiemi Ai, finiti o numerabili, allora anche $\bigcup_{i \in I} A_i$ **è un insieme finito o numerabile.**
La dimostrazione di questo fatto, l'abbiamo vista nell' articolo sull'assioma della scelta, la riporto qui comunque :
Abbiamo visto che l'unione di due insiemi numerabili è numerabile. Usando il principio di induzione, si può dimostrare che l'unione finita di insiemi numerabili è numerabile(per n=2 $A_1 \bigcup A_2$ *è vera, supposta vera per n,* $A_1 \bigcup A_2 .. \bigcup A_n$ *è allora numerabile, basta allora scrivere* $(A_1 \bigcup A_2 .. \bigcup A_n) \bigcup A_{n+1}$ *e ho ancora l'unione di due insiemi numerabili); e se abbiamo una unione numerabile (quindi infinita) di insiemi numerabili?*
L'unione di una famiglia numerabile di insiemi numerabili $\{A_n : n \in N\}$ ***è numerabile.***
Essendo ogni ***An*** *numerabile, esiste una corrispondenza biunivoca:*
gn: N–>An *per ogni n:* $\{g_n : n \in N\}$.
Consideriamo adesso l'insieme ***N x N*** *e costruiamo un funzione* $f: N \times N \to \bigcup_n A_n$ *ponendo* $f(n,m) = g_n(m)$; ***f*** *è suriettiva.*
Infatti se $a \in \bigcup_n A_n$, *allora* $a \in A_n$ *per qualche* ***n****; quindi (essendo* g_n *suriettiva) esiste m tale che* $g_n(m) = a$
Essendo ***f*** *suriettiva, per quanto visto sopra, esiste una funzione iniettiva* $g : \bigcup_n A_n \to N \times N$, *quindi* $|\bigcup_n A_n| \leq |N \times N| = \aleph_0$

*essendo **N x N** numerabile; ma allora* $\bigcup_n A_n$ *è numerabile, essendo* $\aleph_0$ *il minimo ordine di infinito.*
Siamo adesso pronti per dimostrare che:

Il sottoinsieme dei numeri algebrici è numerabile.

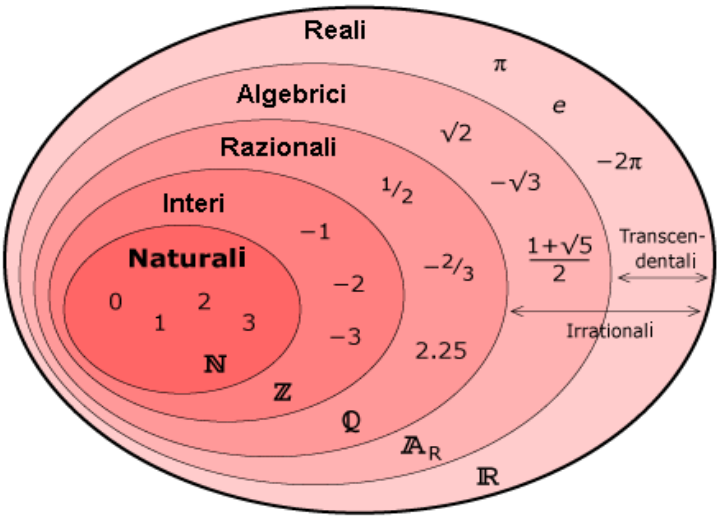
Consideriamo il polinomi di grado **k** e a coefficienti in **Z**:

$a_k x^k + a_{k-1} x^{k-1} + \ldots . a_0$ qualsiasi sia **k**.
Per ogni **k+1-upla**, presa in Z^{k+1}, (**ak,ak-1,….a1,a0**) abbiamo un polinomio.
Noi dobbiamo considerare tutti i polinomi possibili.
In realtà, per aver un **polinomio di grado k**, nella **k+1-upla** dobbiamo avere **k<>0**.
Avremmo allora, **per ogni k**, un sottoinsieme infinito di Z^{k+1}, che comunque, essendo Z^{k+1} numerabile è anch'esso numerabile.
Quindi l'insieme di tutti i polinomi a coefficienti interi è dato dall'unione di tutti i polinomi di grado **k**; chiamiamoli **Pk**; se facciamo l'unione con $k \in N$ li otteniamo tutti.
Quindi avremmo, se chiamiamo **P** l'insieme di tutti questi polinomi:
$P = \bigcup_{k \in N} P^k$. Se applichiamo adesso la ***B),*** otteniamo che P è un insieme numerabile.
Se adesso trasformiamo i polinomi in equazioni, ponendoli uguali a zero, abbiamo che l'insieme delle equazioni polinomiali a coefficienti in Z è numerabile.
Chiamiamo **E0, E1,…Ek** la successione di tali insiemi.
Per ogni **Ei,** associamo ad esso l'insieme delle soluzioni, **Si**, che è un certo insieme finito.
Abbiamo allora ancora che tutte le possibili soluzioni, ovvero i numeri algebrici, sono dati da:
$S = \bigcup_{k \in N} S^k$ che sempre per ***B)*** costituisce un insieme numerabile.
Dunque, il sottoinsieme dei numeri algebrici è numerabile!
Se adesso chiamiamo **A** l'insieme dei numeri algebrici e **T** l'insieme dei numeri trascendenti, **T=R\A**.

Di sicuro **T** non può essere numerabile o finito, perché altrimenti **R=T U A** sarebbe unione di due insiemi numerabili e pertanto sarebbe numerabile. **Quindi T è infinito ed ha cardinalità maggiore di N.**
Nella seconda parte di questo articolo vedremo che **T** ha addirittura la stessa cardinalità di **R**.

