Il sistema dei numeri reali

Appunti per il corso di Analisi Matematica 1,
C.L. Matematica e C.L. Fisica, Università di Parma
a.a. 2015/16

Marino Belloni & Stefano Panizzi

1 Relazioni d'ordine

Dato un insieme non vuoto S, una relazione binaria $\mathcal{R}$ su S è definita come un sottoinsieme del prodotto cartesiano $S \times S$. Diciamo che gli elementi $x \in S$, $y \in S$ sono in relazione, e scriviamo $x\mathcal{R}y$, quando la coppia ordinata $(x, y) \in \mathcal{R}$.

Siamo interessati in particolare alle **relazioni d'ordine**.

Definizione 1. *Una relazione binaria $\mathcal{R}$ sull'insieme S è una* relazione d'ordine *se soddisfa le tre proprietà seguenti:*

1) Per ogni $x \in S$, si ha $x\mathcal{R}x$ [Riflessiva]

2) Per ogni x, y, z in S, se $x\mathcal{R}y$ e $y\mathcal{R}z$, allora $x\mathcal{R}z$ [Transitiva]

3) Per ogni x, y in S, se $x\mathcal{R}y$ e $y\mathcal{R}x$, allora $x = y$ [Antisimmetrica]

La coppia $(S, \mathcal{R})$, ovvero l'insieme S dotato di un ordinamento $\mathcal{R}$, sarà detto insieme ordinato *(da $\mathcal{R}$).*

Esempio 1. *L'insieme dei numeri razionali $\mathbb{Q}$ con la relazione data dall'ordinamento naturale $\leq$, costituisce un esempio di insieme ordinato.*

Esempio 2. *Un esempio meno famigliare di ordinamento è dato dall'insieme dei numeri interi positivi $\mathbb{N}$, ordinato dalla seguente relazione (verificare per esercizio che sono soddisfatte le tre condizioni):*

$$p\mathcal{R}q, \qquad se \quad q \text{ è multiplo di } p.$$

Alla relazione dell'esempio (2) manca una importante proprietà: esistono elementi dell'insieme che non sono in relazione tra loro (ad esempio, 5 e 12).
Nell'insieme $\mathbb{Q}$ con l'ordinamento naturale, invece, due elementi $x, y \in \mathbb{Q}$ sono sempre confrontabili e si ha uno, ed uno solo dei seguenti casi

$$i)\, x < y, \qquad ii)\, x = y, \qquad iii)\, x > y.$$

Definizione 2. *Una relazione d'ordine $\mathcal{R}$ sull'insieme S è una* ***relazione d'ordine totale*** *se per ogni coppia di elementi $(x, y) \in S \times S$, risulta che $x\mathcal{R}y$ oppure $y\mathcal{R}x$.*

D'ora in avanti, pur mantenendo astratto il livello della discussione, dato un insieme S dotato di ordinamento totale, utilizzeremo la più famigliare notazione $x \leq y$ al posto di $x\mathcal{R}y$.

Definizione 3. *Sia A un sottoinsieme dell'insieme totalmente ordinato S.*

- *Un elemento $M \in S$ è detto* ***massimo*** *di A, e si scrive $M = \max A$, se*

$$\begin{cases} M \in A, \\ x \leq M, \text{ per ogni } x \in A. \end{cases}$$

- *Un elemento $m \in S$ è detto* ***minimo*** *di A, e si scrive $m = \min A$, se*

$$\begin{cases} m \in A, \\ x \geq m, \text{ per ogni } x \in A. \end{cases}$$

Esercizio 1. *Provare che il massimo (minimo) se esiste è unico.*

Non sempre un sottoinsieme non vuoto possiede massimo o minimo.

Esempio 3. *L'insieme*

$$A = \{x \in \mathbb{Q} : \ x < 0\},$$

non ha massimo. Infatti se $x \in A$, allora $x < \frac{x}{2} \in A$ (il massimo deve essere un elemento di A). Abbastanza ovviamente A non ha nemmeno minimo: infatti, se $x \in A$ allora $x > (x-1) \in A$.

Osservazione 1. *Ogni sottoinsieme* finito *di un insieme totalmente ordinato possiede massimo e minimo (prendiamola ora per buona sul piano intuitivo, l'affermazione a dire il vero andrebbe dimostrata per induzione).*

Definizione 4. *Sia A un sottoinsieme dell'insieme totalmente ordinato S.*

- *Un elemento $b \in S$ è detto* ***maggiorante*** *di A se $x \leq b$ per ogni $x \in A$. Indicheremo con $\boldsymbol{M}_A$ l'insieme dei maggioranti di A.*
- *Un elemento $b \in S$ è detto* ***minorante*** *di A se $x \geq b$ per ogni $x \in A$. Indicheremo con $\boldsymbol{m}_A$ l'insieme dei minoranti di A.*

Segue in modo naturale la seguente definizione

Definizione 5. *Sia A un sottoinsieme dell'insieme totalmente ordinato S. Diremo che*

- *A è* ***superiormente limitato*** *se $\boldsymbol{M}_A \neq \emptyset$;*
- *A è* ***inferiormente limitato*** *se $\boldsymbol{m}_A \neq \emptyset$.*

Un insieme che sia superiormente e inferiormente limitato è detto ***limitato****.*

Nel precedente esempio (3), il sottoinsieme A di $\mathbb{Q}$ è superiormente limitato (infatti $0 \in \mathbf{M}_A$), mentre non è inferiormente limitato (ovvero $\mathbf{m}_A = \emptyset$).

