Diario del Corso di Matematica di base I

Corso TANDEM
Docente: Sisto Baldo

ATTENZIONE: Il presente Diario del Corso Tandem di Matematica di Base I vuole essere un riassunto abbastanza stringato di quello che è stato detto in aula (senza la parte più euristica e alcune delle chiacchere...), e come tale può essere un utile sussidio per chi voglia sistemare i propri appunti, o per chi sia stato assente e voglia ricostruire i contenuti di una lezione.

Ci si riferisca alle ottime dispense di Enrico Gregorio e Francesca Mantese:
`http://profs.sci.univr.it/~gregorio/MatematicaDiBase.pdf`,
che contengono anche parecchi esercizi!

Dalla Home Page di Enrico Gregorio potete scaricare anche degli esempi di compiti d'esame degli anni precedenti... ai quali fatalmente ci ispireremo per preparare il vostro esame!

Indice

1 Lezione del 1/2/2018

Abbiamo iniziato il corso ricordando cosa sia una *relazione* tra due insiemi A e B: si tratta semplicemente di un sottinsieme $\mathcal{R} \subset A \times B$ del prodotto cartesiano

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

In altre parole, $\mathcal{R}$ è un insieme di *coppie ordinate*, il primo elemento delle quali appartiene ad A ed il secondo a B. Si dice che gli elementi $a \in A$ e $b \in B$ *sono in relazione* o *si corrispondono* secondo $\mathcal{R}$ se e soltanto se $(a, b) \in \mathcal{R}$.

Ricordiamo anche che A si chiama *dominio* e B *codominio* della relazione. Dentro A e B, possiamo individuare i seguenti due importanti sottinsiemi, che si chiamano rispettivamente *insieme di definizione* e *immagine* della relazione:

$$\begin{aligned} \mathrm{Def}(\mathcal{R}) &= \{a \in A : \ \textit{esiste } b \in B \textit{ t.c. } (a, b) \in \mathcal{R}\}. \\ \mathrm{Im}(\mathcal{R}) &= \{b \in B : \ \textit{esiste } a \in A \textit{ t.c. } (a, b) \in \mathcal{R}\}. \end{aligned}$$

Vedremo più avanti che vi sono classi importanti e significative di relazioni, come le relazioni di equivalenza e le relazioni d'ordine (largo e stretto). Oggi vogliamo però occuparci di un'altra classe di relazioni che riveste particolare interesse, quella delle *funzioni*:

DEFINIZIONE: Dati due insiemi A e B, una *funzione* tra A e B è una relazione $f \subset A \times B$ che gode della seguente proprietà (detta *univocità*): se $(a, b) \in f$ e $(a, c) \in f$ allora $b = c$.

In altre parole, ad ogni elemento a dell'insieme di definizione $\mathrm{Def}(f)$ della funzione, la relazione f fa corrispondere *esattamente un elemento* del codominio B: quest'unico elemento del codominio si indica con $f(a)$

Per indicare che f è una funzione tra A e B scriviamo anche $f : A \to B$, mentre per dire che $b = f(a)$ scriviamo anche $a \mapsto f(a)$.

Per esempio, si considerino le seguenti relazioni:

$$\begin{aligned} f &= \{(0, 1), (4, 5), (5, 1)\} \subset \mathbf{N} \times \mathbf{N} \\ g &= \{(0, 1), (3, 4), (3, 6)\} \subset \mathbf{N} \times \mathbf{N} \\ h &= \{(x, y) : \ x \in \mathbf{R}, \ y = \sin x\} \subset \mathbf{R} \times \mathbf{R} \\ k &= \{(x, y) : \ y \in \mathbf{R}, \ x = y^2\} \subset \mathbf{R} \times \mathbf{R} \end{aligned}$$

Abbiamo che f e h sono funzioni (rispettivamente, $f : \mathbf{N} \to \mathbf{N}$, $h : \mathbf{R} \to \mathbf{R}$, mentre g e k non lo sono (a g appartengono le coppie $(3, 4)$ e $(3, 6)$, che

hanno uguale il primo elemento e diverso il secondo e analogamente a k appartengono le coppie $(1,1)$ e $(1,-1)$).

Abbiamo osservato che nel caso di relazioni tra $\mathbf{R}$ e $\mathbf{R}$, possiamo attribuire un ovvio significato geometrico alla definizione di funzione. Infatti, gli elementi del prodotto cartesiano $\mathbf{R} \times \mathbf{R}$ possono essere interpretati come le *coordinate cartesiane di punti del piano euclideo*(in cui, ovviamente, dobbiamo aver scelto l'origine, i due assi cartesiani ortogonali x e y e l'unità di misura!). A questo punto, un sottinsieme f del piano cartesiano (cioè una relazione tra $\mathbf{R}$ e $\mathbf{R}$ è una funzione se e solo se *ogni retta parallela all'asse delle y* incontra f *al più in un punto.*

Tra gli esempi visti sopra, la sinusoide h ha questa proprietà, mentre la parabola con asse orizzontale k non ce l'ha!

Alcune importanti definizioni sono le seguenti:

DEFINIZIONE: Una funzione $f : A \to B$ si dice *totale* se $\mathrm{Def}(f) = A$, ossia *è definita su tutto* A[1].

Si dice *iniettiva* o *uno a uno* se ogni volta che $(a,c) \in f$, $(b,c) \in f$ si ha $a = b$. Questo significa che in punti distinti del suo insieme di definizione la funzione assume valori distinti...ovvero che ogni valore assunto da f viene assunto esattamente una volta.

Si dice *suriettiva* se $\mathrm{Im}(f) = B$, ossia se per ogni $b \in B$ esiste $a \in A$ tale che $b = f(a)$.

Infine, f si dice *biiettiva* se è totale, iniettiva e suriettiva. Questo significa che a *ogni elemento di* A la funzione f associa *uno ed un solo* elemento di B. Una funzione biiettiva tra A e B si chiama anche *corrispondenza biunivoca* tra A e B.

Si noti che per funzioni da $\mathbf{R}$ in $\mathbf{R}$, l'iniettività ha una semplice interpretazione geometrica: una funzione è iniettiva se e solo se ogni retta orizzontale taglia la funzione al più in un punto!

Per concludere questa lezione forse un po' tecnica (ma vi ho promesso qualcosa di più divertente per il prossimo incontro: ci occuperemo infatti di cardinalità!), vogliamo parlare un istante di funzione composta.

