Complemento 1

Gli insiemi $\mathbb{N}$, $\mathbb{Z}$ *e* $\mathbb{Q}$

Il sistema dei numeri reali $(\mathbb{R}, +, \cdot, \leq)$ può essere definito tramite sedici assiomi: quindici "assiomi algebrici" (si veda ad esempio §2.3 in [Giusti, E.: *Analisi Matematica 1*, Terza Edizione Bollati Boringhieri, 2002]) più un "assioma di completezza" (si veda **(ES)** qui sotto).

In questo complemento vengono definiti i numeri naturali ($\mathbb{N}$), interi ($\mathbb{Z}$) e razionali ($\mathbb{Q}$) e vengono dimostrate alcune proprietà fondamentali, usando esclusivamente gli assiomi dei numeri reali.

I numeri naturali

Definizione 1 (i) *Un insieme* $I \subseteq \mathbb{R}$ *viene detto* **induttivo** *se:*

- $1 \in I$
- $x \in I \implies x + 1 \in I$.

(ii) *L'***insieme dei numeri naturali** $\mathbb{N}$ *è il più piccolo insieme induttivo di* $\mathbb{R}$*, cioè*[1]

$$\mathbb{N} := \{x \in \mathbb{R} : \ \forall\, I \subseteq \mathbb{R} \text{ induttivo}, x \in I\} = \bigcap_{I \text{ induttivo}} I.$$

Osservazione 2 (i) Esempi di insiemi induttivi sono $I_1 := \{x \in \mathbb{R} : x \geq 1\}$ e $I_2 := \{1\} \cup \{x \in \mathbb{R} : \ x \geq 2\}$, dove $2 := 1 + 1$. Dunque dalla definizione di $\mathbb{N}$ segue che $\mathbb{N} \subseteq I_1$ e $\mathbb{N} \subseteq I_2$. In particolare, $n \geq 1$ per ogni[2] $n \in \mathbb{N}$ e non ci sono interi tra 1 e 2: *se* $x \in \mathbb{R}$ *è tale che* $1 < x < 2$ *allora* $x \notin \mathbb{N}$.

(ii) Dalla definizione di $\mathbb{N}$ e dagli assiomi algebrici di $\mathbb{R}$ segue immediatamente che $\mathbb{N}$ soddisfa le seguenti proprietà[3]:

(P_1) $1 \in \mathbb{N}$;

(P_2) $n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$;

(P_3) $n \in \mathbb{N} \implies n + 1 \neq 1$;

(P_4) $n, m \in \mathbb{N}$ e $n + 1 = m + 1 \implies n = m$;

(P_5) $I \subseteq \mathbb{N}$, I induttivo $\implies I = \mathbb{N}$.

[1] Si osservi che l'intersezione di insiemi induttivi è un insieme induttivo.

[2] In molti testi l'insieme dei numeri naturali $\mathbb{N}$ "parte da" (contiene) 0: le due convenzioni sono del tutto equivalenti. Ove sia necessario, denoteremo con $\mathbb{N}_0$ l'insieme $\mathbb{N} \cup \{0\}$.

[3] (P_1)÷(P_5) sono note come "assiomi di Peano". Si noti che dal nostro punto di vista essi sono proposizioni matematiche che derivano dagli assiomi algebrici di $\mathbb{R}$ e non sono assiomi.

Proposizione 3 ("Principio di induzione") *Siano $\mathcal{P}(n)$ affermazioni che dipendono da $n \in \mathbb{N}$. Supponiamo che $\mathcal{P}(1)$ sia vera e che dalla verità di $\mathcal{P}(n)$, con $n \geq 1$, segua che $\mathcal{P}(n+1)$ è vera. Allora $\mathcal{P}(n)$ è vera per ogni $n \in \mathbb{N}$.*

Dimostrazione Sia $I := \{n \in \mathbb{N} : \ \mathcal{P}(n) \ \text{è vera}\}$. Dalle ipotesi segue che $I \subseteq \mathbb{N}$ è induttivo e quindi, per (P_5), $I = \mathbb{N}$. ∎

Osservazione 4 Una formulazione equivalente del principio di induzione è:

Se $\mathcal{P}(1)$ è vera e da "$\mathcal{P}(k)$ vera per $1 \leq k \leq n$" segue $\mathcal{P}(n+1)$, allora $\mathcal{P}(n)$ è vera $\forall\, n \in \mathbb{N}$.

