

Capitolo 1

Preliminari

1.1 Elementi di logica matematica

Definizione 1.1 Una Proposizione Logica è un enunciato di cui si può dire con certezza se è vero o falso.

Si parla allora del “valore della verità” di una proposizione.

Esempio 1.1

1. “ 7 è un numero dispari ” è una Proposizione Logica Vera (V)
2. “ $3 > \sqrt{12}$ ” è una Proposizione Logica Falsa (F)
3. “ Le Porte Palatine di Torino furono costruiti dai Romani ” è una Proposizione Logica (V)
4. “ 10^{-4} ” è un numero piccolo Non è una Proposizione Logica

1.1.1 Connettivi Logici

A partire da proposizioni logiche, che indicheremo con lettere minuscole (p, q, r, \dots), si possono costruire nuove proposizioni logiche, attraverso delle operazioni che si esprimono mediante simboli detti *connettivi logici*. Il modo più semplice per definire i connettivi logici è attraverso le tavole di verità, vale a dire delle tabelle che danno i valori di verità della proposizione.

Negazione Logica $\neg p$ (si legge “non pi”). La tavola della verità è la seguente:

p	$\neg p$
V	F
F	V

Esempio 1.2 p : “ $\sqrt{2}$ è razionale”. Allora $\neg p$: “ $\sqrt{2}$ non è razionale”.

Congiunzione Logica $p \wedge q$ (si legge “p e q”): è una proposizione che è vera solo quando sia p che q sono vere. La tavola di verità di $p \wedge q$ è la seguente:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Esempio 1.3 p : “7 è razionale” (V). q : “7 è negativo” (F). Allora $p \wedge q$: “7 è razionale e negativo” (F).

Disgiunzione Logica $p \vee q$ (si legge “ p vel q ” oppure “ p o q ”): è una proposizione che è vera se almeno una delle due proposizioni è vera. La tavola di verità di $p \vee q$ è la seguente:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempio 1.4 p : “7 è razionale” (V). q : “7 è negativo” (F). Allora $p \vee q$: “7 è razionale o negativo” (V).

Implicazione Logica $p \implies q$ (si legge “ p implica q ” oppure “da p segue q ”). La tavola di verità di $p \implies q$ è la seguente:

p	q	$p \implies q$
V	V	V
V	F	F
F	V	V
F	F	V

Osserviamo che da una proposizione falsa può derivare una proposizione vera, mentre da una proposizione vera non può che seguire una proposizione vera.

Esempio 1.5 p : “Tizio sostiene l’esame di Analisi I presso il Politecnico di Torino”. q : “Tizio è studente del Politecnico”.

Se p è vera $\implies q$ è vera.

Se p è falsa (Tizio non sostiene l’esame) \implies Tizio può essere uno studente del Politecnico, ma può anche non esserlo.

Equivalenza Logica (o Biimplicazione) $p \iff q$ (si legge “ p è equivalente a q ” oppure “ p se e solo se q ” oppure “ p biimplica q ”). La tavola di verità di $p \iff q$ è la seguente:

p	q	$p \iff q$
V	V	V
V	F	F
F	V	F
F	F	V

Quando due proposizioni sono equivalenti, si possono sostituire l’una all’altra.

Proposizione 1.1 $(p \implies q) \iff (\neg p \vee q)$.

Dimostrazione. È sufficiente far vedere che le due proposizioni hanno la stessa tavola di verità:

p	q	$\neg p$	$p \implies q$	$\neg p \vee q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

□

Proposizione 1.2 $(p \implies q) \Leftrightarrow (\neg p \implies \neg q)$.

Dimostrazione. È sufficiente far vedere che le due proposizioni hanno la stessa tavola di verità:

p	q	$\neg q$	$\neg p$	$p \implies q$	$\neg q \implies \neg p$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

□

Leggi di De Morgan

$$\neg(p \wedge q) \iff \neg p \vee \neg q \quad (1.1)$$

$$\neg(p \vee q) \iff \neg p \wedge \neg q \quad (1.2)$$

Dimostrare per esercizio facendo vedere che le proposizioni hanno gli stessi valori di verità.

1.1.2 Cosa vuol dire dimostrare un teorema?

Si vuole far vedere come da una proposizione logica vera ne segua un'altra, anch'essa vera. Si vuole cioè usare la implicazione $p \implies q$, assumendo però che p sia vera.

In generale si dice che dall'ipotesi p vera segue che la tesi q è vera. Per ottenere questo risultato si possono utilizzare metodi diversi:

Dimostrazione diretta: usando l'ipotesi p e tutti i risultati precedentemente ottenuti, riusciamo a far vedere che anche la tesi q è vera. È il metodo usato nelle proposizioni precedentemente dimostrate.

Dimostrazione Contronominale. Invece di dimostrare che $p \implies q$, dimostriamo che $\neg q \implies \neg p$, cioè che se la tesi è falsa, allora anche l'ipotesi è falsa.

Esempio 1.6 Vogliamo dimostrare che dalla proposizione p : “ $n \in \mathbb{N}$ è dispari” segue q : “ n non è multiplo di 10”.

Dimostro che $\neg q$ (n è multiplo 10) $\implies \neg p$ (p è pari).

Infatti, se n è multiplo di 10, esiste $k \in \mathbb{N}$ tale che $n = 10k = 2 \cdot 5 \cdot k$. Dunque n è pari.

Questo metodo dimostrativo è un caso particolare della più generale:

Dimostrazione per Assurdo.

Caso 1 $(p \wedge \neg q) \implies \neg p$

Caso 2 $(p \wedge \neg q) \implies (r \wedge \neg r)$

Nel caso 1, assumendo che contemporaneamente sia vera p e falsa q , ne segue la *contraddizione* che p sia anche falsa.

Nel caso 2, assumendo che sia vera p e falsa q , ne segue una contraddizione $(r \wedge \neg r)$, cioè una proposizione sempre falsa.

Esercizio 1.1 1. Dimostrare che $(r \wedge \neg r)$ è sempre falsa.

2. Dimostrare che

$$[(p \wedge \neg q) \implies \neg p] \iff (p \implies q).$$

1.1.3 Predicati logici e quantificatori

Un predicato logico è una proposizione logica che dipende da una o più variabili, che appartengono ad insiemi specificati. Lo indicheremo con $p(x, y, \dots)$ -

Esempi 1.1 1. $p(x) = \{x \in \mathbb{N} \text{ ed è dispari}\}$. $p(5)$ è vero, $p(6)$ è falso.

2. $p(x, y) = \{x, y \in \mathbb{N} \text{ soluzioni di } 2x - y = 1\}$. $p(1, 1)$ è vero, $p(0, 0)$ è falso.

Dato un predicato $p(x)$, ci si chiede per quali x in un insieme dato, $p(x)$ è vero. È particolarmente importante distinguere se è vero “per tutti gli elementi di un insieme” o se ne esiste almeno uno per cui $p(x)$ è vero.

Quantificatore Universale \forall : $\forall x, p(x)$ significa che per tutte le x , $p(x)$ è vero.

Quantificatore esistenziale \exists : $\exists x, p(x)$ significa che esiste (almeno una) x per cui $p(x)$ è vero. Talvolta si usa $\exists! x p(x)$, per dire che esiste un unico x per cui $p(x)$ è vera.

Esempio 1.7 $X = \text{Studenti iscritti al Politecnico}$, $p(x) = x$ è iscritto al corso di laurea di Matematica per l'ingegneria.

- È vero che: $\exists x \in X p(x)$.
- Invece è falso $\forall x \in X p(x)$. Infatti esistono studenti iscritti ad altri corsi di laurea.

Ci interessa adesso capire come si negano le proposizioni precedenti:

$$\neg(\forall x p(x)) \iff (\exists x \neg p(x))$$

$$\neg(\exists x p(x)) \iff (\forall x \neg p(x))$$

Nei predicati logici con più di una variabile è importante la sequenza dei quantificatori ed il loro ordine; alcuni possono essere scambiati, altri no. In particolare:

a) $\forall x \forall y p(x, y) \iff \forall y \forall x p(x, y)$

b) $\exists x \exists y p(x, y) \iff \exists y \exists x p(x, y)$

Invece: $\forall x \exists y p(x, y)$ e $\exists y \forall x p(x, y)$ hanno significati completamente diversi.

Esempio 1.8 $X = \{\text{Studenti iscritti al Politecnico}\}$, $p(x, y) = x$ e y sono compagni di corso.

La proposizione “ $\forall x \in X \exists y \in X, p(x, y)$ ” è vera.

Invece “ $\exists y \in X \forall x \in X, p(x, y)$ ” è falsa.

Esempio 1.9 $X = \mathbb{N}$, $p(x, y) = x \geq y$, $x, y \in \mathbb{N}$.

“ $\forall x \in X \exists y \in X, p(x, y)$ ” è vera (basti pensare ad $y = 0$).

Invece “ $\exists x \in X \forall y \in X, p(x, y)$ ” è falso (basti pensare $y = x + 1 > x$).

Attenzione! ci sono altre due proposizioni possibili:

“ $\forall y \in X \exists x \in X, p(x, y)$ ”, vera (basti pensare $x = y + 1$);

“ $\exists y \in X \forall x \in X, p(x, y)$ ”, vera (basti pensare $y = 0$);

Da sottolineare che le quattro proposizioni hanno significati diversi.