[1]A questo proposito, è importante che vi riveli un triste fatto della vita: a volte, persino i matematici usano notazioni in parziale disaccordo tra di loro! In effetti, nella grande maggioranza dei testi di matematica (comprese, ahimè, le mie dispense di Analisi I, Analisi II, Analisi Funzionale...), la scrittura $f : A \to B$ significa che l'insieme di definizione di f coincide con A: una funzione è *totale per definizione, e non c'è distinzione tra dominio ed insieme di definizione.* Leggendo un testo, è quindi importante capire quale convenzione adotta l'autore... In questo corso, ci atterremo però religiosamente alle definizioni che vi ho dato, che sono quelle della dispensa di Enrico Gregorio e Francesca Mantese!

Date due funzioni f, g, con $g \circ f$ vogliamo indicare la funzione che si ottiene applicando prima f e poi g: $(g \circ f)(a) = g(f(a))$.

Più precisamente

DEFINIZIONE: Siano $f : A \to B$, $g : C \to D$, la funzione composta

$$g \circ f : A \to D$$

è definita dalla regola che $(a, d) \in g \circ f$ se e solo se esiste $c \in C$ tale che $(a, c) \in f$ e $(c, d) \in g$.

Ovviamente, $g \circ f$ avrà insieme di definizione non vuoto se e solo se l'intersezione tra l'immagine di f e l'insieme di definizione di g è non vuoto.

Veniamo ora al concetto di *funzione inversa*. Data una funzione $f : A \to B$, consideriamo la relazione tra B e A

$$f^{-1} = \{(b, a) : \ (a, b) \in f\}$$

che si ottiene "scambiando i ruoli di dominio e codominio".

In generale, la relazione f^{-1} non è più una funzione: ad esempio se $f = \{(x, y) \in \mathbf{R} \times \mathbf{R} : x \in \mathbf{R}, \ y = x^2\}$ allora f^{-1} è la parabola con asse orizzontale vista sopra, che non è una funzione!

Quando possiamo dire che f^{-1} è una funzione? Se ripensiamo alla sostanziale simmetria dei ruoli giocati da dominio e codominio nella *definizione di funzione* e in quella di *funzione iniettiva*... capiamo subito che *f^{-1} è una funzione se e soltanto se f è iniettiva*.

DEFINIZIONE: Se $f : A \to B$ è una *funzione iniettiva*, la sua *funzione inversa* $f^{-1} : B \to A$ è la relazione sopra definita.

In soldoni, data una funzione iniettiva f la funzione inversa f^{-1} associa ad ogni $b \in \mathrm{Im}(f)$ l'unico elemento $a \in \mathrm{Def}(f)$ tale che $f(a) = b$. Abbiamo quindi, per ogni $a \in \mathrm{Def}(f)$, che $f^{-1}(f(a)) = a$... e analogamente per ogni $b \in \mathrm{Im}(f)$ si ha $b = f(f^{-1}(b))$.

A questo punto è facile convincersi che $\mathrm{Def}(f^{-1}) = \mathrm{Im}(f)$ e $\mathrm{Im}(f^{-1}) = \mathrm{Def}(f)$: in particolare f^{-1} è *totale* se e solo se f è suriettiva, è *suriettiva* se e solo se f è totale. Invece, f^{-1} è sempre iniettiva... perché f è una funzione e quindi gode della proprietà di univocità.

In particolare, f è biiettiva se e solo se lo è f^{-1}.

La lezione si è conclusa svolgendo un po' di esercizi, tratti dai compiti d'esame degli anni scorsi.

2 Lezione del 8/2/2018

Concludiamo i discorsi sulla funzione inversa iniziati la volta scorsa. Ovviamente, se $f : A \to B$ non è iniettiva, la relazione inversa f^{-1} non è una funzione e non è possibile *invertire* f. Per farlo, possiamo però restringere artificialmente il dominio di f ad un suo sottinsieme su cui la funzione sia iniettiva. Ad esempio, la funzione $f(x) = x^2$ (modo stenografico per scrivere $f = \{(x, y) : \ x \in \mathbf{R}, \ y = x^2\}$ non è iniettiva se la consideriamo come funzione $f : \mathbf{R} \to \mathbf{R}$, mentre lo è come funzione $f : \mathbf{R}_{\geq 0} \to \mathbf{R}$. Addirittura, diventa biiettiva come funzione $f : \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$: la sua funzione inversa $f^{-1} : \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$ è... ben nota ed è data da $f^{-1}(y) = \sqrt{y}$.

Analogamente, la funzione esponenziale $f(x) = 10^x$ è una funzione totale e iniettiva di $\mathbf{R}$ in $\mathbf{R}$, con $\mathrm{Im}(f) = \mathbf{R}_{>0}$. La sua inversa è una funzione biiettiva $f^{-1} : \mathbf{R}_{>0} \to \mathbf{R}$ ed è data da $f^{-1}(y) = \log_{10}(y)$.

Infine, la funzione periodica $f(x) = \sin x$ è... "assai poco iniettiva" come funzione da $\mathbf{R}$ in $\mathbf{R}$, essendo 2π-periodica. È però biiettiva se la consideriamo come funzione $f : [-\pi/2, \pi/2] \to [-1, 1]$. La sua inversa $f^{-1} : [-1, 1] \to [-\pi/2, \pi/2]$ è la funzione *arcoseno*: $f^{-1}(y) = \arcsin(y)$.

¡¡¡WARNING!!!! DANGER!!! Da quanto appena discusso, dovreste avere ormai capito che con la notazione $f^{-1}(x)$ si denota la *funzione inversa*, che è cosa *ben diversa dal reciproco di* $f(x)$, ossia $f^{-1}(x) \neq 1/f(x)$!!!!

Cominciamo ora a occuparci di qualcosa di più divertente: come possiamo contare quanti elementi contiene un insieme *infinito*?

Se A e B sono insiemi *finiti* con lo stesso numero n di elementi, allora esiste una funzione biiettiva da A in B. Infatti, se A ha n elementi esiste una funzione biiettiva f tra l'insieme $\{0, 1, 2, \ldots, n-1\}$ e A (la funzione che "conta" gli elementi di A). Analogamente, se B ha n elementi c'è una biiezione $g : \{0, 1, 2, \ldots, n-1\} \to B$. Ma allora la funzione $g \circ f^{-1} : A \to B$ è una biiezione.

Viceversa, se due insiemi finiti sono in biiezione, allora hanno lo stesso numero di elementi: supponiamo che A e B siano in biiezione tramite f e che A abbia n elementi. C'è quindi una funzione biiettiva $g : \{0, 1, 2, \ldots, n-1\} \to A$. Ma allora $f \circ g : \{0, 1, 2, \ldots, n-1\} \to B$ è una biiezione e anche g ha n elementi.

