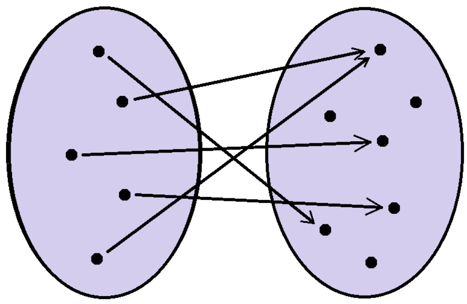
# L'INSIEME DEI NUMERI REALI

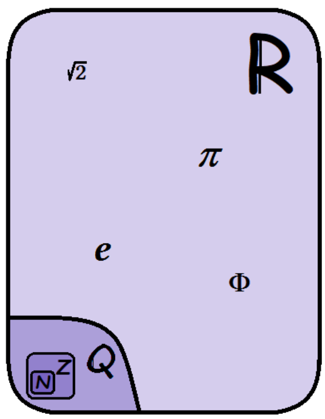
## E I SUOI PRINCIPALI SOTTOINSIEMI

Cosimo De Mitri










ANNO 2020

# A

# INSIEMI – RELAZIONI – FUNZIONI

## A1. Insiemi

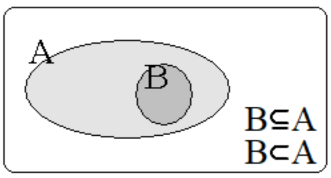
•) Del concetto di *insieme* non diamo una definizione rigorosa, anche perché la questione è piuttosto complessa e tutt'altro che risolta in via definitiva. Quindi *consideriamo il concetto di insieme come un concetto primitivo*, per il quale facciamo affidamento all'intuizione comune, che lo immagina come un *aggregato*, una *collezione*, una *famiglia*, una *classe* di oggetti di tipo qualsiasi. Comunque, allo scopo di evitare paradossi logici, è bene parlare di insiemi solo dopo aver fissato un insieme "universo", ossia l'ambiente da cui vanno presi gli oggetti per formare gli insiemi; la scelta dell'ambiente va fatta volta per volta, e spesso, quando risulta chiara dal contesto, è taciuta.
Gli oggetti che costituiscono un insieme si chiamano *elementi* dell'insieme; per indicare che l'oggetto $x$ è un elemento dell'insieme $A$ si usa la notazione $x \in A$, e si dice che $x$ *appartiene ad* $A$; la negazione di ciò è indicata con la notazione $x \notin A$.
Gli insiemi vengono indicati solitamente con le lettere maiuscole, come s'è visto, e vengono assegnati indicando tra parentesi graffe gli elementi che ne fanno parte, il che si ottiene o elencando esplicitamente questi elementi (e a volte se ne potranno elencare solo alcuni), oppure indicando una proprietà che li caratterizza. Si pensi ad esempio agli insiemi $\{sole,\ terra,\ luna\}$, $\{a, e, i, o, u\}$, $\{mi, sol, si, re, fa\}$, $\{1, 2, 3, 4, 5, \ldots\}$, $\{4, 6, 8, 10\}$, $\{n \in \mathbb{N} \,/\, n \text{ pari},\ 4 \leq n \leq 10\}$, dove si riconosce che gli ultimi due sono costituiti dagli stessi elementi. Gli insiemi costituiti da un unico elemento si chiamano *singoletti*. Un insieme particolare è l'*insieme vuoto*, cioè l'insieme privo di elementi, indicato con i simboli $\{\ \}$ e $\emptyset$. Spesso torna utile rappresentare graficamente gli insiemi mediante figure piane di forma ovale, note con il nome di *diagrammi di Venn*.

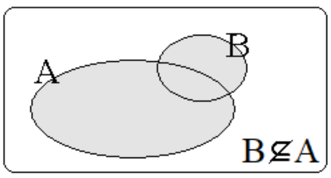
•) Dati gli insiemi $A$ e $B$, si dice che $B$ è *incluso* (o *contenuto*) in $A$, o ancora che $B$ è un *sottoinsieme* (o una *parte*) di $A$, e si scrive $B \subseteq A$, se ogni elemento di $B$ è anche elemento di $A$; si dice che $A$ è *uguale* a $B$, e si scrive $A = B$, se $A \subseteq B$ e $B \subseteq A$; si dice infine che $B$ è *incluso propriamente* in $A$, oppure che $B$ è un *sottoinsieme proprio* di $A$, e si scrive $B \subset A$, se $B \subseteq A$ e $A \neq B$. Riassumendo:

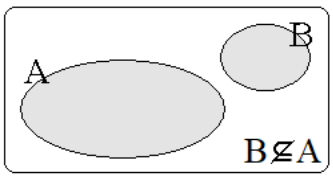
$B \subseteq A \overset{def}{\Longleftrightarrow} \forall x,\ x \in B \ \Rightarrow\ x \in A$;

$A = B \overset{def}{\Longleftrightarrow} \forall x,\ x \in A \ \Leftrightarrow\ x \in B$;

$B \subset A \overset{def}{\Longleftrightarrow} (\forall x,\ x \in B \ \Rightarrow\ x \in A) \ \wedge\ (\exists x :\ x \in A \ \wedge\ x \notin B)$.





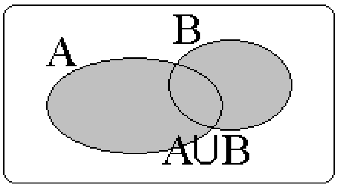


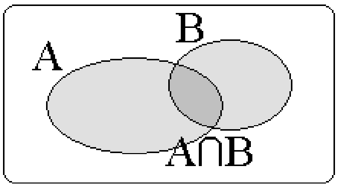
•) Siano dati gli insiemi $A$ e $B$. Si definisce *unione* di $A$ e $B$, e lo si indica con $A \cup B$, l'insieme costituito dagli elementi che appartengono ad almeno uno degli insiemi dati; si definisce *intersezione* di $A$ e $B$, e lo si indica con $A \cap B$, l'insieme costituito dagli elementi che appartengono ad entrambi gli insiemi dati; si definisce *differenza* fra $A$ e $B$, e lo si indica con $A \setminus B$, l'insieme costituito dagli elementi che appartengono ad $A$ e che non appartengono a $B$. Riassumendo:

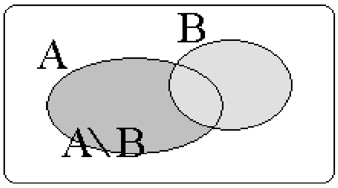
$A \cup B \overset{def}{=} \{x \,/\, x \in A \ \vee \ x \in B\}$;

$A \cap B \overset{def}{=} \{x \,/\, x \in A \ \wedge \ x \in B\}$;

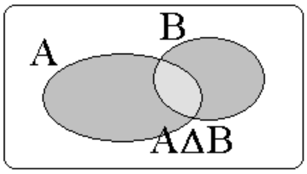
$A \setminus B \overset{def}{=} \{x \,/\, x \in A \ \wedge \ x \notin B\}$.

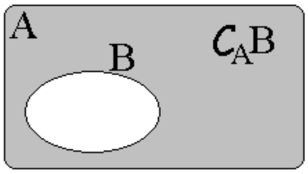







Se $A \cap B = \emptyset$, si dice che gli insiemi $A$ e $B$ sono *disgiunti*.
L'insieme $(A \setminus B) \cup (B \setminus A) = \{x \,/\, x \in A \ \dot{\vee} \ x \in B\}$ [1] è chiamato *differenza simmetrica* fra $A$ e $B$ ed è indicato con $A \triangle B$; è facile riconoscere che $A \triangle B = (A \cup B) \setminus (A \cap B)$.
Se $B \subseteq A$, l'insieme $A \setminus B$ è chiamato anche *complementare* di $B$ in $A$, ed è indicato anche con $\mathcal{C}_A B$, oppure semplicemente con $\mathcal{C}B$ quando l'indicazione dell'insieme $A$ può essere trascurata senza che ciò dia luogo ad equivoci.






**A1.1 Esempio.** Dati $A = \{1, 2, 3, 4, 5\}$ e $B = \{4, 5, 6\}$, si ha che:
$A \cup B = \{1, 2, 3, 4, 5, 6\}$, $A \cap B = \{4, 5\}$, $A \setminus B = \{1, 2, 3\}$, $A \triangle B = \{1, 2, 3, 6\}$.

Fra le numerose proprietà delle operazioni introdotte, tralasciamo sia quelle più facilmente intuibili, come la commutatività di $\cup$ e di $\cap$, sia quelle meno utilizzate, e citiamo solo le seguenti:
-) *proprietà distributive*: $A \cup (X \cap Y) = (A \cup X) \cap (A \cup Y)$, $A \cap (X \cup Y) = (A \cap X) \cup (A \cap Y)$
-) *leggi di De Morgan*: $A \setminus (X \cup Y) = (A \setminus X) \cap (A \setminus Y)$, $A \setminus (X \cap Y) = (A \setminus X) \cup (A \setminus Y)$.

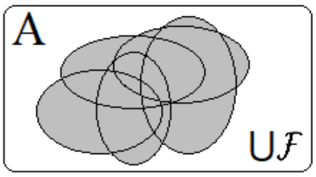
Nel caso che $X, Y \subseteq A$, le leggi di De Morgan assumono il seguente aspetto:
$\mathcal{C}(X \cup Y) = (\mathcal{C}X) \cap (\mathcal{C}Y)$, $\mathcal{C}(X \cap Y) = (\mathcal{C}X) \cup (\mathcal{C}Y)$.

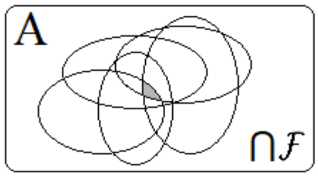
Le dimostrazioni delle suddette proprietà si fanno ricorrendo alle corrispondenti proprietà dei connettivi logici $\vee$ (*vel*) e $\wedge$ (*et*), che supponiamo già note al lettore. Ad esempio, per la prima legge di De Morgan, indicando con $\neg$ il connettivo della negazione, abbiamo:
$a \in \mathcal{C}(X \cup Y) \ \Leftrightarrow \ a \notin X \cup Y \ \Leftrightarrow \ \neg(a \in X \ \vee \ a \in Y) \ \Leftrightarrow \ a \notin X \ \wedge \ a \notin Y \ \Leftrightarrow \ a \in (\mathcal{C}X) \cap (\mathcal{C}Y)$.

---

[1] Il simbolo $\dot{\vee}$ indica la disgiunzione esclusiva, corrispondente al latino *aut*.

Le operazioni di $\cup$ e $\cap$ si estendono al caso in cui sono coinvolti anche più di due insiemi.
Se $\mathcal{F}$ è una famiglia di sottoinsiemi di un dato insieme $A$, si pone:
$\bigcup\limits_{X\in\mathcal{F}} X =: \bigcup\mathcal{F} := \{a \,/\, \exists\, X\in\mathcal{F}:\ a\in X\}$ , $\bigcap\limits_{X\in\mathcal{F}} X =: \bigcap\mathcal{F} := \{a \,/\, \forall\, X\in\mathcal{F},\ a\in X\}$,

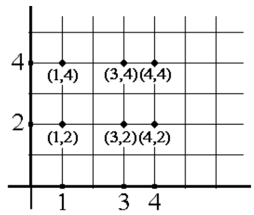



e le leggi di De Morgan diventano:
$\mathcal{C}(\bigcup\limits_{X\in\mathcal{F}} X) = \bigcap\limits_{X\in\mathcal{F}} (\mathcal{C}X)$ , $\mathcal{C}(\bigcap\limits_{X\in\mathcal{F}} X) = \bigcup\limits_{X\in\mathcal{F}} (\mathcal{C}X)$.
Diciamo poi che la famiglia $\mathcal{F}$ costituisce un *ricoprimento* dell'insieme $A$ se $\bigcup\limits_{X\in\mathcal{F}} X = A$, ossia se $\forall\, a\in A\ \exists\, X\in\mathcal{F} : a\in X$; diciamo infine che la famiglia $\mathcal{F}$ è una *partizione* dell'insieme $A$ se $\mathcal{F}$ è un ricoprimento di $A$ formato da insiemi tutti non vuoti ($\forall\, X\in\mathcal{F},\ X\neq\emptyset$) e a due a due disgiunti ($\forall\, X,Y\in\mathcal{F},\ X\neq Y \ \Rightarrow\ X\cap Y=\emptyset$).

**•)** Dati gli insiemi $A$ e $B$, si definisce *prodotto cartesiano* di $A$ per $B$, e lo si indica con $A\times B$, l'insieme costituito da tutte le coppie ordinate con primo elemento in $A$ e secondo elemento in $B$, ossia $A\times B \overset{def}{=} \{(a,b)\,/\,a\in A \wedge b\in B\}$ [1]. L'insieme $A\times A$ viene indicato anche con il simbolo $A^2$. E' importante osservare che l'operazione di prodotto cartesiano non è commutativa.