Definizione 6. *Sia $(S, \leq)$ un insieme totalmente ordinato, e sia $A \neq \emptyset$ un suo sottoinsieme superiormente limitato, ovvero tale che $\boldsymbol{M}_A \neq \emptyset$. Se esiste $\beta = \min \boldsymbol{M}_A$, questo numero viene detto* ***estremo superiore*** *di A e si scrive $\beta = \sup A$.*

Analogamente, dato un insieme A inferiormente limitato, se esiste $\alpha = \max \mathbf{m}_A$, questo numero viene detto **estremo inferiore** e si scrive $\alpha = \inf A$.

Osservazione 2. *Dato un insieme $A \neq \emptyset$, se esiste l'estremo superiore $\beta = \sup A$ questo è unico: essendo $\beta = \min \boldsymbol{M}_A$, quanto affermato, segue dal fatto che il minimo di un insieme, quando esiste, è unico.*
Analogamente si prova che l'estremo inferiore, se esiste, è unico.

Osservazione 3. *Se esiste $M = \max A$, allora esiste anche l'estremo superiore* $\sup A$ *e si ha $M = \max A = \sup A$. Infatti*

- *il massimo M, per definizione, è un maggiorante di A, ovvero $M = \max A \in \boldsymbol{M}_A$;*
- *inoltre $M = \max A \in A$; ne segue che per ogni maggiorante $b \in \boldsymbol{M}_A$ si ha $M \leq b$, ovvero $M = \min \boldsymbol{M}_A$.*

Si può dire che $M = \max A \in A \cap \boldsymbol{M}_A$.

Nel precedente esempio (3), dove $A = \{x \in \mathbb{Q} : \ x < 0\}$, risulta che $0 = \sup A$. Infatti

- 0 è un maggiorante;
- se $x < 0$, allora $x < \frac{x}{2} \in A$, quindi x non può essere un maggiorante. Ne segue che $A \cap \mathbf{M}_A = \emptyset$.

Nel discutere l'ultimo esempio abbiamo sostanzialmente formulato una **caratterizzazione dell'estremo superiore**:

L'elemento $\beta \in S$ è l'estremo superiore dell'insieme superiormente limitato A, ovvero $\beta = \sup A$, se e soltanto se valgono le seguenti due condizioni:
1) *$x \leq \beta$ per ogni $x \in A$;*
2) *per ogni $y \in S$, se $y < \beta$ allora esiste $x \in A$ tale che $y < x \leq \beta$*

La prima dice che β è maggiorante di A, la seconda che non può esistere un maggiorante minore di β (naturalmente, $x < y$ significa $x \leq y$ e $x \neq y$).

Arrivati a questo punto, abbiamo visto che un insieme, anche se superiormente limitato, non è detto che possieda massimo. La domanda cruciale è:

in una struttura d'ordine totale,
un insieme limitato superiormente possiede sempre estremo superiore?

La domanda è naturale se pensiamo che l'estremo superiore estende la nozione di massimo in casi in cui quest'ultimo non esiste. La risposta è in generale negativa, come mostra il seguente:

Esercizio 2. *Si consideri $(\mathbb{Q}, \leq)$, ovvero l'insieme dei razionali con l'usuale relazione d'ordine totale. Provare che l'insieme*

$$B = \{x \in \mathbb{Q} : \ x > 0, \quad x^2 < 2\}$$

è limitato superiormente ma non esiste il $\sup B$. *(Attenzione: l'estremo superiore deve essere un elemento di $\mathbb{Q}$, in questo caso un numero razionale!)*

Dimostrazione. Proviamo che non esiste $\max B$. A tal fine proveremo che comunque si prenda $q \in B$, esiste $N \in \mathbb{N}$ tale che $(q + 1/N) \in B$. Infatti, ricordando che $N < N^2$ per ogni $N > 1$, si ha

$$\left(q + \frac{1}{N}\right)^2 = q^2 + \frac{2q}{N} + \frac{1}{N^2} < q^2 + \frac{2q}{N} + \frac{1}{N} = q^2 + \frac{2q+1}{N}.$$

Ma

$$q^2 + \frac{2q+1}{N} < 2 \Longleftrightarrow \frac{2q+1}{N} < 2 - q^2 \Longleftrightarrow N > \frac{2q+1}{2-q^2}$$

e dunque per ogni $q \in B$ esiste $N > (2q+1)/(2-q^2)$ tale che $(q + 1/N) \in B$. Questo prova che B non ha massimo.

Se ora consideriamo $C = \{x \in \mathbb{Q} : \ x > 0, \quad x^2 > 2\}$, si dimostra che non esiste $\min C$: infatti preso $q \in C$ si ha

$$\left(q - \frac{1}{N}\right)^2 = q^2 - \frac{2q}{N} + \frac{1}{N^2} > q^2 - \frac{2q}{N} - \frac{1}{N} = q^2 - \frac{2q+1}{N}.$$

Ma

$$q^2 - \frac{2q+1}{N} > 2 \Longleftrightarrow \frac{2q+1}{N} < q^2 - 2 \Longleftrightarrow N > \frac{2q+1}{q^2-2}$$

e dunque per ogni $q \in C$ esiste $N > (2q+1)/(2-q^2)$ tale che $(q - 1/N) \in C$. Questo prova che C non ha minimo. Essendo $C = \mathbf{m}_B \cap \mathbb{Q}$, ne segue che non esiste $\sup B$ in $\mathbb{Q}$. $\square$

Nell'esercizio precedente l'estremo superiore di B in $\mathbb{R}$ è $\sqrt{2} \notin \mathbb{Q}$.