Vediamo ora come si negano proposizioni analoghe alle precedenti.

$$\neg(\forall x \exists y p(x, y)) \iff \exists x \forall y \neg p(x, y),$$

cioè dire che “è falso che per ogni x esiste y per cui $p(x, y)$ è vero” è equivalente a dire che “esiste almeno un x tale che $p(x, y)$ è falso per ogni y ”.

Esempio 1.10 $x, y \in \mathbb{N}$, $\forall x \exists y, x > y$ è falsa. Infatti $\exists x = 0$ tale che tutti $y \in \mathbb{N}$ sono tali che $x \leq y$.

Invece:

$$\neg(\exists x \forall y p(x, y)) \iff \forall x \exists y \neg p(x, y).$$

Esempio 1.11 $x, y \in \mathbb{N}$, $\exists x, \forall y, y \leq x$ è falsa (esiste un numero naturale più grande di tutti). Infatti $\forall x \in \mathbb{N} \exists y = x + 1$ t.c. $y > x$.

1.2 Insiemi

Un insieme è definito dai suoi elementi.

Definizione 1.2 Se x è un elemento di un insieme X , si dice che x appartiene ad X , e si scrive $x \in X$.

Se x non è un elemento di X , si scrive $x \notin X$.

Un insieme che non possiede elementi si dice insieme vuoto e si denota con \emptyset .

Esempio 1.1 Detto \mathbb{N} l'insieme dei numeri naturali (cioè dei numeri interi maggiori o uguali di 0), avremo che $1 \in \mathbb{N}$, $\frac{1}{2} \notin \mathbb{N}$.

Gli insiemi possono essere rappresentati in vari modi: di solito un insieme si denota con una lettera maiuscola, mentre si indicano con una lettera minuscola i suoi elementi. Si può poi rappresentare un insieme elencando i suoi elementi; per esempio $\{1, 2, 3\}$ è l'insieme che contiene i numeri 1, 2 e 3. L'insieme $\{1\}$ è l'insieme che contiene il solo elemento 1. In questo caso si scriverà $1 \in \{1\}$.

Se un insieme contiene infiniti elementi, è chiaro che non possono essere descritti tutti. Dato un predicato $p(x)$, se vogliamo descrivere l'insieme degli elementi di un insieme X per cui il predicato è vero, si scrive $\{x \in X : p(x)\}$ oppure $\{x \in X \mid p(x)\}$.

Esempio 1.2

1. L'insieme dei numeri naturali, pari può essere rappresentato come

$$A = \{x \in \mathbb{N} : x \text{ è pari}\} = \{x \in \mathbb{N} : x = 2k, k \in \mathbb{N}\}.$$

2. L'insieme dei numeri naturali minori o uguali a 4 può essere rappresentato come

$$B = \{x \in \mathbb{N} : x \leq 4\} = \{0, 1, 2, 3, 4\}.$$

Definizione 1.3 Due insiemi non vuoti X e Y sono uguali se e solo se contengono gli stessi elementi, cioè

$$(X = Y) \iff (x \in X \iff x \in Y)$$

Definizione 1.4 Si dice che un insieme X è un sottoinsieme di Y , e si scrive $X \subseteq Y$ se tutti gli elementi di X sono elementi di Y , cioè

$$(X \subseteq Y) \iff (x \in X \implies x \in Y).$$

In questo caso si dice anche che X è incluso in Y .

Nel caso in cui $X \subseteq Y$ ed esiste almeno un elemento di Y che non è anche elemento di X (e dunque i due insiemi non sono uguali) si scrive $X \subsetneq Y$, cioè

$$(X \subsetneq Y) \iff [(x \in X \implies x \in Y) \wedge (\exists y \in Y \wedge y \notin X)]$$

si dice che X è un sottoinsieme proprio di Y .

Esempio 1.3

1. Detto X l'insieme dei numeri naturali pari, si ha che $X \subsetneq \mathbb{N}$.
2. Per ogni insieme X , si ha che $X \subseteq X$ e $\emptyset \subseteq X$.

Definizione 1.5 Dato un insieme X , Si definisce insieme delle parti di X , e si denota con $\mathcal{P}(X)$ o con 2^X l'insieme di tutti i sottoinsiemi di X , compreso l'insieme vuoto \emptyset e l'insieme stesso X .

È facile provare che X è finito e contiene n elementi (si dice allora che X ha cardinalità n), l'insieme delle parti di X contiene 2^n elementi.

Esempio 1.4 Sia $X = \{1, 2, 3\}$. Allora

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}$$

che ha $2^3 = 8$ elementi.

Definizione 1.6 Sia X un insieme e $A \subseteq X$. Si dice complementare di A in X e si denota con $\mathcal{C}_X(A)$ o con $X \setminus A$ l'insieme degli elementi di X che non appartengono ad A , dunque

$$x \in \mathcal{C}_X(A) = X \setminus A \iff x \notin A.$$

Esempio 1.5

1. $\mathcal{C}_X(\emptyset) = X$ e $\mathcal{C}_X(X) = \emptyset$.
2. $A = \{x \in \mathbb{N} : x \text{ è pari}\} \implies \mathcal{C}_{\mathbb{N}}(A) = \{x \in \mathbb{N} : x \text{ è dispari}\}.$

1.2.1 Operazioni fra insiemi

Definizione 1.7 Siano dati due insiemi X e Y .

1. Si dice intersezione di X e Y e si denota con $X \cap Y$ l'insieme degli elementi che appartengono sia a X che a Y . Diremo quindi che

$$x \in X \cap Y \iff x \in X \wedge x \in Y.$$

2. Si dice unione di X e Y e si denota con $X \cup Y$ l'insieme degli elementi che appartengono a X o a Y (o a entrambi). Diremo quindi che

$$x \in X \cup Y \iff x \in X \vee x \in Y.$$

3. Si dice che due insiemi sono disgiunti se $X \cap Y = \emptyset$, cioè se i due insiemi non hanno elementi in comune.

Esercizio 1.1 Verificare che, per ogni terna di insiemi X , Y e Z valgono le seguenti proprietà:

1. (a) L'intersezione è commutativa: $X \cap Y = Y \cap X$
 (b) L'intersezione è associativa: $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
 (c) $X \cap \emptyset = \emptyset$
2. (a) L'unione è commutativa: $X \cup Y = Y \cup X$
 (b) L'unione è associativa: $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
 (c) Esiste l'elemento neutro: $X \cup \emptyset = X$

3. Valgono inoltre la proprietà distributiva dell'unione rispetto all'intersezione e dell'intersezione rispetto all'unione:

$$(a) (X \cap Y) \cup Z = (X \cap Z) \cup (Y \cap Z)$$

$$(b) (X \cup Y) \cap Z = (X \cap Z) \cap (Y \cap Z)$$

Definizione 1.8 1. Si dice differenza insiemistica di X e Y e si denota con $X \setminus Y$ l'insieme degli elementi di X che non appartengono a Y , cioè

$$x \in X \setminus Y \iff x \in X \wedge x \notin Y.$$

2. Si definisce differenza simmetrica di X e Y e si denota con $X \Delta Y$ l'insieme degli elementi che stanno in X ma non in Y unito all'insieme degli elementi che stanno in Y ma non in X , cioè

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X).$$

Osserviamo che la differenza insiemistica non è un'operazione commutativa, infatti esistono insiemi tali che $X \setminus Y \neq Y \setminus X$. Per esempio, se $X = \{0, 1, 2, 3\}$ e $Y = \{2, 3, 6, 8, 9\}$, si ha: $X \setminus Y = \{0, 1\}$ e $Y \setminus X = \{6, 8, 9\}$.

Esercizio 1.2 Dimostrare che, per ogni coppia di insiemi X e Y è vero che

1. $X \setminus Y = X \setminus (X \cap Y) = \mathcal{C}_X(X \cap Y)$.
2. $(X \setminus Y) \cap (Y \setminus X) = \emptyset$.
3. $X \Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$.

Nelle definizioni precedenti abbiamo visto che alle operazioni di complementare, intersezione e unione corrispondono rispettivamente i connettivi logici non, et e vel. Vediamo così che anche le Leggi di De Morgan hanno un corrispettivo insiemistico.

Teorema 1.1 (Leggi di De Morgan) Indichiamo con p e q due proposizioni logiche e con X e Y due sottoinsiemi di un insieme Z . È vero che

Logica	Insiemistica
$\neg(p \wedge q) \iff \neg p \vee \neg q$	$\mathcal{C}_Z(X \cap Y) = (\mathcal{C}_Z X) \cup (\mathcal{C}_Z Y)$
$\neg(p \vee q) \iff \neg p \wedge \neg q$	$\mathcal{C}_Z(X \cup Y) = (\mathcal{C}_Z X) \cap (\mathcal{C}_Z Y)$

Definiamo un'ultima operazione, che è ispirata alla rappresentazione cartesiana dei punti nel piano e nello spazio. Come è ben noto, per rappresentare un punto nel piano, possiamo ricorrere ad un sistema di assi cartesiane, cioè si considerano due retti perpendicolari, su ciascuna delle quali è fissata un'unità di misura e un orientamento. Lo 0 è fissato nell'intersezione delle due rette. Ogni punto P del piano può così essere identificato attraverso una coppia di numeri (a, b) , dove a è la coordinata della proiezione ortogonale di P sull'asse orizzontale e b è la coordinata della proiezione ortogonale di P sull'asse verticale. È chiaro che, se $a \neq b$, le coppie (a, b) e (b, a) rappresentano due punti diversi del piano (vedi figura ??). Diciamo allora che (a, b) è una coppia ordinata.

