Teoria degli insiemi

November 24, 2017

Chapter 1

Nozioni di teoria degli insiemi

1.1 Operazioni sugli insiemi

In matematica la parola **insieme** si usa per indicare un raggruppamento, una raccolta, una collezione di elementi. Le nozioni di insieme e di elemento di un insieme sono considerati concetti primitivi, cioè non definibili mediante concetti piú semplici.

Osservazione 1.1.1 *E' importante osservare che un insieme si puó considerare definito solo se è possibile decidere inequivocabilmente se un elemento appartiene o no all'insieme.*

Ad esempio "gli studenti intelligenti della classe I A" non costituiscono un insieme a meno che non si dia un criterio per stabilire gli studenti intelligenti. Per esempio aver superato un determinato test.

Definizione 1.1.2 *Un insieme A è* **infinito** *se preso un numero qualunque di suoi elementi, esiste sempre un altro elemento in A.*

Se A non è infinito si dice **finito.**

Per indicare un elemento a appartiene ad un insieme A si usa il simbolo di appartenenza $\in$ e si scrive $a \in A$.

1.1.1 Rappresentazioni di un insieme

un insieme puó essere rappresentato in tre modi:

Rappresentazione geometrica: mediante i diagrammi di Eulero-Venn.

Rappresentazione per elencazione: quando gli elementi di un insieme sono elencati uno ad uno per esteso.

Ad esempio $X = \{0, 1, 2\}$, $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$

Rappresentazione per caratteristica: se gli elementi di un insieme sono individuati mediante una proprietá caratteristica che consente di stabilire con esattezza se un elemento appartiene o no ad un insieme.

Ad esempio $A = \{x \in \mathbf{N} | x < 4\}$.

Insiemi uguali.

Diremo **uguali** due insiemi A e B quando hanno esattamente gli stessi elementi e si scrive $A = B$. Questo è il cosidetto principio di **equiestensione.**

Ad esempio $A = \{-2, 2\}$ e $B = \{x \in \mathbf{Z} | x^2 = 4\}$ sono due insiemi uguali.

L'uguaglianza tra insiemi gode delle proprietá riflessiva, simmetrica e transitiva.

E' importante osservare che due criteri diversi possono individuare due insiemi uguali.

Ad esempio $A = \{x \in \mathbf{Q} | |x| = 2\}$ e $B = \{x \in \mathbf{Z} | x^2 = 4\}$ sono insiemi uguali ottenuti da criteri diversi.

Definizione 1.1.3 *Due criteri sono* **equivalenti** *se operando nello stesso ambiente danno luogo a insiemi uguali.*

Ad esempio $A = \{x \in \mathbf{Z} | |x| = 2\}$ e $B = \{x \in \mathbf{Z} | x^2 = 4\}$.

Diremo **insieme vuoto** un insieme privo di elementi. Ad esempio $\{x \in \mathbf{N} | x^2 = -1\}$. L'insieme vuoto si indicherá con il simbolo $\emptyset$.

Quando si assegna un insieme mediante una proprietá caratteristica (un criterio), occorre indicare l'ambiente da cui trarre gli elemenenti x dell'insieme. Questo ambiente è detto **insieme universo.**

In ambienti diversi uno stesso criterio puó dar luogo ad insiemi diversi. Ad esempio $A = \{x \in \mathbf{N} | (x-2)(x+3) = 0\} = \{2\}$, $A = \{x \in \mathbf{Z} | (x-2)(x+3) = 0\} = \{2, -3\}$.

Osservazione 1.1.4 *Gli elementi di un insieme possono essere a loro volta degli insiemi, si ha allora un insieme di insiemi. Ad esempio sia $F = \{$ tutte le rette del piano per il punto $P\}$. Poichè ogni retta è un insieme di punti F è un insieme di insiemi.*

E' errato dire che il punto P, centro del fascio, appartiene ad F, perchè P non è un elemento di F essendo un punto e non una retta.

1.1.2 Sottoinsiemi

Dati due insiemi A e B si dice che B è un **sottoinsieme** di A quando ogni elemento di B appartiene anche ad A e si scrive $B \subseteq A$.

Dato un insieme A, l'insieme vuoto ed A stesso sono sottoinsiemi **impropri** di A, tutti gli altri sono sottoinsiemi **propri** di A.

L'inclusione gode della proprietá transitiva: $A \subseteq B, B \subseteq C \Longrightarrow A \subseteq C$.

Inoltre risulta:

$$A \subseteq B, B \subseteq A \Longleftrightarrow A = B$$

che è detta **proprietá antisimmetrica dell'inclusione. Insieme delle parti.**

Dato un insieme A si definisce **insieme delle parti di** A quell'insieme, indicato con $\mathcal{P}(A)$, che ha per elementi tutti i possibili sottoinsiemi di A, compresi quelli impropri.

Ad esempio $A = \{a, b, c\}, \mathcal{P}(A) = \{\emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$. Osserviamo che se $A = \emptyset$ allora $\mathcal{P}(\emptyset) = \{\emptyset\}$ che non indica l'insime vuoto, bensí un insieme unitario il cui unico elemento è l'insieme vuoto quindi $\emptyset \in \{\emptyset\}$.

Teorema 1.1.5 *Se A è finito e $|A| = n$ allora $|\mathcal{P}(A)| = 2^n$.*

Dim. Per induzione su n. Se $n = 0$ allora $A = \emptyset$, $\mathcal{P}(\emptyset) = \{\emptyset\}$ e $|\mathcal{P}(\emptyset)| = 1 = 2^0$.

Se $n = 1$ allora $A = \{x\}$, $\mathcal{P}(A) = \{\emptyset, A\}$ e $|\mathcal{P}(A)| = 2 = 2^1$.

Supposto vero il teorema per $n - 1$ lo vogliamo dimostrare per n.

Sia A un insieme con n elementi e sia A_1 un suo sottoinsieme con $n - 1$ elementi tale che $A = A_1 \cup \{a\}$. I sottoinsiemi di A sono:

- quelli di A_1 in numero di 2^{n-1} per ipotesi di induzione;
- tutti gli insiemi del tipo $B \cup \{a\}$ con $B \in \mathcal{P}(A_1)$. Essi sono ancora in numero di 2^{n-1}.