Basta infatti porre $\mathcal{P}'(n) := \{\mathcal{P}(k) : \ 1 \leq k \leq n\}$ ed applicare la Proposizione 3 a $\mathcal{P}'(n)$.

Proposizione 5 *Siano n e m numeri naturali. Allora:*

(a) $n + m \in \mathbb{N}$*;*

(b) $nm \in \mathbb{N}$*.*

Dimostrazione Segue facilmente dagli assiomi algebrici di $\mathbb{R}$ usando l'induzione su $m \in \mathbb{N}$. ∎

Esercizio Sia I un insieme induttivo. Dimostrare che $x + m \in I$ per ogni $x \in I$ e $m \in \mathbb{N}$, ma che, in generale, non è vero che $x + y \in I$ per ogni $x, y \in I$.

Proposizione 6 *Se $n \in \mathbb{N}$ e $x \in \mathbb{R}$ sono tali che $n < x < n + 1$, allora $x \notin \mathbb{N}$.*

Dimostrazione Per induzione su n. Sia $\mathcal{P}(n)$ la proposizione "se $k \in \mathbb{N}$, $k \leq n$ e $k < x < k + 1$, allora $x \notin \mathbb{N}$". $\mathcal{P}(1)$ è vera per l'Osservazione 2, (i). Assumiamo che sia vera $\mathcal{P}(n)$ con $n \geq 1$ e dimostriamo $\mathcal{P}(n+1)$ per assurdo. Supponiamo che esista $x \in \mathbb{N}$ tale che $k < x < k + 1$ per un qualche $k \leq n + 1$. Poiché $\mathcal{P}(n)$ vera, $k = n + 1$ e quindi $n + 1 < x < n + 2$. Definiamo l'insieme $I := \mathbb{N} \backslash \{x\} = \{m \in \mathbb{N} : \ m \neq x\}$. Poiché $x > 1$, $1 \in I$. Sia $m \in I$. Allora $m \in \mathbb{N}$ e quindi $m + 1 \in \mathbb{N}$. D'altra parte $m + 1 \neq x$ (se fosse $m + 1 = x$, seguirebbe che $x - 1 \in \mathbb{N}$ e poiché $n + 1 < x < n + 2$ si avrebbe che $n < x - 1 < n + 1$ e per l'ipotesi induttiva $x - 1$ non può essere in $\mathbb{N}$ e si avrebbe una contraddizione). Quindi $m + 1$ è in I, cioè I è induttivo, ma questo è assurdo poiché avremmo trovato un insieme induttivo strettamente contenuto in $\mathbb{N}$ il che contraddice la definizione di $\mathbb{N}$. ∎

Corollario 7 *Se n, m sono numeri naturali tali che $n > m$, allora $n \geq m + 1$.*

Dimostrazione Se fosse $n < m + 1$, si avrebbe un naturale $n \neq m$ tra m e $m + 1$ contraddicendo la Proposizione 6. ∎

Proposizione 8 *Siano $n > m$ numeri naturali. Allora $n - m \in \mathbb{N}$.*

Dimostrazione Sia $A := \{h \in \mathbb{N} : \ m+h \leq n\}$. Poiché $n > m$, dal Corollario 7 segue che $n \geq m + 1$ e quindi $1 \in A$. Supponiamo (per assurdo) che ogni elemento h di A sia tale che $m + h < n$. Da questo seguirebbe (di nuovo per il Corollario 7) che $m + h + 1 \leq n$ e quindi anche $h + 1$ sarebbe in A; ma allora A sarebbe un sottoinsieme induttivo di $\mathbb{N}$ e quindi, per (P_5), A coinciderebbe con $\mathbb{N}$ e, in particolare, $n \in A$ ossia $m+n \leq n$, cioè $m \leq 0$, il che è assurdo. Dunque deve esistere un $h \in A$ tale che $m + h = n$, il che implica che $h = n - m \in \mathbb{N}$. ∎

