2 Insiemi numerici

Relazioni di equivalenza e ordine

Una *relazione* su un insieme X è un sottinsieme $\mathcal{R}$ del prodotto cartesiano $X \times X$, e scriviamo $x\mathcal{R}y$ se $(x, y) \in \mathcal{R}$. Ricordiamo le seguenti proprietà:

1. riflessiva: $\forall\, x \in X,\ x\mathcal{R}x\,;$
2. simmetrica: $\forall\, x, y \in X,\ x\mathcal{R}y \Longrightarrow y\mathcal{R}x\,;$
3. antisimmetrica: $\forall\, x, y \in X,\ x\mathcal{R}y$ **e** $y\mathcal{R}x \Longrightarrow x = y\,;$
4. transitiva: $\forall\, x, y, z \in X,\ x\mathcal{R}y$ **e** $y\mathcal{R}z \Longrightarrow x\mathcal{R}z\,.$

Relazioni di equivalenza

Definizione 2.1 Una relazione è di *equivalenza* se gode delle proprietà riflessiva, simmetrica e transitiva. Una relazione di equivalenza si denota con il simbolo "$\simeq$". Data una relazione di equivalenza poniamo per ogni $x \in X$

$$[x] := \{y \in X \mid x \simeq y\}\,,$$

l'insieme $[x]$ è detto *classe di equivalenza* di x.

Proposizione 2.2 *Data una relazione di equivalenza su X, allora per ogni $x, y \in X$ tali che $[x] \cap [y] \neq \emptyset$ risulta $[x] = [y]$.*

Quindi le classi di equivalenza determinano una partizione di X. Possiamo dunque definire l'*insieme quoziente*

$$X/\simeq\ :=\ \{[x]\ :\ x \in X\}\,.$$

Esempio 2.3 Consideriamo l'insieme delle frazioni $X = \{m/n \mid m, n \in \mathbb{Z},\ n \neq 0\}$. Si prova facilmente che la relazione su X definita da $m/n \simeq m'/n' \iff mn' = m'n$ è di equivalenza. Per ogni $m/n \in X$ la classe di equivalenza $[m/n]$ è data da tutte le frazioni equivalenti a m/n. Quindi, l'insieme quoziente definisce l'insieme $\mathbb{Q}$ dei numeri razionali.

Relazioni di ordine

Definizione 2.4 Una relazione è di *ordine* se gode delle proprietà riflessiva, antisimmetrica e transitiva.

Una relazione d'ordine si denota con il simbolo "$\leq$".

Definizione 2.5 Una relazione d'ordine si dice *totale* se due elementi sono sempre confrontabili, i.e. se risulta: $\forall\, x, y \in X,\quad x \leq y$ **o** $y \leq x\,.$

Esempio 2.6 Se $X = \mathcal{P}(U)$, dove U è un insieme non vuoto, la relazione di inclusione "$\subset$" è di ordine, ma in generale non è totale. L'inclusione stretta $\subsetneq$ invece non è una relazione d'ordine.

Esempio 2.7 Se $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, la relazione usuale "$\leq$" è di ordine totale.

Sia $\leq$ una relazione d'ordine totale su X. Come modello teniamo in mente l'ultimo esempio fatto.

Definizione 2.8 Se $A \subset X$, si dice che un elemento $M \in X$ [[$m \in X$]] è un *maggiorante [[minorante]]* di A se

$$\forall\, a \in A,\ a \leq M \quad [[a \geq m]]\ .$$

Indicheremo poi l'insieme dei maggioranti [[minoranti]] di A con $\mathcal{M}_A$ [[m_A]].

Definizione 2.9 Si dice che un insieme $A \subset X$ è *limitato superiormente [[inferiormente]]* se ha dei maggioranti [[minoranti]], i.e. se $\mathcal{M}_A \neq \emptyset$ [[$m_A \neq \emptyset$]]. Inoltre A si dice *limitato* se è limitato sia superiormente che inferiormente, i.e. se

$$\exists\, m, M \in X\ :\ \forall\, a \in A,\ m \leq a \leq M\ .$$

Se $X = \mathbb{R}$, posto $\widetilde{M} := \max\{|m|, |M|\}$, segue facilmente che $A \subset \mathbb{R}$ è limitato se e solo se

$$\exists\, \widetilde{M} \in \mathbb{R}\ :\ \forall\, a \in A,\ |a| \leq \widetilde{M}\ .$$

Definizione 2.10 Se $A \subset X$, si dice che un numero $M \in X$ [[$m \in X$]] è *il massimo [[il minimo]]* di A se appartiene ad A ed è un maggiorante [[minorante]] di A. In tal caso si scrive $M = \max A$ [[$m = \min A$]]. Quindi

$$M = \max A \iff \begin{cases} M \in A \\ \forall\, a \in A,\ a \leq M \end{cases} \qquad m = \min A \iff \begin{cases} m \in A \\ \forall\, a \in A,\ a \geq m\ . \end{cases}$$

Osservazione 2.11 Il massimo [[minimo]] può non esistere, anche se A è limitato superiormente [[inferiormente]]. Si consideri ad esempio $A = [0, 1[$, per cui risulta $\mathcal{M}_A = [1, +\infty)$ e quindi $A \cap \mathcal{M}_A = \emptyset$.

Se però esiste, allora il massimo [[minimo]] di A è *unico.* Infatti, se $M_1 = \max A$ e $M_2 = \max A$, risulta $M_1 \leq M_2$ **e** $M_2 \leq M_1$, per cui $M_1 = M_2$.

Valgono infine le seguenti proprietà:

1) se $A_1 \subset A_2$ allora $\mathcal{M}_{A_2} \subset \mathcal{M}_{A_1}$ [[$m_{A_2} \subset m_{A_1}$]]

2) se $A_1 \subset A_2$ allora $\max A_1 \leq \max A_2$ [[$\min A_1 \geq \min A_2$]] qualora i massimi [[minimi]] esistano

3) se A e B hanno massimo [[minimo]], allora anche l'unione $A \cup B$ ha massimo [[minimo]] e risulta

$$\max(A \cup B) = \max\{\max A, \max B\} \qquad [[\min(A \cup B) = \min\{\min A, \min B\}]]\ .$$

I numeri reali

Assiomi algebrici

L'insieme $\mathbb{Q}$ dei numeri razionali gode delle seguenti propretà algebriche:

1. l'addizione, $+$, è associativa
2. l'addizione è commutativa
3. l'addizione ha elemento neutro, 0
4. ogni numero ha inverso rispetto alla addizione (detto l'opposto)
5. la moltiplicazione, $\cdot$, è associativa
6. la moltiplicazione è commutativa
7. la moltiplicazione ha elemento neutro, 1
8. ogni numero diverso da zero ha inverso rispetto alla moltiplicazione (detto il reciproco)
9. la moltiplicazione è distributiva rispetto all'addizione
10. se $a \leq b$, allora per ogni c si ha $a + c \leq b + c$
11. se $a \leq b$, allora per ogni $c \geq 0$ si ha $a \cdot c \leq b \cdot c$.

L'insieme $\mathbb{R}$ dei numeri reali è definito in modo assiomatico come un insieme $X = \mathbb{R}$ munito di due leggi di composizione interna, addizione e moltiplicazione, e di una relazione d'ordine totale tali che valgano le proprietà algebriche 1.–11. sopra elencate ed in più la seguente *proprietà di separazione.*

Assioma di Dedekind

Definizione 2.12 Se A, B sono due sottoinsiemi non vuoti di $\mathbb{R}$ tali che

$$\forall\, a \in A,\ \forall\, b \in B,\ a \leq b \tag{2.1}$$

allora

$$\exists\, c \in \mathbb{R} :\ \forall\, a \in A,\ \forall\, b \in B,\ a \leq c \leq b\ .$$

Un tale c si dice elemento separatore di A e B.