2 Campi

Le usuali operazioni di addizione e moltiplicazione tra numeri razionali (o reali) soddisfano a proprietà (note dalla scuola primaria: commutativa, associativa, distributiva, ecc.) che nell' Algebra astratta concorrono a formare gli assiomi di ciò che vien detto **campo** o corpo commutativo. Enunciamo gli assiomi in riferimento ad un insieme astratto S (per ora non necessariamente ordinato).

Un insieme S dotato di due operazioni $+$ e $\cdot$ è detto un campo se valgono i seguenti assiomi:

(A1) $x + y = y + x$, per ogni x, y in S;
(A2) $(x + y) + z = x + (y + z)$, per ogni x, y, z in S;
(A3) esiste un elemento $0 \in S$ tale che $x + 0 = x$, per ogni x in S;
(A4) ad ogni $x \in S$ corrisponde un elemento $-x$ tale che $x + (-x) = 0$;
(A5) $x \cdot y = y \cdot x$, per ogni x, y in S;
(A6) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, per ogni x, y, z in S;
(A7) esiste un elemento $1 \in S$ tale che $x \cdot 1 = x$, per ogni x in S;
(A8) ad ogni $x \in S$, $x \neq 0$ corrisponde un elemento $x^{-1} \in S$ tale che $x \cdot x^{-1} = 1$;
(A9) $(x + y) \cdot z = x \cdot y + y \cdot z$, per ogni x, y, z in S.

Dai nove assiomi (A1) - (A9), si possono ricavare diverse altre proprietà ben note: unicità dell'elemento neutro dell'addizione (0) e della moltiplicazione (1), legge di annullamento del prodotto, legge di cancellazione, unicità dell'oppostro $(-x)$ e dell'inverso o reciproco (x^{-1}), ecc. ecc. Omettiamo questa discussione: si trova riportata su tutti i testi di Analisi ed è competenza dell'Algebra (in contesti ancor più generali).

Fino ad ora abbiamo tenuto separate la struttura di ordinamento da quella di ordine (a scanso di equivoci, non c'è in generale nessuna ragione per cui un insieme ordinato sia anche un campo algebrico o viceversa). Se pensiamo però al nostro insieme modello $\mathbb{Q}$, ci rendiamo immediatamente conto che ci sono proprietà che legano le due strutture, ad esempio la conservazione del verso della diseguaglianza quando moltiplichiamo entrambe i membri per un numero positivo.

Definizione 7. *Un **campo ordinato** è un campo S che sia anche un insieme totalmente ordinato soddisfacente ai due assiomi seguenti:*

(B1) per ogni x, y, z in S, se $x \leq y$, allora $x + z \leq y + z$;
(B2) per ogni x, y, z in S, se $x \leq y$ e se $0 \leq z$, allora $xz \leq yz$.

L'insieme $\mathbb{Q}$ dotato dell'ordinamento naturale e delle usuali operazioni costituisce un esempio di campo ordinato.

Mostriamo come le usuali regole operative con le diseguaglianze seguano dagli assiomi di ordinamento e da (A1) - (A9), (B1), (B2).

- ($x \geq 0 \Leftrightarrow -x \leq 0$): da $x \geq 0$ dalla (B1) segue che $0 = x + (-x) \geq -x$.
- ($x \leq y$ e $z \leq 0 \Rightarrow xz \geq yz$): se $z \leq 0$, allora $-z \geq 0$, pertanto per la (B2), risulta che $x(-z) \leq y(-z)$, cioè (unicità dell'opposto e proprietà distributiva), $-xz \leq -yz$, da cui $xz \geq yz$
- (per ogni x, $x^2 \geq 0$): si dimostra per casi usando le due precedenti. In particolare $1 = 1 \cdot 1 > 0$ (!).
- ($xy \geq 0 \Leftrightarrow x, y$ entrambi ≥ 0 oppure entrambi ≤ 0): se fosse $x \geq 0$ e $y < 0$, allora $xy \leq 0y = 0$);
- ($x > 0 \Rightarrow \dfrac{1}{x} > 0$): dato che $0 < 1 = x(1/x)$, per la precedente $1/x > 0$;
- ($0 < x < y \Rightarrow \dfrac{1}{x} > \dfrac{1}{y}$): da $1/x > 0$, si ha $1 = x(1/x) < y(1/x)$. Ancora moltiplicando per $1/y$, $1/y < (1/y)y(1/x) = 1/x$.

3 Definizione di $\mathbb{R}$

Assioma di Completezza: *Ogni insieme non vuoto, limitato superiormente possiede estremo superiore.*

Definizione 8. $\mathbb{R}$ *è un campo ordinato in cui vale l'assioma di completezza.*

Osservazione 4. *L'assioma di completezza a volte viene enunciato nella seguente forma (o in altri modi ancora, vedi [GiustiNEW])*

`Assioma di Dedekind, o dell'esistenza dell'elemento separatore`
Sia S un insieme totalmente ordinato. Data una sezione di S, ovvero due insiemi non vuoti A e B, tali che $A \cap B = \emptyset$, $A \cup B = S$ e per cui valga $a \leq b$ per ogni $a \in A$, $b \in B$, allora esiste $c \in S$ (elemento separatore) tale che $a \leq c \leq b$ per ogni $a \in A$, $b \in B$.