**A1.2 Esempio.** Il prodotto cartesiano degli insiemi $A=\{1,3,4\}$ e $B=\{2,4\}$ è l'insieme $A\times B = \{(1,2),(1,4),(3,2),(3,4),(4,2),(4,4)\}$, rappresentato nella figura che segue come un insieme di punti di una tabella a doppia entrata nella quale compaiono l'insieme $A$ sull'asse orizzontale e l'insieme $B$ sull'asse verticale..




**•)** Dato un insieme $A$, si definisce *insieme delle parti* di $A$, e lo si indica con $\mathcal{P}(A)$, l'insieme costituito da tutti i sottoinsiemi di $A$, compresi quelli banali (cioè l'insieme vuoto $\emptyset$ e l'insieme stesso A). Dunque $\mathcal{P}(A)=\{X\,/\,X\subseteq A\}$.

**A1.3 Esempio.** Dato l'insieme $A=\{1,2,3\}$, si riconosce che l'insieme delle parti di $A$ è l'insieme $\mathcal{P}(A)=\{\{\ \},\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$.

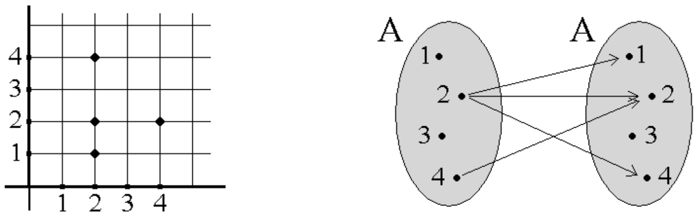
**-)** Il numero degli elementi di un insieme finito $A$ è chiamato *cardinalità* di $A$ ed è indicato con $|A|$. Precisato che il concetto di cardinalità sarà esteso anche al caso di insiemi infiniti, osserviamo intanto che, se $|A|=n$, allora $|\mathcal{P}(A)|=2^n$; cosicché sussiste l'uguaglianza $|\mathcal{P}(A)|=2^{|A|}$. Questa assume un aspetto particolarmente suggestivo se l'insieme delle parti di $A$ viene indicato con $\mathit{2}^A$; la formula diventa infatti $|\mathit{2}^A|=2^{|A|}$.

[1] Ricordiamo che la *coppia ordinata* $(a,b)$ è cosa diversa rispetto all'insieme $\{a,b\}$, il quale è individuato a prescindere dall'ordine; ad esempio, la coppia (1,2) e la coppia (2,1) sono diverse fra loro, mentre gli insiemi $\{1,2\}$ e $\{2,1\}$ sono il medesimo insieme; ed ancora, la coppia (1,1) è formata da due elementi, ancorché uguali, mentre l'insieme $\{1,1\}$ è l'insieme $\{1\}$ ed ha un solo elemento. Un valido espediente per definire in modo rigoroso il concetto di coppia ordinata è quello di porre $(a,b) := \{\{a,b\},a\}$.

## A2. Relazioni

*Dati gli insiemi non vuoti $A$ e $B$, chiamiamo relazione da $A$ in $B$ ogni sottoinsieme del prodotto cartesiano $A \times B$.* Se $\mathcal{R}$ indica una relazione da $A$ in $B$, invece della notazione $(a,b) \in \mathcal{R}$ si usa in genere la notazione $a\mathcal{R}\,b$, e si dice che *$a$ è nella relazione $\mathcal{R}$ con $b$*, oppure che *$b$ è un corrispondente di $a$ nella relazione $\mathcal{R}$*. Se $A = B$, si parla di *relazione in $A$*.

**A2.1 Esempio.** Dato $A = \{1,2,3,4\}$, un esempio di relazione in $A$ è costituito dall'insieme $\mathcal{R} = \{(2,1),(2,2),(2,4),(4,2)\}$. La relazione $\mathcal{R}$ può essere rappresentata sia come un insieme di punti di una tabella a doppia entrata sia come un insieme di frecce che collegano i punti di due diagrammi di Venn, come illustrato qui di seguito.



**A2.1 Osservazione.** Il concetto di relazione così introdotto può sembrare molto lontano dall'idea intuitiva di relazione dell'esperienza comune, dato che in genere una relazione fra gli elementi di un insieme $A$ e quelli di un insieme $B$ è immaginata come una proprietà (vale a dire un predicato) in due variabili, $\mathcal{P}(x,y)$, che collega alcuni elementi di $A$ con alcuni elementi di $B$, nel senso che alcune coppie $(a,b)$ la soddisfano ed altre no. Se ad esempio $A$ è l'insieme delle regioni italiane e $B$ è l'insieme delle città italiane, si potrebbe considerare la proprietà $\mathcal{P}(x,y) =$"$y$ è capoluogo di provincia di $x$". A ben vedere, questi due modi di definire le relazioni sono equivalenti; infatti, ad ogni proprietà $\mathcal{P}(x,y)$ corrisponde una relazione del tipo definito sopra, e precisamente la relazione $\mathcal{R} = \{(a,b) \in A \times B \,/\, \mathcal{P}(a,b)\}$, e, viceversa, ad ogni relazione $\mathcal{R}$ corrisponde una proprietà, e precisamente la proprietà $\mathcal{P}(x,y) =$ "$x\mathcal{R}\,y$".

Tra le relazioni di un insieme in se stesso più importanti per la nostra trattazione citiamo le relazioni di equivalenza e le relazioni d'ordine.

•) RELAZIONI DI EQUIVALENZA. *Una relazione $\mathcal{R}$ nell'insieme $A$ dicesi di equivalenza se è:*
a) *riflessiva*: $\forall\, a \in A,\ a\mathcal{R}a\,;$
b) *simmetrica*: $\forall\, a,b \in A,\ a\mathcal{R}b \ \Rightarrow\ b\mathcal{R}a\,;$
c) *transitiva*: $\forall\, a,b,c \in A,\ a\mathcal{R}b \wedge b\mathcal{R}c \ \Rightarrow\ a\mathcal{R}c\,.$

Data $\mathcal{R}$ relazione di equivalenza in $A$ e dato $a \in A$, l'insieme $[a] := \{x \in A \,/\, x\mathcal{R}a\}$ è chiamato *classe di equivalenza di $a$ modulo $\mathcal{R}$*; si riconosce che ogni elemento di $A$ appartiene ad una ed una sola classe di equivalenza, cosicché l'insieme di tutte le classi di equivalenza costituisce una partizione di $A$; l'insieme delle classi di equivalenza di $A$ rispetto alla relazione $\mathcal{R}$ prende il nome di *insieme quoziente di $A$ modulo $\mathcal{R}$* ed è denotato con $A/\mathcal{R}$. Spesso le relazioni di equivalenza si indicano con i simboli $\equiv$ e $\simeq$, e le scritture $a \equiv b$ e $a \simeq b$ si leggono "$a$ è equivalente a $b$".

**A2.2 Esempio.** La relazione dell'Esempio A2.1 non è né riflessiva, né simmetrica, né transitiva. Per provare ad esempio che non è transitiva, basta osservare che $4\mathcal{R}2 \wedge 2\mathcal{R}1$, ma $4 \not\mathcal{R} 1$.

**A2.3 Esempio.** In goniometria si fa largo uso della *relazione di congruenza modulo* $2\pi$: dati $x, y \in \mathbb{R}$, si pone $x \equiv y \pmod{2\pi} \overset{def}{\iff} \exists\, k \in \mathbb{Z} : \; y - x = 2k\pi$. E' facile provare che la relazione così definita è di equivalenza. La classe di equivalenza ad esempio del numero $\frac{\pi}{2}$ è l'insieme $[\frac{\pi}{2}] = \{\ldots, -\frac{7}{2}\pi, -\frac{3}{2}\pi, \frac{\pi}{2}, \frac{5}{2}\pi, \frac{9}{2}\pi, \frac{13}{2}\pi, \ldots\} = \{\frac{\pi}{2} + 2k\pi \,/\, k \in \mathbb{Z}\}$; tutti gli elementi di questa classe sono rappresentati dal medesimo punto (0,1) della circonferenza goniometrica.

**•)** RELAZIONI D'ORDINE. *Si dice relazione d'ordine in* $A$ *ogni relazione* $\mathcal{R}$ *avente le proprietà:*

*a) riflessiva:* $\forall\, a \in A, \; a\mathcal{R}a\,;$

*b) antisimmetrica:* $\forall\, a, b \in A, \; a\mathcal{R}b \wedge b\mathcal{R}a \;\Rightarrow\; a = b\,;$

*c) transitiva:* $\forall\, a, b, c \in A, \; a\mathcal{R}b \wedge b\mathcal{R}c \;\Rightarrow\; a\mathcal{R}c\,;$

*e si aggiunge che* $\mathcal{R}$ *è una relazione d'ordine totale se ogni elemento di* $A$ *è "confrontabile" con ogni altro elemento di* $A$*, nel senso che* $\mathcal{R}$ *gode anche della*

*d) proprietà di dicotomia:* $\forall\, a, b \in A, \; a\mathcal{R}b \vee b\mathcal{R}a\,.$

Una relazione d'ordine viene spesso indicata con il simbolo $\leq$; se $\leq$ è una relazione d'ordine in $A$, la coppia $(A, \leq)$ prende il nome di *insieme ordinato*, magari precisando che trattasi di *insieme totalmente ordinato* quando la relazione d'ordine è totale.

**A2.4 Esempio.** Nell'insieme $\mathbb{R}$ dei numeri reali è stabilita la cosiddetta *relazione d'ordine usuale* (ne parleremo meglio in seguito), cioè quella che utilizziamo abitualmente, secondo la quale ad esempio risulta $2 \leq \pi$ o $-3{,}5 \leq 0$. La coppia $(\mathbb{R}, \leq)$ è un insieme totalmente ordinato.

**A2.5 Esempio.** Nell'insieme $\mathbb{R}^2$ delle coppie ordinate di numeri reali si può introdurre il seguente ordinamento, detto *lessicografico* perché simile a quello che avrebbe un vocabolario contenente solo le parole con due lettere: $(x_1, y_1) \leq (x_2, y_2) \overset{def}{\iff} (x_1 < x_2) \vee (x_1 = x_2 \wedge y_1 \leq y_2)$. Si riconoscce facilmente che la coppia $(\mathbb{R}^2, \leq)$ è un insieme totalmente ordinato.

**A2.6 Esempio.** Nell'insieme $\mathbb{N}$ dei numeri naturali, oltre alla relazione d'ordine usuale $\leq$, che è la stessa dell'Esempio A2.4 quando la si consideri limitatamente agli elementi di $\mathbb{N}$, si può definire anche una relazione d'ordine fondata sul concetto di divisibilià: $m \leq_d n \overset{def}{\iff} \exists\, h \in \mathbb{N} : n = h\,m\,$. Ad esempio risulta $2 \leq_d 6$, mentre non è vero che $2 \leq_d 5$, nè che $5 \leq_d 2$. Dunque $(\mathbb{N}, \leq_d)$ è un insieme ordinato, ma non è un insieme totalmente ordinato.

**A2.7 Esempio.** Dato un insieme non vuoto $\Omega$, nell'insieme delle parti $\mathcal{P}(\Omega)$ possiamo assumere la relazione di inclusione come relazione d'ordine, ponendo cioè $U \leq V \overset{def}{\iff} U \subseteq V$. Si riconosce che $(\mathcal{P}(\Omega), \subseteq)$ è un insieme ordinato, ma non un è insieme totalmente ordinato, salvo il caso in cui $\Omega$ sia costituito da un unico elemento.

**A2.2 Osservazione.** Ad ogni relazione d'ordine può essere associata una *relazione d'ordine stretto*, ossia una relazione $\mathcal{R}$ avente la proprietà antiriflessiva ($\forall\, a \in A, \; a \not\mathcal{R}\, a$) e la già nota proprietà transitiva; invero, alla relazione d'ordine $\leq$ possiamo associare la relazione d'ordine stretto $<$ definita da $a < b \overset{def}{\iff} a \leq b \wedge a \neq b$. Ad esempio: in $\mathbb{R}$, alla relazione d'ordine usuale $\leq$ è associata la ben nota relazione d'ordine stretto $<$, anch'essa usuale; in $\mathcal{P}(\Omega)$, alla relazione d'ordine $\subseteq$ è associata la relazione d'ordine stretto $\subset$.