Retta reale estesa e intervalli

Definiamo la *retta reale estesa* come $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$. Ricordando che $x < y \iff x \leq y$ **e** $x \neq y$, l'insieme $\overline{\mathbb{R}}$ diventa totalmente ordinato se si pone

$$-\infty < x < +\infty \qquad \forall\, x \in \mathbb{R}\,.$$

Estendiamo inoltre le operazioni di addizione e moltiplicazione ponendo

$$\forall\, x < (+\infty),\ x + (-\infty) = -\infty\ , \qquad \forall\, x > (-\infty),\ x + (+\infty) = +\infty\ ,$$

$$\forall\, x > 0,\ x \cdot (+\infty) = +\infty\ , \qquad \forall\, x > 0,\ x \cdot (-\infty) = -\infty\ ,$$

$$\forall\, x < 0,\ x \cdot (+\infty) = -\infty\ , \qquad \forall\, x < 0,\ x \cdot (-\infty) = +\infty\ .$$

Osservazione 2.13 Non sono definite (e quindi non hanno senso) le operazioni

$$(+\infty) + (-\infty) \qquad \text{e} \qquad 0 \cdot (\pm\infty)\ .$$

Definizione 2.14 Un sottoinsieme I di $\overline{\mathbb{R}}$ si dice un *intervallo* se

$$\forall\, x, y \in I \text{ con } x < y\ \Rightarrow\ \{z \in \mathbb{R} : x < z < y\} \subset I\ .$$

Si verifica facilmente che gli intervalli di $\overline{\mathbb{R}}$ sono tutti del tipo

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\} \qquad]a, b] = \{x \in \mathbb{R} : a < x \leq b\}$$

$$[a, b[= \{x \in \mathbb{R} : a \leq x < b\} \qquad]a, b[= \{x \in \mathbb{R} : a < x < b\}$$

dove $a, b \in \overline{\mathbb{R}}$, con $a \leq b$. Parlando poi di intervalli $I \subset \mathbb{R}$ di numeri reali, le scritture $[-\infty, b]$, $[a, +\infty]$ non hanno senso, come tutte quelle che comprendono $-\infty$ o $+\infty$ nell'insieme I.

I numeri razionali

L'insieme $\mathbb{Q}$ dei numeri razionali è definito mediante classi di equivalenza di frazioni, cf. l'esempio 2.3.

Tutti i numeri razionali sono reali, ma l'insieme dei numeri reali contiene strettamente l'insieme dei razionali, $\mathbb{Q} \subsetneq \mathbb{R}$. Mostriamo intanto che:

Proposizione 2.15 $\sqrt{2} \notin \mathbb{Q}$.

Dimostrazione: Se per assurdo $\sqrt{2} \in \mathbb{Q}$, possiamo scrivere $\sqrt{2} = m/n$, con $m, n \in \mathbb{N}^+$ e primi tra loro. Si avrebbe $m^2/n^2 = (m/n)^2 = 2$, quindi $m^2 = 2n^2$, dunque m è pari, essendolo il suo quadrato. Scritto $m = 2s$, con $s \in \mathbb{N}^+$, abbiamo $4s^2 = m^2 = 2n^2$, da cui $n^2 = 2s^2$ ed anche n dovrebbe essere pari, essendolo il suo quadrato. Questo non è possibile, perchè m ed n sono primi tra loro. $\square$

Dall'assioma di Dedekind, risulta poi che $\sqrt{2} \in \mathbb{R}$:

Esempio 2.16 Poniamo $A := \{x \in \mathbb{Q} \mid x < 0 \ \textbf{o}\ x^2 \leq 2\}$ e $B = \mathbb{Q} \setminus A$. Gli insiemi A e B sono entrambi non vuoti e verificano (2.1). Un elemento separatore di A e B esiste ed è $c = \sqrt{2}$. Dato che tale elemento separatore è unico, cf. la (2.2), concludiamo che $\sqrt{2} \in \mathbb{R}$.

La proprietà di Dedekind non vale sui razionali

L'insieme $\mathbb{Q}$ dei razionali non verifica la proprietà di Dedekind. Infatti, esistono sottinsiemi $A, B \subset \mathbb{Q}$ che verificano (2.1) ma che non hanno elemento separatore in $\mathbb{Q}$, i.e. per i quali

$$\nexists\, c \in \mathbb{Q}:\ \forall\, a \in A,\ \forall\, b \in B,\ a \leq c \leq b\ . \tag{2.2}$$

Presi infatti A e B come nell'esempio 2.16, se esistesse un elemento separatore c in $\mathbb{Q}$, allora $c \in A$ **o** $c \in B$. In entrambi i casi otteniamo un assurdo.

Supposto $c \in A$, si ha $c > 0$ e $c^2 < 2$, in quanto $\sqrt{2} \notin \mathbb{Q}$. Si dimostra che

$$\exists\, n \in \mathbb{N}^+\ :\ (c + 1/n)^2 < 2\,.$$

Questo dà l'assurdo, in quanto $a := c + 1/n \in \mathbb{Q}$ e $a^2 \leq 2$, quindi $a \in A$, ma $a > c$, per cui c non sarebbe elemento separatore di A e B. Quindi $c \notin A$.

Analogamente, supposto $c \in B$ si ottiene un assurdo mostrando che:

$$\exists\, n \in \mathbb{N}^+\ :\ (c - 1/n)^2 > 2\,.$$

Osservazione 2.17 La non esistenza di un elemento separatore razionale si verifica in maniera analoga in prossimità di tutti i punti della retta reale. Questo corrisponde al fatto che l'insieme dei razionali è "bucherellato" e che i buchi vengono riempiti dai numeri reali, grazie all'assioma di Dedekind.

Densità dei razionali

Si dimostra che l'insieme dei numeri reali che hanno rappresentazione decimale periodica coincide con $\mathbb{Q}$.

Osservazione 2.18 Si noti però che, ad esempio, $0,\overline{9} = 1$.

Anche se l'insieme $\mathbb{Q}$ è "bucherellato", vicino ad ogni reale si trova sempre un razionale. Grazie al principio del minimo intero, cf. la proposizione 2.54, si dimostra infatti la seguente

Proposizione 2.19 *Ogni intervallo aperto non vuoto di* $\mathbb{R}$ *contiene almeno un numero razionale.*

Dalla definizione 2.14 di intervallo, segue che la densità dei razionali è equivalente alla proprietà

$$\forall\, \alpha, \beta \in \mathbb{R} \,:\, \alpha < \beta\,, \quad \exists\, q \in \mathbb{Q} \,:\, \alpha < q < \beta$$

la quale permette di approssimare i numeri irrazionali con razionali (ad es., $\sqrt{2} \simeq 1.4142$).

Estremo superiore

Sia X un insieme dotato di un ordinamento totale. La nozione di estremo superiore generalizza il concetto di massimo di un insieme.

Definizione 2.20 Se $A \subset X$ è un insieme non vuoto e limitato superiormente [[inferiormente]], si dice che un numero L [[l]] in X è *estremo superiore [[inferiore]]* di A se è il più piccolo dei maggioranti [[il più grande dei minoranti]] di A. In tal caso si scrive $L = \sup A$ [[$l = \inf A$]].

Essendo $\sup A = \min \mathcal{M}_A$ e $\inf A = \max m_A$, l'estremo superiore [[inferiore]] se esiste è unico. Inoltre:

Proposizione 2.21 *Se* A *ha massimo [[minimo]], allora questo è anche l'estremo superiore [[inferiore]].*

Teorema di esistenza dell'estremo superiore

L'assioma di Dedekind implica l'esistenza dell'estremo superiore in $\mathbb{R}$.

Teorema 2.22 *Ogni insieme* $A \subset \mathbb{R}$ *non vuoto e limitato superiormente ha estremo superiore.*

Dimostrazione: Posto $B = \mathcal{M}_A$, gli insiemi A e B sono entrambi non vuoti, in quanto A è limitato superiormente. Inoltre vale (2.1), dal momento che

$$\forall\, a \in A, \quad \forall\, M \in \mathcal{M}_A, \quad a \leq M\,.$$

Sia $L \in \mathbb{R}$ un elemento separatore di A e B. Abbiamo

$$\forall\, a \in A, \quad \forall\, M \in \mathcal{M}_A, \quad a \leq L \leq M\,.$$

La prima disequaglianza ci dice che L è un maggiorante di A mentre la seconda che L è il più piccolo tra i maggioranti di A, dunque $L = \sup A$. In particolare, l'elemento separatore di A e $\mathcal{M}_A$ è unico. $\square$

Se $A \subset \mathbb{R}$ non è vuoto, la scrittura $\sup A = +\infty$ [[$\inf A = -\infty$]] significa che A non è limitato superiormente [[inferiormente]]. Quindi:

$$\sup A = +\infty \iff \forall\, M \in \mathbb{R}, \exists\, a \in A \,:\, a > M\,, \quad \inf A = -\infty \iff \forall\, m \in \mathbb{R}, \exists\, a \in A \,:\, a < m\,.$$

Le proprietà dell'estremo inferiore sono legate a quelle dell'estremo superiore.

Definizione 2.23 Se $A \subset \mathbb{R}$, chiamiamo opposto di A l'insieme $-A = \{-a : a \in A\}$ degli opposti degli elementi di A.