Esercizio 3. *Posto $S = \mathbb{R}$. Provare che l'elemento separatore di una sezione dei reali è unico.*

Esercizio 4. *Provare che l'assioma di Completezza equivale all'assioma di Dedekind (non facile, vedi [GiustiOLD]) .*

La definizione data di $\mathbb{R}$ è accettabile a condizione che tale campo risulti univocamente determinato dagli assiomi sull'ordinamento, da quelli di campo ordinato (A1)-(A9), (B1)-(B2) e dall'assioma di completezza. In effetti le cose stanno così, nel senso che sebbene costruzioni diverse del modello dei reali conducano a strutture insiemisticamente differenti, tali strutture possono essere formalmente identificate attraverso un *isomorfismo* (una corrispondenza biunivoca che mantiene inalterata la struttura di campo ordinato).

È importante sottolineare che nel sistema $\mathbb{R}$ dei numeri reali si ritrova $\mathbb{Q}$ come sottocampo (restringendo operazioni ed ordinamento ai soli elementi razionali). L'idea è molto semplice: $1 \in \mathbb{R}$, $1 + 1 = 2 \in \mathbb{R}$, $1 + ... + 1 = n \in \mathbb{R}$. A questo punto, $-n \in \mathbb{R}$, così come $1/n \in \mathbb{R}$, e così via. Una discussione completa su come si possano ottenere le proprietà caratterizzanti $\mathbb{N}$ a partire dalla definizione assiomatica di $\mathbb{R}$, si trova in [Giusti OLD cap. 1, sez.6]. Vedremo in seguito qualcosa a proposito del Principio d'induzione.

Dalla proprietà di completezza si ottiene che l'insieme dei numeri naturali non è limitato superiormente. Tradizionalmente l'enunciato assume la forma seguente:

Teorema 1. *(Proprietà archimedea) Comunque presi due numeri reali positivi $a < b$, esiste un numero naturale n_0 per cui $n_0\, a > b$.*

Dimostrazione. Per assurdo, supponiamo che l'insieme $A = \{na : n \in \mathbb{N}\}$ sia limitato superiormente. Per la completezza di $\mathbb{R}$ esiste allora l'estremo superiore β di A. Dato che β è un maggiorante, risulta che $(n+1)a \leq \beta$, per ogni n naturale. Pertanto $na \leq \beta - a$, per ogni n naturale, con la conseguenza che abbiamo trovato un maggiorante $\beta - a$ minore di β, il che è in contraddizione con $\beta = \sup A$. □

Ogni numero reale, in particolare irrazionale (un elemento di $\mathbb{R} \setminus \mathbb{Q}$) può essere approssimato con precisione a piacere da numeri razionali:

Teorema 2. *(Densità dei razionali in $\mathbb{R}$) Presi comunque due numeri reali $a < b$, esiste un numero razionale p per cui $a < p < b$.*

Dimostrazione. Consideriamo il caso $0 < a < b$. Per la proprietà archimedea, esiste $n_0 \in \mathbb{N}$ tale che $n_0(b-a) > 1$, ovvero

$$\frac{1}{n_0} < b - a. \tag{1}$$

Osserviamo che l'insieme

$$B = \left\{ m \in \mathbb{N} : \frac{m}{n_0} < b \right\}$$

è non vuoto ($1 \in B$, dato che $1/n_0 < b - a < b$) ed è finito (per la proprietà archimedea, si ha $m/n_0 > b$ da un certo m in poi). Definiamo

$$m_0 = \max B,$$

ovvero il più grande numero naturale tale che $m_0/n_0 < b$. Dico che $m_0/n_0 > a$.

Per assurdo, se fosse $m_0/n_0 \leq a$, per la diseguaglianza (1), si avrebbe

$$\frac{m_0+1}{n_0} = \frac{m_0}{n_0} + \frac{1}{n_0} \leq a + \frac{1}{n_0} < a + (b-a) = b.$$

Pertanto, $m_0 + 1 \in B$, in contraddizione con $m_0 = \max B$.

La tesi è dunque provata con $p = m_0/n_0$.

Gli altri casi (semplici) sono lasciati come esercizio. □

4 Esistenza dell'estremo inferiore

L'assioma di completezza garantisce l'esistenza dell'estremo superiore per un insieme superiormente limitato in $\mathbb{R}$. Vale anche il seguente teorema

Teorema 3. ***(Esistenza dell'estremo inferiore)*** *Se $A \subset \mathbb{R}$, $A \neq \emptyset$, è un insieme inferiormente limitato, allora esiste $\alpha = \inf A$.*

Dimostrazione. Sia $\mathbf{m}_A$ l'insieme dei minoranti di A, che per ipotesi è non vuoto. Dato che ogni elemento di A è un maggiorante di $\mathbf{m}_A$, quest'ultimo è superiomente limitato. Sia allora $\alpha = \sup \mathbf{m}_A$. Vogliamo provare che α è l'estremo inferiore di A, ovvero $\alpha = \max \mathbf{m}_A$.

- se $x < \alpha$, allora $x \notin A$ (gli elementi di A sono maggioranti di $\mathbf{m}_A$)
- Allora α è un minorante di A, cioè $\alpha \in \mathbf{m}_A$.
- Conclusione: $\alpha = \max \mathbf{m}_A$ e quindi, per definizione, $\alpha = \inf A$.