Vediamo adesso una definizione molto più generale, che riguarda insiemi qualsiasi.

Definizione 1.9

1. Dati due insiemi X e Y , si dice prodotto cartesiano di X e Y , e si scrive $X \times Y$, l'insieme delle coppie ordinate (x, y) , con $x \in X$ e $y \in Y$:

$$X \times Y = \{(x, y) : x \in X \wedge y \in Y\}.$$

2. Dato un numero finito di insiemi X_1, \dots, X_n , si dice prodotto cartesiano degli n insiemi, che si indica con $X_1 \times X_2 \times \dots \times X_n$, l'insieme delle n -uple ordinate (x_1, x_2, \dots, x_n) , con $x_i \in X_i$ ($i = 1, 2, \dots, n$).

Quando $X_1 = X_2 = \dots = X_n = X$, si scrive anche X^n . Per esempio, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ rappresenta il piano, \mathbb{R}^3 rappresenta lo spazio tridimensionale, \mathbb{R}^4 può essere interpretato come lo spazio-tempo.

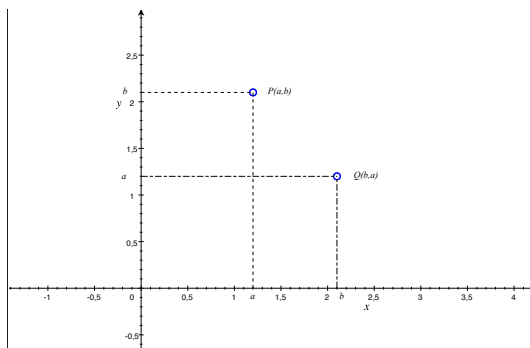


Figura 1.1: Piano cartesiano

1.3 Insiemi Numerici

In questo corso ci occuperemo essenzialmente di insiemi numerici. Facciamo qui una breve illustrazione degli insiemi numerici di cui faremo uso.

1.3.1 Numeri naturali

Si indica con \mathbb{N} l'insieme dei numeri interi maggiori o uguali di 0. Nel 1889 Giuseppe Peano, un matematico torinese, definì i numeri naturali mediante cinque assiomi.

Definizione 1.10 *L'insieme dei numeri naturali \mathbb{N} è un insieme che soddisfa i seguenti assiomi:*

1. $0 \in \mathbb{N}$ (e dunque \mathbb{N} non è un insieme vuoto)
2. Per ogni $n \in \mathbb{N}$, esiste un unico elemento $\mathcal{S}(n) \in \mathbb{N}$, detto *successore di n* (\mathcal{S} è una funzione da \mathbb{N} in \mathbb{N})
3. Per ogni $n \in \mathbb{N}$, $\mathcal{S}(n) \neq 0$
4. Se $n_1 \neq n_2$, allora $\mathcal{S}(n_1) \neq \mathcal{S}(n_2)$ (\mathcal{S} è una funzione iniettiva)
5. Se U è un sottoinsieme di \mathbb{N} tale che

$$(a) \ 0 \in U$$

$$(b) \ \text{se } n \in U \implies \mathcal{S}(n) \in U$$

allora $U = \mathbb{N}$.

Attraverso la funzione successore, possiamo scrivere $\mathcal{S}(0) = 0 + 1$, $\mathcal{S}(1) = 1 + 1 = 2$, e in generale $\mathcal{S}(n) = n + 1$.

Proposizione 1.3 Principio di induzione

Sia $\mathcal{P}(n)$ un predicato logico, definito per tutti gli $n \in \mathbb{N}$. Se

1. $\mathcal{P}(0)$ è vero e
2. per ogni $n \in \mathbb{N}$, $\mathcal{P}(n) \implies \mathcal{P}(n+1)$

allora $\mathcal{P}(n)$ è vero, per ogni $n \in \mathbb{N}$.

Dimostrazione. Basta applicare l'assioma 5 della definizione dei numeri naturali all'insieme $U = \{n : n \text{ è vero}\}$. Per ipotesi, $0 \in U$. Inoltre, se $n \in U$, allora $n+1 \in U$, e dunque $U = \mathbb{N}$ \square

Osserviamo che se nelle ipotesi del principio di induzione sostituiamo a 0 un qualsiasi $n_0 \in \mathbb{N}$, il predicato risulta vero per tutti gli $n \geq n_0$.

Esempi 1.2

1. Vogliamo dimostrare che

$$\mathcal{P}(n) : \quad 0 + 1 + 2 + \cdots + n = \sum_{k=1}^n k = \frac{n(n+1)}{2}$$

è vero per ogni $n \in \mathbb{N}$. Osserviamo che $\mathcal{P}(0)$ è vero, dato che $0 = \frac{0(0+1)}{2}$. Inoltre, se assumiamo che $\mathcal{P}(n-1)$ sia vera, otteniamo che:

$$\mathcal{P}(n) : \quad (1 + 2 + \cdots + (n-1)) + n = \frac{n(n-1)}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n(n+1)}{2}.$$

2. Vogliamo dimostrare che

$$\mathcal{P}(n) = \quad 0 + 1^3 + 2^3 + \cdots + n^3 = \sum_{k=1}^n k^3 = \left[\frac{n(n+1)}{2} \right]^2 = \frac{n^2(n+1)^2}{4}.$$

è vero per ogni $n \in \mathbb{N}$. Anche in questo caso $\mathcal{P}(0)$ è vero, infatti $0^3 = \left[\frac{0(0+1)}{2} \right]^2 = 0$.

Assumiamo che $\mathcal{P}(n-1)$ sia vero. Poiché $\mathcal{P}(n) - \mathcal{P}(n-1) = n^3$, basta dimostrare che

$$\frac{n^2(n+1)^2}{4} - \mathcal{P}(n-1) = \frac{n^2(n+1)^2}{4} - \frac{n^2(n-1)^2}{4} = n^3$$

per ottenere che se $\mathcal{P}(n-1)$, allora $\mathcal{P}(n)$ è vero. In effetti

$$\frac{n^2(n+1)^2}{4} - \frac{n^2(n-1)^2}{4} = \frac{n^2(n+1)^2 - (n-1)^2}{4} = \frac{n^2 \cdot 4n}{4} = n^3.$$

3. Vogliamo dimostrare che

$$\mathcal{P}(n) = 1 + 3 + \cdots + (2n-1) = \sum_{k=1}^n (2k-1) = n^2$$

è vero per ogni intero $n > 0$. In questo caso è facile osservare che: $\mathcal{P}(1) = 1 = 1^2$. Osserviamo, anche se non è necessario, che $\mathcal{P}(2) = 1 + 3 = 4 = 2^2$ e che $\mathcal{P}(3) = 1 + 3 + 5 = 9 = 3^2$. Assumiamo ora che sia vero che $\mathcal{P}(n) = 1 + \cdots + (2n-1) = n^2$. Allora

$$\mathcal{P}(n+1) = 1 + \cdots + (2n-1) + (2(n+1)-1) = n^2 + (2n+1) = (n+1)^2.$$

Abbiamo così dimostrato che il predicato è vero per ogni intero $n > 0$.

Sui numeri naturali si definiscono due operazioni *binarie*:

Definizione 1.11 *La somma è una funzione*

$$\begin{aligned} + : \quad \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (n, m) &\longmapsto n + m \end{aligned}$$

tale che

1. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, n + m = m + n$, cioè la somma è commutativa
2. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, \forall p \in \mathbb{N} (n + m) + p = n + (m + p)$, cioè la somma è associativa
3. $\exists k \in \mathbb{N}, \forall n \in \mathbb{N}, n + k = k + n = n$, cioè la somma ammette elemento neutro, $k = 0$.

Definizione 1.12 Il prodotto è una funzione

$$\begin{aligned} \cdot : \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (n, m) &\longmapsto n \cdot m \end{aligned}$$

tale che

1. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, n \cdot m = m \cdot n$, cioè il prodotto è commutativo
2. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, \forall p \in \mathbb{N} (n \cdot m) \cdot p = n \cdot (m \cdot p)$, cioè il prodotto è associativo
3. $\exists k \in \mathbb{N}, \forall n \in \mathbb{N} \setminus \{0\}, n \cdot k = k \cdot n = n$, cioè il prodotto ammette elemento neutro, $k = 1$.

Si può dimostrare inoltre

Proposizione 1.1

1. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, \forall p \in \mathbb{N} (n + m) \cdot p = n \cdot p + m \cdot p$, cioè vale la proprietà distributiva della somma rispetto al prodotto
2. $\forall n \in \mathbb{N}, n \cdot 0 = 0$, cioè vale la legge di annullamento del prodotto.