Proposizione 9 *Sia $A \subseteq \mathbb{N}$ non vuoto. Allora A ammette minimo cioè esiste $m \in A$ tale che $m \leq n$ per ogni $n \in A$.*

Dimostrazione Supponiamo, per assurdo, che $A \subseteq \mathbb{N}$ non vuoto non abbia minimo; in particolare $1 \notin A$ (altrimenti 1 sarebbe il minimo di A). Definiamo l'insieme $B := \{n \in \mathbb{N} : \ k \notin A, \forall\ k \in \mathbb{N} \text{ con } 1 \leq k \leq n\}$. Ora, $1 \in B$ (poiché $1 \notin A$). Sia $1 \leq n \in B$. Se fosse $n + 1 \in A$, allora $n + 1$ sarebbe il minimo di A contrariamente all'ipotesi. Dunque, $n + 1 \notin A$ e quindi $n + 1 \in B$. Ma allora B è un sottoinsieme induttivo di $\mathbb{N}$ e dunque, per (P_5), $B = \mathbb{N}$, il che implica che $A = \emptyset$ arrivando nuovamente ad una contraddizione. ∎

I risultati che seguiranno fanno uso, oltre che degli assiomi algebrici di $\mathbb{R}$ anche del seguente assioma "di completezza" che, insieme ai quindici assiomi algebrici, completa la descrizione e la caratterizzazione del sistema dei numeri reali.

Assioma dell'esistenza dell'estremo superiore

Definizione 10 *(i) Un maggiorante M di un insieme $A \subseteq \mathbb{R}$ non vuoto, è un numero reale tale che $M \geq x$, per ogni $x \in A$.*

(ii) Sia $A \subseteq \mathbb{R}$ non vuoto. Se esiste $M \in A$ tale che $x \leq M$ per ogni $x \in A$, tale numero $M =: \max A$ si chiama il massimo di A.

(iii) Un insieme $A \subseteq \mathbb{R}$ si dice limitato superiormente se esiste un maggiorante di A.

(iv) Dato un insieme non vuoto $A \subseteq \mathbb{R}$ limitato superiormente, diremo che $s =: \sup A$ è l'estremo superiore di A (o che A ammette estremo superiore s) se s è un maggiorante di A e se $s \leq M$ per ogni maggiorante M di A.

(ES) Assioma dell'estremo superiore
Ogni insieme $A \subseteq \mathbb{R}$ non vuoto e limitato superiormente ammette estremo superiore.

Osservazione 11 (i) L'estremo superiore di un insieme non vuoto, limitato superiormente è unico (esercizio).

(ii) Se un insieme ammette massimo, tale massimo coincide con l'estremo superiore. Chiaramente, il massimo di un insieme A non vuoto, limitato superiormente può non esistere ed in tal caso $\sup A \notin A$.

(iii) Definizioni analoghe (simmetriche) si danno per *minoranti*, *minimo* e per l'*estremo inferiore*[4]. Si noti (esercizio) che $\inf A = -\sup(-A)$ dove l'insieme $-A$ è definito come $-A := \{y = -x : x \in A\}$. Quindi l'estremo inferiore esiste sempre grazie a **(ES)**.

Si ha la seguente caratterizzazione dell'estremo superiore.

Proposizione 12 *$s = \sup A$ se e solo se s è un maggiorante per A e per ogni $t < s$ esiste un elemento x di A tale che $t < x$.*

Dimostrazione Se $s = \sup A$, s è un maggiorante di A e quindi $x \leq s$ per ogni $x \in A$. Sia $t < s$. Se $x \leq t$ per ogni $x \in A$, si avrebbe che t è un maggiorante di A strettamente più piccolo di s contraddicendo la definizione di estremo superiore. Quindi esiste $x \in A$ con $x > t$.
Sia ora s un maggiorante per A tale che per ogni $t < s$ esiste un elemento x di A con $t < x$. Chiaramente non può esistere un maggiorante $M < s$ (si prenda $t = M$) e quindi $s = \sup A$. ∎

Torniamo alle proprietà dei numeri naturali.