Osservando infatti che $\mathcal{M}_{-A} = -m_A$ e $m_{-A} = -\mathcal{M}_A$ si ottiene la seguente

Proposizione 2.24 *Se A è un sottoinsieme non vuoto di $\mathbb{R}$, allora*

$$\sup A = -\inf(-A) \,, \qquad \inf A = -\sup(-A) \,.$$

Di conseguenza, dal Teorema 2.22 si ottiene facilmente l'esistenza dell'estremo inferiore in $\mathbb{R}$.

Proposizione 2.25 *Ogni insieme $A \subset \mathbb{R}$ non vuoto e limitato inferiormente ha estremo inferiore.*

Ricordando poi che $\mathcal{M}_A \supset \mathcal{M}_B$ e $m_A \supset m_B$ se $A \subset B$, si ottiene la seguente

Proposizione 2.26 *Se A, B sono sottoinsiemi non vuoti di $\mathbb{R}$, con $A \subset B$, allora*

$$\inf B \le \inf A \le \sup A \le \sup B \,.$$

Proprietà di Archimede

Dall'esistenza dell'estremo superiore si ottiene la seguente

Proposizione 2.27 *Se $a, b \in \mathbb{R}$ con $a, b > 0$ allora esiste un numero naturale positivo $n \in \mathbb{N}^+$ tale che $na > b$.*

Dalla proprietà di Archimede segue un utile

Corollario 2.28 *Se $x > 0$, allora esiste $n \in \mathbb{N}^+$ tale che $1/n < x$.*
Se invece $x \in \mathbb{R}$ verifica $\forall\, n \in \mathbb{N}^+,\ x \le 1/n$, allora $x \le 0$.

Osservazione 2.29 Dalla proprietà di Archimede segue che $\mathbb{N}$, e quindi anche $\mathbb{Z}$ e $\mathbb{Q}$ (e ovviamente $\mathbb{R}$) non sono limitati superiormente. Poiché $-\mathbb{Z} = \mathbb{Z}$ e $-\mathbb{Q} = \mathbb{Q}$, allora $\mathbb{Z}$ e $\mathbb{Q}$ (e ovviamente $\mathbb{R}$) non sono limitati inferiormente.

Caratterizzazioni

Nel caso di estremi reali, abbiamo

$$L = \sup A \in \mathbb{R} \iff \begin{cases} L \in \mathcal{M}_A \\ \forall\, \lambda < L,\ \lambda \notin \mathcal{M}_A \end{cases} \qquad l = \inf A \in \mathbb{R} \iff \begin{cases} l \in m_A \\ \forall\, \mu > l,\ \mu \notin m_A \,. \end{cases}$$

In modo equivalente si può dunque scrivere

$$L = \sup A \in \mathbb{R} \iff \begin{cases} \forall\, a \in A,\ a \le L \\ \forall\, \lambda < L,\ \exists\, a \in A:\ a > \lambda \end{cases} \qquad l = \inf A \in \mathbb{R} \iff \begin{cases} \forall\, a \in A,\ a \ge l \\ \forall\, \mu > l,\ \exists\, a \in A:\ a < \mu \,. \end{cases}$$

Vale infine la seguente caratterizzazione di maggiore utilità pratica

$$L = \sup A \in \mathbb{R} \iff \begin{cases} \forall\, a \in A,\ a \le L \\ \forall\, \varepsilon > 0,\ \exists\, a \in A:\ a > L - \varepsilon \end{cases}$$

$$l = \inf A \in \mathbb{R} \iff \begin{cases} \forall\, a \in A,\ a \ge l \\ \forall\, \varepsilon > 0,\ \exists\, a \in A:\ a < l + \varepsilon \,. \end{cases} \tag{2.3}$$

Esempio 2.30 Se $a < b$, allora $\sup[a, b[= b$ e $\inf[a, b[= \min[a, b[= a$.

Esempio 2.31 Posto $A = \{n/(n+1) : n \in \mathbb{N}\}$, mostriamo che $\inf A = \min A = 0$ e che $\sup A = 1$.

La prima affermazione è di facile verifica, in quanto 0 è minorante di A ed appartiene ad A. Per la seconda, osserviamo che $1 \in \mathcal{M}_A$. Infatti, per ogni $n \in \mathbb{N}$, $n/(n+1) \le 1 \iff n \le n+1 \iff 0 \le 1$. Per provare che 1 è il più piccolo dei maggioranti di A, verifichiamo che

$$\forall \varepsilon > 0,\ \exists n \in \mathbb{N} :\ \frac{n}{n+1} > 1 - \varepsilon \,.$$

Infatti, supposto $\varepsilon < 1$, altrimenti il fatto è ovvio, si ha

$$\frac{n}{n+1} > 1 - \varepsilon \iff 1 - \frac{1}{n+1} > 1 - \varepsilon \iff \varepsilon > \frac{1}{n+1} \iff n + 1 > \frac{1}{\varepsilon} \iff n > \frac{1}{\varepsilon} - 1 \,.$$

Basta quindi applicare la proprietà di Archimede con $a = 1$ e $b = (1/\varepsilon) - 1$.

Estremi di funzioni

Mediante la nozione di immagine e controimmagine, si introduce la seguente

Definizione 2.32 Sia $A \subset \mathbb{R}$ e sia $f : A \to \mathbb{R}$ una funzione reale; allora

1. si dice che la funzione f è *limitata superiormente [[o inferiormente, o limitata]]* se la sua immagine $f(A)$ è un insieme limitato superiormente [[o inferiormente, o limitato]];
2. si dice che un numero reale ξ è *il massimo [[o minimo, o estremo superiore, o estremo inferiore]] di f* se ξ è il massimo [[o minimo, o estremo superiore, o estremo inferiore]] dell'immagine $f(A)$ di f, e in tal caso si scrive $\xi = \max f$ [[oppure $\min f$, $\sup f$, $\inf f$]];
3. se f non è limitata superiormente [[o inferiormente]] si scrive $\sup f = +\infty$ [[oppure $\inf f = -\infty$]];
4. se f ha massimo [[o minimo]], un elemento $x_0 \in A$ si dice *punto di massimo [[o minimo]]* per f se $f(x_0) = \max f$ [[se $f(x_0) = \min f$]].

Osservazione 2.33 I punti di massimo o di minimo possono non essere unici.

Questi concetti si possono poi localizzare ad un sottoinsieme non vuoto $B \subset A$ come segue.

Definizione 2.34 Si dice che f è *limitata superiormente su B* se l'immagine $f(B)$ di B tramite f è un insieme limitato superiormente; inoltre ξ è *il massimo di f su B* se ξ è il massimo di $f(B)$, e in tal caso si scrive $\xi = \max\limits_B f$; se infine f ha massimo su B, un punto $x_0 \in B$ si dice *punto di massimo per f su B* se $f(x_0) = \max\limits_B f$.

Quindi abbiamo

$$
\begin{aligned}
M = \max f &\iff \begin{cases} \exists\, x_0 \in \operatorname{dom} f : f(x_0) = M \\ \forall\, x \in \operatorname{dom} f,\ f(x) \le M \end{cases} \\
m = \min f &\iff \begin{cases} \exists\, x_0 \in \operatorname{dom} f : f(x_0) = m \\ \forall\, x \in \operatorname{dom} f,\ f(x) \ge m \end{cases} \\
L = \sup f \in \mathbb{R} &\iff \begin{cases} \forall\, x \in \operatorname{dom} f,\ f(x) \le L \\ \forall\, \varepsilon > 0,\ \exists\, x \in \operatorname{dom} f :\ f(x) > L - \varepsilon \end{cases} \\
l = \inf f \in \mathbb{R} &\iff \begin{cases} \forall\, x \in \operatorname{dom} f,\ f(x) \ge l \\ \forall\, \varepsilon > 0,\ \exists\, x \in \operatorname{dom} f :\ f(x) < l + \varepsilon \end{cases} \\
\sup f = +\infty &\iff \forall\, M \in \mathbb{R},\ \exists\, x \in \operatorname{dom} f : f(x) \ge M \\
\inf f = -\infty &\iff \forall\, m \in \mathbb{R},\ \exists\, x \in \operatorname{dom} f : f(x) \le m \\
f \quad \text{è limitata} &\iff \exists\, H, K \in \mathbb{R} :\ \forall\, x \in \operatorname{dom} f,\ H \le f(x) \le K \\
&\iff \exists\, \widetilde{M} > 0 :\ \forall\, x \in \operatorname{dom} f,\ |f(x)| \le \widetilde{M}
\end{aligned}
$$

e le analoghe proprietà localizzate ad un sottoinsieme non vuoto B di $\operatorname{dom} f$, sostituendo $\operatorname{dom} f$ con B dappertutto (e $M = \max\limits_B f$, etc.).