□

5 Principio d'induzione

È interessante vedere come l'idea intuitiva, a cui avevamo accennato in precedenza, di costruire l'insieme dei numeri naturali $\mathbb{N}$ a partire da somme ripetute dell'unità moltiplicativa dei reali (il numero 1) si possa rendere rigorosa.

Definizione 9. *Diciamo che un insieme $S \subset \mathbb{R}$ è induttivo, se soddisfa le seguenti proprietà:*
$1 \in S$
$\forall x \in \mathbb{R}$, $x \in S$ *implica* $x + 1 \in S$

Ad esempio $\mathbb{Q}$ è induttivo. Caratterizziamo $\mathbb{N}$ come il più piccolo insieme induttivo contenuto in $\mathbb{R}$ dando la seguente definizione:

Definizione 10.

$$\mathbb{N} = \{x \in \mathbb{R} : x \in S, \forall S \textit{ induttivo}\}$$

Teorema 4. $\mathbb{N}$ *è induttivo*

Dimostrazione. $1 \in S$, per ogni S induttivo, quindi $1 \in \mathbb{N}$. Se $x \in \mathbb{N}$, allora $x \in S$, per ogni S induttivo. Dalla definizione di insieme induttivo, allora $x + 1 \in S$, per ogni S induttivo. Dalla definizione di $\mathbb{N}$, abbiamo che $x + 1 \in \mathbb{N}$. Quindi $\mathbb{N}$ è induttivo. □

Teorema 5 (**Principio d'induzione**). *Sia $A \subset \mathbb{N}$. Se valgono*
1) $1 \in A$,
2) $n \in A \Rightarrow n + 1 \in A$, $\forall n \in \mathbb{N}$.
Allora $A = \mathbb{N}$.

Dimostrazione. Le condizioni 1) e 2) dicono che A è induttivo. Pertanto, dalla definizione di $\mathbb{N}$, $\mathbb{N} \subset A$. Dato che $A \subset \mathbb{N}$, si ha $A = \mathbb{N}$. □

Se $P(n)$ è una successione di predicati, dipendenti da $n \in \mathbb{N}$ (ad esempio, $P(n)$ potrebbe stare per : $n^3 - n$ è multiplo di 3), per dimostrare che $P(n)$ è vero per ogni $n \in \mathbb{N}$, il principio d'induzione assume il seguente aspetto:

Principio d'induzione (forma dimostrativa)
1) $P(1)$ è vero; *(caso base)*
2) $P(n) \Rightarrow P(n + 1)$, $\forall n \in \mathbb{N}$ *(passo induttivo).*
Allora $P(n)$ è vero per ogni $n \in \mathbb{N}$.

Dimostrazione. Si pone $A = \{n \in \mathbb{N} : P(n) \text{ è vero}\}$ □

È possibile dare una formulazione alternativa del Principio d'induzione (solo apparentemente più forte), nel modo seguente:

Sia $A \subset \mathbb{N}$. Se valgono
1) $1 \in A$,
2') $\{1, ..., n\} \subset A \Rightarrow n + 1 \in A$, $\forall n \in \mathbb{N}$.
Allora $A = \mathbb{N}$.

Si noti come la 2) del principio d'induzione implichi la 2') della formulazione appena data.

Infine, entrambe le formulazioni risultano equivalenti al **Principio del buon ordinamento**:

Ogni sottoinsieme di $\mathbb{N}$ *non vuoto possiede minimo*

Il principio d'induzione figura tra gli assiomi formulati da Giuseppe Peano (1858-1932) a fondamento dell'aritmetica dei numeri naturali (quinto assioma). Noi lo abbiamo ricavato come teorema derivante dagli assiomi su $\mathbb{R}$. Se avessimo seguito il procedimento inverso, avremmo adottato i cinque assiomi di Peano per definire $\mathbb{N}$ e quindi 'costruito' i vari sistemi numerici, $\mathbb{Z}$, $\mathbb{Q}$, ed infine $\mathbb{R}$ (ad esempio tramite il metodo delle sezioni di Dedekind di $\mathbb{Q}$, vedi [GiustiOLD]).

Alcuni predicati che si dimostrano veri $\forall n \in \mathbb{N}$, mediante il principio d'induzione.

(a) Per ogni $n \in \mathbb{N}$, $\displaystyle\sum_{k=1}^{n} k = 1 + 2 + ... + n = \frac{n(n+1)}{2}$

(b) Per ogni $n \in \mathbb{N}$, per ogni $a \neq 1$, $\displaystyle\sum_{k=1}^{n} a^k = \frac{1 - a^{n+1}}{1 - a}$

(c) Per ogni $a \geq -1$, per ogni $n \in \mathbb{N}$, risulta $(1 + a)^n \geq 1 + na$

(d) Per ogni $n \in \mathbb{N}$, $n^3 - n$ è multiplo di n (se si considera 0 multiplo di 3...)

Osservazione Importante. Il Principio di Induzione (che a volte viene detto "Induzione Completa" per distinguerlo dal processo induttivo) **NON** si utilizza per congetturare formule, come ad esempio,

$$\sum_{k=1}^{n} k = 1 + 2 + ... + n = \frac{n(n+1)}{2}.$$

Infatti, per congetturarla, si osserva che

$$\begin{cases} S_n = 1 + 2 + 3 + \ldots + (n-1) + n \\ S_n = n + (n-1) + (n-2) + \ldots + 2 + 1 \end{cases},$$

da cui segue

$$2S_n = (n+1) + (n+1) + (n+1) + \ldots + (n+1) + (n+1) = n(n+1)$$

e infine $S_n = \frac{n(n+1)}{2}$.
Il principio di Induzione si utilizza per **dimostrare** che l'identità è vera per ogni $n \in \mathbb{N}$:

- l'identità è vera per $n = 1$: $S_1 = 1 = \frac{1(1+1)}{2}$;
- l'identità sia vera per n (ipotesi induttiva): $S_n = 1 = \frac{n(n+1)}{2}$;
- provo che l'identità è vera per $n + 1$. Utilizzando l'ipotesi induttiva

$$S_{n+1} = 1 + 2 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

  ovvero quanto volevo dimostrare.