Sappiamo inoltre che ogni intero ammette rappresentazione in base 10, cioè ogni numero naturale n può essere scritto nella forma

$$n = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_1 \cdot 10^1 + c_0 \cdot 10^0 = \sum_{j=0}^k c_j \cdot 10^j.$$

Fissata la posizione dello 0 e dell'1 su una retta, è possibile rappresentare ogni numero naturale sulla retta stessa.

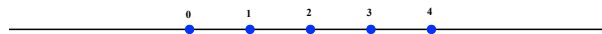


Figura 1.2: Rappresentazione dei numeri naturali sulla retta

1.3.2 Numeri relativi

In molteplici occasioni ci si accorge che i numeri naturali non sono sufficienti a descrivere un fenomeno. Dal punto di vista algebrico, ci si accorge subito che nell'insieme dei numeri naturali non vale la proprietà che, per ogni $n \in \mathbb{N}$, esiste $n' \in \mathbb{N}$ tale che $n + n' = 0$. Affinché questa proprietà sia valida è necessario ampliare l'insieme dei numeri naturali, in modo da includere, per ogni $n \in \mathbb{N}$, il suo *opposto*, cioè quel numero che soddisfa la proprietà sopra illustrata. Otteniamo così l'insieme dei *numeri relativi*, che si indica con \mathbb{Z} :

$$\mathbb{Z} = \{0, +1, -1, +1, -2, \dots\}.$$

Su questo insieme si possono estendere la somma e il prodotto definiti in \mathbb{N} , con le stesse proprietà, a cui si aggiunge l'esistenza dell'inverso additivo, vale a dire che

$$\forall n \in \mathbb{Z} \quad \exists n' \in \mathbb{Z} \quad n + n' = 0.$$

n' si indica con $-n$ e prende il nome di *opposto* di n .

Si dice allora che \mathbb{Z} , con l'operazione di somma, ha una struttura di gruppo abeliano.

Com'è noto, anche i numeri relativi possono essere rappresentati sulla retta.

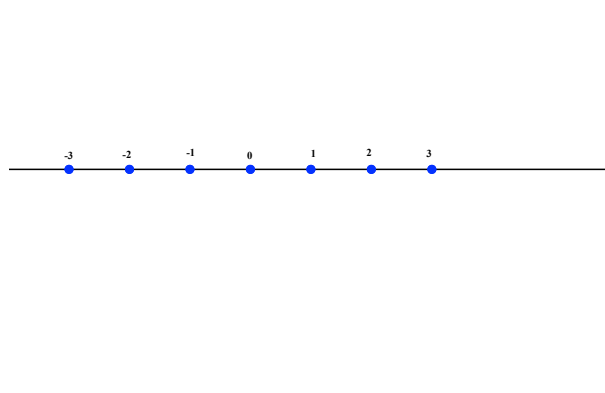


Figura 1.3: Rappresentazione dei numeri relativi sulla retta

1.3.3 Numeri razionali

Anche l'insieme dei numeri relativi non è sufficiente, né da un punto di vista algebrico (in \mathbb{Z} non c'è l'inverso moltiplicativo), né da un punto di vista geometrico (in \mathbb{Z} non è possibile rappresentare le parti di un intero). Per questa ragione, si introducono i numeri razionali, la cui definizione è più complessa delle precedenti. Si considerano innanzitutto le coppie ordinate

$$(p, q) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\}),$$

che indichiamo con $\frac{p}{q}$. Si introduce poi una relazione di equivalenza \sim in modo che $\frac{p}{q}$ e $\frac{r}{s}$ sono equivalenti se esiste $k, h \in \mathbb{N}$ tale che $hr = kp$ e $hs = kq$ (o viceversa). Diremo poi che identifichiamo (cioè consideriamo uguali) due coppie equivalenti.

Per esempio, $\frac{4}{6} = \frac{2}{3}$, dato che $3 \cdot 4 = 2 \cdot 6$ e $3 \cdot 6 = 2 \cdot 9$. Come ben noto, si dice che un numero razionale $\frac{p}{q}$ è *ridotto ai minimi termini* se p e q non hanno fattori comuni.

Tutte le coppie equivalenti fra loro fanno parte della stessa classe di equivalenza, e sono considerate uguali fra loro. L'insieme delle classi di equivalenza è detto in generale insieme quoziente; nel nostro caso, l'insieme quoziente è detto *insieme dei numeri razionali* e viene indicato con \mathbb{Q} .

Le coppie $\frac{p}{1}$ vengono identificate con il numero relativo p , in modo che $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.

Con il metodo visto alle scuole medie, si estendono a \mathbb{Q} le operazioni di somma e prodotto, che mantengono tutte le proprietà precedenti. Inoltre, su \mathbb{Q} esiste anche l'inverso moltiplicativo, vale a dire che

$$\forall x \in \mathbb{Q} \setminus \{0\} \quad \exists y \in \mathbb{Q} \quad \text{tale che} \quad x \cdot y = 1.$$

Il numero y è detto *reciproco* di x .

Anche i numeri razionali ammettono una rappresentazione in base 10, ma in questo caso possono avere una “parte decimale”, vale a dire che, se $x \in \mathbb{Q}$, si ha:

$$x = c_k 10^k + \dots + c_1 10^1 + c_0 10^0 + c_{-1} 10^{-1} + \dots + c_h 10^{-h} + \dots$$

Per esempio

$$\begin{aligned} \frac{1381}{1000} &= 1,381 = 1 \cdot 10^0 + 3 \cdot 10^{-1} + 8 \cdot 10^{-2} + 1 \cdot 10^{-3} \\ \frac{1}{3} &= 0,\bar{3} = 3 \cdot 10^{-1} + 3 \cdot 10^{-2} + \dots \end{aligned}$$

Nel primo caso la parte che segue la virgola (cioè la parte decimale) ha un numero finito di termini, mentre nel secondo la parte decimale contiene infiniti termini (è illimitata), ma con una cifra che si ripete sempre uguale.

Si può dimostrare che i numeri razionali possono avere parte decimale limitata oppure parte decimale illimitata e periodica, vale a dire che da un certo punto in poi ci sono n cifre che si ripetono sempre uguali.

I numeri razionali possono essere agevolmente rappresentati sulla retta, in questo modo:

- Se $x = \frac{p}{q}$ e $p < q$, si suddivide il segmento di vertici 0 e 1 in q parti uguali, e di queste si considerano le prime p . Il punto ottenuto rappresenta il numero x .
- Se $x = \frac{p}{q}$ e $p = q$, allora $x = 1$
- Se $x = \frac{p}{q}$ e $p > q$, per l'algoritmo della divisione sappiamo che esistono un numero $k \in \mathbb{Z}$ e un numero $r \in \mathbb{N}$, con $0 \leq r < q$ tale che $p = kq + r$. Ne segue che $\frac{p}{q} = \frac{kq + r}{q} = k + \frac{r}{q}$.
Dunque, per rappresentare il punto x sulla retta aggiungiamo al segmento di vertici 0 e p il segmento di lunghezza $\frac{r}{q}$, ottenuto con il metodo illustrato in precedenza.

1.3.4 Ordinamento in \mathbb{Q}

Sull'insieme dei numeri razionali è possibile definire una relazione d'ordine, nel modo seguente:

Definizione 1.13 Dato $\frac{p}{q} \in \mathbb{Q}$, con $p \in \mathbb{Z}$ e $q \in \mathbb{N} \setminus \{0\}$, si dice che

- $\frac{p}{q} \geq 0$ se $p \geq 0$

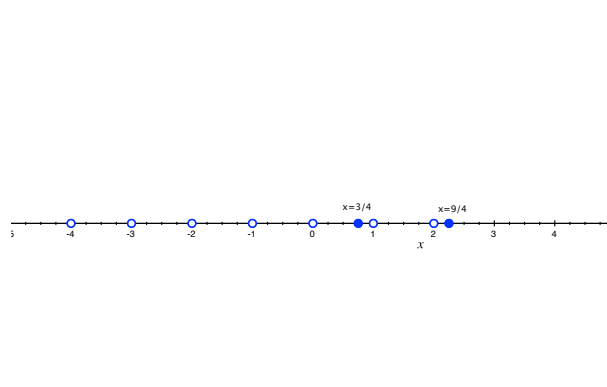


Figura 1.4: Rappresentazione dei numeri razionali sulla retta

- $\frac{p}{q} < 0$ se $p < 0$

Dati $x, y \in \mathbb{Q}$, diciamo che $x \leq y$ se $x - y \leq 0$.

Se $x = \frac{p}{q}$ e $y = \frac{r}{s}$, per stabilire quali dei due numeri è più grande si scrive $\frac{p}{q} = \frac{ps}{qs}$ e $\frac{r}{s} = \frac{rq}{sq}$.
Abbiamo allora che

$$\frac{p}{q} \leq \frac{r}{s} \iff \frac{ps}{qs} \leq \frac{rq}{sq} \iff ps \leq rq.$$

Proposizione 1.2 La relazione di minore o uguale appena introdotta soddisfa le seguenti proprietà:

1. Proprietà riflessiva: $\forall x \in \mathbb{Q}, x \leq x$
2. Proprietà antisimmetrica: Dati $x, y \in \mathbb{Q}, x \leq y \wedge y \leq x \implies x = y$.
3. Proprietà transitiva: Dati $x, y, z \in \mathbb{Q}, x \leq y \wedge y \leq z \implies x \leq z$.
4. Inoltre, $\forall x, y \in \mathbb{Q} \quad x \leq y \vee y \leq x$, cioè in ogni coppia di numeri razionali, uno dei due è minore o uguale all'altro.