Una funzione monotona su un intervallo chiuso assume massimo e minimo agli estremi dell'intervallo.

Proposizione 2.35 *Se $f : [a, b] \to \mathbb{R}$ è debolmente crescente, allora $\min\limits_{[a,b]} f = f(a)$ e $\max\limits_{[a,b]} f = f(b)$; se f è debolmente decrescente, allora $\min\limits_{[a,b]} f = f(b)$ e $\max\limits_{[a,b]} f = f(a)$.*

Vale anche la seguente

Proposizione 2.36 *Date due funzioni reali $f, g : A \to \mathbb{R}$ e dato $B \subset A$ non vuoto, allora:*

1. $\sup_B(-f) = -\inf_B f$ *e* $\inf_B(-f) = -\sup_B f$ *;*
2. $\inf_A f \le \inf_B f \le \sup_B f \le \sup_A f$ *;*
3. *se $f \le g$ su B, allora $\inf_B f \le \inf_B g$ e $\sup_B f \le \sup_B g$;*
4. $\inf f + \inf g \le \inf(f + g) \le \inf f + \sup g \le \sup(f + g) \le \sup f + \sup g$

   (se f e g sono limitate, e analogamente con $\inf_B$ e $\sup_B$ ovunque).

I numeri complessi

Sono introdotti per risolvere equazioni polinomiali che non hanno soluzioni reali, come le equazioni di secondo grado con discriminante negativo, tipo $x^2+1=0$.

Forma algebrica

Definizione 2.37 L'insieme $\mathbb{C}$ dei *numeri complessi* è dato da tutti i numeri della forma $a+\mathbf{i}b$, dove $a,b\in\mathbb{R}$ e $\mathbf{i}$ è l'*unità immaginaria*, che verifica la proprietà

$$\mathbf{i}^2=-1\ .$$

Per ogni numero complesso $z=a+\mathbf{i}b$ definiamo la *parte reale* e la *parte immaginaria*

$$\Re(a+\mathbf{i}b)=a\in\mathbb{R}\ ,\qquad \Im(a+\mathbf{i}b)=b\in\mathbb{R}\ .$$

Quindi $\mathbb{R}\subsetneq\mathbb{C}$, dove $z\in\mathbb{C}$ è un numero reale se e solo se $\Im z=0$. Inoltre $a+\mathbf{i}b=c+\mathbf{i}d$ se e solo se $a=c$ e $b=d$. In particolare, $z=0$ se e solo se $\Re z=0$ e $\Im z=0$.

Sui numeri complessi si *estendono* le operazioni di addizione e moltiplicazione in $\mathbb{R}$ come segue:

$$\begin{aligned}&(a+\mathbf{i}b)+(c+\mathbf{i}d)=(a+c)+\mathbf{i}(b+d)\\&(a+\mathbf{i}b)\cdot(c+\mathbf{i}d)=ac+\mathbf{i}ad+\mathbf{i}bc+\mathbf{i}^2bd=(ac-bd)+\mathbf{i}(ad+bc)\ .\end{aligned}$$

Osservazione 2.38 Nell'insieme $\mathbb{C}$ non è possibile definire una relazione d'ordine totale per la quale valgano ancora le proprietà algebriche 10. e 11. dei numeri reali.

Sui numeri complessi valgono quindi le proprietà algebriche 1.–9. dei numeri reali, dove l'elemento neutro della addizione e della moltiplicazione sono sempre 0 e 1, rispettivamente. In particolare, il *reciproco* di un numero $a+\mathbf{i}b\neq 0$ è dato dalla formula

$$\frac{1}{a+\mathbf{i}b}=\frac{a}{a^2+b^2}+\mathbf{i}\frac{-b}{a^2+b^2}\ ,\qquad a^2+b^2>0\ .$$

Coniugato e modulo

Definizione 2.39 Si dice *coniugato* del numero $z=a+\mathbf{i}b\in\mathbb{C}$ il numero complesso

$$\bar z=\Re z-\mathbf{i}\Im z=a-\mathbf{i}b\ .$$

Valgono quindi le seguenti proprietà di facile verifica, dove $z,w\in\mathbb{C}$:

1. $\Re(z+w)=\Re z+\Re w$, $\Im(z+w)=\Im z+\Im w$
2. $\Re\bar z=\Re z\,,\quad \Im\bar z=-\Im z$
3. $\overline{z+w}=\bar z+\bar w\,,\quad \overline{zw}=\bar z\bar w$
4. $\bar{\bar z}=z\,,\quad z\in\mathbb{R}\iff z=\bar z$
5. $\Re z=\dfrac{z+\bar z}{2}\,,\quad \Im z=\dfrac{z-\bar z}{2\mathbf{i}}=-\dfrac{\mathbf{i}}{2}(z-\bar z)$.

Definizione 2.40 Si dice *modulo* del numero complesso $z=a+\mathbf{i}b\in\mathbb{C}$ il numero reale non negativo

$$|z|=\sqrt{(\Re z)^2+(\Im z)^2}=\sqrt{a^2+b^2}\ .$$

Quindi $z\mapsto|z|$ è una funzione da $\mathbb{C}$ in $\mathbb{R}$, con $|z|\geq 0$ sempre e $|z|=0\iff z=0$. Si noti che se $z\in\mathbb{C}$ è reale, allora $\Im z=0$ e quindi il modulo di z coincide con il valore assoluto del numero reale z.

Valgono le seguenti proprietà:

Proposizione 2.41 *Per ogni $z,w\in\mathbb{C}$ si ha:*

1. $|z|=|\bar z|$

2. $|\Re z|\leq|z|$

3. $|\Im z| \le |z|$

4. $z\bar{z} = |z|^2$

5. $|zw| = |z||w|$

6. $|z+w| \le |z| + |w|$ *(diseguaglianza triangolare)*

7. $|z| \le |\Re z| + |\Im z|$.

Dalla proprietà 4. si ottiene poi un importante risultato sul quoziente di numeri complessi.

Corollario: per ogni $z \in \mathbb{C} \setminus \{0\}$ si ha $\dfrac{1}{z} = \dfrac{\bar{z}}{|z|^2}$, di conseguenza per ogni $w \in \mathbb{C}$ risulta anche $\dfrac{w}{z} = \dfrac{w\,\bar{z}}{|z|^2}$.

Piano di Gauss e forma trigonometrica

I numeri complessi si rappresentano nel *piano di Gauss* associando al numero $z = a + \mathbf{i}b$, dove $a, b \in \mathbb{R}$, il punto di coordinate $(a, b) = (\Re z, \Im z)$. L'asse delle ascisse, di equazione $\Im z = 0$, corrisponde ai numeri reali, mentre l'asse delle ordinate, di equazione $\Re z = 0$, corrisponde ai numeri con parte reale nulla (detti immaginari puri). Vengono quindi detti *asse reale* e *asse immaginario*. Il modulo $|z|$ è la distanza del punto z dall'origine, mentre la distanza tra i punti del piano z e w è data dal modulo della differenza: $\operatorname{dist}(z, w) = |z-w|$. Inoltre, la somma tra complessi corrisponde alla somma tra vettori e la diseguaglianza triangolare 6. descrive una nota proprietà dei triangoli.

Definizione 2.42 Chiamiamo *argomento* $\arg z$ di un numero complesso $z \in \mathbb{C} \setminus \{0\}$ la misura in radianti dell'angolo che la semiretta uscente da 0 e passante per z forma con il semiasse positivo reale.

Quindi se z è diverso da 0 si può scrivere $z = |z|\big(\cos(\arg z) + \mathbf{i}\operatorname{sen}(\arg z)\big)$.

Definizione 2.43 Si chiama *forma trigonometrica* di un numero complesso $z \in \mathbb{C} \setminus \{0\}$ la scrittura

$$z = \rho(\cos\theta + \mathbf{i}\operatorname{sen}\theta)\ ,$$

dove $\rho > 0$ e $\theta \in \mathbb{R}$.

