Assiomatica di $\mathbb{R}$

Parte 1: Assiomi algebrici. Definizione di $\mathbb{N}$. Assioma di completezza

(25/3/2016)

Definizione 1 (i) *Dati due insiemi non vuoti A e B una* **relazione $\mathcal{R}$ di A in B** *è un sottoinsieme*[1] $\mathcal{R} \subseteq A \times B$. *Una* **relazione in** A *è una relazione di A in A.*
(ii) *Una* **funzione** f **di** A **in** B *è una relazione di A in B tale che se $(x, y) \in f$ e $(x, y') \in f$, allora $y = y'$, in altri termini, una funzione è una relazione tale che due elementi distinti non possono avere la stessa prima componente*[2]. *Il* **dominio** *di una funzione $f \subseteq A \times B$ è l'insieme $D_f := \{x \in A \,|\, (x, y) \in f\}$; il* **range** *o l'***immagine** *di f è l'insieme $R_f := f(D_f) := \{y \in B \,|\, (x, y) \in f\}$. Una* **funzione da** A **in** B *è una funzione di A in B con $D_f = A$ (e si denota $f : A \to B$); una* **funzione da** A **su** B *(o funzione "suriettiva") è una funzione da A in B con $R_f = B$; una funzione da A in B si dice* **iniettiva** *se $(x, y) \in f$ e $(x', y) \in f$ implica $x = x'$; una funzione* **biunivoca** *da A in B è una funzione iniettiva da A su B.*
(iii) Una operazione binaria su A è una funzione da $A \times A$ in A; una relazione su A è una relazione di A in A.

Definizione 2 *L'insieme dei numeri reali, denotato $\mathbb{R}$, è un insieme dotato di due operazioni binarie, "somma" (denotata con "$+$") e "prodotto" (denotata con "$\cdot$") e di una relazione*[3] *di "ordine" (denotata "$\leq$"), che soddisfa quindici assiomi "algebrici" enunciati in § 1 più un sedicesimo assioma (di "completezza") enunciato in § 3.*

1 I quindici assiomi algebrici (e prime conseguenze)

Assiomi della addizione:

(S$_1$)	$x + y = y + x \quad \forall\, x, y \in \mathbb{R}$	proprietà commutativa di $+$;
(S$_2$)	$(x + y) + z = x + (y + z) \quad \forall\, x, y, z \in \mathbb{R}$	proprietà associativa di $+$;
(S$_3$)	$\exists\, 0 \in \mathbb{R}$ tale che $x + 0 = x \quad \forall\, x \in \mathbb{R}$	esiste elemento neutro per $+$;
(S$_4$)	$\forall\, x \in \mathbb{R},\ \exists\, y \in \mathbb{R},$ tale che $x + y = 0$	esistenza elemento opposto.

Assiomi della moltiplicazione:

(P$_1$)	$x \cdot y = y \cdot x \quad \forall\, x, y \in \mathbb{R}$	proprietà commutativa di $\cdot$;
(P$_2$)	$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall\, x, y, z \in \mathbb{R}$	proprietà associativa di $\cdot$;
(P$_3$)	$\exists\, 1 \in \mathbb{R}, 1 \neq 0,$ tale che $x \cdot 1 = x \quad \forall\, x \in \mathbb{R}$	esiste elemento neutro per $\cdot$;
(P$_4$)	$\forall\, x \in \mathbb{R},\ x \neq 0,\ \exists\, y \in \mathbb{R}$ tale che $x \cdot y = 1$	esistenza del reciproco.

Proprietà distributiva:
(SP) $x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \forall\, x, y, z \in \mathbb{R}$.

Assiomi di ordine[4] **totale**:

[1] Di solito, una coppia "in relazione" $(x, y) \in \mathcal{R}$ si denota anche $x\mathcal{R}y$.
[2] Di solito, una coppia (x, y) di una funzione f, si denota con $(x, f(x))$; per una funzione f si usano anche le notazioni standard $f : x \mapsto f(x)$ o semplicemente $f(x)$.
[3] Ossia, esistono due operazioni binarie su $\mathbb{R}$ ed una relazione su $\mathbb{R}$.
[4] Una relazione che soddisfi esclusivamente le proprietà riflessiva, antisimmetrica e transitiva, si dice relazione di "ordine parziale". Un ordine parziale è totale quando tutti gli elementi sono in relazione.

(O_1)	$x \leq x \quad \forall\, x \in \mathbb{R}$	proprietà riflessiva di $\leq$;
(O_2)	$x \leq y,\ y \leq x$ allora $x = y$	proprietà antisimmetrica di $\leq$;
(O_3)	$x \leq y,\ y \leq z$ allora $x \leq z$	proprietà transitiva di $\leq$;
(O_4)	$x \leq y$ o $y \leq x \quad \forall\, x, y \in \mathbb{R}$	ordine totale di $\leq$.