Ogni relazione che soddisfa le prime tre proprietà viene detta *relazione d'ordine*. Per esempio la relazione di inclusione fra insiemi è una relazione d'ordine. Se poi la relazione d'ordine soddisfa anche la quarta proprietà, si ha una *relazione d'ordine totale*. La relazione di inclusione non è una relazione d'ordine totale.

Inoltre,

Proposizione 1.3 Sono dati $x, y, z \in \mathbb{Q}$.

1. Se $x \leq y \implies x + z \leq y + z$.
2. (a) Se $x \leq y \wedge z \geq 0 \implies xz \leq yz$
(b) Se $x \leq y \wedge z \leq 0 \implies xz \geq yz$.

1.3.5 Numeri reali

Ci si accorge ben presto che non a tutti i punti della retta può essere associato un numero razionale. Mostriamo per esempio che la lunghezza della diagonale del quadrato di lato 1 non è un numero razionale.

Lemma 1.1 Sia $n \in \mathbb{N}$. Se n^2 è pari, allora n è pari.

Dimostrazione. Utilizziamo la dimostrazione contronominale, cioè mostriamo che se n non è pari (cioè è dispari), allora n^2 è dispari.

Se n è dispari, esiste $k \in \mathbb{N}$ tale che $n = 2k + 1$. Allora

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

cioè n è il successivo di un numero pari, e dunque è un numero dispari. \square

Proposizione 1.4 Sia $x = \sqrt{2}$, cioè quel numero positivo tale che $x^2 = 2$. Allora $\sqrt{2} \notin \mathbb{Q}$.

Dimostrazione. In questo caso utilizziamo la dimostrazione per assurdo, e dunque assumiamo contemporaneamente vera l'ipotesi e falsa la tesi.

Supponiamo quindi che x sia un numero razionale: esistono quindi $p, q \in \mathbb{N}$, privi di fattori comuni, tali che

$$x = \frac{p}{q} \implies \frac{p^2}{q^2} = 2 \implies p^2 = 2q^2.$$

Ne segue che p^2 è pari, e dunque per il lemma (??), anche p è pari, cioè esiste $k \in \mathbb{N}$ tale che $p = 2k$. Dunque

$$p^2 = 4k^2 = 2q^2 \implies q^2 = 2k^2,$$

e quindi anche q è pari. Abbiamo così ottenuto una contraddizione, perchè avevamo supposto che p e q non avessero fattori in comune. \square

Dal punto di vista geometrico, $\sqrt{2}$ è la lunghezza della diagonale di un quadrato di lato 1. Questo segmento può essere riportato sulla retta reale usando il compasso (vedi fig. (??)). Dunque, a non tutti i punti della retta reale è possibile assegnare una coordinata razionale.

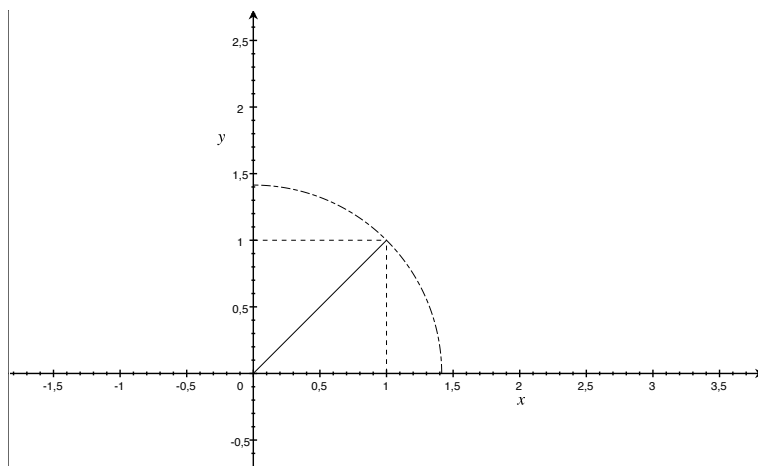


Figura 1.5: $\sqrt{2}$

Dal punto di vista algebrico invece, quanto abbiamo così dimostrato ci dice che non sempre è possibile trovare soluzioni razionali all'equazione $x^2 = a$, con $a \in \mathbb{Q}, a \geq 0$.

Risulta quindi necessario definire un'estensione dell'insieme dei numeri razionali.

Definizione 1.14 Si dice insieme dei numeri reali, che si denota con \mathbb{R} , l'insieme che soddisfa le seguenti proprietà:

1. Si estendono ad \mathbb{R} le operazioni di somma e di prodotto, che soddisfano ancora le proprietà che esse soddisfano in \mathbb{Q} .
2. Si estende ad \mathbb{R} la relazione d'ordine totale \leq .
3. Vale l'assioma di completezza, cioè:

Per ogni coppia di sottoinsiemi $A \subseteq \mathbb{R}$ e $B \subseteq \mathbb{R}$ tali che

- (a) $A \neq \emptyset \quad \wedge \quad B \neq \emptyset$
- (b) $A \cup B = \mathbb{R}$
- (c) $\forall a \in A \quad \wedge \quad \forall b \in B, \quad a \leq b$

esiste $z \in \mathbb{R}$ tale che $\forall a \in A \quad \wedge \quad \forall b \in B, \quad a \leq z \leq b$.

Il numero z viene detto elemento separatore di A e B .

Osserviamo che dall'assioma di completezza segue che:

- ad ogni punto P sulla retta posso assegnare una coordinata $x \in \mathbb{R}$;
- ad ogni $x \in \mathbb{R}$ corrisponde un punto P sulla retta,

cioè c'è una corrispondenza biunivoca fra i numeri reali e la retta, una volta stabilita la posizione di 0 e 1 sulla retta stessa. Per questo si parla spesso di “retta reale”.

Anche i numeri reali ammettono una rappresentazione decimale: se $x \in \mathbb{R} \setminus \mathbb{Q}$, la sua parte decimale è illimitata e non periodica.

Vale la

Proposizione 1.5 (Proprietà archimedeica dei numeri reali)

Per ogni $a \in \mathbb{R}$, $b \in \mathbb{R}$, con $a > 0$, $b > 0$, esiste $n \in \mathbb{N}$ tale che $na > b$.

Questa proposizione ci dice che, anche se $a < b$, posso trovare n tale che, sommando a con se stesso un numero n di volte si ottiene un numero $na > b$.

Corollario 1.1

1. Per ogni $a \in \mathbb{R}$, $a > 0$, esiste $n \in \mathbb{N}$ tale che $na > 1$
2. Per ogni $a \in \mathbb{R}$, $a > 0$, esiste $n \in \mathbb{N}$ tale che $a > \frac{1}{n}$
3. Per ogni $b \in \mathbb{R}$, $b > 0$, esiste $n \in \mathbb{N}$ tale che $n > b$

Nelle prime due proposizioni si applica la Proprietà archimedeica (??) con $b = 1$, mentre nella terza si pone $a = 1$.

Vale inoltre questa importante proprietà:

Teorema 1.1 Densità di \mathbb{Q} in \mathbb{R} Per ogni $x, y \in \mathbb{R}$, con $x < y$, esiste $q \in \mathbb{Q}$ tale che $x < q < y$.

Dimostrazione. Per la Proprietà archimedeica, dato che $y - x > 0$, esiste $n \in \mathbb{N} \setminus \{0\}$ tale che $n(y - x) = ny - nx > 1$.

Osserviamo inoltre che esiste $m \in \mathbb{N}$ tale che $m - 1 \leq nx < m$. Allora:

$$nx < m = (m - 1) + 1 < (m - 1) + (ny - nx) < nx + ny - nx = ny \quad \implies \quad nx < m < ny.$$

Dividendo per $n > 0$ otteniamo che il numero razionale $q = \frac{m}{n}$ è tale che

$$x < \frac{m}{n} < y.$$

Vedremo in seguito che il numero $m - 1$ viene detto *parte intera* di nx , e si indica con $[nx]$. \square

Possiamo avere un'idea della dimostrazione anche pensando alla rappresentazione decimale dei numeri reali. Indicando con c_0 la parte di x che precede la virgola si ha $x = c_0, c_{-1}c_{-2} \dots c_{-n} \dots$ e, analogamente, $y = d_0, d_{-1}d_{-2} \dots d_{-n} \dots$. Affinché x sia minore di y , deve esistere un n tale che $c_n < d_n$. Ne segue che il numero razionale $q = c_0, c_{-1}c_{-2} \dots c_{-n-1}d_n$ risulta essere tale che $x < q < y$.