Esercizio 5. *Dimostrare che* $3^{998} - 2^{499}$ *è divisibile per* 7.

Dimostrazione. Non conviene fare il calcolo diretto (3^{998} è un numero di 470 cifre). Conviene invece considerare $f(n) = 3^{2n} - 2^n$, osservando che $f(1) = 7$, $f(2) = 77$, $f(3) = 721$: sembra che $f(n)$ sia divisibile per 7 per ogni $n \in \mathbb{N}$ (congettura). Per dimostrarlo procediamo per induzione.

- $n = 1$: $f(1) = 7$ è divisibile per 7;
- $f(n) = 3^{2n} - 2^n$ supponiamo (ipotesi induttiva) sia divisibile per 7;
- Vogliamo provare che $f(n+1)$ è divisibile per 7.

  $$f(n+1) = 3^{2n+2} - 2^{n+1} = 3^2 3^{2n} - 22^n + 3^2 2^n - 3^2 2^n$$

  e dunque

  $$f(n+1) = 3^2(3^{2n} - 2^n) + 2^n(3^2 - 2) \Longrightarrow f(n+1) = 3^2 \cdot f(n) + 7 \cdot 2^n$$

  ed essendo $f(n)$ divisibile per 7 (ipotesi induttiva), si ha che anche $f(n+1)$ è divisibile per 7, che quanto si voleva dimostrare.

Abbiamo risolto l'esercizio in quanto $n = 499$ è un caso particolare del risultato generale che abbiamo dimostrato. □

Esercizio 6. *Dimostrare che* $n^3 - n$ *è divisibile per* 3 *per ogni* $n \in \mathbb{N}$.

Dimostrazione. Possiamo procedere per induzione, e lasciamo allo studente questa dimostrazione per esercizio.

Una dimostrazione alternativa si ottiene osservando che

$$n^3 - n = n(n^2 - 1) = (n-1) \cdot n \cdot (n+1).$$

I numeri interi divisibili per 3 sono della forma $3k$, $k = 1, 2, 3, \ldots$, e dunque nel prodotto $(n-1) \cdot n \cdot (n+1)$ cade almeno un numero divisibile per 3: ne segue la tesi. □

Esercizio 7. *Calcolare* $\left(1 - \frac{1}{4}\right) \cdot \left(1 - \frac{1}{9}\right) \cdots \left(1 - \frac{1}{10.000}\right)$.

Dimostrazione. Come nell'esercizio sulla divisibilità per 7, conviene considerare

$$f(n) = \left(1 - \frac{1}{2^2}\right) \cdot \left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{n^2}\right)$$

e osservare che

$$f(2) = \frac{3}{4}, \qquad f(4) = f(3) \cdot \frac{15}{16} = \frac{5}{8}, \quad f(6) = f(5) \cdot \frac{35}{36} = \frac{7}{12}, \ldots$$
$$f(3) = f(2) \cdot \frac{8}{9} = \frac{2}{3}, \quad f(5) = f(4) \cdot \frac{24}{25} = \frac{3}{5}, \quad f(7) = f(6) \cdot \frac{48}{49} = \frac{4}{7}, \ldots$$

da cui si ottiene

$$f(2) = \frac{3}{4}, \qquad f(4) = \frac{5}{8}, \qquad f(6) = \frac{7}{12}, \ldots$$
$$f(3) = \frac{2}{3} = \frac{4}{6}, \quad f(5) = \frac{3}{5} = \frac{6}{10}, \quad f(7) = \frac{4}{7} = \frac{8}{14}, \ldots$$

e dunque si può congetturare che $f(n) = \frac{n+1}{2n}$.

Adesso bisogna provare per induzione che ogni $n > 1$

$$f(n) = \left(1 - \frac{1}{2^2}\right) \cdot \left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

- $n = 2$: $f(2) = \frac{3}{4}$, dunque è vera;
- Supponiamo (ipotesi induttiva) che $f(n) = \frac{n+1}{2n}$ sia vera;
- Vogliamo provare che $f(n+1) = \frac{n+2}{2(n+1)}$. A tal fine si osserva che, utilizzando l'ipotesi induttiva

$$f(n+1) = f(n) \cdot \frac{(n+1)^2 - 1}{(n+1)^2} \Longrightarrow f(n+1) = \frac{n+1}{2n} \cdot \frac{n(n+2)}{(n+1)^2},$$

  e semplificando si ottiene $f(n+1) = \frac{n+2}{2(n+1)}$.