Assioma di somma e ordine:
(SO) $x \leq y$ allora $x + z \leq y + z \quad \forall\, z \in \mathbb{R}$.

Assioma di prodotto e ordine:
(PO) $0 \leq x,\ 0 \leq y$ allora $0 \leq x \cdot y$.

Discutiamo, ora, alcune conseguenze semplici degli assiomi algebrici.

Proposizione 3 *Nelle seguenti affermazioni, x, y, z sono elementi di $\mathbb{R}$.*
(i) (Unicità dell'opposto) *Se $x + y = 0$ e $x + z = 0$ allora $y = z$; quindi l'opposto di x è unico e verrà denotato con $-x$.*

(ii) (Unicità del reciproco) *Se $x \cdot y = 1$ e $x \cdot z = 1$ allora $y = z$; quindi il reciproco di $x \neq 0$ è unico e verrà denotato con x^{-1} o con $1/x$ o $\dfrac{1}{x}$.*

(iii) $-(-x) = x$.

(iv) *Se $x \neq 0$, allora $(x^{-1})^{-1} = x$.*

Dimostrazione[5]
(i): $y \overset{(S_3)}{=} y + 0 = y + (x + z) \overset{(S_2)}{=} (y + x) + z \overset{(S_1)}{=} (x + y) + z = 0 + z \overset{(S_2, S_3)}{=} z$.
(ii) $y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = (x \cdot y) \cdot z = 1 \cdot z = z$.
(iii) $(-x) + x = x + (-x) = 0$ quindi dall'unicità dell'opposto segue l'asserto.
(iv) $x^{-1} \cdot x = x \cdot x^{-1} = 1$ quindi dall'unicità del reciproco segue l'asserto. ∎

Notazioni: $y + (-x)$ si denota $y - x$.
$x \cdot y^{-1}$ si denota anche con x/y o con $\dfrac{x}{y}$.
$2 := 1 + 1$.
$x^2 := x \cdot x$.
$x \geq y$ è equivalente, per definizione, a $y \leq x$.
$x < y$ significa $x \leq y$ e $x \neq y$; $x > y$ è equivalente a $y < x$.
$x + y \cdot z := x + (y \cdot z)$.

Proposizione 4 *Nelle seguenti affermazioni, x, y, z sono elementi di $\mathbb{R}$.*
(i) (Legge di cancellazione per la somma) *Se $x + y = x + z$, allora $y = z$; in particolare, se $x + y = x$, allora $y = 0$.*

(ii) (Legge di cancellazione per il prodotto) *Se $x \neq 0$ e $x \cdot y = x \cdot z$, allora $y = z$; in particolare, se $x \neq 0$ e $x \cdot y = x$, allora $y = 1$.*

(iii) $x \cdot 0 = 0$.

(iv) $(-1) \cdot x = -x$.

[5] Nella prima riga della dimostrazione indichiamo, in ogni uguaglianza, l'assioma che viene usato; invitiamo il lettore a fare lo stesso dalla seconda riga in poi.

Dimostrazione
(i): $y = 0 + y = (x - x) + y = (x + y) - x = (x + z) - x = (x - x) + z = 0 + z = z$; la seconda affermazione segue prendendo $z = 0$.
(ii): $y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot z) = (x^{-1} \cdot x) \cdot z = 1 \cdot z = z$; la seconda affermazione segue prendendo $z = 1$.
(iii): $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ che implica per (i) $x \cdot 0 = 0$.
(iv): $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 - 1) \cdot x = 0 \cdot x = 0$ e dall'unicità dell'opposto segue che $-x = (-1) \cdot x$. ∎

Proposizione 5 *Nelle seguenti affermazioni, x, y, z sono elementi di $\mathbb{R}$.*
(i) *Se $x \geq 0$, allora $-x \leq 0$; se $x \leq 0$ allora $-x \geq 0$.*
(ii) *Se $y \leq z$ e $x \geq 0$, allora $x \cdot y \leq x \cdot z$. Se $y \leq z$ e $x \leq 0$, allora $x \cdot y \geq x \cdot z$.*
(iii) *Se $x \leq 0$ e $y \leq 0$, allora $x \cdot y \geq 0$; se $x \leq 0 \leq y$, allora $x \cdot y \leq 0$.*
(iv) *$x^2 \geq 0$ per ogni x.*
(v) *$1 > 0$.*
(vi) *Se $x > 0$, allora $x^{-1} > 0$; se $x < 0$, allora $x^{-1} < 0$.*