E' altresì evidente che, viceversa, se è data la relazione d'ordine stretto $<$, ad essa si può associare la relazione d'ordine $\leq$ definita da $a \leq b \overset{def}{\iff} a < b \vee a = b\,.$

**•)** Sia $(A, \leq)$ un insieme ordinato e sia $X$ un sottoinsieme non vuoto di $A$.
Un elemento $m \in A$ è detto *massimo di* $X$ se risulta $m \in X$ e, $\forall\, x \in X$, $m \geq x$.
Riconosciamo che, se $X$ ammette massimo, questo è necessariamente unico; se infatti supponiamo $m$ ed $m'$ massimi di $X$, abbiamo che $m \geq m'$ e che $m' \geq m$, da cui segue che $m = m'$.
Se $X$ ammette massimo, il massimo di $X$ è indicato con $\max X$ ed è chiamato anche *il più grande elemento di* $X$.
Il concetto di *minimo* è introdotto e sviluppato in maniera analoga; se $X$ ammette minimo, questo è indicato con $\min X$ ed è chiamato anche *il più piccolo elemento di* $X$.
Un elemento $a \in A$ è detto *maggiorante di* $X$ se, $\forall\, x \in X$, $a \geq x$.
Indicando con $\mathcal{M}_X$ l'insieme dei maggioranti di $X$, diciamo che $X$ è *limitato superiormente* se $\mathcal{M}_X \neq \emptyset$. Supposto che $X$ sia limitato superiormente, se accade che $\mathcal{M}_X$ ammette minimo, questo è chiamato *estremo superiore di* $X$ ed è indicato con $\sup X$.
Riconosciamo facilmente che: se $X$ ammette massimo, allora $X$ ammette estremo superiore e risulta $\sup X = \max X$; se $X$ ammette estremo superiore e $\sup X \in X$, allora $X$ ammette massimo e risulta $\max X = \sup X$.
I concetti di *minorante*, di *insieme limitato inferiormente* e di *estremo inferiore* (che si denota con $\inf X$), sono introdotti e sviluppati in maniera analoga. Aggiungiamo che l'insieme $X$ è detto essere *limitato* se esso è limitato sia inferiormente sia superiormente; se poi $X$ ammette entrambi gli estremi inferiore e superiore, è evidente che risulta $\inf X \leq \sup X$.
Infine riconosciamo che, dati $X$ ed $Y$ sottoinsiemi non vuoti di $A$, entrambi dotati di estremo superiore, se $X \subseteq Y$ allora $\sup X \leq \sup Y$; infatti dalle ipotesi segue che $\sup Y \in \mathcal{M}_X$, e da ciò segue banalmente la tesi, dato che $\sup X$ è il minimo di $\mathcal{M}_X$. Analogamente si riconosce che per gli eventuali estremi inferiori varrebbe la relazione $\inf X \geq \inf Y$.

**A2.8 Esempio.** L'insieme $\mathbb{R}$ con l'ordinamento usuale $\leq$ non ammette massino, né ammette maggioranti; esso non è limitato super/te. Il suo sottoinsieme $[0,1[= \{x \in \mathbb{R} \,/\, 0 \leq x < 1\}$ non ammette massimo; esso ammette maggioranti, alcuni dei quali sono 1, 2, $\frac{8}{3}$, $\sqrt{19}$, e quindi è limitato super/te; inoltre ammette estremo superiore, ed è $\sup[0,1[= 1$. Lo stesso insieme $[0,1[$ ammette minimo, $\min[0,1[= 0 = \inf[0,1[$.
Considerando l'insieme dei numeri razionali $\mathbb{Q}$ (anche di questo parleremo più approfonditamente in seguito) con l'ordinamento usuale $\leq$, il suo sottoinsieme $X = \{x \in \mathbb{Q}^+ / \, x^2 < 2\}$ è limitato superiormente, essendone ad esempio $\frac{3}{2}$ un maggiorante; ma non ammette estremo superiore.

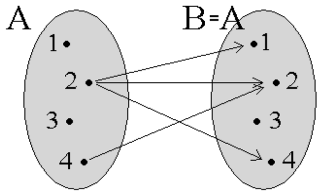
**A2.9 Esempio.** Considerando $\mathbb{N}$ con l'ordinamento usuale $\leq$, il suo sottoinsieme $X = \{2, 4, 6\}$ ammette massimo e minimo, ed è $\max X = 6 = \sup X$ e $\min X = 2 = \inf X$.
Se invece consideriamo in $\mathbb{N}$ l'ordinamento per divisibiltà $\leq_d$, lo stesso sottoinsieme $X$ risulta privo di massimo; tuttavia esso è dotato di maggioranti, che sono i numeri 12, 24, 36 ecc. ecc.; dunque $X$ è limitato super/te, ed inoltre ammette estremo superiore, $\sup X = 12$; in modo analogo osserviamo che $\exists \min X = 2 = \inf X$. In pratica si riconosce che, rispetto alla relazione $\leq_d$, i maggioranti di un qualsiasi sottoinsieme finito di $\mathbb{N}$ sono i multipli comuni degli elementi che ne fanno parte, e l'estremo superiore è il minimo comune multiplo degli stessi, così come i minoranti sono i sottomultipli comuni e l'estremo inferiore è il massimo comun divisore.

**A2.10 Esempio.** Dato $\Omega = \{1, 2, 3, 4, 5\}$, consideriamo l'insieme $\mathcal{P}(\Omega)$ ordinato per inclusione. Posto $\mathcal{F} = \{U, V\}$, con $U = \{1, 2, 4\}$ e $V = \{3, 4\}$, riconosciamo che i minoranti di $\mathcal{F}$ sono gli insiemi $\emptyset$ e $\{4\}$, e i maggioranti sono gli insiemi $\{1, 2, 3, 4\}$ e $\Omega$; inoltre l'estremo inferiore è $\{4\}$ e l'estremo superiore è $\{1, 2, 3, 4\}$. In generale, dato $\mathcal{F}$ sottoinsieme non vuoto di $\mathcal{P}(\Omega)$, i minoranti di $\mathcal{F}$ sono i sottoinsiemi di $\Omega$ contenuti nell'insieme $\bigcap \mathcal{F}$, che è l'estremo inferiore di $\mathcal{F}$, e i maggioranti di $\mathcal{F}$ sono i sottoinsiemi di $\Omega$ contenenti l'insieme $\bigcup \mathcal{F}$, che è l'estremo superiore di $\mathcal{F}$.

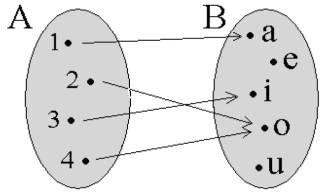
## A3. Funzioni

*Dati gli insiemi non vuoti $A$ e $B$, dicesi relazione funzionale da $A$ in $B$ ogni relazione $\mathcal{R}$ da $A$ in $B$ tale che ogni elemento di $A$ abbia al più un solo corrispondente in $B$; la relazione funzionale $\mathcal{R}$ dicesi poi* funzione *o* applicazione *da $A$ in $B$ se è ovunque definita in $A$, ossia se ogni elemento di $A$ ha un corrispondente in $B$. In definitiva, la relazione $\mathcal{R}$ è una funzione da $A$ in $B$ se verifica la seguente condizione: $\forall\, x \in A\ \exists\,!\, y \in B:\ x \mathcal{R}\, y$ .*

**A3.1 Esempio.** La relazione dell'Esempio A2.1 non è una funzione, sia perché vi è un elemento di $A$ associato a più di un elemento di $B$ e sia perché vi è qualche elemento di $A$ non associato a nessun elemento di $B$. Dati gli insiemi $A = \{1, 2, 3, 4, \}$ e $B = \{a, e, i, o, u\}$, la relazione $\mathcal{R} = \{(1, a), (2, o), (3, i), (4, o)\}$ è una funzione da $A$ in $B$.



Questa relazione non è una funzione



Questa relazione è una funzione

-) La lettera più usata per indicare una funzione è la $f$, e molto usate sono anche $g$, $h$, $F$, $\varphi$. Per indicare che $f$ è una funzione da $A$ in $B$ si usa scrivere $f : A \to B$, che si legge "f definita in $A$ ed a valori in $B$". Al posto della notazione $x\, f\, y$ si scrive $y = f(x)$, che si legge "$y$ è uguale ad $f$ di $x$", e si dice che *$y$ è l'immagine di $x$ mediante $f$*, oppure che *$y$ è il valore di $f$ in $x$*, o *il valore che $f$ assume in $x$*. L'insieme $A$ prende il nome di *dominio* ed è indicato con $\mathrm{Dom}(f)$, mentre $B$ è l'*insieme d'arrivo*; si chiama infine *immagine di $f$* l'insieme $\mathrm{Im}(f) = \{y \in B \,/\, \exists\, x \in A:\ y = f(x)\}$. Il termine *codominio* verrà qui usato per indicare l'insieme immagine, ma avvertiamo che molti autori lo utilizzano invece per indicare l'insieme d'arrivo.

-) Diciamo che la funzione $f$ è *iniettiva* (o *ingettiva*) se $\forall\, x_1, x_2 \in A,\ x_1 \neq x_2 \ \Rightarrow\ f(x_1) \neq f(x_2)$; diciamo che $f$ è *suriettiva* (o *surgettiva*), oppure che $f$ è funzione (da $A$) *su* $B$, se $\mathrm{Im}(f) = B$; diciamo infine che $f$ è *biiettiva* (o *bigettiva*, o *biunivoca*) se è sia iniettiva sia suriettiva, come dire che $\forall\, y \in B\ \exists\,!\, x \in A:\ y = f(x)$ . Osserviamo che l'eventuale mancanza di iniettività di una data funzione non può essere sanata, se non a condizione di modificare drasticamente la funzione sopprimendone alcune coppie che ne fanno parte; invece all'eventuale mancanza di suriettività si può rimediare semplicemente rimpiazzando l'insieme d'arrivo con l'insieme immagine, e quindi lasciando del tutto inalterato l'insieme delle coppie.

-) Sempre con riferimento ad una funzione $f: A \to B$, dato, $U \subseteq A$, chiamiamo *immagine di U mediante f* l'insieme $f(U) = \{y \in B \,/\, \exists\, x \in U:\ y = f(x)\} = \{f(x) \,/\, x \in U\}$; in particolare si ha che $f(A) = \mathrm{Im}(f)$. Analogamente, dato $V \subseteq B$, chiamiamo *controimmagine* (o *immagine inversa*) *di V mediante f* l'insieme $f^{-1}(V) = \{x \in A \,/\, f(x) \in V\}$.
Non è difficile dimostrare che, $\forall\, U \subseteq A$, $U \subseteq f^{-1}(f(U))$, e che vale l'uguaglianza per ogni $U$ se e solo se $f$ è iniettiva; analogamente si ha che, $\forall\, V \subseteq B$, $V \supseteq f(f^{-1}(V))$, e vale l'uguaglianza per ogni $V$ se e solo se $f$ è suriettiva.

**A3.2 Esempio.** Proviamo a fare alcune osservazioni sulla funzione dell'Esempio A3.1.
L'immagine di 2 mediante $f$ è la vocale $o$, $f(2) = o$, che risulta essere anche il valore di $f$ in 4, $o = f(4)$. Risulta anche $f(1) = a$ e $f(3) = i$.
L'insieme immagine, o codominio, della funzione è $\mathrm{Im}(f) = \{a, i, o\}$.
Si riconosce che: $f(\{1\}) = \{a\}$, $f(\{1,2\}) = f(\{1,2,4\}) = \{a, o\}$, $f^{-1}(\{a\}) = f^{-1}(\{a, e\}) = \{1\}$, $f^{-1}(\{e\}) = \emptyset$, $f^{-1}(\{o\}) = \{2, 4\}$.
La funzione $f$ non è iniettiva, perché $f(2) = f(4)$, e neanche suriettiva, perché $\mathrm{Im}(f) \neq B$. Ovviamente $f$ non è bigettiva
Se $U = \{1, 2\}$, allora $U \subset f^{-1}(f(U)) = \{1, 2, 4\}$; se $U = \{1, 3\}$, allora $U = f^{-1}(f(U))$; se $V = \{a, e\}$, allora $V \supset f(f^{-1}(V)) = \{a\}$; se $V = \{a, o\}$, allora $V = f(f^{-1}(V))$.

**A3.1 Osservazione.** Spesso per una funzione $f$ si usa la notazione $x \in A \to f(x) \in B$, e si parla della funzione che "ad $x \in A$ associa $f(x) \in B$", pensando alla funzione come ad una "legge" che consente di associare ad ogni elemento dell'insieme $A$ uno ed un solo elemento dell'insieme $B$.
Avvertiamo che molti autori definiscono proprio in questo modo il concetto di funzione, pur lasciando imprecisato il significato del termine "legge", e chiamano *grafico* della funzione $f$ l'insieme $\mathcal{G}(f) = \{(x, y) \in A \times B \,/\, y = f(x)\}$, vale a dire proprio quel sottoinsieme di $A \times B$ che per noi è appunto la funzione. A dire il vero, a partire da subito anche noi in questi appunti il più delle volte seguiremo questa impostazione.
A conferma di quanto detto, osserviamo che spesso in Matematica una funzione viene assegnata semplicemente assegnando un qualche algoritmo di calcolo che consente di passare dai valori della cosiddetta variabile indipendente a quelli della cosiddetta variabile dipendente; in questo caso il dominio, se non è espressamente indicato, deve intendersi coincidente con l'*insieme di definizione*, ossia l'insieme di tutti i valori che può assumere la variabile indipendente in modo che quel calcolo sia consentito. Ciò vale ad esempio per la funzione $f(x) = \sqrt{4 - x^2}$, il cui dominio s'intende essere l'insieme $\mathrm{Dom}(f) = \{x \in \mathbb{R} \,/\, -2 \leq x \leq 2\}$; come pure per la funzione $f(x, y) = \frac{x\,y}{x+y}$, in cui la variabile indipendente è la coppia $(x, y)$ e il cui dominio è l'insieme $\mathrm{Dom}(f) = \{(x, y) \in \mathbb{R}^2 / \, x + y \neq 0\}$. Invece nel caso della funzione $f(x) = \begin{cases} -x & \text{se } x \leq 0 \\ x^2 & \text{se } 0 < x \leq 1 \end{cases}$ il dominio è espressamente indicato, ed è l'insieme $\mathrm{Dom}(f) = \{x \in \mathbb{R} \,/\, x \leq 1\}$.