Proposizione 13 *Sia $A \subseteq \mathbb{N}$ non vuoto e limitato superiormente. Allora A ammette massimo cioè esiste $m \in A$ tale che $m \geq n$ per ogni $n \in A$.*

Dimostrazione Sia $m = \sup A$ (garantito dall'assioma dell'estremo superiore) e supponiamo, per assurdo, che $m \notin A$. Allora esisterebbe $n \in A$ tale che $m - 1 < n < m$; analogamente esisterebbe un altro numero $k \in A$ tale che $n < k < m$. Ma allora $0 < k - n < m - (m - 1) = 1$ cioè $n < k < n + 1$, il che è impossibile per la Proposizione 6. Dunque $m \in A$ e quindi m è il massimo di A. ∎

Proposizione 14 ("Proprietà archimedea")
Siano x e y numeri reali strettamente positivi. Esiste $n \in \mathbb{N}$ tale che $nx > y$.

[4]Un minorante di un insieme $A \subseteq \mathbb{R}$ è un numero m tale che $m \leq x$ per ogni $x \in A$; il minimo di A (qualora esista) è un numero $m \in A$ tale che $m \leq x$ per ogni $x \in A$; un insieme si dice *limitato inferiormente* se ha un minorante; l'estremo inferiore $r = \inf A$ di un insieme A non vuoto e limitato inferiormente è un minorante r tale che $r \geq m$ per ogni minorante m di A.

Dimostrazione Sia $z := y/x > 0$ e si noti che la tesi è equivalente a dimostrare che esiste $n \in \mathbb{N}$ tale che $n > z$. Se $z < 1$ possiamo prendere $n = 1$. Se $z \geq 1$, sia $A := \{m \in \mathbb{N} : \ m \leq z\}$. A è non vuoto ($1 \in A$ poiché $z \geq 1$) ed è limitato superiormente (da z). Per la Proposizione 13 esiste m massimo di A; tale numero soddisfa $m \leq z < m + 1$ (se fosse $m + 1 \leq z$, $m + 1$ apparterrebbe a B e m non ne sarebbe il massimo). La tesi segue con $n := m + 1$. ∎

La proprietà archimedea è equivalente a dire che $\mathbb{N}$ non è un insieme limitato.

Definizione 15 *Per $n \in \mathbb{N}$, sia $F_n := \{k \in \mathbb{N} : \ k \leq n\}$. Un insieme A si dice finito (o di cardinalità finita) se esiste $n \in \mathbb{N}$ ed una funzione iniettiva*[5] *$f : A \mapsto F_n$; se f è anche suriettiva*[6] *diremo che la cardinalità di A è n. Un insieme A si dice infinito se non è finito.*

Osservazione 16 (i) Dalla Proposizione 13 segue che $A \subseteq \mathbb{N}$ è limitato se e solo se $A \subseteq F_n$ per qualche n (si può prendere $n = \max A$).

(ii) Se A è finito, esiste $k \in \mathbb{N}$ e una funzione biunivoca f da A su[7] F_k.

(iii) Dall'osservazione precedente segue che *A è finito se e solo se esiste una applicazione biunivoca da A in F_n per un qualche n.*

(iv) F_k e F_n hanno la stessa cardinalità (ossia esiste una funzione biunivoca da F_k in F_n) se e solo se $k = n$ (Esercizio).

(v) Dalla Proposizione 14 segue che $\mathbb{N}$ è infinito.

(vi) Se A è finito allora non esiste alcuna applicazione iniettiva da A in un suo sottoinsieme proprio[8].

(vii) La contrapposizione dell'osservazione precedente si legge: "Se esiste un'applicazione iniettiva da A in suo sottoinsieme proprio, allora A è infinito". Ad esempio $f : n \in \mathbb{N} \to 2n$ mette in corrispondenza biunivova $\mathbb{N}$ con il suo sottoinsieme proprio formato dai numeri naturali pari.