Dimostrazione
(i): $x \geq 0$ implica (per (SO)) $x - x \geq -x$ ossia $0 \geq -x$; $x \leq 0$ implica (per (SO)) $x - x \leq -x$ ossia $0 \leq -x$.
(ii): Se $y \leq z$, allora (per (SO)) $0 \leq z - y$ e (per (PO)) $0 \leq x \cdot (z - y)$, che (per (SO)) è equivalente a $x \cdot y \leq x \cdot z$. La seconda affermazione deriva dalla prima e da (i).
(iii): Segue da (ii) con $z = 0$.
(iv): Segue da (PO) (se $x \geq 0$) e da (iii) (se $x \leq 0$).
(v): $1 = 1 \cdot 1 \geq 0$ (per (iv)) e, per (P_3), $1 \neq 0$ quindi $1 > 0$.
(xi): Innanzitutto dalla Proposizione 4–(iii) segue che $x^{-1} \neq 0$ (per ogni $x \neq 0$): se fosse $x^{-1} = 0$ si avrebbe $1 = x \cdot x^{-1} = x \cdot 0 = 0$, contraddicendo (P_3). Sia ora $x > 0$; se fosse $x^{-1} < 0$ si avrebbe $1 = x \cdot x^{-1} \leq 0$ per (iii), il che contraddice $1 > 0$. Sia $x < 0$; se fosse $x^{-1} > 0$ si avrebbe $1 = x \cdot x^{-1} \leq 0$ per (iii), il che, di nuovo, contraddice $1 > 0$. ∎

2 I numeri naturali $\mathbb{N}$: definizione e prime proprietà

Definizione 6 (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*[6]

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

Osservazione 7 (i) Esempi di insiemi induttivi sono $I_1 := \{x \in \mathbb{R} \,|\, x \geq 1\}$ e $I_2 := \{1\} \cup \{x \in \mathbb{R} \,|\; x \geq 2\}$. 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[7] $n \in \mathbb{N}$ e non ci sono interi tra 1 e 2: *se $x \in \mathbb{R}$ è tale che $1 < x < 2$ allora $x \notin \mathbb{N}$.*

[6] Si osservi che l'intersezione di insiemi induttivi è un insieme induttivo.
[7] 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 $\mathbb{N} \cup \{0\}$.

(ii) Dalla definizione di $\mathbb{N}$ e dagli assiomi algebrici di $\mathbb{R}$ segue immediatamente che $\mathbb{N}$ soddisfa le seguenti proprietà[8]:

(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 $\implies I = \mathbb{N}$.

Proposizione 8 ("Principio di induzione") *Siano $\mathcal{P}(n)$ affermazioni che dipendono da $n \in \mathbb{N}$. Supponiamo che $\mathcal{P}(1)$ sia vera e che se vale $\mathcal{P}(n)$, con $n \geq 1$, allora vale $\mathcal{P}(n+1)$. Allora $\mathcal{P}(n)$ è vera per ogni $n \in \mathbb{N}$.*

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

Osservazione 9 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 $\mathcal{P}'(n) := \{\mathcal{P}(k) \mid \ 1 \leq k \leq n\}$ ed applicare la Proposizione 8 a $\mathcal{P}'(n)$.

Proposizione 10 *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 11 *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 7, (i). Assumiamo che sia vera $\mathcal{P}(n)$ con $n \geq 1$ e dimostriamo $\mathcal{P}(n+1)$ per assurdo, ossia, supponiamo che $x \in \mathbb{N}$. Poiché $\mathcal{P}(n)$ vera, si deve avere $n+1 < x < n+2$. Definiamo, ora, l'insieme $I := \mathbb{N} \backslash \{x\} = \{m \in \mathbb{N} \mid \ m \neq x\}$. Poiché $x > n+1 > 1$, $1 \in I$. 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 $n+1 < m+1 < n+2$ ossia $n < m < n+1$ contraddicendo $\mathcal{P}(n)$). 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 12 *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 11. ∎

[8] (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 13 *Siano $n > m$ numeri naturali. Allora $n - m \in \mathbb{N}$.*

Dimostrazione Sia $A := \{h \in \mathbb{N} \mid \ m + h \leq n\}$. Poiché $n > m$, dal Corollario 12 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 12) 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 14 *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 $B := \{n \in \mathbb{N} \mid \ k \notin A, \forall\ k \in \mathbb{N} \text{ con } 1 \leq k \leq n\}$. 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. ∎

3 XVI assioma: Assioma di completezza o dell'esistenza dell'estremo superiore

Definizione 15 (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 16 (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*[9]. Si noti (esercizio) che $\inf A = -\sup(-A)$ dove l'insieme $-A$ è definito come $-A := \{y = -x \mid x \in A\}$. Quindi l'estremo inferiore esiste sempre grazie a **(ES)**.

[9] 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.

Si ha la seguente caratterizzazione dell'estremo superiore.

Proposizione 17 *$s = \sup A$ 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 $s = \sup A$.
$\blacksquare$