Ne segue che $|\mathcal{P}(A)| = 2^{n-1} + 2^{n-1} = 2^n$. □

1.1.3 Operazioni con gli insiemi

Dati due insiemi A e B diremo:

- **Intersezione** di A e B l'insieme i cui elementi appartengono contemporaneamente ad A e B e si scrive $A \cap B = \{x | x \in A \wedge x \in B\}$.
- **Unione** di A e B l'insieme i cui elementi appartengono ad A oppure a B e si scrive $\mathcal{A}cupB = \{x | x \in A \vee x \in B\}$.
- **Complementare** di A rispetto all'ambiente universo U l'insieme degli elementi di U che non appartengono ad A e si scrive $\overline{A} = \{x | x \in U \wedge x \notin A\}$.
- **Differenza** di A e B l'insieme costituito dagli elementi di A che non appartengono a B e si scrive $A - B = \{x | x \in A \wedge x \notin B\}$.

$A - B = \{x | x \in A \wedge x \notin B\} = \{x | x \in A \wedge x \in \overline{B}\} = A \cap \overline{B}$.

Le operazioni di unione, intersezione e differenza sono operazioni binarie interne. L'operazione di complemento è un'operazione unaria interna.

Valgono le seguenti proprietá :

$A \cap A$	$=$	A	(idempotenza)
$A \cup A$	$=$	A	(idempotenza)
$A \cap B$	$=$	$B \cap A$	(commutativa)
$A \cup B$	$=$	$B \cup A$	(commutativa)
$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$	(associativa)
$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$	(associativa)
$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$	(distributiva)
$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C)$	(distributiva)
$\overline{A \cap B}$	$=$	$\overline{A} \cup \overline{B}$	(legge di De Morgan)
$\overline{A \cup B}$	$=$	$\overline{A} \cap \overline{B}$	(legge di De Morgan)
$A \cap (A \cup B)$	$=$	A	(assorbimento)
$A \cup (A \cap B)$	$=$	A	(assorbimento)
$A \cap \overline{A}$	$=$	$\emptyset$	(complementarietá)
$A \cup \overline{A}$	$=$	U	(complementarietá)

1.2 Prodotto cartesiano

Si dice **coppia ordinata** un insieme di due elementi, presi in un certo ordine.

La scrittura (a, b) indica la coppia ordinata il cui primo elemento è a e il cui secondo elemento è b.

Definizione 1.2.1 *Dati due insiemi A e B si dice* **prodotto catesiano** *di A e B, e si indica $A \times B$ l'insieme di tutte le coppie ordinate formate prendendo il primo elemento in A e il secondo elemento in B. In simboli:*

$$A \times B = \{(a, b) | a \in A \wedge b \in B.\}$$

Osservazione 1.2.2

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$ *(proprietá distributiva del prodotto cartesiano rispetto all'intersezione).*
- *Se $|A| = n$ e $|B| = m$ allora $|A \times B| = mn$.*
- $A \times B \neq B \times A$
- $A \times \emptyset = \emptyset \times A = \emptyset$. *(ove $\emptyset = \{\}$, mentre $\{\emptyset\}$ è l'insieme il cui unico elemento è l'insieme vuoto.)*

Il **prodotto cartesiano** di n insiemi $A_1, A_2, \ldots, A_n$ è l'insieme delle n-ple ordinate $(a_1, a_2, \ldots, a_n)$ con $a_i \in A_i$. Se $A_1 = A_2 = \cdots A_n = A$ si indica con A^n.

Il prodotto cartesiano di due insiemi si puó rappresentare tramite un diagramma cartesiano:

Sia $A = \{1, 2, 3\}$, $B = \{4, 5\}$ allora $A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$.

Chapter 2

Relazioni

2.1 Definizione

Una **relazione** $\mathcal{R}$ tra un insieme A ed un insieme B è un sottoinsieme del prodotto cartesiano $A \times B$. Se la coppia $(a, b) \in \mathcal{R}$ scriveremo $a\mathcal{R}b$ e diremo che a è in relazione con b.

Esempio 2.1.1 *Sia* $A = \{1, 3, 5, 7\}$ *e* $B = \{2, 4, 6\}$. *Un esempio di relazione tra* A *e* B *è* $\mathcal{R} = \{(1, 2), (1, 4), (1, 6), (3, 4), (3, 6), (5, 6)\}$ *in cui ogni elemento di* $\mathcal{R}$ *ha la prima coordinata minore della seconda.*

Osservazione 2.1.2 *Nella definizione di relazione non è escluso il caso* $A = B$*; in questo caso si parla di relazione in un insieme*

Una relazione tra due insiemi A è B puó essere rappresentata in diversi modi:

- **Rappresentazione per elencazione**: $\mathcal{R} \subseteq A \times B$ è data tramite elencazione dei suoi elementi, come nell'esempio precedente.
- **Rappresentazione per caratteristica**: $x\mathcal{R}y \iff$ la coppia $(x, y) \in A \times B$ soddisfa una condizione.

  Ad esempio sia $A = \{-2, -1, 1, 2, 3\}$ e $B = \{1, 4, 9, 10\}$ e sia

  $$x\mathcal{R}y \iff x^2 = y, x \in A, y \in B$$

  si ha allora $\mathcal{R} = \{(-2, 4), (-1, 1), (1, 1), (2, 4), (3, 9)\}$.
- **Diagramma cartesiano:** dopo aver rappresentato con un diagramma cartesiano l'insieme $A \times B$ contrassegniamo i punti $(a, b) \in \mathcal{R}$. Nel caso dell'esempio precedente abbiamo la seguente rappresentazione:

Sia $\mathcal{R}$ una relazione tra A e B. Possiamo, a partire da $\mathcal{R}$, definire un'altra relazione. Si dice **relazione inversa di** $\mathcal{R}$ e si indica con $\mathcal{R}^{-1}$ la relazione tra B e A cosí definita: $y\mathcal{R}^{-1}x \iff x\mathcal{R}y$. Ovviamente $\mathcal{R} \subseteq A \times B$ e $\mathcal{R}^{-1} \subseteq B \times A$.

Ad esempio sia $X = \{1, 2, 3, 4, 5, 6\}$ e $Y = \{2, 3\}$ e consideriamo la relazione $x\mathcal{R}y$ sse x è multiplo di y. Abbiamo $\mathcal{R} = \{(2, 2), (4, 2), (6, 2), (3, 3), (6, 3)\} \subset X \times Y$. La relazione inversa risulta essere $y\mathcal{R}^{-1}x$ sse y è un divisore di x. Pertanto $\mathcal{R}^{-1} = (2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\} \subset Y \times X$.

Si dice **relazione complementare di** un relazione $\mathcal{R}$ e si indica con $\not\mathcal{R}$ la relazione tra A e B cosí definita:

$$x \not\mathcal{R} y \iff (x, y) \notin \mathcal{R}.$$

Ovviamente $\not\mathcal{R}$ è il complemtare di $\mathcal{R}$ in $A \times B$.

