Assiomatica di $\mathbb{R}$

Parte 2: Proprietà archimedea; $\mathbb{Z}$; $\mathbb{Q}$.

(5/4/2016)

4 Proprietà archimedea di $\mathbb{N}$

Proposizione 18 *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 11. Dunque $m \in A$ e quindi m è il massimo di A. ∎

Proposizione 19 ("Proprietà archimedea")
Siano x e y numeri reali strettamente positivi. Esiste $n \in \mathbb{N}$ tale che[9] *$nx > y$.*

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 $A := \{m \in \mathbb{N} \mid m \leq z\}$. A è non vuoto ($1 \in A$ poiché $z \geq 1$) ed è limitato superiormente (da z). Per la Proposizione 18 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.

5 I numeri interi $\mathbb{Z}$

Definizione 20 *L'insieme dei numeri interi $\mathbb{Z}$ è l'insieme $\mathbb{Z} := \mathbb{N} \cup \{0\} \cup -\mathbb{N}$.*

Osservazione 21 Dalla definizione di $\mathbb{Z}$ e dalla Proposizione 11 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 12 e la Proposizione 18 si estendono immediatamente (assieme alle loro dimostrazioni) agli interi:

(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[10]:

(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 $\forall\, n \geq N$.*

[9] Da ora in poi spesso ometteremo il simbolo di moltiplicazione "$\cdot$" scrivendo xy al posto di $x \cdot y$ per due numeri reali x e y.

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

Anche la Proposizione 10 si estende a $\mathbb{Z}$:

Proposizione 22 *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 10. 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 10. 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 23 *Sia $x \in \mathbb{R}$ si definisce* **parte intera di** *x, e si denota $[x]$, il massimo dell'insieme*[11] *$\{n \in \mathbb{Z} \mid n \leq x\}$. Tale intero verifica $[x] \leq x < [x]+1$.*

6 I numeri razionali $\mathbb{Q}$

Definizione 24 *L'insieme dei numeri razionali è definito come $\mathbb{Q} := \{r = \frac{p}{q} \mid p \in \mathbb{Z}\ ,\ q \in \mathbb{N}\}$. I numeri in $\mathbb{R}\backslash\mathbb{Q}$ si chiamano irrazionali.*

Osservazione 25 Se $p, q \in \mathbb{Z}$ e $q < 0$, allora $pq^{-1} = (-p)(-q)^{-1} \in \mathbb{Z}$.

Proposizione 26 *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 10 e 22 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 27 *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 23) 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.

[11] Si noti che per la Proposizione 19 esiste $n > |x| = \max\{x, -x\}$ e dunque $-n < x$ mostrando che l'insieme $\{n \in \mathbb{Z} \mid n < x\} \neq \emptyset$ e dunque (poiché tale insieme è limitato per definizione) segue dal punto (iii) dell'Osservazione 21 che tale massimo esiste.

Definizione 28 *(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) Un numero naturale $n > 1$ si dice **primo** *se gli unici divisori di n sono 1 e n.*

(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] *$D := \{d \in \mathbb{N} \,|\, d|a \text{ e } d|b\}$.*

(iv) Due interi m ed n si dicono **primi tra loro** *o coprìmi se $(m, n) = 1$ ossia se l'unico intero positivo che divide sia m che n è 1.*

Proposizione 29 *Sia r è un numero razionale non nullo. Esiste una ed una sola coppia $(p, q) \in \mathbb{Z} \times \mathbb{N}$ tale che $r = pq^{-1}$ con p e q coprìmi.*

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 14 esiste $q = \min D$ (a tale q è unico). 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 coprìmi: 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 30 *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 30 un antico risultato.

Proposizione 31 *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 coprìmi (Proposizione 29). 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 coprìmi (avendo 2 come divisore comune). ∎

Dimostrazione (della Proposizione 30). $1 \in D$ e 2 è un maggiorante per D (se fosse $r > 2$ 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 la Proposizione 31, $r^2 \neq 2$ 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. ∎

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

[13] $r \geq t \geq 0 \implies r^2 \geq rt \geq t^2$; vedi anche la (3).