I numeri interi

Definizione 17 *L'insieme dei numeri interi $\mathbb{Z}$ è l'insieme $\mathbb{Z} := \mathbb{N} \cup \{0\} \cup -\mathbb{N}$.*

Osservazione 18 Dalla definizione di $\mathbb{Z}$ e dalla Proposizione 6 segue immediatamente che

(i) *Se $n \in \mathbb{Z}$ e $x \in \mathbb{R}$ sono tali che $n < x < n + 1$, allora $x \notin \mathbb{Z}$.*

Il Corollario 7 e la Proposizione 13 si estendono immediatamente (assieme alle loro dimostrazioni) agli interi:

[5] $f : A \mapsto B$ si dice *iniettiva* se $f(x) = f(y)$ implica che $x = y$.

[6] $f : A \mapsto B$ si dice *suriettiva* se $\forall\ y \in B$, $\exists\ x \in A$ tale che $y = f(x)$.

[7] Esercizio (suggerimento: sia g un'applicazione iniettiva da A in F_n per un qualche n e si usi la Proposizione 9 per scrivere $g(A)$ come $\{m_1, ..., m_k\}$ con $m_j \in \mathbb{N}$ e $m_j < m_{j+1}$).

[8] Esercizio [segue facilmente dalle osservazioni (ii) e (iv)].

(ii) *Se n, m sono numeri interi tali che $n > m$, allora $n \geq m + 1$.*

(iii) *Sia $A \subseteq \mathbb{Z}$ non vuoto e limitato superiormente. Allora A ammette massimo.*

Dalla simmetria di $\mathbb{Z}$ rispetto all'opposto segue anche che:

(iv) *Sia $A \subseteq \mathbb{Z}$ non vuoto e limitato inferiormente. Allora A ammette minimo.*

Il principio di induzione si estende immediatamente come segue[9]:

(v) *Sia $N \in \mathbb{Z}$. Se $\mathcal{P}(N)$ è vera e da $\mathcal{P}(n)$, con $n \geq N$, segue $\mathcal{P}(n+1)$, allora $\mathcal{P}(n)$ è vera $\forall\ n \geq N$;*

(vi) *Se $\mathcal{P}(N)$ è vera e da "$\mathcal{P}(k)$ vera per $N \leq k \leq n$" segue $\mathcal{P}(n+1)$, allora $\mathcal{P}(n)$ è vera $\forall\ n \geq N$.*

Anche la Proposizione 5 si estende a $\mathbb{Z}$:

Proposizione 19 *Siano n e m numeri interi. Allora:*

(a) $n + m \in \mathbb{Z}$;

(b) $nm \in \mathbb{Z}$.

Dimostrazione (a): Se o n o m sono uguali a zero, la tesi è immediata. Supponiamo n e m entrambi diversi da zero e consideriamo i vari casi possibili. Se $n, m > 0$, la tesi segue direttamente dalla Proposizione 5. Se $n, m < 0$, $n+m = -\Big(-n+(-m)\Big) \in -\mathbb{N} \subseteq \mathbb{Z}$. Siano, ora $n > 0 > m$ (il caso $(m > 0 > n$ è solo un cambio di nomi) e si osservi che $-m \in \mathbb{N}$. Se $n > -m$, poiché $n + m = n - (-m) \in \mathbb{N}$. Se $n < -m$, $n + m = -\Big((-m) - n\Big) \in -\mathbb{N} \subseteq \mathbb{Z}$.

(b): Come sopra, se o n o m sono uguali a zero, la tesi è vera. Supponiamo n e m entrambi diversi da zero e consideriamo i vari casi possibili. Se $n, m > 0$, la tesi segue dalla Proposizione 5. Se $n, m < 0$, $nm = -(-n)(-m) \in -\mathbb{N} \subseteq \mathbb{Z}$. Se $n > 0 > m$, $nm = -\Big(n(-m)\Big) \in -\mathbb{N} \subseteq \mathbb{Z}$ e analogamente per $n < 0 < m$. ∎

Definizione 20 *Sia $x \in \mathbb{R}$ si definisce* **parte intera di** *x, e si denota $[x]$, il massimo dell'insieme*[10] *$\{n \in \mathbb{Z} : n \leq x\}$. Tale intero verifica $[x] \leq x < [x] + 1$.*