**A3.3 Esempio.** Riportiamo alcune funzioni che possiamo considerare fondamentali.

-) Dati gli insiemi non vuoti $A$ e $B$, e dato $\overline{y} \in B$, la funzione $x \in A \to \overline{y} \in B$ è chiamata *funzione costante*, di valore $\overline{y}$. E' evidente che l'immagine di questa funzione è il singoletto $\{\overline{y}\}$.

-) Dati gli insiemi non vuoti $U$ ed $A$, con $U \subseteq A$, la funzione $x \in U \to x \in A$ è chiamata *inclusione* o *immersione* di $U$ in $A$. Nel caso particolare $U = A$, la funzione prende il nome di *funzione identica*, o *identità*, su $U$, e sarà indicata con $i_U$.

-) Dati gli insiemi non vuoti $U$ ed $A$, con $U \subseteq A$, la funzione $\chi_U : A \to \{0,1\}$ definita da $\chi_U(x) = \begin{cases} 1 & \text{se } x \in U \\ 0 & \text{se } x \notin U \end{cases}$ è detta *funzione caratteristica* di $U$ in $A$. Attraverso la nozione di funzione caratterista viene stabilita una corrispondenza biunivoca tra gli elementi di $\mathcal{P}(A)$ e le funzioni da $A$ in $\{0,1\}$.

Considerato che in generale l'insieme delle funzioni da $X$ in $Y$, con $X$ ed $Y$ insiemi qualsiasi non vuoti, può essere indicato con $Y^X$, per l'insieme delle funzioni da $A$ in $\{0,1\}$ possiamo utilizzare anche il simbolo $\{0,1\}^A$. Questo, a sua volta, previa la trasformazione di $\{0,1\}$ in $\mathit{2}$, diventa $\mathit{2}^A$, come abbiamo già avuto modo di vedere in precedenza, quando abbiamo proposto la notazione $\mathit{2}^A$ al posto di $\mathcal{P}(A)$. Il simbolo $\mathit{2}^A$ mette in risalto il dualismo della condizione *appartenenza no - appartenenza sì*, ossia *appartenenza 0 - appartenenza 1.* Per superare questo dualismo, che impedisce alla Matematica di descrivere ambienti propri di scienze non esatte quali ad esempio la Biologia, l'Economia, la Sociologia, si è pensato qualche decennio fa(1) di sostituire la coppia $\mathit{2} = \{0,1\}$ con l'intervallo $I = [0,1]$, e quindi l'insieme inteso come elemento di $\mathit{2}^A$ con l'insieme inteso come elemento di $I^A$, il quale presenta tutta una gamma di *gradi di appartenenza*, che comprende sì i gradi 0 e 1 ma non si esaurisce con questi. Gli elementi di $I^A$ vengono chiamati *insiemi fuzzy*, mentre, a confronto con questi, gli elementi di $\mathit{2}^A$ vengono chiamati *insiemi crisp.*

-) Date $f : A \to B$ e $g : B \to C$, è possibile definire la funzione $g \circ f : x \in A \to g(f(x)) \in C$, detta *funzione composta* da $f$ e da $g$. Dunque per definizione risulta $(g \circ f)(x) = g(f(x)), \forall x \in A$. A ben vedere non è necessario che l'insieme d'arrivo di $f$ coincida con il dominio di $g$; ciò che conta è che $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$. Osserviamo inoltre che, anche nel caso in cui sono definite sia $g \circ f$ sia $f \circ g$, è comunque molto improbabile che queste due funzioni risultino uguali.

-) Data la funzione $f : A \to B$, e dato $U \subseteq A$, $U \neq \emptyset$, si chiama *restrizione* di $f$ ad $U$ la funzione $f_{|U} : U \to B$ definita da $f_{|U}(x) = f(x)$, $\forall x \in U$. Si vede subito che $f_{|U} = f \circ i_U$.

-) Data la funzione $f : A \to B$, e dato $U \supseteq A$, una qualunque funzione $\varphi : U \to B$ tale che, $\forall x \in A$, $\varphi(x) = f(x)$ è detta essere un *prolungamento* di $f$ su $U$.

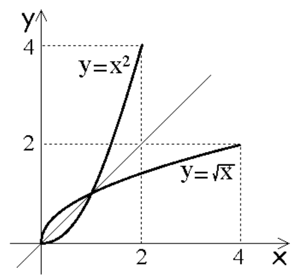
**A3.4 Esempio.** Date le funzioni $f : x \in [-2,2] \to \sqrt{4-x^2} \in \mathbb{R}$ e $g : y \in \mathbb{R} \to \operatorname{sen} y \in \mathbb{R}$, ha senso considerare la funzione $g \circ f$, che è definita da $(g \circ f)(x) = \operatorname{sen}\sqrt{4-x^2}$, $\forall x \in [-2,2]$.
Si osserva che in questo caso, poiché $\mathrm{Im}(g) = [-1,1] \subseteq \mathrm{Dom}(f)$, ha senso considerare anche la composizione $f \circ g$: invero, dopo avere riscritto le due funzioni nella forma $g : x \in \mathbb{R} \to \operatorname{sen} x \in \mathbb{R}$ ed $f : y \in [-2,2] \to \sqrt{4-y^2} \in \mathbb{R}$ (tanto per uniformare le notazioni allo standard usuale), riconosciamo che $(f \circ g)(x) = \sqrt{4-\operatorname{sen}^2 x}$, $\forall x \in \mathbb{R}$.

(1) L.H. Zadeh, *Fuzzy sets*, Information and Control 8 (1965), 338-353.

**A3.5 Esempio.** La funzione $h$ definita dall'espressione $h(x) = \log(1 - x^2)$, avente come dominio naturale l'insieme $]-1, 1[$, può essere interpretata come il risultato della composizione delle funzioni $f : x \in ]-1, 1[ \to 1 - x^2 \in \mathbb{R}$ e $g : y \in ]0, +\infty[ \to \log y \in \mathbb{R}$. L'operazione di composizione è consentita dal fatto che $\mathrm{Im}(f) = ]0, 1] \subseteq \mathbb{R}^+ = \mathrm{Dom}(g)$.
E' importante osservare che il dominio naturale dell'espressione $1 - x^2$ non è $]-1, 1[$ bensì $\mathbb{R}$, ma la funzione $\varphi : x \in \mathbb{R} \to 1 - x^2 \in \mathbb{R}$ non può essere composta con la funzione $g$, dato che $\mathrm{Im}(\varphi) = ]-\infty, 1] \nsubseteq \mathrm{Dom}(g)$.

**-)** Se $f : A \to B$ è iniettiva, allora, $\forall\, y \in B\ \exists!\, x \in A : f(x) = y$. E' dunque possibile definire la nuova applicazione $f^{-1} : f(A) \to A$, detta *inversa* di $f$, che ad ogni $y \in f(A)$ associa l'unico $x \in A$ tale che $f(x) = y$. In pratica si è posto per definizione che, $\forall\, x \in A$ e $\forall\, y \in f(A)$, $f^{-1}(y) = x \Leftrightarrow f(x) = y$. Le funzioni iniettive, per il fatto che ammettono la funzione inversa, sono dette anche *invertibili.* Se $f$ è invertibile, hanno significato sia $f^{-1} \circ f$ sia $f \circ f^{-1}$, e risulta $f^{-1} \circ f = i_A$ e $f \circ f^{-1} = i_{f(A)}$, cioè, $\forall\, x \in A, f^{-1}(f(x)) = x$ e, $\forall\, y \in f(A)$, $f(f^{-1}(y)) = y$.
Si osserva che, se $f$ viene riguardata come un insieme di coppie del prodotto cartesiano $A \times B$, allora le coppie di $B \times A$ costituenti $f^{-1}$ si ottengono da quelle di $f$ scambiando in ciascuna di esse le due coordinate l'una con l'altra; in altri termini, i grafici di $f$ e di $f^{-1}$, se rappresentati nello stesso sistema di riferimento cartesiano, risultano simmetrici uno dell'altro rispetto alla bisettrice del primo e terzo quadrante.

**A3.6 Esempio.** La funzione $f : x \in [-2, 2] \to x^2 \in \mathbb{R}$ non è iniettiva. Lo è però la sua restrizione all'intervallo $[0, 2]$, $\varphi = f_{|[0,2]}$, la quale pertanto risulta invertibile. Osservato che $\varphi$ ha immagine $[0, 4]$, si ha che $\varphi^{-1} : y \in [0, 4] \to \sqrt{y} \in [0, 2]$.
Nella figura che segue sono rappresentati i grafici delle funzioni $\varphi$ e $\varphi^{-1}$; allo scopo di utilizzare per $\varphi^{-1}$ lo stesso sistema di riferimento utilizzato per $\varphi$, occorre immaginare che anche per $\varphi^{-1}$ si usi la lettera $x$ per denotare la variabile indipendente; in altri termini, nel sistema di riferimento $Oxy$, rappresentiamo la curva di equazione $y = x^2$, con $x \in [0, 2]$, e la curva di equazione $y = \sqrt{x}$, con $x \in [0, 4]$.




**•)** Operazioni. Si osserva che la nota operazione di addizione, ad esempio nell'insieme dei numeri naturali $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$, può essere riguardata come una funzione, vale a dire come la funzione $(x, y) \in \mathbb{N} \times \mathbb{N} \to x + y \in \mathbb{N}$.
Più in generale, dati un insieme $\Omega$ ed un insieme $A \subseteq \Omega \times \Omega$, in certi contesti ogni funzione $\perp : A \to \Omega$ è detta *operazione* in $\Omega$ o anche *legge di composizione interna* ad $\Omega$, e in generale l'immagine di $(x, y)$ mediante $\perp$ è denotata con $x \perp y$ invece che con $\perp(x, y)$. Se poi risulta $A = \Omega \times \Omega$, si dice che l'operazione è *ovunque definita* in $\Omega$. Ad esempio, l'addizione citata sopra è una operazione ovunque definita in $\mathbb{N}$, mentre la sottrazione non è ovunque definita in $\mathbb{N}$, dato che il suo dominio è l'insieme $A = \{(m, n) \in \mathbb{N} \times \mathbb{N} \,/\, m > n\} \subset \mathbb{N} \times \mathbb{N}$. D'altra parte la sottrazione è ovunque definita nell'insieme degli interi relativi $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \pm4, \ldots\}$. Ed ancora, la moltiplicazione è un'operazione ovunque definita in $\mathbb{R}$, mentre la divisione non è ovunque definita in $\mathbb{R}$, dato che il suo dominio è $A = \mathbb{R} \times (\mathbb{R} \setminus \{0\}) \subset \mathbb{R} \times \mathbb{R}$.

# B

# I NUMERI REALI

## B.1. Il sistema dei numeri reali

Vi sono fondamentalmente due modi per definire i numeri reali, quello *costruttivo* e quello *assiomatico*. Il primo consiste nel definire inizialmente l'insieme $\mathbb{N}$ dei numeri naturali e poi nel "costruire", per successivi ampliamenti, l'insieme $\mathbb{Z}$ dei numeri interi, l'insieme $\mathbb{Q}$ dei numeri razionali ed infine, appunto, l'insieme $\mathbb{R}$ dei numeri reali; quanto all'insieme $\mathbb{N}$, il primo anello della catena, questo a sua volta può essere introdotto sia in modo assiomatico, utilizzando ad esempio gli assiomi di Peano, sia costruendolo a partire dalla teoria degli insiemi. Invece in questa nota, soprattutto per ragioni di brevità, scegliamo di introdurre già in prima battuta l'insieme $\mathbb{R}$, caratterizzandolo mediante un ben preciso complesso di assiomi; successivamente in esso sarà individuato un sottoinsieme particolare, che sarà l'insieme $\mathbb{N}$ dei numeri naturali, da cui poi scaturiranno, come detto sopra, gli insiemi $\mathbb{Z}$ e $\mathbb{Q}$.