Possiamo usare la stessa idea per "confrontare" insiemi infiniti:

DEFINIZIONE: Diremo che due insiemi A e B hanno la stessa cardinalità (e scriveremo $|A| = |B|$) se e soltanto se esiste una funzione biiettiva $f : A \to B$.

La proprietà di "avere la stessa cardinalità" gode della *proprietà riflessiva*: $|A| = |A|$ per ogni insieme A e della *proprietà simmetrica*: se $|A| = |B|$ allora

$|B| = |A|$. Gode anche della *proprietà transitiva*: se $|A| = |B|$ e $|B| = |C|$, allora $|A| = |C|$.

Si tratta di tre proprietà che ci aspettiamo da qualcosa che in fondo vogliamo interpretare come una sorta di "uguaglianza" (l'uguaglianza del "numero di elementi", intesa in un senso opportuno per gli insiemi infiniti). Tutte assieme, ci consentono "quasi" di dire che "avere la stessa cardinalità" è una *relazione di equivalenza* (ne parleremo diffusamente in seguito!), anche se non sarebbe del tutto corretto perchè la classe di tutti gli insiemi non è un insieme...

Per gli insiemi finiti, avere la stessa cardinalità è la stessa cosa che avere lo stesso numero di elementi: in particolare, nessun insieme finito può essere in biiezione con un suo sottinsieme proprio.

Questo non è più vero per gli insiemi infiniti! A questo proposito, vi ho raccontato la simpatica storiella dell'*albergo di Hilbert*, che può essere distillata come segue: i seguenti 4 insiemi, che diventano sempre più piccoli da sinistra a destra, hanno tutti la stessa cardinalità

$$|\mathbf{Z}| = |\mathbf{N}| = |\mathbf{N} \setminus \{0\}| = |2\mathbf{N}|$$

(con $2\mathbf{N} = \{2n : n \in \mathbf{N}\}$ denotiamo l'insieme dei numeri naturali pari). Una biiezione tra $\mathbf{N}$ e $\mathbf{N} \setminus \{0\}$ è data da $n \mapsto n + 1$, una tra $\mathbf{N}$ e $2\mathbf{N}$ è data da $n \mapsto 2n$. Infine, una biiezione tra $\mathbf{Z}$ e $\mathbf{N}$ è data da

$$n \mapsto \begin{cases} 2n & \text{se } n \geq 0, \\ -2n - 1 & \text{se } n < 0. \end{cases}$$

Gli insiemi che hanno la stessa cardinalità di $\mathbf{N}$ si dicono *numerabili* (in quanto una biiezione $f : \mathbf{N} \to A$ non fa altro che "contare" o "enumerare" gli elementi di A). Sono numerabili gli insiemi scritti sopra, ma vedremo presto che lo sono anche insiemi apparentemente molto più grossi come $\mathbf{Q}$!

Abbiamo visto (si pensi all'albergo di Hilbert) che $\mathbf{N}$ ha la stessa cardinalità di diversi suoi sottinsiemi propri. Questo fatto caratterizza gli insiemi infiniti (numerabili e non):

PROPOSIZIONE: Un insieme A è infinito se e soltanto se esiste un suo sottinsieme proprio B tale che $|B| = |A|$.

DIM.: Abbiamo già visto che se A è finito allora non c'è alcun sottinsieme proprio con tale proprietà.

Se invece A è infinito, è possibile costruire una funzione $f : \mathbf{N} \to A$ totale e iniettiva.

Per farlo, scegliamo $x_0 \in A$ (c'è perché A, essendo infinito, non è vuoto). Scegliamo poi $x_1 \in A \setminus \{x_0\}$ (c'è perché altrienti A avrebbe 1 elemento). Segliamo poi $x_2 \in A \setminus \{x_0, x_1\}$, $x_3 \in A \setminus \{x_0, x_1, x_2\}$,... Questo processo non si arresta perchè togliendo ad A un numero finito di elementi rimane sempre qualcosa! La funzione $f : \mathbf{N} \to A$ data da $n \mapsto x_n$ è chiaramente totale e iniettiva.

Sia $B = A \setminus \{x_0\}$ e costruiamo la seguente biiezione $h : A \to B$

$$h(a) = \begin{cases} a & \textit{se } a \notin \mathrm{Im}(f), \\ x_{n+1} & \textit{se } a = x_n \textit{ per un } n \in \mathbf{N}. \end{cases}$$

In sostanza, la funzione h lascia fermi gli elementi di A che non appartengono alla successione x_n, mentre sposta ogni elemento di questa in quello che lo segue: si trata di un trucco alla "albergo di Hilbert" che libera il punto x_0! Q.E.D.

Nella dimostrazione del teorema precedente, per costruire la funzione f abbiamo scelto un sottinsieme numerabile $\{x_0, x_1, x_2, \ldots\}$ dell'insieme infinito A: in qualche modo, questo ci dice che gli insiemi infiniti hanno "come minimo" cardinalità numerabile.

Per formalizzare questa intuizione diamo la seguente

DEFINIZIONE: Scriviamo $|A| \leq |B|$ se e soltanto se esiste una funzione *totale* e *iniettiva* $f : A \to B$.

In effetti, notiamo subito che se $C \subset B$, allora $|C| \leq |B|$: la cardinalià di un sottinsieme è sempre più piccola di quella dell'insieme di di partenza (basta prendere la funzione totale e iniettiva $c \mapsto c$). Inoltre, una funzione totale e iniettiva $f : A \to B$ è una biiezione tra A e $\mathrm{Im}(f) \subset B$: A ha quindi la stessa cardinalità di un sottinsieme di B.