La terna $(\mathbb{Z}, +, \cdot)$ è un esempio di *anello associativo, commutativo e con unità moltiplicativa* ossia '+' e '$\cdot$' sono operazioni su $\mathbb{Z}$ associative e commutative

[9] La (v) è un semplice cambio di nome (si ponga $\mathcal{P}'(n) := \mathcal{P}(N + n - 1)$), mentre per (vi) si ponga $\mathcal{P}'(n) := \{\mathcal{P}(k) :\ N \leq k \leq N + n - 1\}$.

[10] Si noti che per la Proposizione 14 esiste $n > |x| = \max\{x, -x\}$ e dunque $-n < x$ mostrando che l'insieme $\{n \in \mathbb{Z} : n < x\} \neq \emptyset$ e dunque (poiché tale insieme è limitato per definizione) segue dal punto (iii) dell'Osservazione 18 che tale massimo esiste.

ed hanno elementi neutri, inoltre $\forall\ n \in \mathbb{Z}$ esiste l'opposto e vale la proprietà distributiva.

I numeri razionali

Definizione 21 *L'insieme dei numeri razionali è definito come*[11]
$\mathbb{Q} := \{r = p/q : \quad p \in \mathbb{Z}\ ,\ q \in \mathbb{N}\}$.

Osservazione 22 Se $p, q \in \mathbb{Z}$ e $q < 0$, allora $pq^{-1} = (-p)(-q)^{-1} \in \mathbb{Z}$.

Proposizione 23 *Siano r e s numeri razionali. Allora:*

(a) $r + s \in \mathbb{Q}$*;*

(b) $rs \in \mathbb{Q}$.

Dimostrazione Siano $r = p/q$ e $s = m/n$ (con $p, m \in \mathbb{Z}$ e $q, n \in \mathbb{N}$). Dalle Proposizioni 5 e 19 segue:
(a): $r + s = pq^{-1} + mn^{-1} = (pn)(qn)^{-1} + (qm)(qn)^{-1} = (pn + qm)(qn)^{-1} \in \mathbb{Q}$;
(b): $pq^{-1} \cdot mn^{-1} = (pm) \cdot q^{-1} \cdot n^{-1} = (pm) \cdot (qn)^{-1} \in \mathbb{Q}$. ∎

I numeri razionali sono "densi" in $\mathbb{R}$ ossia:

Proposizione 24 *Per ogni $a, b \in \mathbb{R}$ con $a < b$, esiste $r \in \mathbb{Q}$ tale che $a < r < b$.*

Dimostrazione Sia N un numero naturale tale che $N > (b - a)^{-1}$ (la cui esistenza è garantita dalla proprietà archimedea), sia $k = [aN]$ (Definizione 20) e sia $r := (k + 1)/N \in \mathbb{Q}$. Allora $k \leq aN < k + 1$ e quindi

$$\frac{k}{N} \leq a < \frac{k+1}{N} = r = \frac{k}{N} + \frac{1}{N} \leq a + \frac{1}{N} < b. \quad \blacksquare$$

Descriviamo brevemente la "rappresentazione standard" dei numeri razionali.

Definizione 25 *(i) Un intero m è divisibile per un intero $d \neq 0$ se esiste $n \in \mathbb{Z}$ tale che $m = dn$; in tal caso scriveremo $d|m$ e diremo che d è un divisore di m.*
(ii) Dati due interi m e n si definisce il massimo comun divisore (m.c.d.), e si denota con (m, n), il massimo dell'insieme[12] $D := \{d \in \mathbb{N} : \ d|a \text{ e } d|b\}$.
(iii) Due interi m ed n si dicono primi tra loro o coprimi se $(m, n) = 1$ ossia se l'unico intero positivo che divide sia m che n è 1.

Proposizione 26 *Sia r è un numero razionale non nullo. Esiste una coppia $(p, q) \in \mathbb{Z} \times \mathbb{N}$ tale che $r = pq^{-1}$ con p e q coprimi.*

[11] Le notazioni in "forma di frazione" p/q e $\frac{p}{q}$, per definizione, significano pq^{-1}.