Se $\mathcal{R}$ è una relazione in $A \times B$ ed $A = B$ parleremo di **relazione in un insieme** e quindi $\mathcal{R} \subseteq A^2$.

Esempio 2.1.3 *Sia $A = \{$ rette del piano $\}$. Siano $r, s \in A$ e definiamo in A^2 la relazione $||$ data da*

$$r||s \iff r \cap s = \emptyset \vee r = s.$$

E' interessante notare che la sua complementare è la relazione di incidenza cioè

$$r \not|| \iff r \cap s \neq \emptyset \wedge r \neq s.$$

Una relazione $\mathcal{R}$ in un insieme A puó godere delle seguenti proprietá :

- **Riflessiva** se $x\mathcal{R}x, \forall x \in A$.

  Ad esempio $x\mathcal{R}y$ sse $x \leq y$ con $x, y \in \mathbf{N}$ è una relazione riflessiva perchè $x \leq x$ è sempre vera.

- bf Antiriflessiva se $x \not\mathcal{R}x, \forall x \in A$.

  Ad esempio $x\mathcal{R}y$ sse $x < y$ con $x, y \in \mathbf{N}$ è una relazione antiriflessiva perchè la relazione $x < x$ è sempre falsa.

  Osservazione. Dire che una relazione è non riflessiva non vuol dire che è antiriflessiva. Affinche $\mathcal{R}$ sia non riflessiva basta che esista un x tale che $x \not\mathcal{R}x$ e non necessariamente per ogni x $x \not\mathcal{R}x$ come avviene per le relazioni anitiriflessive.

Osservazione 2.1.4 *Nel diagramma cartesiano di A^2 l'insieme delle coppie (a, a) si chiama la* **diagonale principale** *D . Se una relazione $\mathcal{R}$ è riflessiva risulta $\mathcal{R}supseteqD$. Se $\mathcal{R}$ è antiriflessiva essa non contiene alcun punto di D. Altrimenti se non è nè riflessiva nè antiriflessiva alcuni punti di D sono in $\mathcal{R}$ e altri no.*

Esempio 2.1.5 *1. $A = \{0, 1, 2, 3\}$ in esso la relazione $x \geq y$ è riflessiva, come si vede anche dal diagramma: 2. $A = \{0, 1, 2, 3\}$ in esso la relazione $x > y$ è antiriflessiva, come si vede anche dal diagramma: 3. $A = \{0, 1, 2, 3\}$ in esso la relazione $x + y < 3$. Dal suo diagramma si deduce che non è nè riflessiva nè antiriflessiva.*

Proprietá simmetrica. Una relazione $\mathcal{R}$ in un insieme A è **simmetrica** se $x\mathcal{R}y \Longrightarrow y\mathcal{R}x$.

Ad esempio la relazione di parallelismo tra rette è simmetrica.

Osservazione 2.1.6 *Se $\mathcal{R}$ è una relazione simmetrica allora la sua relazione inversa $\mathcal{R}^{-1}$ coincide con $\mathcal{R}$. Infatti $x\mathcal{R}^{-1}y$ equivale a $y\mathcal{R}x$ ma essendo $\mathcal{R}$ simmetrica ció equivale a $x\mathcal{R}y$.*

Proprietá antisimmetrica. Una relazione è **antisimmetrica** se

$$x \neq y \wedge x\mathcal{R}y \Longrightarrow y \not\mathcal{R}x.$$

Ad esempio la relazione $\leq$ tra numeri interi è antisimmetrica.

Graficamente il diagramma cartesiano di una relazione simmetrica è simmetrico rispetto alla diagonale principale.

Il diagramma cartesiano di una relazione antisimmetrica non deve mai contenere punti simmetrici rispetto alla diagonale principale. Se una relazione non è simmetrica non è detto che sia antisimmetrica.

Una relazione $\mathcal{R}$ in un insieme A è **transitiva** se $x\mathcal{R}y, y\mathcal{R}z \Longrightarrow x\mathcal{R}z$.
Ad esempio la relazione $\leq$ tra numeri interi.

Una relazione si dice di **equivalenza** se è :

- riflessiva;
- simmetrica;
- transitiva.

Ad esempio la relazione di parallelismo tra rette è di equivalenza.
Data una relazione di equivalenza $\mathcal{R}$ in un insieme A, si chiama **classe di equivalenza** di $a \in A$ e si indica con $[a]_{\mathcal{R}}$ il sottoinsieme di A cosí definito:

$$[a]_{\mathcal{R}} = \{x \in A | x\mathcal{R}a\},$$

cioè l'insieme degli elementi di A in relazione $\mathcal{R}$ con a. La scrittura $[a]$ sta ad indicare che l'elemento a è preso come rappresentante della classe di equivalenza cui appartiene. Sussiste il seguente:

Teorema 2.1.7 *Sia $\mathcal{R}$ una relazione di equivalenza definita in A e $a, b \in A$. Le seguenti affermazioni sono equivalenti:*

$$b\mathcal{R}a \Longleftrightarrow b \in [a] \Longleftrightarrow [b] = [a].$$

Dato un insieme A ed una famiglia F di parti di A, $F = \{A_1, A_2, \ldots\}$ con $A_i \subseteq A$, diremo che F è una **partizione** di A se:

- $A_1 \cup A_2 \cup ..... = A$;
- $A_i \neq A_j$ allora $A_i \cap A_j = \emptyset$.

Teorema 2.1.8 *Sia $\mathcal{R}$ una relazione di equivalenza in un insieme A, le classi di equivalenza costituiscono una partizione di A.*

Le classi di equivalenza possono essere considerate come elementi di un nuovo insieme detto **insieme quoziente**.

Sia $\mathcal{R}$ una relazione di equivalenza in A e siano $A_1, A_2, \ldots$ tutte le classi di equivalenza. Si chiama **insieme quoziente** di A rispetto ad $\mathcal{R}$ e si indica con $A/\mathcal{R}$ l'insieme $\{A_1, A_2, \ldots\}$ i cui elementi sono le classi di equivalenza di A rispetto ad $\mathcal{R}$. Una relazione $\mathcal{R}$ definita in

A è una **relazione di ordine** se essa gode delle proprietá :

- antisimmetrica;
- transitiva.