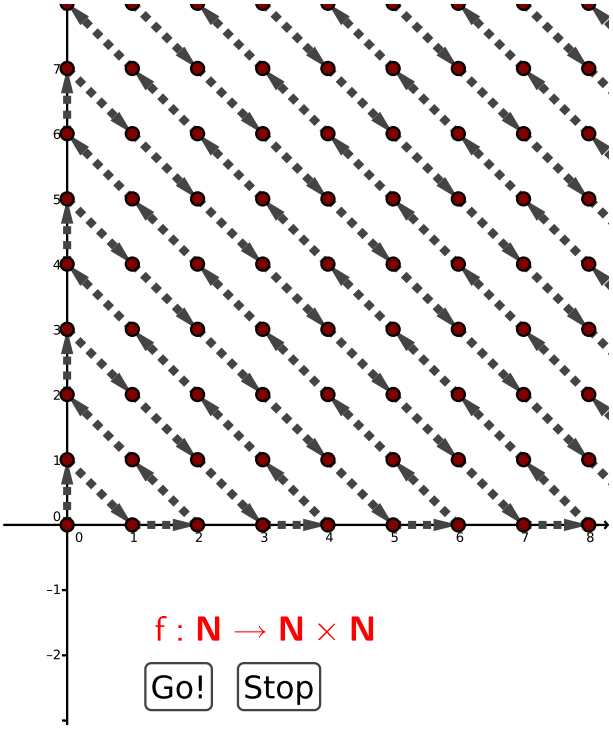
Alla luce di questa definizione, vediamo subito che dimostrando il teorema precedente (costruzione della funzione f) abbiamo in realtà dimostrato anche il seguente importante risultato:

PROPOSIZIONE: Se A è infinito, allora $|\mathbf{N}| \leq |A|$.

Anche insiemi apparentemente molto più "grossi" di $\mathbf{N}$ sono numerabili: abbiamo già visto che $|\mathbf{Z}| = |\mathbf{N}|$. Però vale anche che $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$, fatto un bel po' meno ovvio!

PROPOSIZIONE: Si ha $|\mathbf{N}| = |\mathbf{N} \times \mathbf{N}| = |\mathbf{Z} \times \mathbf{Z}|$.

DIM.: Una funzione biiettiva $f : \mathbf{N} \to \mathbf{N} \times \mathbf{N}$ può essere costruita utilizzando l'idea in figura.



Per vedere una versione animata della costruzione, che ho realizzato con GeoGebra, si clicchi sulla figura o si vada a
`http://www.geogebratube.org/student/m86268`

Poiché $|\mathbf{N}| = |\mathbf{Z}|$, dal fatto che $\mathbf{N} \times \mathbf{N}$ è numerabile segue che anche $\mathbf{Z} \times \mathbf{Z}$ è numerabile: vedremo tra un attimo come da questo discenda la numerabilità di $\mathbf{Q}$. Q.E.D.

La prossima volta vedremo un risultato molto profondo della teoria delle cardinalità: il *Teorema di Cantor-Schroeder-Bernstein*, che afferma che dati due insiemi A e B, se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$. Si tratta di un risultato importante e per nulla banale!

Se però, per il momento, lo diamo per buono, possiamo dimostrare molto facilmente che $|\mathbf{Q}| = |\mathbf{N}|$:

PROPOSIZIONE: L'insieme dei numeri razionali è numerabile

DIM.: Si ha ovviamente $|\mathbf{N}| \leq |\mathbf{Q}|$, perché i numeri naturali sono un sottinsieme dei razionali.

D'altra parte, possiamo costruire una funzione totale e iniettiva g da $\mathbf{Q}$ in $\mathbf{Z} \times \mathbf{Z}$ nel modo seguente: se $q \in \mathbf{Q}$, possiamo scrivere in modo unico $q = m/n$ ove $m \in \mathbf{Z}$, $n \in \mathbf{N}_{>0}$ e $MCD(m, n) = 1$ (ossia la frazione è ridotta ai minimi termini). Poniamo allora $g(q) = (m, n)$. Ne segue che $|\mathbf{Q}| \leq |\mathbf{Z} \times \mathbf{Z}| = |\mathbf{N}|$ e grazie al teorema di Cantor-Schröder-Bernstein $|\mathbf{Q}| = |\mathbf{N}|$. Q.E.D.

3 Lezione del 15/2/2018

Torniamo alla disuguaglianza tra cardinalità: ricordo che, per definizione, $|A| \leq |B|$ se e solo se esiste una funzione totale e iniettiva $f : A \to B$.

Siccome la composizione di due funzioni totali e iniettive $f : A \to B$, $g : B \to C$ è totale e iniettiva, abbiamo subito la proprietà transitiva: $|A| \leq |B|$, $|B| \leq |C|$ implica $|A| \leq |C|$. Meno ovvio è che valga la proprietà antisimmetrica: è la tesi del seguente teorema...grazie al quale la nostra disuguaglianza tra cardinalità gode di tutte le proprietà che ci attendiamo!

TEOREMA (Cantor-Schröder-Bernstein): Siano A, B due insiemi tali che $|A| \leq |B|$ e $|B| \leq |A|$. Allora $|A| = |B|$.

DIM.: Abbiamo due funzioni totali e iniettive $f : A \to B$ e $g : B \to A$. Dobbiamo usarle per costruire una funzione biiettiva! L'idea consiste nel seguire la... genealogia degli elementi di A e B: dato $b \in B$, diciamo che $a \in A$ è il suo *genitore* se $b = f(a)$. Il genitore potrebbe non esserci (cioè b potrebbe essere orfano), altrimenti è unico perché f è iniettiva.

Analogamente, se $a \in A$, diremo che un elemento $b \in B$ è il suo genitore se $a = g(b)$: anche stavolta, se c'è un genitore esso è unico!

Dato $a \in A$, andiamo ad analizzare la sua genealogia: potrebbe avere un genitore in B, che a sua volta potrebbe essere orfano oppure avere un genitore in A, che a sua volta potrebbe essere orfano o avere un genitore in B... Questo processo di "ricerca degli antenati" potrebbe continuare all'infinito, oppure fermarsi in un elemento orfano (che chiamiamo il *capostipite* di a). Suddividiamo dunque A in tre insiemi due a due disgiunti

- A_0 è costituito dagli elementi di A che hanno una successione infinita di antenati.
- A_A è costituito dagli elementi di A che hanno un capostipite in A.
- A_B è costituito dagli elementi di A che hanno un capostipite in B.

In maniera del tutto analoga, andando ad analizzare gli antenati degli elementi di B, riusciamo a partizionare B nei tre sottinsiemi B_0, B_A e B_A definiti analogamente a prima.

Consideriamo la funzione $f : A_0 \to B_0$. Essa è ovviamente totale e iniettiva. È anche suriettiva: se $b \in B_0$, esso per definizione non è orfano, ed il suo genitore appartiene ad A_0. Quindi f è una biiezione tra A_0 e B_0. Anche $f : A_A \to B_A$ è una biiezione: è totale e iniettiva, inoltre il genitore di qualunque $b \in B_A$ deve necessariamente appartenere ad A_A. Infine, per l'analogo motivo $g : B_B \to A_B$ è una biiezione.