In tal caso allora ρ è il modulo di z e θ è argomento di z. Quindi se $z \in \mathbb{C} \setminus \{0\}$ si scrive (in forma algebrica) come $z = a + \mathbf{i}b$, per passare alla forma trigonometrica si risolve

$$\rho = |z| = \sqrt{a^2+b^2} \qquad \text{e} \qquad \begin{cases} \cos\theta = \dfrac{\Re z}{|z|} = \dfrac{a}{\sqrt{a^2+b^2}} \\ \operatorname{sen}\theta = \dfrac{\Im z}{|z|} = \dfrac{b}{\sqrt{a^2+b^2}} \end{cases} .$$

In particolare se $a = \Re z \neq 0$ allora $\tan\theta = \dfrac{\Im z}{\Re z} = \dfrac{b}{a}$. Se $\theta = \arg z$, allora ogni numero del tipo $\theta + 2k\pi$, con $k \in \mathbb{Z}$, è ancora un argomento di z. Definiamo quindi l'*argomento minimo* di z come

$$\theta = \arg\min z \iff [\theta = \arg z \quad \mathbf{e} \quad 0 \le \theta < 2\pi]\ .$$

Operazioni in forma trigonometrica

Proposizione 2.44 *Se $z \neq 0$ si scrive nella forma $z = \rho(\cos\theta + \mathbf{i}\operatorname{sen}\theta)$, allora*

$$\bar{z} = \rho\big(\cos(-\theta) + \mathbf{i}\operatorname{sen}(-\theta)\big) \qquad e \qquad \frac{1}{z} = \frac{1}{\rho}\big(\cos(-\theta) + \mathbf{i}\operatorname{sen}(-\theta)\big)\ .$$

Dimostrazione: Infatti $\bar{z} = \rho(\cos\theta - \mathbf{i}\operatorname{sen}\theta) = \rho(\cos(-\theta) + \mathbf{i}\operatorname{sen}(-\theta))$, mentre $z^{-1} = |z|^{-2}\bar{z}$, da cui otteniamo $|z^{-1}| = |z|^{-2}|\bar{z}| = |z|^{-1}$ e dunque la seconda formula. □

Proposizione 2.45 *Se* $z, w \in \mathbb{C} \setminus \{0\}$ *si scrivono in forma trigonometrica come*

$$z = \rho(\cos\theta + \mathbf{i}\,\mathrm{sen}\,\theta)\ , \qquad w = R(\cos\phi + \mathbf{i}\,\mathrm{sen}\,\phi)$$

allora il loro prodotto si scrive

$$zw = (\rho\, R)\big(\cos(\theta+\phi) + \mathbf{i}\,\mathrm{sen}(\theta+\phi)\big)$$

il quoziente

$$\frac{z}{w} = \frac{\rho}{R}\big(\cos(\theta-\phi) + \mathbf{i}\,\mathrm{sen}(\theta-\phi)\big)$$

e la potenza n*-esima di* z *come*

$$z^n = \rho^n\big(\cos(n\theta) + \mathbf{i}\,\mathrm{sen}(n\theta)\big)\ , \qquad n \in \mathbb{N}\ .$$

Dimostrazione: La formula del prodotto segue dalle formule di duplicazione di seno e coseno:

$$\begin{aligned} zw &= \rho\, R\,(\cos\theta + \mathbf{i}\,\mathrm{sen}\,\theta)(\cos\phi + \mathbf{i}\,\mathrm{sen}\,\phi) \\ &= \rho\, R\,[(\cos\theta\cos\phi - \mathrm{sen}\,\theta\,\mathrm{sen}\,\phi) + \mathbf{i}(\cos\theta\,\mathrm{sen}\,\phi + \mathrm{sen}\,\theta\cos\phi)] \\ &= \rho\, R\,[\cos(\theta+\phi) + \mathbf{i}\,\mathrm{sen}(\theta+\phi)]\,. \end{aligned}$$

La formula del quoziente si ottiene da quella del prodotto scrivendo $z/w = z\,w^{-1}$ e ricordando che $w^{-1} = R^{-1}(\cos(-\phi) + \mathbf{i}\,\mathrm{sen}(-\phi))$.

La formula della potenza n-esima è ovvia per $n = 0, 1$, mentre per $n = 2$ segue applicando la formula del prodotto con $w = z$. Assumendo poi che vale per un grado $n \in \mathbb{N}$ e scrivendo $z^{n+1} = z^n z$, si ottiene facilmente che vale anche per $n+1$. Quindi per il principio di induzione, che vedremo nel teorema 2.59, vale per ogni $n \in \mathbb{N}$. □

Osservazione 2.46 Se in particolare w ha modulo $R = 1$, allora il prodotto wz sta sulla circonferenza di centro l'origine cui appartiene z, e si ottiene ruotando z in verso antiorario di un angolo di $\phi = \arg w$ radianti. Ad esempio, $\mathbf{i}z$ si ottiene ruotando z di un quarto dell'angolo giro. Quindi in generale wz si scrive a partire da z mediante una rotazione di $\phi = \arg w$ seguita da un'omotetia di ragione $R = |w|$.

Radici complesse

Definizione 2.47 Se $n \in \mathbb{N}^+$ e $z \in \mathbb{C}$, un numero complesso w è radice n-esima di z se $w^n = z$.

Dalla formula della potenza n-esima otteniamo quindi il seguente

Teorema 2.48 *Per ciascun valore di* $n \in \mathbb{N}^+$ *ogni numero complesso* z *diverso da zero ha esattamente* n *radici* n*-esime distinte. Inoltre, in forma trigonometrica, se* $z = \rho(\cos\theta + \mathbf{i}\,\mathrm{sen}\,\theta)$*, le radici* n*-esime di* z *sono i numeri complessi* $w_k = R(\cos\phi_k + \mathbf{i}\,\mathrm{sen}\,\phi_k)$ *di modulo* $R = \rho^{1/n}$ *e argomento*

$$\phi_k = \frac{\theta}{n} + \frac{k\cdot 2\pi}{n}\ , \qquad k = 0, 1, \ldots, n-1\ .$$

Dimostrazione: Sia $w = R(\cos\phi + \mathbf{i}\,\mathrm{sen}\,\phi)$. Se $w^n = z$, allora $R^n = |w|^n = |w^n| = |z| = \rho$, quindi $R = \rho^{1/n}$. Inoltre dalla formula della potenza n-esima $w^n = R^n(\cos(n\phi) + \mathbf{i}\,\mathrm{sen}(n\phi))$ per cui, essendo $R^n = \rho$, si ha

$$w^n = z \iff R^n(\cos(n\phi) + \mathbf{i}\,\mathrm{sen}(n\phi)) = \rho(\cos\theta + \mathbf{i}\,\mathrm{sen}\,\theta) \iff \cos(n\phi) + \mathbf{i}\,\mathrm{sen}(n\phi) = \cos\theta + \mathbf{i}\,\mathrm{sen}\,\theta\,.$$

Uguagliando parte reale e parte immaginaria, ne segue che l'argomento ϕ deve essere soluzione del sistema

$$\begin{cases} \cos(n\phi) = \cos\theta \\ \mathrm{sen}(n\phi) = \mathrm{sen}\,\theta \end{cases}$$

che è risolto da $\phi_k = \theta/n + k\cdot 2\pi/n$ per ogni valore di $k \in \mathbb{Z}$. Dalla periodicità delle funzioni seno e coseno concludiamo che i valori di k per i quali si ottengono distinti numeri complessi $\cos\phi_k + \mathbf{i}\,\mathrm{sen}\,\phi_k$ sono esattamente n, dati ad esempio da $k \in \{0, 1, \ldots, n-1\}$. □

Osservazione 2.49 Si noti quanto segue:

1. se $n = 2$ le due radici quadrate sono l'una l'opposta dell'altra;
2. se $n = 2m$ è pari, trovate le prime m radici $w_0, \ldots, w_{m-1}$, le altre m sono le opposte di queste, i.e. $w_{k+m} = -w_k$ per $k = 0, \ldots, m-1$;
3. se z è reale positivo la prima radice n-esima è la radice n-esima reale;
4. le radici n-esime di z stanno sui vertici di un n-agono regolare inscritto nella circonferenza di centro l'origine e raggio $|z|^{1/n}$;
5. uno dei vertici si trova dividendo in n parti uguali l'angolo θ che corrisponde all'argomento di z.

Equazioni complesse

Grazie all'esistenza delle radici quadrate complesse, possiamo risolvere le equazioni di secondo grado. Come nel campo reale, dati $a, b, c \in \mathbb{C}$, con $a \neq 0$, e denotato con $\Delta := b^2 - 4ac$ il discriminante, scriviamo

$$az^2 + bz + c = a\Big(z^2 + \frac{b}{a}z + \frac{c}{a}\Big) = a\Big(z^2 + \frac{b}{a}z + \frac{b^2}{4a^2} - \frac{\Delta}{4a^2}\Big) = a\Big[\Big(z + \frac{b}{2a}\Big)^2 - \frac{\Delta}{4a^2}\Big].$$

Quindi un numero $z \in \mathbb{C}$ risolve l'equazione $az^2 + bz + c = 0$ se e solo se il numero $w = z + b/2a$ è una radice quadrata complessa del numero $\Delta/4a^2$. Si vede facilmente che le due radici quadrate di $\Delta/4a^2$ sono $\pm\sqrt{\Delta}/2a$, dove abbiamo indicato con $\sqrt{\Delta}$ una delle due radici quadrate in $\mathbb{C}$ del discriminante Δ.