Si dice anche che l'insieme A è ordinato. Sia $\mathcal{R}$ una relazione di ordine in A. Diremo che

$\mathcal{R}$ è una relazione di ordine **stretto** ($<$) se è antiriflessiva. Diremo che $\mathcal{R}$ è una relazione di ordine **largo** ($\leq$) se è riflessiva. Data una relazione di ordine $\mathcal{R}$ in A diciamo che due

elementi distinti a e b sono **confrontabili** se $a\mathcal{R}b$ o $b\mathcal{R}a$.

Diciamo che $\mathcal{R}$ è una relazione di ordine **totale** se comunque si scelgano due elementi distinti di A essi sono sempre confrontabili. Altrimenti la relazione è **parziale.**

Ad esempio la relazione $<$ in $\mathbf{N}$ è di ordine stretto totale. La relazione di divisibilitá in $\mathbf{N_0}$ è un ordine largo parziale. La relazione di inclusione propria tra sottoinsiemi è un ordine stretto parziale. La relazione $\leq$ in $\mathbf{N}$ è un ordine largo totale.

Chapter 3

Applicazioni o funzioni

3.1 Definizione di applicazione

Una relazione $\mathcal{R}$ tra un insieme A ed un insieme B si dice un' **applicazione** se per ogni $x \in A$ esiste uno ed un sol $y \in B$ tale che $x\mathcal{R}y$.

Per denotare che una relazione $\mathcal{R}$ è un'applicazione useremo lettere tipo f, g, h e scriveremo $f : A \to B$. Se $y = f(x)$ diremo che y è l'**immagine** di x nella f e che x è **controimmagine** di y. Diremo inoltre che A è il **dominio** di f e $f(A) = \{y \in B | y = f(x)\}$.

Date due funzioni $f : A \to B$ e $g : B \to C$ definiamo **funzione composta** di f e g la funzione $h : A \to C$ tale che $h(x) = g(f(x))$ e scriveremo anche $h = g \circ f$. La composizione di funzioni non è commutativa. Vale invece la proprietá associativa: $(h \circ g) \circ f = h \circ (g \circ f)$.

3.2 Funzioni iniettiva, suriettive, biettive

Sia $f : A \to B$ una funzione. Diremo che f è **iniettiva** se

$$x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$$

o equivalentemente

$$f(x_1) = f(x_2) \Longrightarrow x_1 = x_2.$$

Ad esempio $f : \mathbf{N} \to \mathbf{N}$ tale che $f(x) = x^2$ è una funzione iniettiva. Sia $f : A \to B$ una

funzione. Diremo che f è una funzione **suriettiva** se $f(A) = B$. Cioè ogni elemento di B è immagine di almeno un elemento di A. Ad esempio $f : \mathbf{Z} \to \{-1, 0, 1\}$ con $f(x) =$

segno di x è suriettiva. Una funzione $f : A \to B$ si dirá **biunivoca** se è sia iniettiva che

suriettiva. Ad esempio $f : x \in \mathbf{R} \to x + 1 \in \mathbf{R}$ è biunivoca. La composizione di due

funzioni biunivoche è biunivoca. Se $f : A \to B$ è una funzione biunivoca allora diremo **inversa** di f la funzione $f^{-1} : B \to A$ tale che $x = f^{-1}(y) \iff y = f(x)$. Ad esempio $f : \mathbf{N} \to A$ ove A è l'insieme dei quadrati perfetti con $f(x) = x^2$ è biunivoca. La f^{-1} sará la funzione $y = \sqrt{x}$.

Chapter 4

Cardinalitá di un insieme, insiemi infiniti e confronto tra essi

4.1 Potenza di un insieme

Definizione 4.1.1 *Un insieme A è* **infinito** *se preso un numero qualunque di suoi elementi, esiste sempre un altro elemento nell'insieme. Se A non è infinito si dice* **finito.**

Diremo che due insiemi A e B hanno la **stessa potenza** o sono **equipotenti** ($p(A) = p(B)$) se esiste una corrispondenza biunivoca tra A e B.

Risultano evidenti le seguenti proprietá :

a) Due insiemi finiti sono equipotenti sse hanno lo stesso numero di elementi.

b) Un insieme finito A non è mai equipotente ad una sua parte propria B e risulta $p(A) > p(B)$.

Se A è un insieme finito la potenza di A, $p(A)$ che coincide con il numero di elementi di A è detta anche cardinalitá di A e si denota $|A|$.

Quindi:

A, B finiti con $B \subset A$ allora $p(B) = |B| < |A| = p(A)$.

Mentre per insiemi infiniti ció non vale in quanto esistono:

A, B infiniti con $B \subset A$ tale che $p(A) = p(B)$.

Vale sempre, con A e B finiti o infiniti:

$B \subset A \Longrightarrow p(B) \leq p(A)$.

Esempio 4.1.2 *Sia* $\mathbf{N}$ *l'insieme dei numeri naturali e P l'insieme dei numeri pari. Allora $P \supset \mathbf{N}$ e $f : n \in \mathbf{N} \to 2n \in P$ è una biezione. Pertanto $p(\mathbf{N}) = p(P)$.*

Si puó quindi dare anche la seguente definizione:

Definizione 4.1.3 *A è* **infinito** *se esiste $B \subset A$ in corrispondenza biunivoca con A.*

Definizione 4.1.4 *Se A è in corrispondenza biunivoca con* $\mathbf{N}$ *allora A si dirá* **numerabile.** *La potenza del numerabile si denota anche con χ_0.*

Proposizione 4.1.5 *Se $I \subset \mathbf{N}$ allora I è finito o numerabile*

Dim. Se I è finito OK. Sia allora I infinito. Sia $a_0 \in I$, poniamo $\alpha(a_0) = 0$. Consideriamo ora $I - \{a_0\}$ e sia $a_1 \in I - \{a_0\}$ poniamo $\alpha(a_1) = 1$. Cosí proseguendo costruiamo la seguente applicazione $\alpha : a_n \in I \to n \in \mathbf{N}$ che è biunivoca perchè preso un qualunque $n \in \mathbf{N}$ esiste un unico elemento in I di posto n che è a_n. Pertanto $p(I) = p(\mathbf{N}) = \chi_0$. □

Da ció segue la

Proposizione 4.1.6 *Ogni insieme infinito A ha potenza maggiore o uguale del numerabile.*

Dim. Sia A infinito. Se per assurdo $p(A) < p(\mathbf{N}) = \chi_0$ allora esiste un $I \subset \mathbf{N}$ tale che A è in biezione con I. Poichè A è infinito, tale è anche I e per la proposizione precedente $p(I) = \chi_0 = p(A)$, il che è assurdo. □

Da ció segue che non esiste un'infinitá piú piccola del numerabile

4.2 Confronto tra insiemi

Si dice che A è **prevalente** a B e si scrive $A >> B$ se B è equivalente a un sottoinsieme proprio di A. In tal caso risulta $p(A) \geq p(B)$.