**B1.1 Definizione.** *Chiamiamo sistema dei numeri reali la quaterna* $(\mathbb{R}, \leq, +, \cdot)$, *nella quale* $\mathbb{R}$ *rappresenta un insieme,* $\leq$ *(minore o uguale) una relazione in* $\mathbb{R}$, $+$ *e* $\cdot$ *due operazioni (addizione e moltiplicazione) ovunque definite in* $\mathbb{R}$, *tali che siano soddisfatte alcune proprietà, gli assiomi, che riportiamo qui di seguito:*

a$_1$) $\forall\, x\in\mathbb{R},\;\; x \leq x$ *(proprietà riflessiva)*;

a$_2$) $\forall\, x,y\in\mathbb{R},\;\; x \leq y \;\wedge\; y \leq x \;\Rightarrow\; x = y$ *(proprietà antisimmetrica)*;

a$_3$) $\forall\, x,y,z\in\mathbb{R},\;\; x \leq y \;\wedge\; y \leq z \;\Rightarrow\; x \leq z$ *(proprietà transitiva)*;

a$_4$) $\forall\, x,y\in\mathbb{R},\;\; x \leq y \;\vee\; y \leq x$ *(proprietà di dicotomia)*;

b$_1$) $\forall\, x,y\in\mathbb{R},\;\; x + y = y + x \;\text{ e }\; x \cdot y = y \cdot x$ *(proprietà commutative)*;

b$_2$) $\forall\, x,y,z\in\mathbb{R},\;\; (x + y) + z = x + (y + z) \;\text{ e }\; (x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(proprietà associative)*;

b$_3$) $\exists\, 0,1\in\mathbb{R},\; 0 \neq 1$, *tali che*, $\forall\, x\in\mathbb{R},\;\; x + 0 = x \;\text{ e }\; x \cdot 1 = x$ *(elementi neutri)*;

b$_4$) $\forall\, x\in\mathbb{R}\;\exists\, \overline{x}\in\mathbb{R} :\; x + \overline{x} = 0\,,\;\; \forall\, x\in\mathbb{R}\setminus\{0\}\;\exists\, \tilde{x}\in\mathbb{R} :\; x \cdot \tilde{x} = 1$ *(elementi simmetrici)*;

b$_5$) $\forall\, x,y,z\in\mathbb{R},\quad x \cdot (y + z) = x \cdot y + x \cdot z$ *(proprietà distributiva)*;

c$_1$) $\forall\, x,y,z\in\mathbb{R},\quad x \leq y \;\Rightarrow\; x + z \leq y + z$ *(compatibilità di* $\leq$ *rispetto a* $+$*)*;

c$_2$) $\forall\, x,y,z\in\mathbb{R},\; z \geq 0,\quad x \leq y \;\Rightarrow\; x \cdot z \leq y \cdot z$ *(compatibilità di* $\leq$ *rispetto a* $\cdot$*)*;

d) *ogni sottoinsieme di* $\mathbb{R}$ *limitato superiormente ammette estremo superiore (completezza).*

**B1.1 Osservazione.**

1) La (a$_1$) è implicita nella (a$_4$).

2) Gli elementi $x + y$ e $x \cdot y$ sono detti rispettivamente la *somma* e il *prodotto* di $x$ ed $y$; in genere la notazione $x \cdot y$ è sostituita dalla notazione $x\,y$, quando ciò non causa confusione.

3) A causa della ($b_1$), ciascuno degli elementi neutri della ($b_3$) è unico; invero, se esistessero anche $0'$ e $1'$, si avrebbe: $0 = 0 + 0' = 0' + 0 = 0'$ e $1 = 1 \cdot 1' = 1' \cdot 1 = 1'$.

4) A causa di ($b_1$) e ($b_2$), per ogni fissato $x$ ciascuno degli elementi simmetrici della ($b_4$) è unico; invero, se esistessero anche $\overline{x}'$ e $\tilde{x}'$, si avrebbe: $\overline{x} = \overline{x} + 0 = \overline{x} + (x + \overline{x}') = (\overline{x} + x) + \overline{x}' = 0 + \overline{x}' = \overline{x}' + 0 = \overline{x}'$ e $\tilde{x} = \tilde{x} \cdot 1 = \tilde{x} \cdot (x \cdot \tilde{x}') = (\tilde{x} \cdot x) \cdot \tilde{x}' = 1 \cdot \tilde{x}' = \tilde{x}' \cdot 1 = \tilde{x}'$ .
L'elemento $\overline{x}$ è chiamato *opposto di* $x$ ed è indicato con $-x$; l'elemento $\tilde{x}$ è chiamato *reciproco di* $x$ ed è indicato con $x^{-1}$.

5) La coppia $(\mathbb{R}, \leq)$ con le proprietà ($a_i$) è un *insieme totalmente ordinato*; la terna $(\mathbb{R}, +, \cdot)$ con le proprietà ($b_i$) è un *campo*; la quaterna $(\mathbb{R}, \leq, +, \cdot)$ con le proprietà ($a_i$), ($b_i$) e ($c_i$) è un *campo ordinato*; la quaterna $(\mathbb{R}, \leq, +, \cdot)$ con le proprietà ($a_i$), ($b_i$), ($c_i$) e (d) è un *campo ordinato completo*.

6) Tenuto conto di quanto detto nel punto precedente, il sistema dei numeri reali può essere definito sinteticamente come un campo ordinato completo.
E' possibile dimostrare, mediante un procedimento costruttivo, l'esistenza di almeno un campo ordinato completo; inoltre se ne può dimostrare anche l'unicità, a meno di isomorfismi (ciò vuol dire che, se $(\mathbb{K}, \preceq, \perp, *)$ è un altro campo ordinato completo, allora esiste un'applicazione bigettiva $f : \mathbb{R} \to \mathbb{K}$ tale che, $\forall\, x, y \in \mathbb{R}$, vale: $x \leq y \Leftrightarrow f(x) \preceq f(y)$ , $f(x+y) = f(x) \perp f(y)$ , $f(x \cdot y) = f(x) * f(y)$).

## B2. Le regole dell'algebra elementare

Dagli assiomi ($a_i$), ($b_i$) e ($c_i$) discendono le usuali regole dell'algebra elementare. Qui di seguito presentiamo le più importanti, inquadrandole nel campo ordinato dei numeri reali, essendo tuttavia evidente che esse valgono in un campo ordinato qualsiasi.

**•)** Le prime proprietà che presentiamo non coinvolgono l'ordinamento e richiedono soltanto la struttura di campo, cioè solo le operazioni $+$ e $\cdot$ con le proprietà ($b_i$).

**01)** $\forall\, a, b, x \in \mathbb{R}$, $a{+}x = b{+}x \Rightarrow a = b$ , $\forall\, a, b, x \in \mathbb{R}$, $x \neq 0$, $a\,x = b\,x \Rightarrow a = b$ (cancellazione).
Dim. Per provare la prima, basta aggiungere $-x$ ai due membri; per la seconda, basta moltiplicare i due membri per $x^{-1}$.

**02)** $\forall\, a \in \mathbb{R}$, $a\,0 = 0$ .
Dim. $a\,0 = a\,(0 + 0) = a\,0 + a\,0$ ; dunque $a\,0 = a\,0 + a\,0$, e da ciò segue la tesi aggiungendo $a\,0$ ai due membri.

**03)** *0 non ha reciproco.*
Dim. Se esistesse il reciproco $0^{-1}$, si avrebbe $0 \cdot 0^{-1} = 1$, ma anche, per la (2), $0 \cdot 0^{-1} = 0$, da cui seguirebbe che $0 = 1$.

**04)** $\forall\, a, b \in \mathbb{R}$, $a\,b = 0 \Rightarrow a = 0 \vee b = 0$ (annullamento del prodotto).
Dim. Se $a = 0$ la tesi è già acquisita; se $a \neq 0$, da $a\,b = 0$ segue, moltiplicando ambo i membri per $a^{-1}$, che $b = 0$.

**05)** $\forall a \in \mathbb{R},\ \ -(-a) = a\,;\ \ \forall a \in \mathbb{R}\setminus\{0\},\ \ (a^{-1})^{-1} = a\,.$

Dim. La prima stabilisce che $a$ è l'opposto di $-a$, ossia che $-a + a = 0$, che è banale; la seconda stabilisce che $a$ è il reciproco di $a^{-1}$, ossia che $a^{-1}a = 1$, anch'essa banale.

**06)** $\forall a, b \in \mathbb{R},\ \ a\,(-b) = -(a\,b)$ *e* $(-a)\,(-b) = a\,b\,;\ \ \forall a, b \in \mathbb{R}\setminus\{0\},\ \ (a\,b)^{-1} = a^{-1}b^{-1}\,.$

Dim. La prima stabilisce che $a\,(-b)$ è l'opposto di $a\,b$, ossia che $a\,b + a\,(-b) = 0$, che si prova con la ($b_5$) e con la (2); la seconda si prova applicando due volte la prima e tenendo conto della prima delle (5); la terza stabilisce che $a^{-1}b^{-1}$ è il reciproco di $a\,b$, ossia che $(a\,b)\,(a^{-1}b^{-1}) = 1$, che si prova con ($b_1$) e ($b_2$).

**07)** $\forall a, b \in \mathbb{R}$ *si pone* $a - b = a + (-b)$ *(esistenza della sottrazione).*

Si vede facilmente che $a - b$ è l'unico $x \in \mathbb{R}$ tale che $b + x = a\,.$

**08)** $\forall a, x\, y \in \mathbb{R},\ \ a\,(x - y) = a\,x - a\,y\,.$

Dim. $a\,(x - y) = a\,(x + (-y)) = a\,x + a\,(-y) = a\,x + (-(a\,y)) = a\,x - a\,y.$

**09)** $\forall a, b \in \mathbb{R},\ b \neq 0,$ *si pone* $\frac{a}{b} = a\,b^{-1}$ *(esistenza della divisione).*

Si vede facilmente che $\frac{a}{b}$ è l'unico $x \in \mathbb{R}$ tale che $b\,x = a\,.$

**10)** $\forall x \in \mathbb{R}\setminus\{0\},\ \ \frac{1}{x} = x^{-1}\,.$

Dim. $\frac{1}{x} = 1\,x^{-1} = x^{-1}\,.$

**11)** $\forall a, b \in \mathbb{R}, \forall x, y \in \mathbb{R}\setminus\{0\},\ \ \frac{a}{x} + \frac{b}{y} = \frac{a\,y + b\,x}{x\,y},$ e $\frac{a}{x}\,\frac{b}{y} = \frac{a\,b}{x\,y}\,.$

Dim. $\frac{ay+bx}{xy} = (a\,y + b\,x)\,(x\,y)^{-1} = (a\,y + b\,x)(x^{-1}y^{-1}) = ((a\,y)(x^{-1}y^{-1}) + (b\,x)(x^{-1}y^{-1})) = a\,x^{-1} + b\,y^{-1} = \frac{a}{x} + \frac{b}{y}\,;\ \ \frac{a\,b}{x\,y} = (a\,b)\,(x\,y)^{-1} = (a\,b)\,(x^{-1}y^{-1}) = (a\,x^{-1})\,(b\,y^{-1}) = \frac{a}{x}\,\frac{b}{y}\,.$

**•)** Le proprietà che seguono richiedono la struttura di campo ordinato, ossia la relazione $\leq$ e le operazioni $+$ e $\cdot$ con le proprietà ($b_i$) e ($c_i$). Precisiamo che $x < y$ significa $x \leq y \ \wedge\ x \neq y\,,$ e osserviamo che, a causa di ($a_4$), $\forall x, y \in \mathbb{R}$ si verifica uno ed uno solo dei seguenti tre casi: $x < y\,,\ x = y\,,\ x > y.$ Poniamo $\mathbb{R}^+ = \{x \in \mathbb{R}\,/\,x > 0\}$ e chiamiamo *positivi* i suoi elementi, mentre chiamiamo *negativi* i numeri reali $x$ tali che $x < 0\,.$

**12)** $\forall a \in \mathbb{R},\ \ a \geq 0 \ \Rightarrow\ -a \leq 0\,,\ \ a \leq 0 \ \Rightarrow\ -a \geq 0\,.$

Dim. Per entrambe basta aggiungere $-a$ ai due membri, in base alla ($c_1$).

**13)** $\forall a, b, x \in \mathbb{R},\ x \leq 0,\ \ a \leq b \ \Rightarrow\ a\,x \geq b\,x\,.$

Dim. Da $a \leq b$ e $-x \geq 0$ segue che $a(-x) \leq b(-x)$; poi si aggiunge $ax + bx$ ai due membri.

**14)** $\forall a, b, x, y \in \mathbb{R},\ \ \begin{pmatrix} a \leq b \\ x \leq y \end{pmatrix} \Rightarrow\ (\,a + x \leq b + y\,)\,,\ \ \ \begin{pmatrix} 0 \leq a \leq b \\ 0 \leq x \leq y \end{pmatrix} \Rightarrow\ a\,x \leq b\,y\,.$

Dim. Da $a \leq b$ segue $a + x \leq b + x$, da $x \leq y$ segue $b + x \leq b + y$, e la tesi si ottiene per transitività; in modo analogo si procede per la seconda implicazione.

**15)** $\forall a \in \mathbb{R},\ \ a^2 \geq 0$ *e inoltre* $a^2 = 0 \ \Leftrightarrow\ a = 0\,.$ [1]

Dim. Per ($a_4$) risulta $a \geq 0$ o $a \leq 0$; nell'uno e nell'altro caso si moltiplichino ambo i membri per $a$. La seconda parte è conseguenza di (2) e (4).

**16)** $\forall a \in \mathbb{R},\ \ 0 \leq a \leq b \ \Rightarrow\ a^2 \leq b^2\,.$

Dim. Basta usare la seconda delle (14) con $x = a$ e $y = b$.

---

(1) Con il simbolo $a^2$ denotiamo il prodotto $a\,a$.