In conclusione l'equazione $az^2 + bz + c = 0$, dove $a \neq 0$, ha due soluzioni complesse date da

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a}, \qquad z_2 = \frac{-b - \sqrt{\Delta}}{2a}, \qquad \Delta := b^2 - 4ac.$$

Teorema fondamentale dell'algebra

Come conseguenza, si deduce che l'insieme dei numeri complessi è algebricamente chiuso:

Teorema 2.50 *Sia $P_n(z)$ un polinomio di grado $n \in \mathbb{N}$ a coefficienti complessi. Allora l'equazione $P_n(z) = 0$ ha esattamente n soluzioni complesse (contate con la loro molteplicità).*

Osserviamo ora che se $P_n(z)$ ha coefficienti reali, allora il suo coniugato è $\overline{P_n(z)} = P_n(\overline{z})$. Quindi, $P_n(z) = 0 \iff P_n(\overline{z}) = 0$, da cui segue:

Corollario 2.51 *Sia $P_n(z)$ un polinomio di grado $n \in \mathbb{N}$ a coefficienti reali. Se un numero $z \in \mathbb{C} \setminus \mathbb{R}$ è soluzione dell'equazione $P_n(z) = 0$, allora anche il coniugato $\overline{z}$ è soluzione dell'equazione $P_n(z) = 0$ (con la stessa molteplicità di z).*

Forma esponenziale

Osservazione 2.52 L'esponenziale complesso $z \mapsto \mathsf{e}^z$ è una funzione con dominio e codominio $\mathbb{C}$ definita in modo tale che per ogni $b \in \mathbb{R}$ risulta $\mathsf{e}^{\mathbf{i}b} = \cos b + \mathbf{i} \operatorname{sen} b$, cf. l'osservazione 6.83. Inoltre valgono le proprietà delle potenze, nel senso che $\mathsf{e}^z = \mathsf{e}^{\Re z + \mathbf{i}\Im z} = \mathsf{e}^{\Re z}\mathsf{e}^{\mathbf{i}\Im z}$ ed anche $\mathsf{e}^z\mathsf{e}^w = \mathsf{e}^{z+w}$.

Quindi un numero complesso z di modulo ρ e argomento θ si scrive in *forma esponenziale* come $z = \rho\,\mathsf{e}^{\mathbf{i}\theta}$. Dalle formule note si ottiene dunque, in coerenza con le proprietà delle potenze: $\overline{z} = \rho\,\mathsf{e}^{-\mathbf{i}\theta}$, $z^{-1} = \rho^{-1}\,\mathsf{e}^{-\mathbf{i}\theta}$, $z^n = \rho^n\,\mathsf{e}^{\mathbf{i}n\theta}$ ed infine, se $w = R\,\mathsf{e}^{\mathbf{i}\phi}$, allora $zw = \rho\,R\,\mathsf{e}^{\mathbf{i}(\theta+\phi)}$. Poiché ad esempio -1 ha modulo 1 e argomento π, si ottiene la famosa equazione di Eulero $\mathsf{e}^{\mathbf{i}\pi} + 1 = 0$, che comprende i cinque numeri più importanti dell'analisi matematica.

Esempio 2.53 Un'onda elettromagnetica piana agisce su un conduttore elettrico rettilineo e si propaga nella direzione delle x. Dalle equazioni di Maxwell si deduce che il campo elettrico e il campo magnetico sono ortogonali fra loro. L'onda è dunque descritta dalla funzione complessa $\phi(x,t) = \phi(x)\,\mathsf{e}^{\mathbf{i}\omega t}$, dove $\omega > 0$ è la frequenza angolare dell'onda e $\phi(x) = A\,\mathsf{e}^{\mathbf{i}\alpha x}$, dove $A > 0$ ed il numero complesso $\alpha \in \mathbb{C}$ dipende dalla conducibilità elettrica σ, dalla permeabilità elettrica ε e dalla permeabilità magnetica μ

tramite la formula $\alpha^2 = \omega^2\varepsilon\mu - \mathbf{i}\omega\delta\mu$, con $\Re\alpha > 0$ e $\Im\alpha > 0$. Abbiamo $\mathsf{e}^{\mathbf{i}\alpha x} = \mathsf{e}^{\mathbf{i}(\Re\alpha)x}\mathsf{e}^{-(\Im\alpha)\,x}$, per cui possiamo scrivere

$$\phi(x,t) = A\,\mathsf{e}^{-(\Im\alpha)\,x}\,\mathsf{e}^{\mathbf{i}[(\Re\alpha)x+\omega t]} = A\,\mathsf{e}^{-(\Im\alpha)\,x}\,\big(\cos((\Re\alpha)x+\omega t) + \mathbf{i}\,\mathrm{sen}((\Re\alpha)x+\omega t)\big)\,.$$

Quindi l'onda elettromagnetica si trasferisce lungo il conduttore come una oscillazione smorzata, con uno sfasamento tra parte reale (campo elettrico) e immaginaria (campo magnetico).

I principi del minimo intero e di induzione

Il *principio del minimo intero* esprime il buon ordinamento dei naturali. Il *principio di induzione* dà senso alle definizioni ricorsive ed è utile nella verifica di proprietà che dipendono da un numero naturale.

Principio del minimo intero

Applicando il teorema di esistenza dell'estremo superiore si dimostra la seguente

Proposizione 2.54 *Ogni insieme $A \subset \mathbb{N}$ non vuoto ha minimo.*

Come conseguenza, si ottiene facilmente l'analoga proprietà sugli interi relativi:

Corollario 2.55 *Sia $A \subset \mathbb{Z}$ un insieme non vuoto. Se A è limitato inferiormente, allora ha minimo. Analogamente, se A è limitato superiormente, allora ha massimo.*

Possiamo quindi definire il *successivo* di un numero intero e la *parte intera* di un numero reale:

Definizione 2.56 Successivo di un intero $n \in \mathbb{Z}$ è il minimo dell'insieme $A := \{m \in \mathbb{Z} \mid m > n\}$. La parte intera $\lfloor x \rfloor$ di un numero $x \in \mathbb{R}$ è definita come il massimo dell'insieme $B := \{n \in \mathbb{Z} \mid n \leq x\}$.

Osservazione 2.57 Nell'esempio 2.31, se $\varepsilon \in]0,1[$, il più piccolo n per il quale $n/(n+1) > 1-\varepsilon$ è dato da $n_\varepsilon := \lfloor \varepsilon^{-1} - 1 \rfloor + 1$ e quindi dipende da ε. In particolare la funzione $\varepsilon \mapsto n_\varepsilon$ è decrescente su $]0,1[$.

Osservazione 2.58 L'esistenza del successivo, che vale sugli interi relativi, non vale per l'insieme dei numeri razionali, in quanto dipende dal principio del minimo intero, anch'esso falso in $\mathbb{Q}$, in quanto ad esempio non esiste il più piccolo numero razionale positivo.

Principio di induzione

Teorema 2.59 *Sia $S \subset \mathbb{N}$ un insieme che verifica:*

1) $0 \in S$

2) per ogni $n \in S$, anche $n+1 \in S$.
Allora $S = \mathbb{N}$.

Dimostrazione: Se $S \neq \mathbb{N}$, allora l'insieme di numeri naturali $A := \mathbb{N} \setminus S$ è non vuoto. Per il principio del minimo intero A ha minimo: $\exists\, m = \min A$. Dalla 1) sappiamo che $0 \notin A$, quindi $m \in \mathbb{N}^+$ e scriviamo $m = n+1$, con $n \in \mathbb{N}$. Poiché $n \notin A$, in quanto $n < m = \min A$, allora $n \in S$. Ma allora, per la 2) si ottiene che $m = n+1 \in S$. Ma questo è un assurdo, in quanto $m \in A$ e per definizione $A \cap S = \emptyset$. □

Usiamo il principio di induzione per definire il *fattoriale.*

Definizione 2.60 La funzione fattoriale $f : \mathbb{N} \to \mathbb{N}$ è data da

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1)\cdot f(n) & \text{se } n \geq 0 \end{cases}$$

e si denota $f(n) = n!$. Quindi $0! = 1$ mentre $n! = 1\cdot 2\cdots(n-1)\cdot n$ per ogni $n \in \mathbb{N}^+$. Si noti poi che il simbolo ! di fattoriale ha la precedenza sulle altre operazioni: ad esempio $2\cdot(n!) = 2n! \neq (2n)!$.