Valgono i seguenti:

Teorema 4.2.1 *Se A è finito e $|A| = n = p(A)$ allora $|\mathcal{P}(A)| = 2^n$.*

Teorema 4.2.2 *Dato un insieme è risulta $p(\mathcal{P}(A)) > p(A)$.*

Dim. Se A è finito e $|A| = n$ allora $|\mathcal{P}(A)| = 2^n > n$.

Sia A infinito consideriamo la seguente biezione:

$$a \in A \to \{a\} \in A^* \subset \mathcal{P}(A)$$

ove $A^* = \{\{x\}\}_{x \in A}$ allora $p(A) = p(A^*) \leq p(\mathcal{P}(A))$. Resta da dimostrare che $p(A) \neq p(\mathcal{P}(A))$. Se per assurdo $p(A) = p(\mathcal{P}(A))$ allora esiste una biezione $f : a \in A \to f(a) \in \mathcal{P}(A)$. Per ogni $x \in A$ risulta $x \in f(x)$ oppure $x \notin f(x)$. Sia $A' = \{x \in A | x \notin f(x)\}$. Poichè f è biettiva e $A' \in \mathcal{P}(A)$ allora esiste un $y \in A$ tale che $y = f^{-1}(A')$. Se $y \notin f(y) = A'$ allora $y \in A'$, il che è assurdo. Se $y \in f(y) = A'$ allora $y \notin A'$ il che è assurdo. Pertanto $p(\mathcal{P}(A)) > p(A)$. □

Teorema 4.2.3 $\mathbf{Q}$ *è numerabile.*

Dim.

$$\mathbf{Q}^+ = \{\frac{p}{q}\}_{p,q\in\mathbf{N}}$$

Diciamo **altezza** di p/q l'intero $h = p + q$. Le frazioni p/q di altezza h sono in numero di $h - 1$.

$$\begin{array}{cccccc} p & 1 & & 2 & \cdots & h-1 \\ q & h-1 & h-2 & & \cdots & 1 \end{array}$$

$$\begin{array}{cccc} h=2 & a_1 = \frac{1}{1} & . & . \\ h=3 & a_2 = \frac{1}{2} & a_3 = \frac{2}{1} & . \\ h=4 & a_4 = \frac{1}{3} & \not{\frac{2}{2}} & a_5 = \frac{3}{1} \\ .. & .. & .. & .. \end{array}$$

allora costriuamo una biezione $n \in \mathbf{N} \to a_n \in \mathbf{Q}^+$. Ne segue che Q^+ è numerabile. Poniamo ora $b_n = -p/q = -a_n$ e costruiamo la biezione tra $\mathbf{N}$ e $\mathbf{Q}$ cosí definita:

$$\begin{array}{ccc} \mathbf{N} & \to & \mathbf{Q} \\ 2n & \mapsto & a_n \\ 2n-1 & \mapsto & -a_n \end{array}$$

Teorema 4.2.4 $\mathbf{R}$ *non è numerabile.*

Dim. (Dimostrato la prima volta da Liouville (1809-1882). Qui daremo la dimostrazione di Cantor.)

Basta provare che esiste un insieme A infinito, $A \subset \mathbf{R}$, A non-numerabile. Sia ad esempio $A = [0, 1]$. Per assurdo supponiamo che esista una biezione tra A e $\mathbf{N}$ cosí definita: $\alpha_n \in A \to n \in \mathbf{N}$.

Gli elementi di A sono:

$$\begin{array}{ccc} \alpha_1 & = & 0, a_{11}a_{12}a_{13}... \\ \alpha_2 & = & 0, a_{21}a_{22}a_{23}... \\ ... & ... & ... \\ \alpha_n & = & 0, a_{n1}a_{n2}a_{n3}... \\ .... & .... & ... \end{array}$$

Sia $\alpha = 0, \epsilon_{11}\epsilon_{22}\epsilon_{33}....$ con

$$\epsilon_{ii} = \begin{array}{ccc} 1 & \text{se } a_i i & \text{è pari} \\ 0 & \text{se } a_i i & \text{è dispari} \end{array}$$

Ovviamente $\alpha \in A$ ma non esiste j tale che $\alpha = \alpha_j$. Infatti se $\alpha = \alpha_j = 0, a_{j1}a_{j2}....a_{jj}... = 0, \epsilon_{11}\epsilon_{22}....\epsilon_{jj}....$

Ma $\epsilon_{jj} = 1$ se $a_j j$ è pari il che è assurdo essendo $\epsilon_{jj} = a_{jj}$ ed è $\epsilon_{jj} = 0$ se $a_j j$ è dispari il che è ancora assurdo perchè $\epsilon_{jj} = a_{jj}$. Pertanto $\alpha \neq \alpha_j$ e quindi non esiste una biezione tra A ed $\mathbf{N}$. □

Osservazione 4.2.5

$$\begin{array}{rcll} p(\mathbf{N}) & = & \chi_0 & \textit{potenza del numerabile} \\ p(\mathbf{R}) & = & \chi_1 = c & \textit{potenza del continuo} \\ p(\mathcal{P}(\mathbf{N})) & = c & & . \end{array}$$

Osservazione 4.2.6 (Osservazioni su insiemi finiti e infiniti) *E' evidente che se tra due insiemi finiti vi è una corrispondenza biunivoca i due insiemi devono avere lo stesso numero di elementi.*

Se invece i due insiemi non sono finiti si possono presentare i paradossi all'infinito.

Nessun insieme finito si puó porre in corrispondenza biunivoca con una sua parte propria. Ció negli insiemi infiniti è possibile. Ad esempio i naturali possono porsi in corrispondenza biunivoca con i numeri pari.

Un altro esempio è il seguente: L'insieme dei punti di una retta puó essere posto in corrispondenza biunivoca con l'insieme dei punti di un suo segmento aperto.

Infatti la semicirconferenza è in corrispondenza biunivoca con il segmento AB tramite proiezione ortogonale ed è anche in corrispondenza biunivoca con tutta la retta tramite proiezione sterografica dal punto O. Ne segue che il segmento AB è in corrispondenza biunivoca con tutta la retta. Un altro esempio si ottiene al seguente modo: I punti interni

di un quadrato si possono mettere in corrispondenza biunivoca con i punti di un suo lato. Consideriamo il quadrato di vertici $(0,0),(1,0),(1,1),(0,1)$. Sia $P(x,y)$ un suo punto interno. Allora $x = 0, a_1a_2a_3\ldots, y = 0, b_1b_2b_3\ldots$ Al punto P facciamo corrispondere il punto $P'(0, a_1b_1a_2b_2\ldots; 0)$ che appartiene ad un lato del quadrato. Tale corrispondenza è biunivoca.