**17)** $1 > 0$.

Dim. Tenendo conto della (15) si ha che $1 = 1^2 \geq 0$; inoltre in ($b_3$) è precisato che $1 \neq 0$.

**18)** *L'equazione* $x^2 + 1 = 0$ *non ha soluzioni.*

Dim. Se esistesse $x \in \mathbb{R}$ tale che $x^2 + 1 = 0$, si avrebbe $1 = -x^2 \leq 0$, in contrasto con la (17).

**19)** $\forall\, a \in \mathbb{R},\ \ a > 0 \ \Rightarrow\ a^{-1} > 0 \ \text{ e } \ a < 0 \ \Rightarrow\ a^{-1} < 0$.

Dim. Supposto $a > 0$, se fosse $a^{-1} < 0$ si avrebbe $1 = a^{-1}a \leq 0\, a = 0$; in modo analogo si dimostra la seconda parte.

**20)** $\forall\, a, b \in \mathbb{R},\ \ 0 < a \leq b \ \Rightarrow\ a^{-1} > b^{-1}$.

Dim. Basta moltiplicare ambo i membri di $a \leq b$ per $a^{-1}$ e per $b$.

**21)** *Dato* $a \in \mathbb{R}$*,* $a \geq 0$*, se* $\forall\, \varepsilon \in \mathbb{R}^+$ *risulta* $a < \varepsilon$*, allora dev'essere* $a = 0$.

Dim. Se fosse $a > 0$, assumendo 1 e poi $a^2$ nel ruolo di $\varepsilon$ avremmo $a < 1$ e $a < a^2$; d'altra parte da $a < 1$ seguirebbe, moltiplicando ambo i membri per $a$, che $a^2 \leq a$.

## B3. L'assioma di completezza

**•)** L'assioma di completezza stabilisce che *ogni sottoinsieme di* $\mathbb{R}$ *limitato super/te ammette estremo superiore*. Esso è noto anche con il nome di *assioma di Dedekind*, e corrisponde sul piano geometrico al *postulato di continuità* della retta.

E' facile riconoscere che, se $X$ è limitato super/te e $\sigma = \sup X$, allora l'insieme $X' := \{x \in \mathbb{R} \,/\, -x \in X\}$ è limitato infer/te e risulta $\inf X = -\sigma$; e viceversa. Ne segue che l'assioma di completezza può essere formulato equivalentemente affermando che:

*ogni sottoinsieme di* $\mathbb{R}$ *limitato infer/te ammette estremo inferiore.*

Nell'insieme $\mathbb{R}$, come del resto in un qualsiasi altro insieme totalmente ordinato, vale la seguente caratterizzazione.

**B3.1 Proprietà caratteristiche dell'estremo superiore.** *Dato $X$ sottoinsieme non vuoto di* $\mathbb{R}$*, e dato* $\sigma \in \mathbb{R}$*, allora*

$$X \text{ è limitato super/te e } \sigma = \sup X \quad \Longleftrightarrow \quad \begin{pmatrix} a)\ \forall\, x \in X,\ x \leq \sigma \\ b)\ \forall\, a \in \mathbb{R},\ a < \sigma \ \Rightarrow\ \exists\, x \in X : x > a \end{pmatrix}.$$

Le proprietà (a) e (b) sono note rispettivamente come $1^a$ e $2^a$ proprietà dell'estremo superiore. La prima esprime il fatto che $\sigma$ è un elemento dell'insieme $\mathcal{M}_X$, l'insieme dei maggioranti di $X$, e la seconda stabilisce che ogni numero minore di $\sigma$ non appartiene ad $\mathcal{M}_X$, ossia che gli elementi di $\mathcal{M}_X$ sono maggiori o uguali rispetto a $\sigma$; quindi le due proprietà congiunte equivalgono al fatto che $\sigma$ è il minimo di $\mathcal{M}_X$. Inoltre, poiché ogni $a < \sigma$ si può scrivere nella forma $\sigma - \varepsilon$ con $\varepsilon \in \mathbb{R}^+$, la proprietà (b) può essere riformulata come segue:

$b')$ $\forall\, \varepsilon \in \mathbb{R}^+,\ \exists\, x \in X : x > \sigma - \varepsilon$.

E' evidente che considerazioni analoghe possono essere ripetute con riferimento ad un qualsiasi sottoinsieme di $\mathbb{R}$ limitato infer/te ed al suo estremo inferiore.

Concludiamo questa parte introducendo alcune convenzioni.
Si pone $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty, \infty\}$, e si conviene che, $\forall\, x \in \mathbb{R}$, $-\infty < x < +\infty$.
Se $X$ è un sottoinsieme non vuoto di $\mathbb{R}$ illimitato infer/te, conveniamo che $\inf X = -\infty$; se invece $X$ è illimitato super/te, conveniamo che $\sup X = +\infty$.
Infine conveniamo che $\inf \emptyset = +\infty$ e che $\sup \emptyset = -\infty$.

**•)** Dati due sottoinsiemi non vuoti $A$ e $B$ di $\mathbb{R}$, diciamo che essi sono *separati* se $\forall\, a \in A$ e $\forall\, b \in B$ risulta $a \leq b$. Si riconosce che ciò equivale ad affermare che $A$ è limitato super/te, $B$ è limitato infer/te e $\sup A \leq \inf B$. Se $A$ e $B$ sono in queste condizioni, i numeri $\sup A$ e $\inf B$ e tutti gli altri fra essi compresi sono detti *elementi di separazione* dei due insiemi. Se poi accade che $\sup A = \inf B$, allora si dice che gli insiemi $A$ e $B$ sono *contigui*.

**B3.2 Proposizione.** *Siano $A$ e $B$ due insiemi separati, nel senso che $\forall\, a \in A$ e $\forall\, b \in B\; a \leq b$. Allora: $A$ e $B$ sono contigui se e solo se $\forall\, \varepsilon \in \mathbb{R}^+\; \exists\, a \in A\, \exists\, b \in B : b - a < \varepsilon$.*

**Dim.**($\Rightarrow$). Fissiamo $\varepsilon \in \mathbb{R}^+$. Per la $2^a$ proprietà degli estremi superiore ed inferiore, esiste $a \in A$ tale che $a > \sup A - \frac{\varepsilon}{2}$, ossia $-a < -\sup A + \frac{\varepsilon}{2}$, ed esiste $b \in B$ tale che $b < \inf B + \frac{\varepsilon}{2}$; sommando membro a membro la seconda e la terza disuguaglianza e tenendo conto dell'ipotesi $\sup A = \inf B$, si ottiene che $b - a < \varepsilon$ ▪

**Dim.**($\Leftarrow$). Poiché $A$ e $B$ sono separati, risulta $\inf B - \sup A \geq 0$; in base alla proprietà (21) del paragrafo precedente, resta solo da provare che, $\forall\, \varepsilon \in \mathbb{R}^+$, $\inf B - \sup A < \varepsilon$. Fissato $\varepsilon \in \mathbb{R}^+$, per l'ipotesi esistono $a \in A$ e $b \in B$ tali che $b - a < \varepsilon$; da $a \leq \sup A$, che equivale a $-\sup A \leq -a$, e $\inf B \leq b$ segue, sommando membro a membro, che $\inf B - \sup A \leq b - a$, e la tesi si ottiene per transitività ▪

**•)** Dato $a \in \mathbb{R}$, definiamo:
$[a, +\infty[\, = \{x \in \mathbb{R} \,/\, x \geq a\}$, *intervallo illimitato superiormente, chiuso, di estremo sinistro* $a$,
$]a, +\infty[\, = \{x \in \mathbb{R} \,/\, x > a\}$, *intervallo illimitato superiormente, aperto, di estremo sinistro* $a$,
$]-\infty, a] = \{x \in \mathbb{R} \,/\, x \leq a\}$, *intervallo illimitato inferiormente, chiuso, di estremo destro* $a$,
$]-\infty, a[\, = \{x \in \mathbb{R} \,/\, x < a\}$, *intervallo illimitato inferiormente, aperto, di estremo destro* $a$.


**[a,+∞[** **]a,+∞[** **]-∞,a]** **]-∞,a[**

Dati $a, b \in \mathbb{R}$, con $a < b$, definiamo:
$[a, b] = \{x \in \mathbb{R} \,/\, a \leq x \leq b\}$, *intervallo limitato, chiuso, di estremi* $a$ *e* $b$,
$[a, b[\, = \{x \in \mathbb{R} \,/\, a \leq x < b\}$, *intervallo limitato, semiaperto a destra, di estremi* $a$ *e* $b$,
$]a, b] = \{x \in \mathbb{R} \,/\, a < x \leq b\}$, *intervallo limitato, semiaperto a sinistra, di estremi* $a$ *e* $b$,
$]a, b[\, = \{x \in \mathbb{R} \,/\, a < x < b\}$, *intervallo limitato, aperto, di estremi* $a$ *e* $b$.


**[a,b]** **[a,b[** **]a,b]** **]a,b[**

Se $I$ è un qualsiasi intervallo limitato di estremo sinistro $a$ ed estremo destro $b$, il numero $b-a$ è chiamato *lunghezza di* $I$, e il numero $\frac{a+b}{2}$ (1) è chiamato *centro di* $I$.

E' facile riconoscere che ogni intervallo $I$ gode della seguente proprietà: *presi comunque* $x_1, x_2 \in I$, *con* $x_1 < x_2$, *l'intervallo* $[x_1, x_2]$ *è tutto contenuto in* $I$. Nella proposizione che segue è stabilito che questa proprietà, detta di *connessione*, caratterizza gli intervalli fra tutti i possibili sottoinsiemi non vuoti di $\mathbb{R}$, nel senso che gli intervalli sono gli unici sottoinsiemi non vuoti di $\mathbb{R}$ che la soddisfano.

**B3.3 Proposizione.** *Sia $X$ un sottoinsieme non vuoto di $\mathbb{R}$. Se $\forall\, x_1, x_2 \in X$ con $x_1 < x_2$ si ha che $[x_1, x_2] \subseteq X$, allora $X$ è un intervallo.*

**Dim.** Dimostreremo che $X$ è uno degli intervalli di estremi $\inf X$ e $\sup X$, considerando a mo' d'esempio il caso in cui $\inf X \in \mathbb{R}$ e $\sup X = +\infty$. Si tratta di provare che, preso $x \in \mathbb{R}$ con $x > \inf X$, si ha che $x \in X$. A causa della $2^a$ proprietà dell'estremo inferiore, esiste $x_1 \in X$ tale che $x_1 < x$; poiché $X$ è illimitato super/te, $x$ non può esserne maggiorante, ossia esiste $x_2 \in X$ tale che $x < x_2$. Ne segue, in virtù dell'ipotesi, che $x \in X$ ∎

## B4. L'insieme dei numeri naturali

•) Lo scopo è quello di individuare un particolare sottoinsieme di $\mathbb{R}$ che goda di quelle proprietà che normalmente si richiedono all'insieme dei numeri naturali.

**B4.1 Osservazione.** Quando parliamo di proprietà che normalmente si richiedono all'insieme dei numeri naturali, il riferimento è sostanzialmente agli *assiomi di Peano*, i quali consentirebbero di definire l'insieme $\mathbb{N}$ dei numeri naturali in modo assiomatico, dunque indipendentemente da $\mathbb{R}$ e dalla sua struttura. Seguendo l'impostazione assiomatica, diremmo che $\mathbb{N}$ è un insieme tale che esista un'applicazione $\sigma : \mathbb{N} \to \mathbb{N}$ con le seguenti proprietà:

1) $\sigma$ *è iniettiva;*

2) $\sigma$ *non è suriettiva, cioè esiste un elemento di $\mathbb{N}$, denotato con 1, tale che* $1 \notin \sigma(\mathbb{N})$;

3) $\forall\, A \subseteq \mathbb{N},\ \begin{pmatrix} 1 \in A \\ \forall\, n \in \mathbb{N},\ n \in A \Rightarrow \sigma(n) \in A \end{pmatrix} \Rightarrow (\, A = \mathbb{N}\,)$ *(principio di induzione).*

Tornando ora alla nostra trattazione, introduciamo il concetto di insieme induttivo.

Dato $A \in \mathbb{R}$, diciamo che $A$ è un *insieme induttivo* se verifica le seguenti condizioni:

a) $1 \in A$,

b) $\forall\, x \in \mathbb{R},\ x \in A \Rightarrow x + 1 \in A$.

Ad esempio sono induttivi gli insiemi $\mathbb{R}$, $\mathbb{R}^+$, $[1, +\infty[$.

Indicata con $\mathcal{I}$ la famiglia degli insiemi induttivi, riconosciamo facilmente che l'insieme $\bigcap \mathcal{I}$ è anch'esso un insieme induttivo e che è contenuto in ogni insieme induttivo, in altri termini esso è il più piccolo insieme induttivo di $\mathbb{R}$; è questo l'insieme che viene indicato con $\mathbb{N}$ e viene chiamato *insieme dei numeri naturali*.

(1) Come vedremo più avanti, il simbolo 2 denota la somma $1 + 1$.