1.3.6 Sottoinsiemi di \mathbb{R}

Definizione 1.1 Dati due numeri reali a, b , con $a < b$, si definiscono i sottoinsiemi, detti intervalli:

- Intervallo chiuso di estremi a e b : $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- Intervallo aperto di estremi a e b : $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- Intervallo di estremi a e b : $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$; intervallo aperto a destra e chiuso a sinistra (o semiaperto)
- Intervallo di estremi a e b : $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$; intervallo aperto a sinistra e chiuso a destra (o semiaperto)

Si definiscono inoltre le semirette (che si considerano particolari tipi di intervalli):

- Semiretta chiusa di estremo (sinistro) a : $[a, +\infty) = \{x \in \mathbb{R} : a \leq x\}$
- Semiretta aperta di estremo (sinistro) a : $(a, +\infty) = \{x \in \mathbb{R} : a < x\}$
- Semiretta chiusa di estremo (destro) a : $(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$
- Semiretta aperta di estremo (destro) a : $(-\infty, a) = \{x \in \mathbb{R} : x < a\}$

Osserviamo che i simboli $-\infty$ e $+\infty$ non rappresentano dei numeri reali!

Definizione 1.2 Si dice valore assoluto o modulo di un numero reale il numero non-negativo

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

Geometricamente, se al numero x corrisponde un punto P sulla retta, $|x|$ rappresenta la distanza del punto P dall'origine O , vale a dire la lunghezza del segmento di estremi O e P . Analogamente, se consideriamo due numeri reali x, y , $|x - y|$ rappresenta la distanza fra il punto P di coordinata x e il punto Q di coordinata y .

Proposizione 1.4 Proprietà del valore assoluto

1. $|x| \geq 0$, per ogni $x \in \mathbb{R}$.
 $|x| = 0$ se e solo se $x = 0$
2. $|x - y| = |y - x|$, per ogni $x, y \in \mathbb{R}$
3. Disuguaglianza triangolare
Per ogni $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$
4. Per ogni $x, y \in \mathbb{R}$, $|x \cdot y| = |x| \cdot |y|$
5. Per ogni $a > 0$, $\{x \in \mathbb{R} : |x| \leq a\} = [-a, a]$
6. Per ogni $a > 0$, $\{x \in \mathbb{R} : |x| \geq a\} = (-\infty, -a] \cup [a, +\infty)$
7. Fissati $a > 0$ e $x_0 \in \mathbb{R}$, $\{x \in \mathbb{R} : |x - x_0| \leq a\} = [x_0 - a, x_0 + a]$.

Interpretando il valore assoluto come una distanza, tutte le proprietà elencate hanno dimostrazione immediata.

1.4 Massimo, minimo, estremo superiore e inferiore

Definizione 1.3

- Un insieme $A \subseteq \mathbb{R}$ si dice limitato superiormente se

$$\exists M \in \mathbb{R} : \forall x \in A, \quad x \leq M \quad (1.3)$$

cioè se esiste un numero reale M più grande di tutti gli elementi di A .

- Ogni numero M che soddisfa (??) è detto maggiorante di A .
- Ogni numero m che soddisfa (??) è detto minorante di A .
- Si dice che A è illimitato superiormente se non è limitato superiormente, vale a dire se $\forall M \in \mathbb{R} \exists x \in A : x \geq M$.
- Un insieme $A \subseteq \mathbb{R}$ si dice limitato inferiormente se

$$\exists m \in \mathbb{R} : \forall x \in A, \quad x \geq m \quad (1.4)$$

cioè se esiste un numero reale m più piccolo di tutti gli elementi di A .

- Ogni numero m che soddisfa (??) è detto minorante di A .
- Si dice che A è illimitato inferiormente se non è limitato inferiormente, vale a dire se $\forall m \in \mathbb{R} \exists x \in A : x \leq m$.
- Si dice che A è limitato se è limitato superiormente e inferiormente, vale a dire se esistono $m, M \in \mathbb{R}$ tali che $\forall x \in A, m \leq x \leq M$.
- Si dice che A è illimitato se non è limitato, cioè se è illimitato superiormente o inferiormente.

Dimostrare **per esercizio** la seguente proposizione.

Proposizione 1.5 $A \subseteq \mathbb{R}$ è limitato $\iff \exists L > 0 : \forall x \in A, |x| < L$.

Esercizio 1.2 Dimostrare che se M è un maggiorante di A , allora tutti gli elementi di $[M, +\infty)$ sono maggioranti di A .

Analogamente, dimostrare che se m è un minorante di A , allora tutti gli elementi di $(-\infty, m]$ sono minoranti di A .

Esempi 1.3

1. $\mathbb{N} = \{0, 1, 2, \dots\}$ è limitato inferiormente e illimitato superiormente.
Per esempio, $y = -2$ è un minorante di \mathbb{N} . Invece, fissato qualunque $M \in \mathbb{R}$, il numero intero $n = [M] + 1 > M$ per definizione.
2. \mathbb{Z} è illimitato sia superiormente che inferiormente.
3. $A = (2, 3)$ è limitato. 2 è un minorante e 3 è un maggiorante di A . Né 2 né 3 appartengono ad A .
4. $B = (-\infty, \sqrt{2}]$ è illimitato inferiormente e limitato superiormente. $\sqrt{2}$ è un maggiorante di B che appartiene a B .
5. L'insieme $C = \left\{ \frac{1}{n} : n \in \mathbb{N} \setminus \{0\} \right\}$ è tale che $0 < \frac{1}{n} \leq 1$, per ogni $n \in \mathbb{N}$. Dunque C è limitato. Osserviamo inoltre che $0 \notin C$ è un minorante di C , mentre $1 \in C$ è un maggiorante di C .

In tutti gli esempi precedenti, viene istintivo scegliere un maggiorante e un minorante (quando esistono) particolari, che ci paiono “migliori” degli altri. Per esempio rispettivamente 1 e 0 nell’esempio 5, 3 e 2 nell’esempio 3. Vogliamo adesso formalizzare questa idea intuitiva.

Definizione 1.4 *Sia dato un insieme $A \subseteq \mathbb{R}$ superiormente limitato. Si dice estremo superiore di A , che si indica con $\sup A$, il più piccolo dei maggioranti di A , vale a dire quel numero reale s tale che*

1. $\forall x \in A, x \leq s$; cioè, s è un maggiorante di A .
2. $\forall \varepsilon > 0, \exists x \in A : s - \varepsilon < x \leq s$; cioè, ogni numero più piccolo di s non è un maggiorante di A .

Definizione 1.5 *Sia dato un insieme $A \subseteq \mathbb{R}$ inferiormente limitato. Si dice estremo inferiore di A , che si indica con $\inf A$, il più piccolo dei maggioranti di A , vale a dire quel numero reale i tale che*

1. $\forall x \in A, i \leq x$; cioè, i è un minorante di A .
2. $\forall \varepsilon > 0, \exists x \in A : i \leq x < i + \varepsilon$; cioè, ogni numero più grande di i non è un minorante di A .

Proposizione 1.6

1. Se A è limitato superiormente, allora A ha estremo superiore $s \in \mathbb{R}$
2. Se A è limitato inferiormente, allora A ha estremo inferiore $i \in \mathbb{R}$

Dimostrazione.

Dimostriamo il caso 1. Sia C l’insieme dei maggioranti di A . Abbiamo visto che se c è un maggiorante di A , allora $[c, +\infty) \subseteq C$. Consideriamo poi l’insieme $B = \mathbb{R} \setminus C$ dei numeri che non sono maggioranti di A . Abbiamo che $B \cup C = \mathbb{R}$ e che per ogni $b \in B$ e per ogni $c \in C$, $b < c$. Siamo allora nelle ipotesi dell’assioma di completezza dei numeri reali; dunque esiste un elemento separatore $z \in \mathbb{R}$, vale a dire un numero tale che, $\forall b \in B, \forall c \in C, b \leq z \leq c$. Quindi z è un maggiorante di A , ma non ci sono maggioranti di A più piccoli. Ne segue che $z = \sup A$.

La dimostrazione del punto 2 è lasciata al lettore. \square

Osservazione 1.1 Se un sottoinsieme di \mathbb{Q} è limitato superiormente, il suo estremo superiore non è necessariamente un numero razionale. Per esempio, $A = (-\infty, \sqrt{2}] \cap \mathbb{Q}$ ha $\sup A = \sqrt{2} \notin \mathbb{Q}$. Infatti, $\sqrt{2}$ è un maggiorante di A ; inoltre, per ogni $\varepsilon > 0$, per la densità di \mathbb{Q} in \mathbb{R} esiste $x \in A$ tale che $\sqrt{2} - \varepsilon < x < \sqrt{2}$.

In taluni casi l’estremo superiore e l’estremo inferiore di A possono essere elementi di A .

Definizione 1.6

- Se A è limitato superiormente e $s = \sup A \in A$, si dice che s è il massimo di A , e lo si indica con $\max A$.
- Se A è limitato inferiormente e $i = \inf A \in A$, si dice che i è il minimo di A , e lo si indica con $\min A$.

Proposizione 1.7

1. A ha massimo $s \iff \exists s \in A : \forall x \in A, x \leq s$.
2. A ha minimo $i \iff \exists i \in A : \forall x \in A, i \leq x$.

Esempi 1.4

1. Se $A = (1, 2)$, $\inf A = 1 \notin A$ e $\sup A = 2 \notin A$. Dunque A non ha né massimo né minimo.
2. Se $A = (-1, 3]$, $\inf A = -1 \notin A$ e $\sup A = 3 \in A$. Dunque $\max A = \sup A = 3$.
3. $A = [2, +\infty)$ è illimitato superiormente, quindi non ha estremo superiore; A è limitato inferiormente e $2 = \inf A \in A$, e dunque $\min A = \inf A = 2$.
4. $A = \left\{ \frac{1}{n} : n \in \mathbb{N} \setminus \{0\} \right\}$ è limitato, e $\sup A = \max A = 1$. Dimostriamo ora che $\inf A = 0$, e cioè che 0 è il più grande dei minoranti di A .