Tali paradossi hanno suggerito ai matematici la seguente definizione.

Un insieme è **infinito** quando si puó porre in corrispondenza biunivoca con un suo sottoinsieme proprio.

Chapter 5

Gli insiemi numerici: $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$

5.1 I numeri naturali

Esponiamo un metodo assiomatico per l'introduzione dei numeri naturali, dovuto a Peano matamatico italiano nel 1899. Il metodo di Peano rappresenta il primo rigoroso e preciso tentativo di assiomatizzare l'aritmetica, cercando di stabile la teoria dei numeri naturali sul piú piccolo numero possibile di premesse (concetti primitivi) e di proprietá non dimostrabili (assiomi o postulati), dai quali, successivamente, far derivare tutta la teoria con procedimenti esclusivamente logici.

Peano parte da tre idee fondamentali, concetti primitivi (cioè non definibili) che sono quelli di:

zero, numero e successivo

e da cinque assiomi (detti i cinque postulati di Peano) e cioè :

I lo zero è un numero: $0 \in \mathbf{N}$;

II il successivo di un numero $n \in \mathbf{N}$ è un numero n^*.

III se i successivi di due numeri sono uguali, lo sono anche i numeri ($n* = m* \Longrightarrow n = m$);

IV Lo zero non è sucessivo di alcun numero ($n* \neq 0$ per ogni $n \in \mathbf{N}$);

V Se un insieme di numeri contiene lo zero e se contentendo un altro numero contiene anche il successivo allora l'insieme contiene tutti i numeri. Ossia:

se K è un sottoinsieme di $\mathbf{N}$ con le proprietá :

- $0 \in K$;
- se $k \in K$ allora $k^* \in K$

allora $K = \mathbf{N}$.

Il principio di induzione matematica.
Consideriamo la proposizione:

$$P(m) : m^* \neq m, \forall m \in \mathbf{N}.$$

Faremo vedere che come questa proposizione si possa ottenere utilizzando solo gli assiomi di Peano. Definiamo:

$$K = \{k \in \mathbf{N} | P(k) \text{ è vera}\}$$

sappiamo, dall'assioma I che $0 \in \mathbf{N}$ e che $0^* \neq 0$ e quindi $P(0)$ è vera e $0 \in K$.

Sia ora $k \in K$ allora $P(k)$ è vera ossia $k^* \neq k$. Vogliamo dimostrare che $k^* \in K$ cioè che $(k^*)^* \neq k^*$. Se per assurdo $(k^*)^* = k^*$ allora dall'assioma IV seguirebbe $k^* = k$ ossia $P(k)$ falsa che è una contraddizione. Quindi $k^* \in K$. Pertanto K ha le due proprietá enunciate dall'assioma V e quindi $K = N$ e la proposizione $P(m)$ è valida per ogni $m \in \mathbf{N}$.

Dimostrando la validitá della proposizione precedente abbiamo dimostrato il principio di induzione matematica.

bf Principio di induzione matematica. Una proposizione $P(m)$ è vera per tutti gli $m \in \mathbf{N}$ se:

- $P(0)$ è vera;
- e se per ogni $k \in \mathbf{N}$, $P(k)$ vera implica $P(k^*)$ vera.

Osservazione 5.1.1 *Peano affermó che i cinque postulati definiscono in maniera implicita i tre concetti primitivi, i postulati sarebbero cioè caratteristici per i concetti di zero, numero e successivo.*

Fu proprio questa affermazione che scatenó la critica di Russel, il quale dimostró che i cinque postulati definiscono logicamente i concetti di zero, numero e successivo ma non li caratterizzano, nel senso che i tre concetti fondamentali si presentano in una infinitá di interpretazioni, ciascuna soddisfacente i postulati stessi.

Esempio 5.1.2 *Supponiamo che la parola zero rappresenti il numero* 25*, la parola numero rappresenti un qualsiasi numero naturale* ≥ 25 *e che successivo significhi un numero aumentato di uno. Tutti e cinque i postulati sono soddisfatti.*

5.1.1 Le operazioni in N.

Addizione. Ad ogni coppia $a, b \in \mathbf{N}$ si associa un terzo numero neturale $a + b$ detto somma tale che:

i) il successivo di un numero è la somma di esso e del numero 1, cioè $a^* = a + 1$, dove 1 è il successivo di 0.

ii) $a + 0 = a$; $a + b^* = a + (b + 1) = (a + b) + 1 = (a + b)^*$.

Successivamente Peano dimostra che le condizioni i) e ii) individuano un'operazione binaria univoca per la quale sussistono la proprietá commutativa, associativa e di monotonia. Ossia:

- $a + b = b + a$;
- $(a + b) + c = a + (b + c)$;
- $a = b \iff a + c = b + c$ (regola di cancellazione);
- $a \leq b, b \leq a \implies a = b$ ($\leq$ è antisimmetrica);
- $(a < b, c < d) \implies a + c < b + d$ (monotonia);
- $a \leq b, b \leq c \implies a \leq c$ ($\leq$ è transitiva).

Moltiplicazione. Ad ogni coppia $a, b \in \mathbf{N}$ è associato un numero naturale ab detto prodotto tale che:

$$a1 = 1a = a; \qquad ab^* = a(b + 1) = ab + a$$

segue in particolare che 1 è l'elemento neutro della moltiplicazione e che $a0 = 0a = 0$. Inoltre in tal modo si individa un'operazione binaria univoca per la quale sussistono la proprietá commutativa, associativa e di monotonia. Ossia:

- $ab = ba$;
- $(ab)c = a(bc)$;
- $a = b \iff ac = bc, c \neq 0$ (regola di cancellazione);
- $(a < b, c < d) \implies ac < bd$ (monotonia);
- $a(b + c) = ab + ac$ (distributiva del prodotto rispetto alla somma).