Possiamo quindi definire una biiezione da $h : A \to B$ nel modo seguente: sugli elementi di A_0 e A_A, h coincide con f, mentre sugli elementi di A_B essa coincide con g^{-1}. Q.E.D.

Il teorema di Cantor-Schröder Bernstein (dovuto essenzialmente a Cantor nonostante i 3 nomi...) è un risultato piuttosto profondo: si provi per esempio a costruire "a mano" una biiezione tra gli intervalli $[0,1] = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$ e $[0,1) = \{x \in \mathbf{R} : \ 0 < x \leq 1\}$. Vedrete che non è facilissimo (se non ci riuscite posso dirvi come fare...).

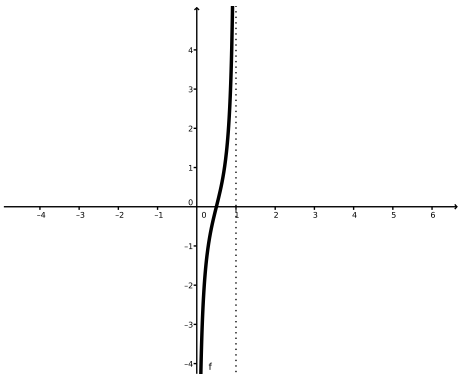
Invece, con il teorema di Cantor Schröder Bernstein, si vede subito che la cardinalità dei due intervalli è la stessa. Infatti, $|[0,1)| \leq |[0,1]|$ perché il primo intervallo è un sottinsieme del secondo. Invece, una funzione totale e iniettiva da $[0,1]$ in $[0,1)$ è data per esempio da $x \mapsto x/2$, da cui $|[0,1]| \leq |[0,1)|$.

Ci sono però anche insiemi di cardinalità strettamente maggiore del numerabile.

Dimostriamo subito che, anche nel senso delle cardinalità infinite, i numeri reali sono *più* dei numeri naturali!

PROPOSIZIONE: $|\mathbf{N}| < |\mathbf{R}|$ *(ossia* $|\mathbf{N}| \leq |\mathbf{R}|$ *e i due insiemi non hanno la stessa cardinalità).*

DIM.: Innanzitutto osserviamo che l'intervallo $(0,1)$ ha la stessa cardinalità di $\mathbf{R}$: una biiezione tra questi due insiemi è data per esempio da $x \mapsto \tan(\pi(x - \frac{1}{2}))$ o da $x \mapsto \frac{x-\frac{1}{2}}{x(1-x)}$. Ecco il grafico della seconda di queste due funzioni:



Per far vedere che $(0,1)$ non ha la stessa cardinalità di $\mathbf{N}$, basta far vedere che una *qualunque* funzione totale $f : \mathbf{N} \to (0,1)$ *non può essere suriettiva.*

Sia dunque f una tale funzione: scriviamo i numeri reali $f(0)$, $f(1)$, $f(2)$,... come *numeri decimali* con infinite cifre dopo la virgola. Per rendere

unica la scrittura, conveniamo di evitare le scritture che terminano con una "coda" di infiniti 9: grazie a questo accorgimento, due numeri decimali sono uguali se e solo se tutte le loro cifre coincidono!

Avremo dunque

$$\begin{aligned} f(0) &= 0, a_0a_1a_2a_3a_4a_5\ldots \\ f(1) &= 0, b_0b_1b_2b_3b_4b_5\ldots \\ f(2) &= 0, c_0c_1c_2c_3c_4c_5\ldots \\ f(3) &= 0, d_0d_1d_2d_3d_4d_5\ldots \\ f(4) &= 0, e_0e_1e_2e_3e_4e_5\ldots \\ \ldots &\quad \ldots \end{aligned}$$

Costruiamo un nuovo numero decimale $x_0 = 0, \alpha_0\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\ldots$ in cui le cifre sono scelte in modo che α_k sia *diversa* dalla k-esima cifra di $f(k)$ e da 9: per esempio, se la k-esima cifra di $f(k)$ è pari, scegliamo $\alpha_k = 5$, se la k-esima cifra di $f(k)$ è dispari scegliamo $\alpha_k = 2$.

x_0 è un numero reale compreso tra 0 e 1 che non appartiene ad $\mathrm{Im}(f)$ perché per come è stato costruito differisce da tutti gli $f(k)$. Q.E.D.

Si può dimostrare in maniera abbastanza semplice che la cardinalità di $\mathbf{R}$ è uguale a quella dell'*insieme delle parti* di $\mathbf{N}$, ossia a quella dell'insieme $\mathcal{P}(\mathbf{N})$ di tutti i sottinsiemi di $\mathbf{N}$ (vedremo poi la dimostrazione):

PROPOSIZIONE: Esiste una funzione biiettiva da $\mathbf{R}$ *a* $\mathcal{P}(\mathbf{N})$.

Che l'insieme delle parti sia "più grosso" dell'insieme di partenza è un fatto del tutto generale: dato un qualunque insieme A, l'insieme $\mathcal{P}(A)$ dei suoi sottinsiemi (detto insieme delle parti di A) ha cardinalità strettamente maggiore di quella di A. In particolare, esistono cardinalità infinite arbitrariamente grandi!

TEOREMA (Cantor): Se A *è un insieme e* $\mathcal{P}(A)$ *l'insieme di tutti i suoi sottinsiemi, allora* $|A| < |\mathcal{P}(A)|$.

DIM.: La dimostrazione usa un metodo diagonale che generalizza (in maniera un pochino più astratta) quello che abbiamo usato per mostrare che $\mathbf{R}$ non è numerabile.

Innanzitutto, notiamo che la funzione $f : A \to \mathcal{P}(A)$ definita da $a \mapsto \{a\}$ è totale e iniettiva, per cui $|A| \leq |\mathcal{P}(A)|$.

Mostriamo che una qualsiasi data funzione $g : A \to \mathcal{P}(A)$ *non può essere suriettiva*, per cui vale la disuguaglianza stretta. È sufficiente considerare il seguente insieme $B \in \mathcal{P}(A)$:

$$B = \{a \in A : \ a \notin g(a)\}.$$

Dico che non esiste alcun $a \in A$ tale che $g(a) = B$. Infatti, o $a \in B$ o $a \notin B$. Se $a \in B$ allora per definizione $a \notin g(a)$ e quindi $B \neq g(a)$. Viceversa, se $a \notin B$ allora $a \in g(a)$ e abbiamo ancora $B \neq g(a)$. Q.E.D.