[12] $1 \in D = \{d \in \mathbb{N} : \ d|a \text{ e } d|b\}$ ed un maggiorante di D è $\max\{|m|, |n|\}$.

Dimostrazione Sia $D := \{n \in \mathbb{N} : \exists m \in \mathbb{Z} \text{ per cui } r = mn^{-1}\}$, "l'insieme dei denominatori di r". Per definizione di $\mathbb{Q}$, $D \neq \emptyset$. Per la Proposizione 9 esiste $q = \min D$. Per definizione di D esiste $p \in \mathbb{Z}$ tale che $r = pq^{-1}$ e poiché $r \neq 0$, $p \neq 0$ e tale p è unico. Inoltre p e q sono coprimi: se non lo fossero esisterebbe un divisore comune $h > 1$, $h \in \mathbb{N}$ e si avrebbe $p = \bar{p}h$ e $q = \bar{q}h$ con $\bar{p} \in \mathbb{Z}$ e $\bar{q} \in \mathbb{N}$; allora $r = \bar{p}\bar{q}^{-1}$ con $\bar{q} < q$, il che contraddirrebbe la definizione di q. ∎

$\mathbb{Q}$ è un "campo ordinato" ossia verifica i quindici assiomi algebrici di $\mathbb{R}$. D'altra parte $\mathbb{Q}$ non soddisfa l'assioma dell'estremo superiore:

Proposizione 27 *Sia $D = \{r \in \mathbb{Q}, r > 0 : \ r^2 < 2\}$. D è non vuoto e 2 ne è un maggiorante ma non ammette estremo superiore in $\mathbb{Q}$: $s = \sup D \in \mathbb{R}\backslash\mathbb{Q}$.*

Premettiamo alla dimostrazione della Proposizione 27 un antico risultato.

Lemma 28 *Non esiste alcun razionale r tale che $r^2 = 2$.*

Dimostrazione Supponiamo per assurdo che esista $r \in \mathbb{Q}$ tale che $r^2 = 2$ e sia $r = pq^{-1}$ la sua rappresentazione standard con $q \in \mathbb{N}$ e p e q coprimi (Proposizione 26). Si ha $p^2 = 2q^2$ e (poiché il quadrato di un numero dispari è dispari) p è un numero pari, cioè, $p = 2k$ con $k \in \mathbb{Z}$. Quindi $(2k)^2 = 2q^2$, cioè $2k^2 = q^2$ e per lo stesso motivo anche q dovrebbe essere pari. Ma allora p e q non sarebbero coprimi (avendo 2 come divisore comune). ∎

Dimostrazione (della Proposizione 27). $1 \in D$ e 2 è un maggiorante per D (se $r > 2$ allora $r^2 > 4$ e $r \notin D$). Quindi D ammette estremo superiore $s = \sup D \in \mathbb{R}$. Supponiamo per assurdo che $s \in \mathbb{Q}$ e definiamo il numero razionale positivo

$$t := \frac{2s+2}{s+2} = s - \frac{s^2-2}{s+2} \ . \tag{1}$$

Si noti che

$$t^2 - 2 = 2\frac{s^2-2}{(s+2)^2} \ . \tag{2}$$

Per il Lemma 28, $r^2 \neq 2$ per ogni razionale r e quindi o $s^2 > 2$ o $s^2 < 2$.

Se $s^2 > 2$, da (2) segue che anche $t^2 > 2$, e da (1) segue che $s > t$. Se $r \in D$, $r^2 < 2 < t^2$ cioè $r^2 < t^2$, che implica[13] $r < t$. Quindi t è un maggiorante di D. Dalla definizione di estremo superiore segue che $s \leq t$, che contraddice $s > t$.

Se $s^2 < 2$, da (2) segue che $t^2 < 2$ e quindi $t \in D$. Da (1) segue anche che $t > s$ e quindi s non è un maggiorante di D contraddicendo la definizione di s. ∎

[13] $r \geq t \geq 0 \implies r^2 \geq rt \geq t^2$.