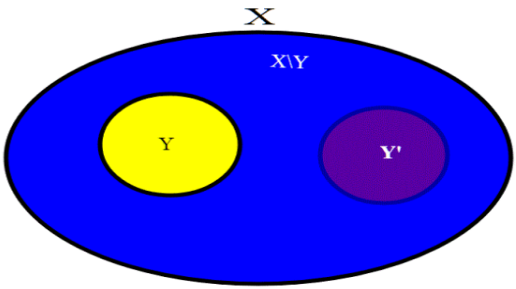
Cantor e i numeri trascendenti. Parte seconda.

Riprendo in sintesi quanto fatto nella prima parte dell'articolo.
Si definiscono numeri trascendenti quei numeri reali che non sono algebrici, ovvero non sono soluzione di alcuna equazione algebrica a coefficienti interi.
Cantor riuscì a dimostrare che i numeri trascendenti sono infiniti, anzi sono più che numerabili!.

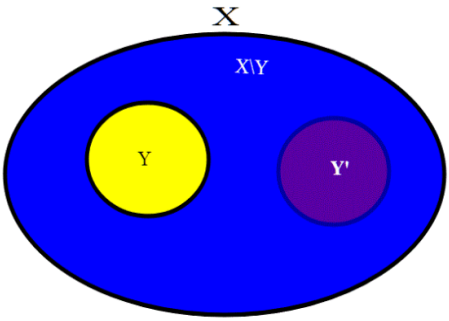


Infatti se chiamiamo **A** l'insieme dei numeri algebrici e **T** l'insieme dei numeri trascendenti, **T=R\A**.
Abbiamo visto che **A** è numerabile.
Di sicuro **T** non può essere numerabile o finito, perché altrimenti **R=T U A** sarebbe unione di due insiemi numerabili e pertanto sarebbe numerabile. Quindi **T** è infinito ed ha cardinalità maggiore di **N**.
Non possiamo però dire subito che **T** ha la cardinalità di **R**, escludendo cardinalità **x** comprese fra il numerabile e il continuo, ovvero **|N|<x<|R|**.
(questo dilemma è noto come Ipotesi del continuo).

Dobbiamo perciò dimostrarlo.
Facciamolo in modo generico, staccandoci dal nostro caso particolare.
Prima però, una osservazione.
Consideriamo un insieme **A** infinito.
Vogliamo dimostrare che contiene un insieme numerabile.
Se procediamo formalmente, dovremmo creare una funzione ricorsiva che però non so se piaccia a tanti.
Possiamo dimostrarlo in modo più intuitivo.
Vogliamo trovare una funzione iniettiva di **f: N—>A.**
Se **A** è infinito, senz'altro non è vuoto.
Scelgo allora un elemento di **A** che chiamo **f(0). f(0)** è quindi l'immagine di **0**.
Poi scelgo un elemento **f(1) diverso da f(0)**, e che diventa l'immagine di **1**.
Continuo così; **f(n)** altro non è che un elemento di **A** diverso da tutti i precedenti, ovvero appartenente a **A\{f(0),f(1),…f(n-1)}**.
Posso fare queste infinite associazioni perché **A** è infinito, quindi riesco sempre a trovare un elemento che sia diverso da tutti quelli scelti in precedenza.
Quindi l'applicazione così costruita è iniettiva, ed è anche biunivoca su **f(N)**.
Quindi l'insieme **f(N)** è l'insieme cercato, ovvero un insieme numerabile sottoinsieme di **A**.
Adesso sia **X** un insieme infinito, **Y** un insieme numerabile (nel nostro caso **X=R**, ma ormai che ci siamo vogliamo dimostrare una cosa generica).
Dimostriamo che **|X\Y |=|X|**, ovvero che la cardinalità di **X\Y** è uguale a quella di **X**.



Notare che **Y e Y'** sono insiemi disgiunti; **Y'** è infatti sottoinsieme del complementare di **Y.**
Per quello che abbiamo visto sopra, essendo **X\Y** infinito, esiste un sottoinsieme di **X\Y** che chiamiamo **Y'**, che è numerabile. **Y'** è disgiunto da **Y**.
Se **Y'** è numerabile, esiste allora una funzione biunivoca **f** fra
f: Y'—>Y'UY; infatti anche **Y' U Y** è numerabile, essendo unione di insiemi numerabili.
Per dimostrare che **|X\Y |=|X|,** dobbiamo trovare una funzione biunivoca **g** che va da **g:X\Y—>X**.



La funzione **g** deve andare dalla parte Blu **(X\Y)** più la parte viola **(Y')** su tutto **X**.
La definiamo così: (g è definita su **Y' U (X -(Y U Y'))=X\Y**)
g(x)=f(x) e $x \in Y'$; sappiamo che **f(x)** copre **Y'UY**, inoltre è iniettiva
g(x)=x se $x \in X - (Y \cup Y')$; la funzione **x** (identità) copre tutto $X - (Y \cup Y')$ ed è iniettiva, ma allora **Y'UY U**$X - (Y \cup Y')$ **=X**, quindi **g** è suriettiva su **X**, ed è inoltre iniettiva.
Quindi è una biezione, **g:X\Y—>X.**

I numeri trascendenti hanno la stessa potenza del continuo.

Nel nostro caso, **X** è l'insieme **R** dei reali. **Y** è invece **A**, insieme dei numeri algebrici. **X\Y** rappresenta per noi **R\A=T**, insieme dei numeri trascendenti. Quindi l'insieme dei numeri trascendenti ha la **stessa potenza** del continuo. ***All'interno dei reali, ci sono dunque più numeri trascendenti che altro!***