PROPOSIZIONE: Esiste una funzione biiettiva da $\mathbf{R}$ *a* $\mathcal{P}(\mathbf{N})$.

DIM.: Grazie al teorema di Cantor-Schröder-Bernstein, ci basta costruire due funzioni totali e iniettive $f : [0,1) \to \mathcal{P}(\mathbf{N})$ e $g : \mathcal{P}(\mathbf{N}) \to [0,1)$. Al posto di $\mathbf{R}$, usiamo l'intervallo $[0,1)$ che tanto ha la stessa cardinalità[2].

Osserviamo preliminarmente che i numeri reali tra 0 e 1 si possono rappresentare come *decimali binari* o *numeri decimali in base* 2 ossia con una scrittura del tipo $x = 0, a_0a_1a_2a_3a_4\ldots$, ove le cifre a_i $(i = 0, 1, 2, 3, \ldots)$ possono essere soltanto 0 o 1. Questa scrittura va letta nel modo seguente:

$$x = \frac{a_0}{2} + \frac{a_1}{2^2} + \frac{a_2}{2^3} + \frac{a_3}{2^4} + \ldots + \frac{a_k}{2^{k+1}} + \ldots,$$

in perfetta analogia con l'usuale interpretazione dei numeri decimali in base 10. Come per i decimali in base 10, ci sono dei casi in cui la scrittura decimale binaria non è unica: questo succede precisamente per i numeri razionali che a denominatore hanno una potenza di due, che si possono scrivere usando un numero finito di cifre binarie diverse da 0, oppure con una coda infinita di tutti 1... In questi casi, conveniamo di scegliere la rappresentazione che *non* termina con una coda di infiniti 1.

A questo punto, dato $x \in [0,1)$, lo rappresentiamo come sopra come decimale binario e definiamo

$$f(x) = \{n \in N : \ a_n = 1\}$$

(ossia $f(x)$ è l'insieme dei numeri naturali che corrispondono al numero d'ordine delle cifre binarie diverse da 0 di x). La funzione f è evidentemente totale e iniettiva da $[0,1)$ in $\mathcal{P}(N)$. L'iniettività viene proprio dalla nostra convenione che ci ha permesso di eliminare ogni ambiguità nella rappresentazione decimale binaria.

Non è purtroppo suriettiva: non contiene nessun sottinsieme di $\mathbf{N}$ che contenga tutti i numeri naturali "da un certo punto in poi", per esempio non contiene $\mathbf{N}$ stesso.

Poco male: definiamo $g : \mathcal{P}(\mathbf{N}) \to [0,1)$ totale e iniettiva come segue. Dato $A \subset \mathbf{N}$, prendiamo il numero decimale binario $f(A) = 0, b_0b_1b_2b_3b_4\ldots$

[2]Abbiamo visto esplicitamente che $[0,1]$ e $(0,1]$ hanno la stessa cardinalità... In maniera del tutto analoga si dimostra che $[0,1)$ e $(0,1)$ hanno la stessa cardinalità e sappiamo già che l'intervallo aperto ha la stessa cardinalità di $\mathbf{R}$! Si mostri più in generale per esercizio che tutti gli intervalli non banali di $\mathbf{R}$ hanno cardinalità uguale a quella di $\mathbf{R}$.

tale che ha *tutte le cifre di posto dispari pari a* 0, mentre per le cifre pari scegliamo $b_{2k} = 1$ se $k \in A$, 0 altrimenti ($k = 0, 1, 2, 3, \ldots$). Q.E.D.

Abbiamo concluso la lezione svolgendo gli esercizi sulle cardinalità infinite di alcuni compiti d'esame degli anni scorsi.

4 Lezione del 22/2/2018

Conclusa la parte sulle cardinalità, abbiamo ripreso le relazioni, imparando cosa sono le relazioni di equivalenza e le relazioni d'ordine... e abbiamo svolto qualche esercizio "tipo esame".

Riassumo le principali definizioni che abbiamo usato (vedere le già citate dispense di Enrico e Francesca!).

DEFINIZIONI: Sia $R \subset X \times X$ una relazione su un insieme X.

- R si dice *riflessiva* se $\forall x \in X$ si ha $(x, x) \in R$.
- R si dice *simmetrica* se $(x, y) \in R$ implica $(y, x) \in R$.
- R si dice *transitiva* se $(x, y) \in R,\ (y, z) \in R$ implica $(x, z) \in R$.
- Se R è riflessiva, simmetrica e transitiva, allora si dice *relazione d'equivalenza*.
- R si dice *antiriflessiva* se $\forall\ x \in X$ si ha $(x, x) \notin R$.
- Se R è antiriflessiva e transitiva, allora si dice *relazione d'ordine stretto* Si usa la notazione $x \prec y \Leftrightarrow (x, y) \in R$.
- R si dice *antisimmetrica* se $(x, y) \in R$ e $(y, x) \in R$ implica $x = y$.
- Se R è transitiva, antisimmetrica e riflessiva, allora si dice *relazione d'ordine largo*. Si usa la notazione $x \preceq y \Leftrightarrow (x, y) \in R$.

ESEMPI: Cominciamo con alcuni esempi di relazioni d'equivalenza.

- $R = \{(x, y) \in X \times X :\ x = y\}$, ove X è un insieme fissato.
- $R = \{(x, y) \in \mathbf{N} \times \mathbf{N} :\ x, y$ hanno lo stesso resto della divisione per $n\}$ ove $n \in \mathbf{N}$ è fissato.
- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} :\ x - y = 2k\pi,\ k \in \mathbf{Z}\}$.
- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} :\ x - y \in \mathbf{Q}\}$.

Alcuni esempi di relazioni d'ordine stretto:

- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} :\ x < y\}$.
- $R = \{(A, B) :\ A, B \subset X,\ A \subsetneq B\}$, X un insieme fissato.
- $R = \{(m, n) \in \mathbf{N} \times \mathbf{N} :\ m$ divide $n,\ m \neq n\}$.

Alcuni esempi di relazioni d'ordine largo:

- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} : \ x \leq y\}$.
- $R = \{(A, B) : \ A, B \subset X, \ A \subset B\}$, X insieme fissato.
- $R = \{(m, n) \in \mathbf{N} \times \mathbf{N} : \ m \text{ divide } n\}$.

Si intuisce facilmente che c'è un forte legame tra le relazioni d'ordine strette e larghe su un insieme. Precisamente:

TEOREMA: Se R è una relazione d'ordine largo su X, allora $R' = \{(a, b) \in R : \ a \neq b\}$ è una relazione d'ordine stretto. Analogamente, se S è una relazione d'ordine stretto su X, allora $S' = S \cup \{(a, a) : a \in X\}$ è una relazione d'ordine largo su X.