5.2 I numeri interi

Il sistema dei numeri naturali ha una evidente limitazione che consiste in questo: dati $m, s \in \mathbf{N}$ l'equazione $m + x = s$ non sempre ha soluzione in $\mathbf{N}$ ad esempio $5 + x = 3$ non ha soluzioni naturali. Si rimedia a questa situazione aggiungendo ai numeri naturali gli interi negativi per formare il sistema $\mathbf{Z}$ degli interi. Faremo vedere come si puó costruire il sistema degli interi a partire dal sistema dei numeri naturali. Si consideri il prodotto cartesiano

$$L = \mathbf{N} \times \mathbf{N} = \{(s, m) : s, m \in \mathbf{N}\}$$

e consideriamo la relazione binaria ρ definita in L nel seguente modo:

$$(s,m)\rho(t,n) \Longleftrightarrow s+n=t+m$$

ad esempio $(2,5)\rho(6,9)$, $(r^*,s^*)\rho(r,s)$. La ρ è una relazione di equivalenza e quindi dá luogo ad una ripartizione di L nell'insieme delle classi di equivalenza $\mathbf{Z}=\{[s,m],[t,n],\ldots\}$ dove

$$[s,m]=\{(a,b)\in L|(a,b)\rho(s,m\}$$

Somma e prodotto in Z.
La somma e il prodotto in **Z**sono definiti da:

$$[s,m]+[t,n]=[(s+t),(m+n]$$

$$[s,m]\cdot[t,n]=[(st+mn),(sn+mt)]$$

Si dimostra che la somma e il prodotto cosí definiti sono ben poste, ossia non dipendono dai rappresentanti scelti.

Gli interi positivi.
Sia $r\in\mathbf{N}$. Da $0+r=r$ segue che r è soluzione dell'equazione $0+x=r$. Consideriamo ora l'applicazione

$$[n,0]\leftrightarrow n, n\in\mathbf{N}.$$

Risulta

$$[r,0]+[s,0]=[(r+s),0]\leftrightarrow r+s$$

$$[r,0]\cdot[s,0]=[rs,0]\leftrightarrow rs$$

Quindi la biezione definita è un isomorfismo tra $\{[n,0]|n\in\mathbf{N}\}$ e $\mathbf{N}$.
Supponiamo ora che $[s,m]=[n,0]$ allora $(s,m)\rho(n,0)$ ossia $s=m+n$ e quindi $s\geq m$. Questo individua in $\mathbf{Z}$ l'insieme $\mathbf{Z}^+$ degli interi positivi o nulli dato da:

$$\mathbf{Z}^+=\{[s,m]\in\mathbf{Z}|s\geq m\}.$$

Tenendo presente l'isomorfismo si puó sostuire $\mathbf{Z}^+$ ad $\mathbf{N}$.

Gli interi negativi.
Ricordiamo che $[r,r]=[0,0]\leftrightarrow 0$. Inoltre poichè risulta

$$[n,0]+[0,n]=[n,n]=[0,0]$$

l'intero $[0,n]$ è l'opposto dell'intero positivo $[n,0]$. Supponiamo ora che $[s,m]=[0,n]$ allora $(s,m)\rho(0,n)$ ossia $s+n=m$ quindi $s\leq m$. Questo individua in $\mathbf{Z}$ l'insieme $\mathbf{Z}^-$ degli interi positivi o nulli dato da:

$$\mathbf{Z}^-=\{[s,m]\in\mathbf{Z}|s\leq m\}.$$

Denotiamo con $-[n,0]$ l'opposto $[n,0]$ ossia $[0,n]$. In generale quindi l'opposto di $[s,m]$ è $[m,s]$ che denotiamo con $-[s,m]$.

Osserviamo che ora in $\mathbf{Z}$ l'equazione $5+x=2$ ha soluzione. Infatti $5 \leftrightarrow [5,0]$, $2 \leftrightarrow [2,0]$ e $[5,0]+[0,3]=[2,0]$ pertanto $[0,3]=-[3,0] \leftrightarrow -3$ è la soluzione.

5.3 I numeri razionali

Il sistema dei numeri interi ha un'evidente limitazione che consiste in questo: l'equazione $4x=6$ non ha soluzione in $\mathbf{Z}$. Si puó rimediare a questa limitazione aggiungendo agli interi ulteriori numeri e formando il sistema $\mathbf{Q}$ dei numeri razionali.

Sia

$$K=\mathbf{Z}\times(\mathbf{Z}-\{0\})=\{(s,m),s\in\mathbf{Z},m\in\mathbf{Z}-\{0\}\}$$

definiamo in K la seguente relazione di equivalenza:

$$(s,m)\rho(t,n)\Longleftrightarrow sn=mt$$

abbiamo quindi la ripartizione di K in classi di equivalenza

$$\mathbf{Q}=\{[s,m],[t,n],\ldots\}$$

dove

$$[s,m]=\{(a,b)\in K|(a,b)\rho(s,m\}$$

Somma e prodotto in Q.

La somma e il prodotto in $\mathbf{Q}$sono definiti da:

$$[s,m]+[t,n]=[(sn+mt),mn]$$

$$[s,m]\cdot[t,n]=[st,mn]$$

Si dimostra che la somma e il prodotto cosí definiti sono ben poste, ossia non dipendono dai rappresentanti scelti.

Gli interi positivi.

Sia $r\in\mathbf{N}$. Da $0+r=r$ segue che r è soluzione dell'equazione $0+x=r$. Consideriamo ora l'applicazione

$$[n,0]\leftrightarrow n,n\in\mathbf{N}.$$

Risulta

$$[r,0]+[s,0]=[(r+s),0]\leftrightarrow r+s$$

$$[r,0]\cdot[s,0]=[rs,0]\leftrightarrow rs$$

Quindi la biezione definita è un isomorfismo tra $\{[n,0]|n\in\mathbf{N}\}$ e $\mathbf{N}$.

Supponiamo ora che $[s,m]=[n,0]$ allora $(s,m)\rho(n,0)$ ossia $s=m+n$ e quindi $s\geq m$. Questo individua in $\mathbf{Z}$ l'insieme $\mathbf{Z}^+$ degli interi positivi o nulli dato da:

$$\mathbf{Z}^+=\{[s,m]\in\mathbf{Z}|s\geq m\}.$$

Tenendo presente l'isomorfismo si puó sostuire $\mathbf{Z}^+$ ad $\mathbf{N}$.

Gli interi negativi.

Ricordiamo che $[r,r]=[0,0]\leftrightarrow 0$. Inoltre poichè risulta

$$[n,0]+[0,n]=[n,n]=[0,0]$$

l'intero $[0,n]$ è l'opposto dell'intero positivo $[n,0]$. Supponiamo ora che $[s,m]=[0,n]$ allora $(s,m)\rho(0,n)$ ossia $s+n=m$ quindi $s\leq m$. Questo individua in $\mathbf{Z}$ l'insieme $\mathbf{Z}^-$ degli interi positivi o nulli dato da:

$$\mathbf{Z}^-=\{[s,m]\in\mathbf{Z}|s\leq m\}.$$

Denotiamo con $-[n,0]$ l'opposto $[n,0]$ ossia $[0,n]$. In generale quindi l'opposto di $[s,m]$ è $[m,s]$ che denotiamo con $-[s,m]$. Infatti $[s,m]+[m,s]=[0,0]$.