Sommatorie

Il simbolo di *sommatoria* permette di abbreviare le notazioni.

Definizione 2.61 Dati i numeri reali $a_1, a_2, \dots, a_n$, denotiamo con

$$\sum_{i=1}^{n} a_i = \sum_{1\le j\le n} a_j = \sum_{h=k+1}^{k+n} a_{h-k} = a_1 + a_2 + \cdots + a_n$$

la somma di tali n numeri, dove gli indici i, j, h, k sono muti. Se I è un insieme finito di indici, denotiamo con $\sum_{i\in I} a_i$ la somma di tutti i numeri a_i, dove l'indice i assume tutti i valori compresi nell'insieme I.

Se I, J sono insiemi di indici, e tutti i numeri che compaiono sono numeri reali, allora:

1. se I e J sono disgiunti, $\sum_{i\in I\cup J} a_i = \sum_{i\in I} a_i + \sum_{j\in J} a_j$
2. $\sum_{i\in I}(a_i + b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i$
3. $\sum_{i\in I} c\cdot a_i = c\cdot \sum_{i\in I} a_i \qquad \forall\, c\in\mathbb{R}$.

Principio di induzione applicato ai predicati

Se $\mathcal{P}(n)$ denota un predicato che dipende dal numero naturale n – questo significa che $\mathcal{P}(n)$ è una proposizione, vera o falsa, per ogni fissato n – la verità della proposizione $\mathcal{P}(n)$ per ogni n può essere dimostrata facendo uso della seguente forma equivalente del principio di induzione, ottenuta ponendo $S := \{n\in\mathbb{N} \mid \mathcal{P}(n) \text{ è vera }\}$.

Proposizione 2.62 *Sia $\mathcal{P}(n)$ un predicato definito per ogni $n\in\mathbb{N}$ e che verifica le seguenti proprietà:*
1) $\mathcal{P}(0)$ è vero
2) per ogni $n\in\mathbb{N}$, supponendo vero $\mathcal{P}(n)$ risulta vero anche $\mathcal{P}(n+1)$.
Allora $\mathcal{P}(n)$ è vero per ogni $n\in\mathbb{N}$.

Esempio 2.63 Proviamo mediante il principio di induzione che per ogni naturale n la somma dei numeri interi da 0 ad n vale $n(n+1)/2$.

Detto $\mathcal{P}(n)$ il predicato

$$\sum_{j=0}^{n} j = \frac{n(n+1)}{2} \ ,$$

dimostriamo per induzione che $\mathcal{P}(n)$ è vera per ogni $n\in\mathbb{N}$. Ovviamente $\mathcal{P}(0)$ è vera. Proviamo quindi che $\forall\, n\in\mathbb{N}^+,\ \mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$. Sostituendo $n-1$ al posto di n, abbiamo che per ipotesi induttiva vale

$$\sum_{j=0}^{n-1} j = \frac{(n-1)\big((n-1)+1\big)}{2} = \frac{(n-1)n}{2} \ .$$

A questo punto, isolando l'ultimo termine nella sommatoria, e usando l'ipotesi induttiva, risulta

$$\sum_{j=0}^{n} j = \sum_{j=0}^{n-1} j + n = \frac{(n-1)n}{2} + n = \frac{n(n-1)+2n}{2} = \frac{n(n+1)}{2} \ .$$

Quindi, valendo $\mathcal{P}(n)$ abbiamo la dimostrato la tesi.

Esempio 2.64 Dimostriamo per induzione la formula

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q} \qquad \forall\, n\in\mathbb{N} \quad \text{se} \quad q\ne 1 \tag{2.4}$$

sulla somma di una progressione geometrica.

Fissato $q \neq 1$, e detto $\mathcal{P}(n)$ il predicato $\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$, verifichiamo che $\mathcal{P}(0)$ è vera, in quanto $1 = \frac{1-q}{1-q}$. Supposta vera $\mathcal{P}(n)$, proviamo allora che vale $\mathcal{P}(n+1)$, i.e. che $\sum_{k=0}^{n+1} q^k = \frac{1-q^{n+2}}{1-q}$. Infatti calcoliamo

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} = \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q} = \frac{1-q^{n+2}}{1-q} \,,$$

per cui dal principio di induzione segue l'asserto.

Forma equivalente del principio di induzione

Nelle applicazioni risulta utile la seguente forma equivalente del principio di induzione, ottenuta ponendo $\mathcal{P}(n) = \mathcal{Q}(n+n_0)$ nella proposizione 2.62:

Proposizione 2.65 *Dato $n_0 \in \mathbb{N}$, sia $\mathcal{Q}(n)$ un predicato definito per ogni naturale $n \geq n_0$ e che verifica le seguenti proprietà:*

1) $\mathcal{Q}(n_0)$ è vero

2) $\forall\, n \geq n_0$, $\mathcal{Q}(n) \Rightarrow \mathcal{Q}(n+1)$.

Allora $\mathcal{Q}(n)$ è vero per ogni $n \geq n_0$.

Esempio 2.66 Dimostriamo la diseguaglianza di Bernoulli

$$\forall\, a \geq -1, \ \forall\, n \in \mathbb{N}^+ \Rightarrow (1+a)^n \geq 1 + na \,. \tag{2.5}$$

Fissato $a \geq -1$, chiamiamo $\mathcal{Q}(n)$ il predicato $(1+a)^n \geq 1+na$. Ovviamente $\mathcal{Q}(1)$ è vera, in quanto diventa $1+a \geq 1+a$. Proviamo ora che $\mathcal{Q}(n) \Rightarrow \mathcal{Q}(n+1)$ per ogni $n \in \mathbb{N}^+$. Poiché $\mathcal{Q}(n+1)$ si scrive come $(1+a)^{n+1} \geq 1+(n+1)\,a$, e $(1+a) \geq 0$ se $a \geq -1$, usando $\mathcal{Q}(n)$ abbiamo che

$$(1+a)^{n+1} = (1+a)(1+a)^n \geq (1+a)(1+na) \,,$$

per cui $Q(n+1)$ è vera in quanto

$$(1+a)(1+na) \geq 1+(n+1)\,a \quad \Longleftrightarrow \quad 1+a+na+na^2 \geq 1+na+a \quad \Longleftrightarrow \quad na^2 \geq 0 \,.$$

Calcolo combinatorio

Permutazioni, disposizioni e combinazioni

Definizione 2.67 Dati n oggetti distinti, disposti in fila in un certo ordine, ogni altro modo di metterli in fila si chiama *permutazione* della collocazione ordinata di partenza. Se indichiamo con P_n il numero di permutazioni di n oggetti, allora risulta $P_1 = 1$. Inoltre, presi $n+1$ oggetti da mettere in fila, possiamo scegliere (in $n+1$ modi diversi) il primo oggetto e poi, per ognuno di questi casi, sistemare gli altri n oggetti in P_n modi. Quindi $P_{n+1} = (n+1)\,P_n$ da cui segue che

$$P_n = n! \qquad \forall\, n \in \mathbb{N}^+ \,.$$

Definizione 2.68 Le *disposizioni di n oggetti presi a k per volta*, dove $1 \leq k \leq n$, sono i modi distinti in cui possiamo mettere in fila k oggetti scelti tra un gruppo di n. Il loro numero si denota con $D_{n,k}$ ed è dato da

$$D_{n,k} = \frac{n!}{(n-k)!} = n \cdot (n-1) \cdots (n-k+1) \,.$$

Infatti, possiamo mettere in fila gli n oggetti (in P_n modi diversi) e scartare gli ultimi $n-k$. Inoltre, ad ogni disposizione dei primi k oggetti ottenuta corrispondono P_{n-k} modi diversi di disporre gli ultimi $n-k$, per cui

$$n! = P_n = D_{n,k} \cdot P_{n-k} = D_{n-k} \cdot (n-k)!$$

Osservazione 2.69 Ricordiamo il simbolo di *produttoria*: dati i numeri $a_1, a_2, \ldots, a_n$

$$\prod_{i=1}^{n} a_i = \prod_{1\le j\le n} a_j = \prod_{h=k+1}^{k+n} a_{h-k} = a_1 \cdot a_2 \cdots a_n$$

Poiché per ogni $n \in \mathbb{N}^+$ risulta $n! = \prod_{i=1}^{n} i$, allora si ottiene $D_{n,k} = \prod_{i=0}^{k-1}(n-i) \in \mathbb{N}$ per ogni $1 \le k \le n$.