DIM.: R' è antiriflessiva per costruzione. Bisogna solo verificare che rimane transitiva. Siano dunque $(a, b) \in R'$, $(b, c) \in R'$: ci chiediamo se è vero che $(a, c) \in R'$. Abbiamo certamente $(b, c) \in R$ (transitività di R), per cui se fosse per assurdo $(a, c) \notin R'$ avremmo $a = c$. Ma questo è assurdo perché la proprietà antisimmetrica ci darebbe $a = b$.

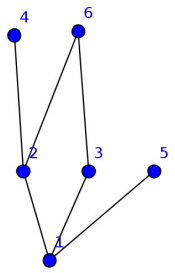
Analogamente, S' è chiaramente riflessiva e transitiva. Verifichiamo che è antisimmetrica: sia $(a, b) \in S'$, $(b, a) \in S'$. Non può essere che queste due coppie stiano in S, altrimenti per transitività avremmo $(a, a) \in S$ che è vietato dalla proprietà antiriflessiva. Quindi almeno una delle due non vi appartiene e abbiamo necessariamente $a = b$. Q.E.D.

Abbiamo concluso la lezione facendo un po' di esercizi sulle relazioni di equivalenza e d'ordine.

5 Lezione del 1/3/2018

Un buon modo, molto espressivo, per rappresentare una relazione d'ordine (largo o stretto) R su insiemi finiti, è dato dai cosiddetti *diagrammi di Hasse*. La regola è che se $(a, b) \in R$ e "non ci sono punti in mezzo" (cioè non c'è nessun c, distinto da a e b, tale che $(a, c) \in R$ e $(c, b) \in R$), allora rappresentiamo nel nostro diagramma i due punti, con b *sopra* a e connessi da un segmento. In sostanza, mettiamo i punti "più grandi" sopra quelli "più piccoli" e li colleghiamo in modo da sottolineare che stanno in relazione. Per semplificare il diagramma, omettiamo però i collegamenti che sono impliciti per la proprietà transitiva.

Per esempio, ecco il diagramma di Hasse della relazione di stretta divisibilità sull'insieme dei numeri naturali compresi tra 1 e 6:



Le seguenti sono definizioni importanti nello studio degli insiemi ordinati e delle proprietà dei loro sottinsiemi dal punto di vista della relazione d'ordine:

DEFINIZIONI: Sia $\prec$ una relazione d'ordine stretto su un insieme X, $S \subset X$.

- $y \in X$ si dice *maggiorante* per S se per ogni $x \in S$ si ha $x = y$ oppure $x \prec y$: y è confrontabile con tutti gli elementi di S ed è "più grande" di tutti questi. Analogamente si definiscono i *minoranti* di S: sono elementi $y \in X$ tali che per ogni $x \in S$ si ha $y = x$ oppure $y \prec x$. Maggioranti e minoranti possono non esistere, oppure possono essercene tanti!

- $y \in S$ si dice *massimo* di S se per ogni $x \in S$ si ha $x = y$ oppure $x \prec y$. Analogamente si definisce il *minimo* di un sottinsieme di X: è l'elemento $y \in S$ tale che per ogni $x \in S$ si ha $x = y$ oppure $y \prec x$. Massimo e minimo possono non esistere, se ci sono sono unici.

- $y \in X$ è l'*estremo superiore* di S se è il *minimo* dei maggioranti di S. Analogamente, $z \in X$ è l'*estremo inferiore* di S se è il *massimo dei minoranti di* S. Potrebbero non esistere. Se uno di essi c'è, è anche unico! Se per caso uno di essi appartiene a S, ne è rispettivamente massimo o minimo.

- $y \in S$ è un elemento *massimale* di S se per ogni $x \in S$ si ha $y = x$ oppure $(y, x) \notin R$: y è più grande di tutti gli elementi di S *con cui è confrontabile*. Analogamente $y \in S$ si dice *minimale* di S se per ogni $x \in S$ si ha $y = x$ oppure $(x, y) \notin R$: y è più piccolo di tutti gli elementi di S con cui è confrontabile. Gli elementi massimali e minimali, in generale, possono non esistere o non essere unici.

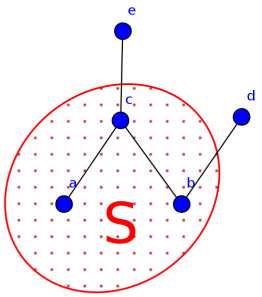
Nel caso di insiemi finiti, è facile individuare questi elementi utilizzando dei diagrammi di Hasse. Svolgiamo un esercizio di esempio tratto da un compito (in aula ne abbiamo visti altri):

ESERCIZIO: Sull'insieme $X = \{a, b, c, d, e\}$ si consideri la relazione

$$R = \{(a, c), (b, c), (b, d), (c, e), (a, e), (b, e)\}.$$

Verificare se si tratta di una relazione d'ordine stretto. In caso affermativo, determinare gli eventuali maggioranti, minoranti, massimali, minimali, estremo superiore, estremo inferiore, massimo, minimo del sottinsieme $S = \{a, b, c\}$.

Sol.: Costruiamo il diagramma di Hasse della nostra relazione:



(abbiamo cerchiato i 3 elementi dell'insieme X che fanno parte del sottinsieme S).

Notiamo subito, cosa non evidente a priori dal diagramma di Hasse, che la relazione è transitiva (vi appartengono infatti (a, e) e (b, e)) e antiriflessiva (nessun elemento è in relazione con se stesso): si tratta proprio di una relazione d'ordine stretto.

Dal diagramma, vediamo subito che S ha a e b come elementi minimali (che non sono né minimi né minoranti). Invece, c è sia elemento massimale che massimo che maggiorante che estremo superiore. Anche e è un maggiorante di S.

Il concetto di estremo superiore è estremamente utile nello studio delle proprietà dei numeri reali.

Facendo mente locale, ci si rende facilmente conto che passare dall'aritmetica sui numeri razionali a quella sui reali non è affatto un'operazione indolore: qualunque sia il modello dei numeri reali che assumiamo (per esempio quello dei numeri decimali infiniti), non è poi semplicissimo definire le quattro operazioni e dimostrare che esse godono di tutte le proprietà che ci attendiamo!