Nel caso particolare $n = 100$ si ottiene $f(100) = 101/200$. □

6 Valore assoluto

In $\mathbb{R}$ si definisce la funzione **valore assoluto** $|\cdot| : \mathbb{R} \to \mathbb{R}$ nel modo seguente:

$$|x| = \max\{x, -x\}, \quad \text{per ogni } x \in \mathbb{R}.$$

Questa funzione è molto importante per il corso di Analisi Matematica 1 in quanto permette di definire la distanza (euclidea) tra due punti della retta reale, ovvero $x, y \in \mathbb{R}$, ponendo $d(x, y) = |x - y|$. Come vedremo, risulta essenziale per definire il concetto fondamentale di *intorno* di un punto. Molti studenti avranno visto la funzione valore assoluto o modulo, definita come segue

$$|x| = \begin{cases} x, & \text{se } x > 0 \\ 0, & \text{se } x = 0 \\ -x, & \text{se } x < 0, \end{cases}$$

e come vedremo nel seguente teorema questa definizione è equivalente a quella data in questa sezione.

Teorema 6. *La funzione modulo soddisfa le seguenti proprieà*

1) $|x| = \begin{cases} x, & \text{se } x > 0 \\ 0, & \text{se } x = 0 \\ -x, & \text{se } x < 0 \end{cases}$

2) $|x| \geq 0$ *per ogni* $x \in \mathbb{R}$*;*

3) $|x| = 0$ *se, e soltanto se,* $x = 0$*;*

4) $|x| = |-x|$ *per ogni* $x \in \mathbb{R}$*;*

5) $-|x| \leq x \leq |x|$ *per ogni* $x \in \mathbb{R}$*;*

7) $|x| < y$ *se, e soltanto se,* $-y < x < y$*, per ogni* $x, y \in \mathbb{R}$*;*

8) $|x| > y$ *se, e soltanto se,* $x > y$ ***o*** $-x > y$*, per ogni* $x, y \in \mathbb{R}$*;*

9) $|x + y| \leq |x| + |y|$*, per ogni* $x, y \in \mathbb{R}$*;*

10) $||x| - |y|| \leq |x - y|$*, per ogni* $x, y \in \mathbb{R}$*.*

Dimostrazione.

1) Se $x > 0$, $\max\{-x, x\} = x$; se $x < 0$, $\max\{-x, x\} = -x$; se $x = 0$, $\max\{-x, x\} = 0$.

2) Segue dall'esame dei tre casi $x > 0$, $x = 0$, $x < 0$.

3) Se $x = 0$ allora segue $|x| = 0$. Per provare il viceversa proviamo la contronominale, ovvero $x \neq 0$ implica $|x| > 0$: se $x > 0$, allora $|x| = x > 0$ mentre se $x < 0$, allora $|x| = -x > 0$ e quindi la tesi è provata.

4) $|x| = \max\{x, -x\} = \max\{-x, x\} = \max\{-x, -(-x)\} = |-x|$.

5) Per ogni $x \in \mathbb{R}$, $|x| = \max\{-x, x\}$, da cui $\begin{cases} |x| \geq x \\ |x| \geq -x \end{cases}$, e dunque $-|x| \leq x \leq |x|$.

7) Per ogni $x, y \in \mathbb{R}$,

$$|x| = \max\{x, -x\} < y \iff \begin{cases} x < y \\ -x < y \end{cases} \iff \begin{cases} x < y \\ -y < x \end{cases} \iff -y < x < y.$$

8) Per ogni $x, y \in \mathbb{R}$

$$|x| = \max\{x, -x\} > y \iff [x > y \textbf{ o } -x > y].$$

9) Per ogni $x, y \in \mathbb{R}$ si ha

$$\begin{cases} -|x| \leq x \leq |x| \\ -|y| \leq y \leq |y| \end{cases} \implies -|x| - |y| \leq x + y \leq |x| + |y|,$$

e dalla 7) si ottiene $|x + y| \leq |x| + |y|$.

10) Per ogni $x, y \in \mathbb{R}$ si ha

$$\begin{cases} |x| = |(x-y) + y| \leq |x-y| + |y| \\ |y| = |(y-x) + x| \leq |x-y| + |x| \end{cases} \implies \begin{cases} |x| - |y| < |x-y| \\ |y| - |x| < |x-y| \end{cases} \implies \begin{cases} |x| - |y| < |x-y| \\ -|x-y| < |x| - |y|. \end{cases}$$

Per la 7), si deduce $||x| - |y|| \leq |x - y|$. $\square$

Esercizio 8. *Risolvere le seguenti equazioni (per via analitica e grafica)*

1) $|x - 3| = |2x - 3| - 2$.

2) $1 + |x - 1| = |x + 2|$.

Esercizio 9. *Risolvere le seguenti disequazioni (ove possibile anche per via grafica)*

1) $|x + 1| \leq |x - 2|$.

2) $3 \leq x + |x - 1|$.

3) $|2x - |x^2 - 3|| < 1$.

7 Esistenza della radice e sviluppi decimali

Per apprezzare la portata dell'assioma di completezza, la discussione sul sistema dei numeri reali si conclude con la dimostrazione dell'esistenza di $\sqrt{a}$, per ogni $a \geq 0$, e con la costruzione dello sviluppo decimale, eventualmente illimitato, di ogni numero reale.

Teorema 7. ***(Esistenza della radice)*** *Per ogni numero reale positivo a, esiste un unico numero reale positivo tale che $y^2 = a$*

Premettiamo due lemmi.