Uno degli elementi di $\mathbb{N}$ è il numero 1; poiché $\mathbb{N}$ è induttivo, anche il numero $1+1$, che denotiamo con il simbolo 2, appartiene ad $\mathbb{N}$; ciò vale anche per il numero $2+1$, che denotiamo con il simbolo 3; e così di seguito. E' noto che, sebbene i numeri naturali siano infiniti, è possibile rappresentarli tutti combinando opportunamente un numero finito di simboli, ad esempio dieci nel sistema di numerazione usuale.

•) Un'immediata proprietà di $\mathbb{N}$ è espressa nella seguente proposizione.

**B4.1 Principio di induzione.** *Sia* $S \subseteq \mathbb{N}$.

$$\begin{pmatrix} 1 \in S \\ \forall\, n \in \mathbb{N},\ n \in S \ \Rightarrow\ n+1 \in S \end{pmatrix} \ \Rightarrow\ (S = \mathbb{N})\,.$$

**Dim.** Le ipotesi garantiscono che $S$ è un sottoinsieme induttivo di $\mathbb{R}$, e quindi $S \supseteq \mathbb{N}$, per come $\mathbb{N}$ è definito. Se ne conclude che $S = \mathbb{N}$ ▪

E' facile riconoscere che l'insieme $\mathbb{N}$ soddisfa le proprietà di cui tratta l'Osservazione B4.1, assumendo nel ruolo di $\sigma$ l'applicazione che ad ogni numero naturale $n$ associa il numero naturale $n+1$, *successivo di* $n$.

Un'altra proprietà di $\mathbb{N}$, che si può dimostrare essere equivalente al principio di induzione, è il cosiddetto *buon ordinamento*, grazie al quale si può dire che $\mathbb{N}$ è un insieme *bene ordinato*.

**B4.2 Principio del buon ordinamento.** *Ogni sottoinsieme di* $\mathbb{N}$ *ammette minimo.*

Il principio di induzione è il fondamento su cui poggia un metodo utilizzato molto frequentemente per dimostrare tutte le proposizioni di una data successione di proposizioni $(P_n)_{n\in\mathbb{N}}$ . Il simbolo $(P_n)_{n\in\mathbb{N}}$ è utilizzato per denotare una famiglia di proposizioni indicizzate su $\mathbb{N}$, ossia appunto una *successione di proposizioni.*

**B4.3 Proposizione.** *Sia* $(P_n)_{n\in\mathbb{N}}$ *una successione di proposizioni. Si ha che:*

$$\begin{pmatrix} P_1 \\ \forall\, n \in \mathbb{N},\ P_n \ \Rightarrow\ P_{n+1} \end{pmatrix} \ \Rightarrow\ (\forall\, n \in \mathbb{N},\ P_n)\,.$$

**Dim.** Basta considerare l'insieme $S := \{n \in \mathbb{N} \,/\, P_n\}$ ed osservare che $S$ verifica le ipotesi della Proposizione B4.1 ▪

Una formulazione più generale della proposizione precedente è riportata qui di seguito.

**B4.4 Proposizione.** *Sia* $(P_n)_{n\in\mathbb{N}}$ *una successione di proposizioni. Si ha che:*

$$\begin{pmatrix} \exists\, \overline{n} \in \mathbb{N} : P_{\overline{n}} \\ \forall\, n \geq \overline{n},\ P_n \ \Rightarrow\ P_{n+1} \end{pmatrix} \ \Rightarrow\ (\forall\, n \geq \overline{n},\ P_n)\,.$$

**Dim.** Basta porre, $\forall\, n \in \mathbb{N}$, $Q_n = P_{\overline{n}+n-1}$ ed applicare a $(Q_n)_{n\in\mathbb{N}}$ la Proposizione B4.3 ▪

Il principio di induzione è utilizzato anche nelle definizioni. Invero, considerata una successione di enti $(E_n)_{n\in\mathbb{N}}$, se è data una definizione dell'ente $E_1$ e se, $\forall\, n \in \mathbb{N}$, è data una definizione dell'ente $E_{n+1}$ che utilizza $E_n$ nel ruolo di definiens, allora, $\forall\, n \in \mathbb{N}$, è definito l'ente $E_n$.

Diamo qui di seguito un esempio di definizione per induzione ed un esempio di dimostrazione per induzione.

**Potenza ad esponente naturale**. Volendo definire, $\forall\, n \in \mathbb{N}$, la potenza $x^n$, dove $x$ è un assegnato numero reale, si può procedere così: si pone $x^1 = x$ , e poi si pone, $\forall\, n \in \mathbb{N}$, $x^{n+1} = x^n x$.

**Disuguaglianza di Bernoulli.** *Dato* $a \in \mathbb{R}$*, con* $a \geq -1$*,* $\forall\, n \in \mathbb{N}$ *si ha che* $(1+a)^n \geq 1 + na$.

**Dim.** Poniamo, $\forall\, n \in \mathbb{N}$, $P_n =$ " $(1+a)^n \geq 1 + na$ ". La proposizione $P_1$ è " $1+a \geq 1+a$ ", ed è vera. Fissato $n \in \mathbb{N}$ e supposto che $P_n$ sia vera, osserviamo che $(1+a)^{n+1} = (1+a)^n(1+a) \geq (1+na)(1+a) = 1 + na + a + na^2 \geq 1 + na + a = 1 + (n+1)a$, cosicché anche $P_{n+1}$ è vera ∎

**B4.1 Esempio.** E' facile riconoscere che la disuguaglianza $2^n \geq n^3$ non è verificata da ogni $n \in \mathbb{N}$. Si può dimostrare che essa è induttiva per $n \geq 7$, e si osseva che è soddisfatta per $n = 10$. Dunque essa è vera per ogni $n \geq 10$.

**•)** Infine ci vogliamo occupare di una proprietà di $\mathbb{R}$ che coinvolge l'insieme $\mathbb{N}$, nota come *proprietà archimedea* del campo ordinato dei numeri reali. Di essa riportiamo due diverse formulazioni, che dimostreremo essere equivalenti. La prima è quella classica, e, interpretata geometricamente, stabilisce che, dati a caso due segmenti, ciascuno di essi ammette un multiplo più lungo dell'altro; la seconda esprime il fatto che l'insieme $\mathbb{N}$ non è limitato super/te.

**B4.5 Proprietà archimedea.** *Valgono le seguenti proprietà, tra loro equivalenti.*
a) $\forall\, a, b \in \mathbb{R}^+, \exists\, n \in \mathbb{N} : \, n\, a > b$;
a') $\forall\, x \in \mathbb{R}^+, \exists\, n \in \mathbb{N} : \, n > x$.

**Dim.**((a)⇒(a')). Preso $x \in \mathbb{R}^+$, basta applicare la (a) con $a = 1$ e $b = x$ ∎

**Dim.**((a')⇒(a)). Presi $a, b \in \mathbb{R}^+$, basta applicare la (a') con $x = \frac{b}{a}$ ∎

**Dim.**((a')). Per assurdo sia $\mathbb{N}$ limitato super/te, con $\sigma = \sup \mathbb{N}$. Per la $2^a$ proprietà dell'estremo superiore, esiste $n \in \mathbb{N}$ tale che $n > \sigma - 1$, ossia $n + 1 > \sigma$. D'altra parte, poiché $n + 1 \in \mathbb{N}$, dev'essere $n + 1 \leq \sigma$ ∎

## B5. L'insieme dei numeri interi

Una volta introdotto $\mathbb{N}$ è facile definire l'insieme $\mathbb{Z}$ degli interi relativi: si pone
$\mathbb{Z} := \{x \in \mathbb{R} \,/\, x = 0 \ \vee \ x \in \mathbb{N} \ \vee \ -x \in \mathbb{N}\} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$.

Conseguenza del buon ordinamento di $\mathbb{N}$ è la seguente proprietà di $\mathbb{Z}$:
*ogni sottoinsieme non vuoto di* $\mathbb{Z}$ *ammette massimo se limitato super/te, ammette minimo se limitato infer/te.*

Questa proprità consente di definire il concetto di parte intera di un numero reale, cui fa seguito quello di parte decimale.
Dato $x \in \mathbb{R}$, chiamiamo *parte intera di* $x$ il numero intero $[x] := \max\{h \in \mathbb{Z} \,/\, h \leq x\}$, e chiamiamo *parte decimale di* $x$ il numero $\{x\} := x - [x]$.
Da $[x] \leq x < [x] + 1$ segue che $0 \leq \{x\} < 1$, e quindi l'uguaglianza $x = [x] + \{x\}$ può essere vista come la decomposizione del generico numero reale $x$ nella somma di un numero intero e di un numero reale compreso fra 0 e 1.
Ad esempio: $5{,}2 = 5 + 0{,}2$ , $4 = 4 + 0$ , $-3 = -3 + 0$ , $-5{,}2 = -6 + 0{,}8$.

## B6. L'insieme dei numeri razionali

Si pone $\mathbb{Q} := \{x \in \mathbb{R} \,/\, \exists\,(h,n) \in \mathbb{Z}\times\mathbb{N} : x = \frac{h}{n}\}$. L'espressione $\frac{h}{n}$ è detta *rappresentazione frazionaria di* $x$; essa non è unica, dato che $\frac{h}{n} = \frac{2h}{2n} = \frac{3h}{3n} = \dots$.
Si riconosce facilmente che $\mathbb{Q}$ è stabile rispetto all'addizione ed alla moltiplicazione, nel senso che, se $x$ ed $y$ appartengono a $\mathbb{Q}$, allora anche $x+y$ e $x \cdot y$ appartengono a $\mathbb{Q}$. Tenendo conto anche di questo fatto, si osserva che la quaterna $(\mathbb{Q}, \leq, +, \cdot)$, dove la relazione $\leq$ e le operazioni $+$ e $\cdot$ sono prese da $\mathbb{R}$, è un campo ordinato. E si può dimostrare che anche il campo ordinato $\mathbb{Q}$ gode della proprietà archimedea. Vedremo però tra poco che $\mathbb{Q}$ non soddisfa l'assioma di completezza, ed è questo il particolare che lo rende diverso da $\mathbb{R}$.

Intanto dimostriamo la seguente

**B6.1 Proposizione.** *Non esiste alcun numero razionale* $x$ *tale che* $x^2 = 2$.

**Dim.** Per assurdo sia $x \in \mathbb{Q}^+$ tale che $x^2 = 2$. Posto $x = \frac{m}{n}$, con $m$ ed $n$ naturali primi fra loro, si ha che $m^2 = 2n^2$. Dunque il 2 è divisore di $m^2 = m\,m$, e quindi dev'esserlo anche di $m$. Ciò vuol dire che esiste $h \in \mathbb{N}$ tale che $m = 2h$. Ne segue che $4h^2 = 2n^2$, cosicché $n^2 = 2h^2$. Ma allora il 2 è divisore anche di $n$, contro il fatto che $m$ ed $n$ sono primi fra loro ∎

Il passo successivo consiste nell'individuare un sottoinsieme di $\mathbb{Q}$ che sia limitato super/te in $\mathbb{Q}$ ma che non abbia estremo superiore in $\mathbb{Q}$. Nella proposizione che segue si dimostrerà che l'insieme $C = \{x \in \mathbb{Q}^+ \,/\, x^2 < 2\}$, che non è vuoto essendo $1 \in C$, risponde a questi requisiti.

**B6.2 Incompletezza di $\mathbb{Q}$.** *Il campo ordinato* $(\mathbb{Q}, \leq, +, \cdot)$ *non è completo.*

**Dim.** Riconosciamo subito che il numero razionale $\frac{3}{2}$ è un maggiorante dell'insieme $C$ definito sopra: preso infatti il generico $x \in C$, se fosse $x > \frac{3}{2}$ si avrebbe $x^2 > \frac{9}{4}$, e quindi $x^2 > 2$, che è falso. Dunque $C$ è limitato super/te in $\mathbb{Q}$.
Per provare che $C$ non ammette estremo superiore in $\mathbb{Q}$, procediamo per assurdo, supponendo invece che esista $\varrho = \sup C \in \mathbb{Q}$.
Sappiamo già che non può essere $\varrho^2 = 2$. Proveremo ora che non può aversi neanche né $\varrho^2 < 2$ né $\varrho^2 > 2$, contro il fatto che $\varrho^2$ dovrebbe comunque essere confrontabile con 2.
Supponiamo per assurdo che sia $\varrho^2 < 2$, e consideriamo un $n \in \mathbb{N}$ tale che $(\varrho + \frac{1}{n})^2 < 2$. Osserviamo che un tale $n$ esiste, in quanto la relazione suddetta equivale a $\varrho^2 + \frac{2\varrho}{n} + \frac{1}{n^2} < 2$, che è in particolare soddisfatta se $\varrho^2 + \frac{2\varrho}{n} + \frac{1}{n} < 2$, ossia assumendo $n > \frac{1+2\varrho}{2-\varrho^2}$. Si ha allora che $\varrho + \frac{1}{n} \in C$, e quindi che $\varrho + \frac{1}{n} \leq \varrho$, che è falso.
Supponiamo infine che sia $\varrho^2 > 2$, e consideriamo un $n \in \mathbb{N}$ tale che $(\varrho - \frac{1}{n})^2 > 2$. Osserviamo che un tale $n$ esiste, in quanto la relazione suddetta equivale a $\varrho^2 - \frac{2\varrho}{n} + \frac{1}{n^2} > 2$, che è in particolare soddisfatta se $\varrho^2 - \frac{2\varrho}{n} - \frac{1}{n} > 2$, ossia assumendo $n > \frac{1+2\varrho}{\varrho^2-2}$. Si ha allora che $\varrho - \frac{1}{n}$ è un maggiorante per $C$; infatti, $\forall\, x \in C$, risulta $(\varrho - \frac{1}{n})^2 > x^2$, e da qui segue, essendo $\varrho - \frac{1}{n} > 0$ (in quanto $\frac{1}{n} < \frac{\varrho^2-2}{1+2\varrho} < \varrho$), che $\varrho - \frac{1}{n} > x$. Si ha allora che $\varrho - \frac{1}{n} \geq \varrho$, che è falso ∎

Tornando all'insieme $C = \{x \in \mathbb{Q}^+ / \, x^2 < 2\}$, è ovvio che esso è limitato super/te anche in $\mathbb{R}$, e dunque, per l'assioma di completezza, esiste $\sigma = \sup C \in \mathbb{R}$. Ragionando come nella dimostrazione precedente, si prova che non può aversi neanche qui né $\sigma^2 < 2$ né $\sigma^2 > 2$, e quindi deve necessariamente risultare $\sigma^2 = 2$. Il numero $\sigma$, unico numero reale positivo il cui quadrato è uguale a 2, prende il nome di *radice quadrata di* 2, ed è indicato con il simbolo $\sqrt{2}$. I numeri reali non appartenenti a $\mathbb{Q}$ sono chiamati *numeri irrazionali.*

Nella proposizione che segue è stabilita una proprietà nota come *densità di* $\mathbb{Q}$ *in* $\mathbb{R}$.