Abbiamo già osservato in precedenza che 0 è un minorante di A . Affinché ne sia anche l'estremo inferiore, dobbiamo mostrare che ogni numero più grande di 0 non è un minorante di A . Dobbiamo quindi dimostrare che, per ogni $\varepsilon > 0$, esiste $n \in \mathbb{N} \setminus \{0\}$ tale che $0 \leq \frac{1}{n} < \varepsilon$. Ma ciò segue dal corollario (??) alla proprietà archimedeo (??) dei numeri reali.

Esercizio 1.3 Dimostrare che se A ha estremo superiore (o inferiore), esso è unico. Analogamente, se A ha massimo (o minimo), esso è unico.

Introduciamo adesso una **notazione** utile:

- Per dire che A è illimitato superiormente, scriviamo $\sup A = +\infty$.
- Per dire che A è illimitato inferiormente, scriviamo $\inf A = -\infty$.

Attenzione! I simboli $+\infty$ e $-\infty$ **non** rappresentano dei numeri, e **non** è possibile estendere a $\mathbb{R} \cup \{-\infty, +\infty\}$ le operazioni di somma e di prodotto definite in \mathbb{R} .

1.5 Topologia di \mathbb{R}

Introduciamo in questo capitolo alcune proprietà degli insiemi che rientrano nel più ampio ambito della topologia.

Definizione 1.7 Dato un insieme A si definisce distanza o metrica su A una funzione

$$d : A \times A \rightarrow \mathbb{R}$$

tale che:

- $\forall X, Y \in A, d(X, Y) \geq 0$,
- $d(X, Y) = 0 \iff X = Y$,
- $\forall X, Y \in A, d(X, Y) = d(Y, X)$, (la distanza è simmetrica),
- $\forall X, Y, Z \in A, d(X, Y) \leq d(X, Z) + d(Z, Y)$ (disuguaglianza triangolare).

Definizione 1.8 Ogni insieme A su cui è possibile definire una distanza d viene detto spazio metrico. Si usa la notazione (A, d) .

In particolare, \mathbb{R}^n è uno spazio metrico, in cui si definisce la *distanza euclidea*, che è la naturale estensione a dimensione qualunque della distanza definita nel piano:

$$\forall X = (x_1, \dots, x_n), Y = (y_1, \dots, y_n) \in \mathbb{R}^n:$$

$$d(X, Y) = |X - Y| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

Osserviamo che questa definizione corrisponde alle definizioni di distanza già note in \mathbb{R} e nel piano \mathbb{R}^2 :

1. se $x, y \in \mathbb{R}$, $d(x, y) = \sqrt{(x - y)^2} = |x - y|$.
2. se $X = (x_1, x_2)$, $Y = (y_1, y_2) \in \mathbb{R}^2$, $d(X, Y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$ è la lunghezza del segmento XY , calcolato utilizzando il teorema di Pitagora. Proprio dal caso piano prende il nome la “disuguaglianza triangolare”: un ben noto teorema di geometria euclidea dice che la lunghezza di un lato del triangolo è sempre minore o uguale alla somma delle lunghezze degli altri due lati del triangolo stesso.

Definizione 1.9 Dato un qualunque spazio metrico (A, d) , si dice

- intorno sferico di centro X e raggio ρ l'insieme dei punti di A che hanno distanza da X minore di ρ :

$$B_\rho(X) = \{Y \in A : d(X, Y) < \rho\}.$$

- intorno di X un qualunque insieme $U \subseteq A$ che contiene un intorno sferico di X .

Vediamo alcuni esempi:

Esempi 1.5

1. Se $x \in \mathbb{R}$, $B_\rho(x) = \{y \in \mathbb{R} : |x - y| < \rho\} = (x - \rho, x + \rho)$, cioè l'intorno sferico è un intervallo aperto, costituito da tutti i punti che hanno distanza inferiore a ρ dal punto x .
2. Se $X \in \mathbb{R}^2$, l'intorno sferico di X di raggio ρ

$$\begin{aligned} B_\rho(X) &= \left\{ Y \in \mathbb{R}^2 : \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} < \rho \right\} = \\ &= \left\{ Y \in \mathbb{R}^2 : (x_1 - y_1)^2 + (x_2 - y_2)^2 < \rho^2 \right\} \end{aligned}$$

è il cerchio di centro X e raggio ρ , esclusa la circonferenza di centro X e raggio ρ .

3. Se $X \in \mathbb{R}^3$, $B_\rho(X)$ risulta essere la sfera piena di centro X e raggio ρ , esclusa la superficie sferica di centro X e raggio ρ .

La lettera B usata nella rappresentazione degli intorni sferici rimanda al fatto che abbiamo a che fare con delle “sfere”, o più colloquialmente, con delle “palle”: in inglese, “balls” (e infatti in inglese si parla di *ball of centre X and radius ρ*).

Nel seguito formuleremo tutte le definizioni nello spazio metrico \mathbb{R} . Tuttavia, tutte le definizioni possono essere estese a qualunque spazio metrico, perché sono basate esclusivamente sui concetti di intorno e di distanza.

Definizione 1.10 Sia dato un insieme $A \subseteq \mathbb{R}$

1. Si dice che un punto $x \in A$ è interno ad A se esiste un intorno $B_\rho(x)$ tale che $B_\rho(x) \subseteq A$.
2. Si dice interno di A , e si indica con $\text{Int } A$, l'insieme dei punti interni ad A .
3. Un punto $x \notin A$ si dice esterno ad A se esiste un intorno $B_\rho(x)$ tale che $B_\rho(x) \cap A = \emptyset$.

Osserviamo che in generale $\text{Int } A \subseteq A$.

Esercizio 1.4 Dimostrare che un punto è esterno ad A se e solo se è interno al suo complementare.

Definizione 1.11 Si dice che un insieme A è aperto se $\text{Int } A = A$.

Osservazione 1.1

1. $\text{Int}(\text{Int } A) = \text{Int } A$; dunque l'interno di A è sempre un insieme aperto.
2. Se un insieme è aperto, ogni suo punto è interno all'insieme stesso. Ciò significa che insieme al punto, nell'insieme è contenuto anche un suo intorno.

Esempi 1.6

1. Un intervallo $A = (a, b)$ (con $a < b$) è un insieme aperto. Infatti, per ogni $x_0 \in (a, b)$, se consideriamo $\rho = \frac{1}{2} \min\{|a - x_0|, |b - x_0|\}$, abbiamo che $B_\rho(x_0) \subseteq A$.
Dunque ogni punto di A è interno ad A , e quindi A è aperto.
2. Consideriamo ora $B = [a, b)$. Abbiamo già dimostrato che tutti i punti di (a, b) sono punti interni a B . Il punto a invece non è un punto interno. Infatti, ogni intorno di a interseca sia B (nei punti a destra di a) che il suo complementare (nei punti a sinistra di a).
Dunque, $\text{Int } B = (a, b)$ e B non è aperto.
3. $C = \{1, 2, 3\}$. Vediamo che $\text{Int } C = \emptyset$, mostrando che uno qualunque dei suoi elementi, per esempio $x = 1$, non è interno a C . Infatti, ogni intorno $B_\rho(1)$ contiene punti del complementare di C .
4. $D = (1, 2] \cup \{\pi\}$. Come in tutti gli intervalli, i punti $x \in (1, 2)$ sono punti interni a D , mentre 2 non lo è. Anche il punto π non è un punto interno (vedi esempio 3). Dunque $\text{Int } D = (1, 2)$ e D non è aperto.
5. Ogni intorno sferico è un insieme aperto.
6. \mathbb{Q} non ha punti interni. cioè $\text{Int } \mathbb{Q} = \emptyset$. Infatti, preso $x \in \mathbb{Q}$, ogni suo intorno $B_\rho(x) = (x - \rho, x + \rho)$ non è interamente contenuto in \mathbb{Q} . Infatti, per la densità di \mathbb{Q} in \mathbb{R} , in ogni intervallo sono contenuti anche numeri irrazionali.
7. \emptyset e \mathbb{R} sono aperti.

Definizione 1.12 Sia dato un insieme $A \subseteq \mathbb{R}$.

1. Si dice che $x \in \mathbb{R}$ è un punto di frontiera di A se

$$\forall \rho > 0 \quad B_\rho(x) \cap A \neq \emptyset \quad \wedge \quad B_\rho(x) \cap (\mathbb{R} \setminus A) \neq \emptyset$$

cioè ogni intorno di x interseca sia A che il suo complementare.

2. Si dice frontiera di A , e si indica con ∂A , l'insieme dei punti di frontiera di A .

Talvolta la frontiera di un insieme A viene anche detta *bordo* di A (dall'inglese "boundary").

Esercizio 1.5 Dimostrare che, se x è un punto interno ad A , allora x non è un suo punto di frontiera.

Esempi 1.7

Consideriamo l'intervallo $A = (1, 2)$.