Lemma 7.1. *Sia $x \in \mathbb{R}$. Se $|x| < \varepsilon$, per ogni $\varepsilon > 0$, allora $x = 0$.*

Dimostrazione. Per assurdo, se $x \neq 0$, allora $|x| > 0$. L'ipotesi ci consente di considerare $\varepsilon = |x|/2$, ed ottenere $0 < |x| < |x|/2$, il che è assurdo. □

Esercizio 10. *Sia $x \in \mathbb{R}$. Se $|x| < \dfrac{1}{n}$, per ogni $n \in \mathbb{N}$, allora $x = 0$. (Procedere per assurdo, utilizzare la proprietà archimedea)*

Lemma 7.2. *Siano $a, b \in \mathbb{R}$, con $a < b$. Se $a < c < b$, e $a < c' < b$, allora $|c - c'| < b - a$.*

Dimostrazione. Esercizio. □

Dimostrazione del Teorema. L'unicità della radice segue dalla diseguaglianza $y_1^2 < y_2^2$ se $0 < y_1 < y_2$. Per la dimostrazione dell'esistenza consideriamo per ora solo il caso $a \geq 1$.

Consideriamo l'insieme,

$$A = \{x > 0 : x^2 \leq a\}.$$

Tale insieme è non vuoto in quanto $1 \in A$ ed è limitato superiormente in quanto a è un maggiorante di A dato che $x > a$, implica $x^2 > a^2 \geq a$ (ricordare che $a \geq 1$!). Grazie all'assioma di completezza, esiste pertanto

$$y = \sup A.$$

Dico che $y^2 = a$. Infatti, sia ε una qualsiasi numero reale tale $0 < \varepsilon < y$. Abbiamo

$$0 < y - \varepsilon < y < y + \varepsilon \implies (y - \varepsilon)^2 < y^2 < (y + \varepsilon)^2. \tag{2}$$

D'altra parte, per la caratterizzazione del $\sup A$, esiste almeno $x \in A$, tale che

$$y - \varepsilon < x \implies (y - \varepsilon)^2 < x^2 \leq a.$$

Inoltre deve essere $a < (y + \varepsilon)^2$, in caso contrario avremmo $y + \varepsilon \in A$, portando ad una contraddizione con y maggiorante di A. In definitiva, vale

$$(y - \varepsilon)^2 < a < (y + \varepsilon)^2. \tag{3}$$

Dalle diseguaglianze (2) e (3), grazie al Lemma 7.2, otteniamo

$$|y^2 - a| < (y + \varepsilon)^2 - (y - \varepsilon)^2 = 4\varepsilon y.$$

Possiamo applicare il Lemma 7.1, e concludere che $y^2 - a = 0$, grazie all'arbitrarietà di $\varepsilon > 0$ (si noti che la presenza del fattore moltiplicativo $4y$ sia ininfluente, in quanto y dipende solo dal numero a fissato; altrettanto ininfluente risulta la limitazione $\varepsilon < y$). Il caso $0 < a < 1$, si riconduce al precedente considerando la soluzione dell'equazione $z^2 = 1/a$ e ponendo $y = 1/z$ □

Per definire lo sviluppo decimale di un numero reale, procederemo per induzione considerando per semplicità solo il caso $x > 0$. Cominciamo con il definire (mettiamo $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$)

$$n_0 = \max\{n \in \mathbb{N}_0 : \, n \leq x\}.$$

Il passo successivo definisce la prima cifra decimale (eventualmente nulla) di x:

$$n_1 = \max\{n \in \mathbb{N}_0 : \, n_0 + n_1/10 \leq x\}.$$

È chiaro che $n_1 \in \{0, 1, ..., 9\}$, così come

$$n_0 + \frac{n_1}{10} \leq x < n_0 + \frac{n_1}{10} + \frac{1}{10}.$$

A questo punto, date le prime k cifre decimali di x, ovvero il numero decimale $n_0, n_1 ... n_k$, tale che

$$n_0 + \frac{n_1}{10} + ... + \frac{n_1}{10^k} = n_0, n_1 ... n_k \leq x < n_0, n_1 ... n_k + \frac{1}{10^k},$$

definiamo (passo induttivo), la $(k+1)$-esima:

$$n_{k+1} = \max\{n \in \mathbb{N}_0 : \, n_0, n_1 ... n_k \, + \, n_{k+1}/10^{k+1} \leq x\}.$$

Grazie al principio d'induzione, risulta definita l'intera successione delle cifre decimali n_k, $k \in \mathbb{N}_0$. Dimostriamo che

$$x = \sup\{n_0, n_1 ... n_k \, : k \in \mathbb{N}_0\},$$

il che consente di identificare ogni numero reale positivo con un ben determinato allineamento decimale. Poniamo per brevità $\alpha_k = n_0, n_1 ... n_k$. Per come abbiamo costruito la successione degli α_k, si ha

$$\alpha_k \leq x < \alpha_k + \frac{1}{10^k}, \quad \forall k \in \mathbb{N}_0.$$

Pertanto x è un maggiorante. Sia ora $y < x$ e sia $k_0 \in \mathbb{N}_0$ tale che $10^{-k_0} < x - y$ (l'esistenza di un tale k_0 è sicuramente data per vera intuitivamente ma potrebbe essere dimostrata rigorosamente grazie alla diseguaglianza $10^k \geq 1 + 9k$, vedi sez. sull'induzione). Abbiamo pertanto,

$$\alpha_{k_0} - y = -(x - \alpha_{k_0}) + (x - y) > -\frac{1}{10^{k_0}} + x - y > 0,$$

quindi $\alpha_{k_0} > y$. Per la caratterizzazione dell'estremo superiore, abbiamo dimostrato quanto affermato.

Osservazione 5. *Quando avremo a disposizione qualche risultato sui limiti delle successioni, quanto dimostrato sugli sviluppi decimali apparirà come un semplice esercizio.*