**B6.3 Proposizione.** *Dati* $a, b \in \mathbb{R}$, *con* $a < b$, *esiste almeno un* $r \in \mathbb{Q}$ *tale che* $a < r < b$.

**Dim.** Sia $n \in \mathbb{N}$ tale che $n > \frac{1}{b-a}$, e sia $k = [na]$, in modo che $k \leq na < k+1$, ossia $\frac{k}{n} \leq a < \frac{k+1}{n}$. Posto $r = \frac{k+1}{n}$, è immediato constatare che $r \in \mathbb{Q}$ e che $r > a$. Risulta anche $r < b$: infatti, se fosse $r \geq b$, ossia $\frac{k}{n} + \frac{1}{n} \geq b$, si avrebbe $\frac{1}{n} \geq b - \frac{k}{n} \geq b - a$ ■

La proprietà suesposta può essere enunciata anche così: $\forall\, x \in \mathbb{R}, \forall\, \varepsilon \in \mathbb{R}^+, \exists\, r \in \mathbb{Q} : x - \varepsilon < r < x$. Essa stabilisce in sostanza che ogni numero reale può essere approssimato con precisione arbitraria per mezzo di numeri razionali. Questo fatto, particolarmente significativo se $x$ è irrazionale, è ciò che rende concretamente possibili i calcoli numerici: stabilito in partenza un margine d'errore da considerare invalicabile, ogni numero che ricorre nel calcolo da effettuare viene rimpiazzato da un opportuno numero razionale.

Si osservi che, in virtù della Proposizione B6.3, fra due numeri reali $a$ e $b$ esistono infiniti numeri razionali. Invero, trovato $r_1 \in \mathbb{Q}$ tale che $a < r_1 < b$, esisterà $r_2 \in \mathbb{Q}$ tale che $r_1 < r_2 < b$, e poi esisterà $r_3 \in \mathbb{Q}$ tale che $r_2 < r_3 < b$, e così via. La dimostrazione rigorosa si ottiene verificando col principio di induzione che: $\forall\, n \in \mathbb{N}$ esistono $n$ numeri razionali compresi fra $a$ e $b$.

Infine dimostriamo che anche i numeri irrazionali sono densi in $\mathbb{R}$.

**B6.4 Proposizione.** *Dati* $a, b \in \mathbb{R}$, *con* $a < b$, *esiste almeno un* $s \in \mathbb{R} \setminus \mathbb{Q}$ *tale che* $a < s < b$.

**Dim.** Sia $\xi$ un qualsiasi numero irrazionale. Preso $r \in \mathbb{Q}$ tale che $a - \xi < r < b - \xi$, si ha che $a < r + \xi < b$, ed è evidente che $r + \xi \notin \mathbb{Q}$.

## B7. Cardinalità dei principali insiemi numerici

Vogliamo qui accennare, sia pure in modo informale, al problema della cardinalità degli insiemi numerici fin qui introdotti.

**-)** Dati due insiemi non vuoti $A$ e $B$, si dice che essi sono *equipotenti* o che hanno la *stessa cardinalità*, e si scrive $A \simeq B$, se esiste un'applicazione bigettiva da $A$ in $B$. Si dice che $A$ ha *cardinalità minore* rispetto a $B$ se $A \not\simeq B$ ed esiste un'applicazione iniettiva da $A$ in $B$.

E' evidente che *la relazione di equipotenza è una relazione di equivalenza.* Pertanto la cardinalità di un insieme non è che la classe di equivalenza di quell'insieme rispetto alla relazione suddetta.

Un insieme $A$ si dice *finito* se è vuoto oppure $\exists\, n \in \mathbb{N}$ tale che $A \simeq \{1, 2, \ldots, n\}$. Questo $n$, se esiste, è unico. Un insieme che non sia finito si dice *infinito*.

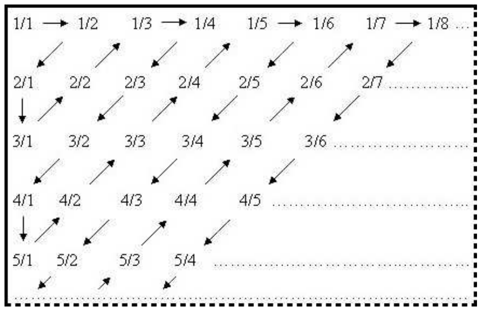
-) E' evidente che *l'insieme $\mathbb{N}$ è infinito*; si dimostra inoltre che *$\mathbb{N}$ ha cardinalità minore di qualsiasi altro insieme infinito che non gli sia equipotente*.

Un insieme equipotente ad $\mathbb{N}$ si dice *numerabile*. Chiaramente *$\mathbb{N}$ è numerabile*. Sorprendentemente sono numerabili anche ad esempio l'insieme dei numeri pari, l'insieme dei quadrati perfetti, come pure *l'insieme $\mathbb{Z}$ dei numeri interi*. Invero, indicati con $\mathbb{N}_d$ e con $\mathbb{N}_p$ rispettivamente l'insieme dei naturali dispari e quello dei naturali pari, si riconosce che l'applicazione $f : n \in \mathbb{N} \to \begin{cases} \frac{n-1}{2} & \text{se } n \in \mathbb{N}_d \\ -\frac{n}{2} & \text{se } n \in \mathbb{N}_p \end{cases}$ è bigettiva da $\mathbb{N}$ in $\mathbb{Z}$. Ciò equivale a dire che gli elementi di $\mathbb{Z}$ possono essere "enumerati" nel seguente modo: $0, -1, 1, -2, 2, -3, \ldots$.

Si può dimostrare che è *proprio una caratteristica degli insiemi infiniti il fatto di essere equipotenti a qualcuno dei loro sottoinsiemi propri*.

-) Si dimostra che anche *l'insieme $\mathbb{Q}$ è numerabile*. E anche questo fatto è controintuitivo, perché sembra contrastare con la proprietà di densità.

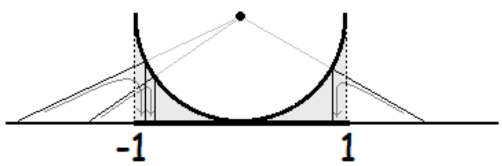
Nella figura è illustrato il noto *procedimento diagonale di Cantor*, che mostra un modo per "mettere in successione" i numeri razionali, cioè un criterio per scegliere quale debba essere il numero da "etichettare" come primo, quello da "etichettare" come secondo, ecc. ecc.. Occorre avere alcune accortezze: premettere lo zero, anteporre ad ogni numero il suo opposto, eliminare le ripetizioni.




-) Invece *l'insieme $\mathbb{R}$ ha cardinalità superiore rispetto ad $\mathbb{N}$*. Supponiamo per assurdo che gli elementi di $\mathbb{R}$ si possano mettere in successione: $\alpha_1, \alpha_2, \alpha_3, \ldots$; consideriamo il numero $\beta = 0, c_1 c_2 c_3 \ldots$, dove la generica cifra decimale $c_k$ vale 1 se la $k$–ima cifra decimale di $\alpha_k$ è 5, e vale 5 altrimenti; ma allora il numero $\beta$ non sta nella successione, dato che esso differisce da $\alpha_1$ nella prima cifra decimale, da $\alpha_2$ nella seconda, e in generale da $\alpha_n$ nella $n$–ima.

Evidentemente la maggiore "numerosità" di $\mathbb{R}$ rispetto ad $\mathbb{N}$, e quindi anche a $\mathbb{Q}$, è dovuta alla presenza dei numeri irrazionali. Potremmo dire, con un'immagine fantasiosa ma efficace, che, *sparando a caso sull'asse reale, la probabilità di colpire un numero razionale è praticamente nulla*! La cardinalità di $\mathbb{R}$ è detta *potenza del continuo*.

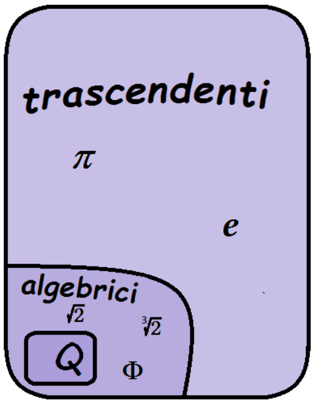
Altro esempio interessante è l'equipotenza fra l'insieme $\mathbb{R}$ e l'intervallo ]-1,1[, sebbene questo, a differenza di quello, sia limitato.
La figura mostra come si possa passare, in modalità biunivoca, dai punti dell'asse reale a quelli della semicirconferenza, e da questi a quelli del segmento ]-1,1[.



-) Si può dimostrare che, a dispetto del "salto dimensionale", *l'insieme* $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ *ha la stessa cardinalità di* $\mathbb{R}$. Esempio analogo è l'equipotenza fra [0,1] e $[0,1]^2$, che si potrebbe commentare, con un'interpretazione anche qui di tipo geometrico, dicendo che *i punti di una quadrato sono tanti quanti quelli di uno qualsiasi dei suoi lati*!

-) Si dimostra che $\mathbb{R}$ *ha la stessa cardinalità dell'insieme delle parti di* $\mathbb{N}$, $\mathbb{R} \simeq \mathcal{P}(\mathbb{N})$. Per avere un ulteriore salto di cardinalità dopo quella di $\mathbb{R}$, bisogna passare all'insieme $\mathcal{P}(\mathbb{R})$; e così di seguito se si vuol passare a cardinalità via via maggiori.
Le cardinalità di $\mathbb{N}$, di $\mathcal{P}(\mathbb{N})$, di $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ ecc. sono indicate con i simboli $\aleph_0$, $\aleph_1$, $\aleph_2$ ecc., che rappresentano i cosiddetti *numeri cardinali transfiniti.* E' questione ancora assai dibattuta nella comunità dei matematici se sia "più giusto" ritenere che esistano oppure no cardinalità intermedie fra quella di $\mathbb{N}$ e quella di $\mathcal{P}(\mathbb{N})$, come anche fra quella di $\mathcal{P}(\mathbb{N})$ e quella di $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, ecc. ecc..

-) Tornando all'insieme dei numeri reali, osserviamo che essi si possono distinguere anche in algebrici e trascendenti.
Si dice *algebrico* ogni numero reale che può essere ottenuto come soluzione di un'equazione algebrica a coefficienti interi.
I numeri reali non algebrici sono chiamati *trascendenti.*
E' evidente che l'insieme degli algebrici contiene $\mathbb{Q}$, e conseguentemente i trascendenti sono tutti irrazionali. Un numero algebrico importante è il cosiddetto *numero d'oro*, $\Phi = \frac{1+\sqrt{5}}{2}$, ossia il rapporto tra un qualsiasi segmento e la sua sezione aurea, che è soluzione dell'equazione $x^2 - x - 1 = 0$.
Fra i trascendenti citiamo il numero $\pi$, rapporto fra circonferenza e relativo diametro, e il numero $e$, estremo superiore della successione dei numeri $(1+\frac{1}{n})^n$ (1) .




Si dimostra che l'insieme degli algebrici è numerabile, cosicché i veri responsabili della superiore cardinalità di $\mathbb{R}$ rispetto ad $\mathbb{N}$ sono i numeri irrazionali trascendenti.

(1) La trascendenza di $\pi$ è stata dimostrata da Lindemann nel 1882. Qualche anno prima, nel 1873, Hermite aveva dimostrato la trascendenza di $e$.