Definizione 2.70 Le *combinazioni di n oggetti presi a k per volta*, dove $1 \le k \le n$, sono i modi distinti in cui possiamo scegliere (senza badare all'ordine) k oggetti tra un gruppo di n. Il loro numero si denota con $C_{n,k}$ ed è dato da

$$C_{n,k} = \frac{n!}{k!(n-k)!} = \frac{n\cdot(n-1)\cdots(n-k+1)}{1\cdot 2\cdots(k-1)\cdot k} \, .$$

Infatti, presa una combinazione di k oggetti tra n, facendo permutare gli oggetti in P_k modi si ottengono le corrispondenti disposizioni, per cui $C_{n,k}\cdot P_k = D_{n,k}$, da cui segue la formula. Si noti che $C_{n,k} \in \mathbb{N}^+$.

Osservazione 2.71 Le combinazioni si denotano anche usando i *coefficienti binomiali*, che studieremo in seguito, definiti per ogni $n \in \mathbb{N}$ e $k \in \mathbb{Z}$ da

$$\binom{n}{k} := \begin{cases} 1 & \text{se} \quad k=0 \\ C_{n,k} = \dfrac{n!}{k!(n-k)!} & \text{se} \quad 1 \le k \le n \\ 0 & \text{se} \quad k > n \text{ oppure } k < 0. \end{cases} \tag{2.6}$$

Disposizioni e combinazioni con ripetizioni

Dati $n, k \in \mathbb{N}^+$, le disposizioni con ripetizione $D^r_{n,k}$ di k oggetti scelti tra n sono ovviamente n^k.

Invece, per calcolare le combinazioni con ripetizione, partiamo dall'esempio di n scatole numerate in fila in cui collochiamo k oggetti uguali tra loro. Messi $n+1$ paletti a separare le n scatole, dobbiamo mettere i k oggetti all'interno dei paletti. Quindi contiamo le posizioni di k oggetti indistinguibili in una stringa di $(n-1)+k$ entrate. Le combinazioni con ripetizione $C^r_{n,k}$ di k oggetti scelti tra n sono dunque uguali alle combinazioni di k oggetti scelti tra $n-1+k$, i.e. $C^r_{n,k} = \binom{n-1+k}{k} \quad \forall\, n,k \in \mathbb{N}^+$.

Probabilità finita

Nella *probabilità finita* si contempla il caso di eventi che variano in un *insieme finito di possibilità*, che assumeremo *tutte equiprobabili*. In tal caso definiremo la probabilità di un evento tramite il numero razionale compreso tra 0 e 1 dato dal rapporto

$$p = \frac{\text{numero di eventi favorevoli}}{\text{numero di eventi possibili}} \in \mathbb{Q} \cap [0,1] \, .$$

Esempio 2.72 Calcoliamo la somma più probabile ottenuta lanciando due dadi a sei facce. Abbiamo $6^2 = 36$ eventi possibili, suddivisi nelle possibili somme da 2 a 12. Si verifica che alle somme 2 e 12 corrisponde un solo evento favorevole, alle somme 3 e 11 ne corrispondono 2, alle somme 4 e 10 ne corrispondono 3, alle somme 5 e 9 ne corrispondono 4, alle somme 6 e 8 ne corrispondono 5 e, infine, alla somma 7 ne corrispondono 6. Le corrispondenti probabilità sono rispettivamente 1/36, 1/18, 1/12, 1/9, 5/36 e infine 1/6 per la somma 7. Quindi è più probabile ottenere somma 7.

Esempio 2.73 Data una tavola rotonda con $n \ge 3$ posti, su cui n persone si siedono a caso, qual è la probabilità $p = p(n)$ che Tizio e Caio si siedano in due posti affiancati?

Conviene fissare il posto in cui è seduto Tizio. A questo punto le altre $n-1$ persone si possono sedere in $P_{n-1} = (n-1)!$ modi, il numero di eventi possibili. Tra questi, gli eventi favorevoli sono dati da quelli in cui Caio è a destra o a sinistra di Tizio, ad ognuno dei quali corrispondono P_{n-2} modi in cui si siedono le restanti $n-2$ persone. Quindi gli eventi favorevoli sono $2\,(n-2)!$ e la probabilità richiesta è

$$p = p(n) = \frac{2\,(n-2)!}{(n-1)!} = \frac{2}{n-1} \, .$$

Si noti che $p(3) = 1$ e che $p(n)$ è decrescente (i.e. decresce al crescere di n).

La *probabilità condizionata* di un evento A, sapendo che sia certo un evento B, è definita da

$$\mathbb{P}(A \mid B) := \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}, \qquad \mathbb{P}(B) > 0 .$$

Esempio 2.74 Un'urna contiene 3 palline bianche e 5 rosse (numerate). Estraendo due palline a caso, calcolate:

1. la probabilità che siano entrambe rosse;
2. la probabilità che siano entrambe rosse, sapendo che almeno una è rossa.

L'insieme degli eventi possibili Ω ha cardinalità $\#\Omega = C_{8,2} = \binom{8}{2} = \frac{8 \cdot 7}{2} = 28$ e detto A l'evento "entrambe le palline estratte sono rosse", abbiamo

$$\#A = C_{5,2} = \binom{5}{2} = \frac{5 \cdot 4}{2} = 10 , \quad \mathbb{P}(A) = \#A/\#\Omega = 10/28 = 5/14 .$$

Nel secondo caso, denotiamo con B l'evento "almeno una delle due palline estratte è rossa", per cui

$$\#B = C_{5,2} + C_{5,1}C_{3,1} = 10 + 5 \cdot 3 = 25 , \quad \mathbb{P}(B) = \frac{\#B}{\#\Omega} = \frac{25}{28} .$$

Pertanto, essendo $A \cap B = A$, calcoliamo la probabilità condizionata

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \frac{\mathbb{P}(A)}{\mathbb{P}(B)} = \frac{10/28}{25/28} = \frac{2}{5} .$$

Si noti che diversa cosa è dire che, avendo già estratto una pallina rossa, nell'urna ci sono 7 palline di cui 3 bianche e 4 rosse, estraendone una delle quali a caso, la probabilità che sia rossa è 4/7.

Per *eventi indipendenti*, la probabilità si calcola mediante il *prodotto* delle probabilità dei singoli eventi. Infatti, se la conoscenza che si è verificato B non cambia la probabilità che si verifichi A, allora si deve avere $\mathbb{P}(A|B) = \mathbb{P}(A)$. Quindi, supposto ancora $\mathbb{P}(B) > 0$, se A e B sono indipendenti risulta

$$\frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \mathbb{P}(A) \iff \mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B) .$$

Esempio 2.75 In una gara di lancio di una moneta, vince il primo tra Tizio e Caio che arriva a quota 5 "testa" o cinque "croce", rispettivamente. Dopo sei lanci, Tizio è a 4 punti e Caio a 2 punti. Qual è la probabilità che vinca Caio?

Al settimo lancio, Caio ha probabilità 1/2 andare sul punteggio di 4 a 3 per Tizio. Nel caso a lui favorevole, all'ottavo lancio Caio ha probabilità 1/2 di pareggiare 4 a 4. Nel caso a lui favorevole, all'ottavo lancio ha ancora probabilità 1/2 di vincere per 5 a 4. In definitiva, dopo i primi sei lanci Caio ha probabilità $(1/2)^3 = 1/8$ di vincere, mentre in tutti gli altri casi vince Tizio, che dunque ha probabilità di vittoria $1 - 1/8 = 7/8$.

Coefficienti binomiali

Ricordiamo la definizione (2.6) dei coefficienti binomiali. Vale la seguente:

Proposizione 2.76 *Per ogni $n \in \mathbb{N}$ si ha:*

1. $\binom{n}{0} = 1$ *e* $\binom{n}{n} = 1$
2. $\forall\, k$, $\binom{n}{k} = \binom{n}{n-k}$
3. $\forall\, k$, $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Il nome di coefficienti binomiali deriva dalla formula seguente, in cui si pone per convenzione $0^0 = 1$ per trattare direttamente i casi banali in cui $ab = 0$ o $a + b = 0$.

Proposizione 2.77 (Formula del binomio di Newton). *Per ogni $a, b \in \mathbb{R}$ e $n \in \mathbb{N}$ si ha:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \,. \tag{2.7}$$

Osservazione 2.78 La formula (2.7) si dimostra usando il principio di induzione e la proprietà 3. Quest'ultima permette di costruire il triangolo di Tartaglia con il quale si ricavano i coefficienti della potenza $(n+1)$-esima sapendo i coefficienti della potenza n-esima di un binomio. Notiamo inoltre che applicando (2.7) con $a = b = 1$ si ottiene la formula sulla somma della riga n-esima del triangolo di Tartaglia:

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n \qquad \forall\, n \in \mathbb{N}^+ \,.$$