D'altra parte, i numeri reali diventano indispensabili se vogliamo estrarre radici quadrate e definire le funzioni trascendenti: storicamente, è stato proprio il fatto che la radice quadrata di 2 non esiste nei razionali (non esiste alcun numero razionale che elevato al quadrato dia 2) a indurre i matematici greci alla definizione di quantità irrazionali!

Qualunque sia il nostro modello di $\mathbf{R}$, è però relativamente facile dimostrare che l'insieme $\mathbf{R}$ dei numeri reali ha la seguente proprietà:

ASSIOMA DI COMPLETEZZA DI $\mathbf{R}$*: Ogni insieme non vuoto* $A \subset \mathbf{R}$ *che possegga almeno un maggiorante reale, ha estremo superiore in* $\mathbf{R}$.

Questa proprietà (o una delle sue numerose formulazioni equivalenti) risulta la chiave per dimostrare, per esempio, che esiste la radice quadrata di un numero reale non negativo! Vediamo come fare...

Consideriamo la parabola $y = x^2$. Dato $a > 0$, il numero $\sqrt{a}$ è l'ascissa dell'unico punto della parabola situato nel primo quadrante e con ordinata a (ovvero l'ascissa b dell'intersezione, situata nel primo quadrante, tra la parabola e la retta $y = a$).

Il fatto che retta e parabola si debbano intersecare è plausibile... ma è anche evidente che richiede l'assioma di completezza: geometricamente, dobbiamo essere sicuri che sia la retta che la parabola siano curve "continue e senza buchi", altrimenti l'intersezione potrebbe non esserci!

Osserviamo che la funzione $f(x) = x^2$ è strettamente crescente (e quindi iniettiva) per $x > 0$: se un numero positivo b tale che $b^2 = a$ esiste, esso è certamente unico.

Inoltre, osserviamo che $0^2 < a$ e che esiste un numero $M > 0$ tale che $M^2 > a$: ci sono punti della semiretta dei reali non negativi sopra i quali la parabola è *più bassa* della retta $y = a$ (per esempio $x = 0$) ed altri in cui è *più alta*. Per esibire un tale M, basta scegliere $M = 1$ se $a < 1$, $M = a$ se $a > 1$ (per $a = 1$ l'enunciato del teorema è ovvio con $b = 1$).

Per $k = 0, 1, 2, 3, \ldots$, definiamo una successione di intervalli $[\alpha_k, \beta_k]$, ciascuno contenuto nel precedente e con lunghezze che diventano arbitrariamente piccole, utilizzando il seguente *metodo di bisezione*.

Cominciamo da $[\alpha_0, \beta_0] = [0, M]$. Dividiamo poi l'intervallo a metà tramite il punto centrale $m_0 = M/2$: se $m_0^2 = a$ abbiamo vinto, altrimenti si ha $m_0^2 < a$ oppure $m_0^2 > a$. Nel primo caso, definiamo $[\alpha_1, \beta_1] = [m_0, \beta_0]$, nel secondo $[\alpha_1, \beta_1] = [\alpha_0, m_0]$: con questa scelta avremo che $\alpha_1^2 < a$, $\beta_1^2 > a$.

Allo stesso modo, dividiamo il nuovo intervallo $[\alpha_1, \beta_1]$ a metà tramite il punto m_1: ancora, se $m_1^2 = a$ abbiamo vinto, altrimenti si avrà $m_1^2 < a$ oppure $m_1^2 > a$. Nel primo caso definiamo $[\alpha_2, \beta_2] = [m_1, \beta_1]$, nel secondo $[\alpha_2, \beta_2] = [\alpha_1, m_1]$: con questa scelta avremo che $\alpha_2^2 < a$, $\beta_2^2 > a$. Procediamo poi allo stesso modo: dividiamo a metà $[\alpha_2, \beta_2$ tramite il suo punto di mezzo e scegliamo quella delle due metà (la chiameremo $[\alpha_3, \beta_3]$) che ha la proprietà che $\alpha_3^2 < a < \beta_3^2 \ldots$ e così via.

L'insieme dei punti $\{\alpha_k : \ k = 0, 1, 2, \ldots\}$ ammette estremo superiore $b \in \mathbf{R}$ grazie all'assioma di completezza: questo sarà anche l'unico punto comune a tutti gl intervalli che abbiamo costruito. È immediato intuire che $b^2 = a$.

Per dimostrarlo, osserviamo che

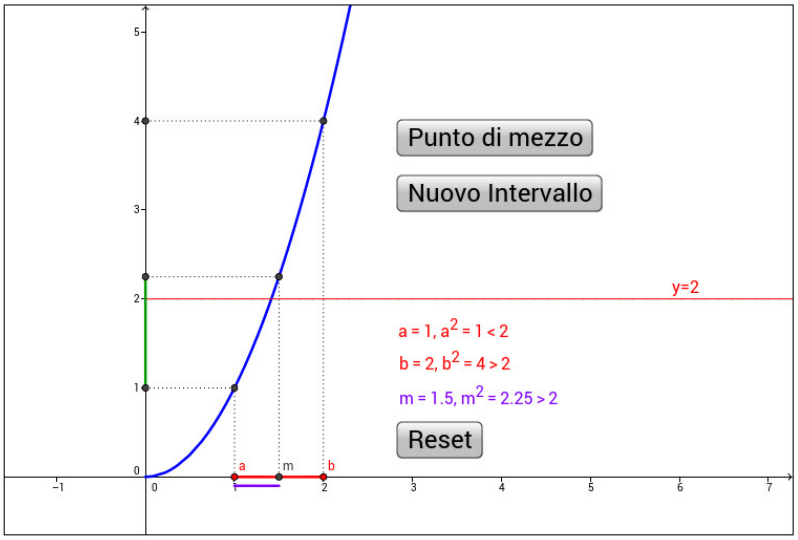
$$\alpha_k^2 \leq b^2 \leq \beta_k^2.$$

In più, α_k^2 e β_k^2 diventano arbitrariamente vicini tra loro al crescere di k:

$$\beta_k^2 - \alpha_k^2 = (\beta_k - \alpha_k)(\beta_k + \alpha_k) \leq \frac{2M}{2^k}.$$

Ne segue subito che b^2, compreso tra esse, deve necessariamente essere uguale ad a perché questo è l'unico punto comune agli intervalli $[\alpha_k^2, \beta_k^2]$. Abbiamo trovato la radice quadrata di a, cioè un numero positivo il cui quadrato è a. Q.E.D.

Ecco un'animazione GeoGebra del metodo di bisezione applicato a questo problema (con $a = 2$).



Versione interattiva su `http://tube.geogebra.org/student/muV3bEZJm`