- Tutti i punti di A sono interni ad A , quindi non sono punti di frontiera di A .
- Se $x < 1$, x è esterno ad A . Infatti, se consideriamo per esempio $\rho = \frac{1}{2}|x - 1|$, l'intorno $B_\rho(x) \subseteq \mathbb{R} \setminus A$. Analogamente, tutti i punti $x > 2$ sono esterni ad A .
- Se $x = 2$, ogni intorno $B_\rho(2) = (2 - \rho, 2 + \rho)$ interseca A a sinistra di 2 e interseca il suo complementare a destra di 2 . Quindi 2 è un punto di frontiera di A . Analogamente, 1 è punto di frontiera di A . Tutti gli altri punti di \mathbb{R} o sono punti interni o sono punti esterni ad A .

Ne segue che $\partial A = \{1, 2\}$. Osserviamo che in questo esempio i punti di frontiera non sono punti di A .

2. In modo analogo si può vedere che la frontiera di ogni intervallo limitato di \mathbb{R} di estremi a e b è l'insieme $\{a, b\}$. I due punti di frontiera appartengono o no ad A , a seconda che A sia un intervallo chiuso, aperto o semiaperto.
3. Consideriamo l'insieme $A = \mathbb{Q}$. Dalla densità di \mathbb{Q} in \mathbb{R} segue che, per ogni $x \in \mathbb{R}$, per ogni intorno x è vero che

$$B_\rho(x) \cap \mathbb{Q} = (x - \rho, x + \rho) \cap \mathbb{Q} \neq \emptyset \quad \wedge \quad B_\rho(x) \cap (\mathbb{R} \setminus \mathbb{Q}) = (x - \rho, x + \rho) \cap (\mathbb{R} \setminus \mathbb{Q}) \neq \emptyset.$$

Dunque

$$\mathbb{Q} \subsetneq \partial \mathbb{Q} = \mathbb{R}.$$

4. $B = \{1, 2, 3\}$. In questo caso, preso per esempio $x = 2$, ogni intorno di 2 interseca B almeno in $x = 2$ e interseca anche il suo complementare. Lo stesso accade per gli altri punti di B . Se consideriamo invece $x \in \mathbb{R} \setminus B$ e $\rho = \frac{1}{2} \min\{|x - 1|, |x - 2|, |x - 3|\}$, si ha che $B_\rho(x) \cap B = \emptyset$.

Ne segue che $\partial B = B$.

5. $C = [1, 2] \cup \{\pi\}$. Come abbiamo già osservato in precedenza, 1 e 2 sono punti di frontiera. Analogamente a quanto fatto nell'esempio precedente, possiamo vedere che anche π è un punto di frontiera. Tutti i punti di $\mathbb{R} \setminus C$ sono punti esterni a C . Dunque $\partial C = \{1, 2, \pi\} \subsetneq C$.
6. $\partial \emptyset = \emptyset$ e $\partial \mathbb{R} = \emptyset$.

Definizione 1.13 Si dice che un insieme $A \subseteq \mathbb{R}$ è chiuso se $\partial A \subseteq A$, cioè se tutti i punti di frontiera sono punti di A .

Si può dimostrare la seguente

Proposizione 1.8 $A \subseteq \mathbb{R}^n$ è aperto $\iff \mathbb{R}^n \setminus A$ è chiuso.

Ciò non significa che ogni insieme è aperto o chiuso. Per esempio gli intervalli $[a, b)$ e $(a, b]$ non sono né chiusi né aperti: infatti, non contengono uno dei due punti della loro frontiera.

Gli insiemi \emptyset e \mathbb{R}^n sono insiemi sia chiusi che aperti di \mathbb{R}^n .

Definizione 1.14 Dato un insieme $A \subseteq \mathbb{R}^n$, si dice chiusura di A , e si indica con \overline{A} , l'insieme $\overline{A} = A \cup \partial A$.

Si può dimostrare

Proposizione 1.9 Dato un insieme $A \subseteq \mathbb{R}^n$, allora

1. \overline{A} è chiuso e $\partial(\overline{A}) = \partial A$
2. \overline{A} è il più piccolo insieme chiuso che contiene A .

In generale si ha $\text{Int } A \subseteq A \subseteq \overline{A}$.

Esempi 1.8

1. Se $A = (1, 2)$, $\partial A = \{1, 2\}$ e $\overline{A} = [1, 2]$.
2. \mathbb{N} è un insieme chiuso di \mathbb{R} .
3. $A = \mathbb{Q}$ e $\partial A = \mathbb{R}$. Dunque la sua chiusura è $\overline{\mathbb{Q}} = \mathbb{R}$.

Definizione 1.15 Si dice che $A \subseteq \mathbb{R}$ è denso in \mathbb{R} se $\overline{A} = \mathbb{R}$.

Per esempio, l'insieme \mathbb{Q} è denso (in senso topologico) in \mathbb{R} .

Definizione 1.16 Sia dato un insieme $A \subseteq \mathbb{R}$.

1. Si dice che $\bar{x} \in \mathbb{R}$ è un punto di accumulazione di A se

$$\forall \rho > 0 \quad B_\rho(\bar{x}) \cap (A \setminus \{\bar{x}\}) \neq \emptyset.$$

cioè se ogni intorno di \bar{x} contiene punti di A diversi da \bar{x} .

2. Si dice che $\bar{x} \in A$ è un punto isolato di A se non è punto di accumulazione per A , cioè è tale che

$$\exists B_\rho(\bar{x}) \quad B_\rho(\bar{x}) \cap A = \{\bar{x}\}.$$

Osservazione 1.2

1. Tutti i punti interni di A sono punti di accumulazione di A (**dimostrare per esercizio**).
2. Un punto di accumulazione può essere un elemento dell'insieme oppure non esserlo.
3. Tutti i punti di A che non sono punti di accumulazione di A sono punti isolati di A .
4. L'insieme dei punti di accumulazione di A è detto *derivato* di A .

Proposizione 1.10 Se A ha punti di accumulazione $\implies A$ contiene infiniti elementi.

Dimostrare per esercizio.

Esempi 1.9

1. $A = [0, 1)$. Tutti i punti di $[0, 1]$ sono punti di accumulazione di A .
2. \mathbb{N} è costituito da punti isolati.
3. Tutti i punti di \mathbb{R} sono punti di accumulazione di \mathbb{Q} .
4. Sia $A = \left\{ \frac{1}{n}, n \in \mathbb{N} \setminus \{0\} \right\}$. Mostriamo che tutti i punti di A sono punti isolati e che 0 è il suo unico punto di accumulazione.

- Sia $x = \frac{1}{n} \in A$. Se consideriamo $\rho = \frac{1}{n} - \frac{1}{n+1}$, l'intorno $B_\rho(x)$ interseca A solo in $x = \frac{1}{n}$. Ne segue che x è un punto isolato di A .
- Sia $x = 0$. Per ogni $\rho > 0$, la proprietà archimedeica (??) dei numeri reali garantisce l'esistenza di un n tale che $\frac{1}{n} < \rho$. Ne segue che ogni intorno $B_\rho(0)$ contiene elementi di A , e dunque 0 è un punto di accumulazione di A .
- A non ha altri punti di accumulazione: *perché?*

Ricordiamo la definizione di insieme limitato data in precedenza: la riformuliamo in termini di intorni. Osserviamo che questa definizione, come tutte le altre date in precedenza, può essere estesa a tutti gli spazi metrici, e in particolare a \mathbb{R}^n . Infatti in tutte le definizioni si fa uso soltanto del concetto di intorno e di distanza.

Definizione 1.17 Un insieme $A \subseteq \mathbb{R}$ si dice limitato se

$$\exists M > 0 : \forall x \in A, \quad x \in B_M(0).$$

Equivalentemente, potremo dire che $\exists M > 0$ tale che $A \subseteq B_M(0)$, o anche che $\exists M > 0$, tale che $\forall x \in A, d(x, 0) < M$.

Definizione 1.18 Un insieme $A \subseteq \mathbb{R}$ si dice compatto se è chiuso e limitato.

Esempi 1.10

1. Ogni insieme che contiene un numero finito di elementi è compatto.
2. Gli intervalli chiusi e limitati sono compatti di \mathbb{R} .
3. L'unione di un numero finito di insiemi compatti è compatto.

Esercizi 1.1 Dimostrare le seguenti proposizioni. (*Ricordiamo che per dimostrare una proposizione non è sufficiente verificarne la validità con un esempio.*)

1. L'unione di due insiemi aperti è un insieme aperto.
2. L'intersezione di due insiemi aperti è un insieme aperto.
3. L'unione di due insiemi chiusi è un insieme chiuso.
4. L'intersezione di due insiemi chiusi è un insieme chiuso.
5. L'unione di due intorni di \bar{x} è un intorno di \bar{x} .
6. L'intersezione di due intorni di \bar{x} è un intorno di \bar{x} .
7. Ogni insieme che contiene un numero finito di elementi contiene solo punti isolati.
Suggerimento: ordinare gli elementi dell'insieme, e per ciascun punto dell'insieme trovare un intorno che lo isola dal precedente e dal successivo elemento dell'insieme.
8. Ogni insieme che contiene un numero finito di elementi è compatto, cioè è chiuso e limitato.