Osserviamo che ora in $\mathbf{Z}$ l'equazione $5+x=2$ ha soluzione. Infatti $5\leftrightarrow[5,0]$, $2\leftrightarrow[2,0]$ e $[5,0]+[0,3]=[2,0]$ pertanto $[0,3]=-[3,0]\leftrightarrow -3$ è la soluzione.

Consideriamo la seguente applicazione:

$$[t,1]\leftrightarrow t\in\mathbf{Z}$$

essa è un isomorfismo tra il sottoinsieme $\{[t,1]|t\in\mathbf{Z}\}$ di $\mathbf{Q}$ e $\mathbf{Z}$.

Infatti

$$[s,1]+[t,1]=[s+t,1]\leftrightarrow s+t$$

$$[s,1][t,1]=[st,1]\leftrightarrow st.$$

Ricordiamo che $[r,r]=[1,1]\leftrightarrow 1$. Inoltre poichè risulta

$$[n,1][1,n]=[n,n]=[1,1]\leftrightarrow 1$$

il razionale $[1,n]$ è l'inverso del razionale $[n,1]$. Quidi $[n,1]^{-1}=[1,n]$.

Notiamo ora che $[s,m]=[s,1][1,m]=sm^{-1}$ che denoteremo con s/m.

Osserviamo inoltre che $[s,m][m,s]=[sm,ms]=[1,1]$ quindi $[m,s]=[s,m]^{-1}$ che con le notazione introdotte è $(s/m)^{-1}=m/s$.

Osserviamo infine che l'equazione $4x=6$ si puó scrivere come $[4,1]x=[6,1]$ da cui $x=[6,1][1,4]=[6,4]=[3,2]=3/2$.

5.4 I numeri reali

Il sistema dei numeri razionali ha un'evidente limitazione che consiste in questo: l'equazione $x^2 = 2$ non ha soluzione in $\mathbf{Q}$. Infatti se esiste un razionale p/q, con p e q coprimi, tale che $(p/q)^2 = 2$ allora $p^2 = 2q^2$. Ma poichè p e q sono primi tra loro allora anche p^2 e q^2 risultano coprimi ma allora non puó essere $p^2 = 2q^2$, in quanto p^2 sarebbe multiplo di q^2. Pertanto non esiste alcun razionale il cui quadrato è 2.

Si puó rimediare a questa limitazione aggiungendo ai razionali ulteriori numeri e formando il sistema $\mathbf{R}$ dei numeri reali.

Introduciamo i numeri reali seguendo il metodo delle sezioni di Dedekind (1831- 1911).

Ricordiamo che oltre ai numeri $\sqrt{2}, \sqrt{5}, \sqrt[3]{7}$ altri numeri irrazionali sono π che è il rapporto costante tra una qualsiasi circonferenza e il suo diametro, il numero e di Nepero, la maggior parte dei logaritmi o i valori delle funzioni goniometriche di un generico angolo (funzioni irrazionali trascendenti).

Si puó poi costruire un generico numero irrazionale assegnando le infinite cifre decimali con una legge arbitraria. Ad esempio $1,23456742456853...$

Definiamo **numero irrazionale** ogni numero non razionale, cioè ogni numero che non puó essere messo sotto forma di frazione, ossia ogni numero decimale illimitato non periodico.

Tale definizione di numero irrazionale è in un certo senso "provvisoria" perchè abbiamo chiamato numeri degli enti con i quali non sappiamo ancora per il momento operare (cioè confrontarli, sommarli, moltiplicarli).

Allo scopo di definire con maggiore precisione un numero reale e, di conseguenza un numero irrazionale, occorre introdurre il concetto di classi contigue di numeri razionali.

Ad esempio $17/6 = 2,8333....$ che è un numero razionale. E' possibile costruire i seguenti insiemi $C_1 = \{2, 2, 8, 2, 83, 2, 833, 2, 8333, ...\}$ che ha per elementi le approssimazioni per difetto di $17/6$ a meno di $10^0, 10^{-1}, 10^{-2}, ...$ Analogamente possiamo costruire l'insieme $C_2 = \{3, 2, 9, 2, 84, 2, 834, 2, 8334, ...\}$ costituito dai valori approssimanti per eccesso il numero $17/6$ a meno di $10^0, 10^{-1}, 10^{-2}, ...$ Gli insiemi C_1 e C_2 si chiamano anche classi di numeri razionali.

Verifichiamo ora che le due classi godono delle seguenti proprietá

a) ogni numero di C_1 è minore di ogni numero di C_2 (le classi sono separate);

b) fissato un numero positivo e piccolo a piacere ϵ è sempre possibile determinare un elemento di C_2 e un elemento di C_1 tali che la loro differenza sia minore di ϵ (le due classi sono indefinitamente ravvicinate).

La *a*) è evidente. Per la *b*) fissiamo $\epsilon = 10^{-6}$, consideriamo in C_1 e C_2 i valori approssimanti di $17/6$ a meno di 10^{-7}. Abbiamo $2,8333334 - 2,8333333 = 10^{-7} < 10{-}6$.

Nel nostro esempio le due classi definiscono il numero $17/6$ che è il loro unico elemento separatore.

Nell'esempio considerato C_1 e C_2 individuavano un razionale che era decimale periodico. Si possono costruire analoghe classi per definire sia i numeri interi, sia i numeri razionali che sono decimali finiti, come ad es. $15/4 = 3,75$; in tal caso le due classi sono:

$$C_1 = \{3, 3, 7, 3, 74, 3, 749, 3, 7499, ...\}, C_2 = \{4, 3, 8, 3, 76, 3, 751, 3, 7501, ...\}$$

cioè $15/4$ è l'elemento separatore di C_1 e C_2 e anche in tal caso non appartiene a nessuna delle due classi.

Passiamo ora a costruire le due classi contigue di approssimazioni del numero irrazionale $\sqrt{2}$.

$$1^2 < 2 < 2^2 \text{ quindi } 1 < \sqrt{2} < 2$$

$$1,4^2 < 2 < 1,5^2 \text{ quindi } 1,4 < \sqrt{2} < 1,5$$

$$1,41^2 < 2 < 1,42^2 \text{ quindi } 1,41 < \sqrt{2} < 1,42$$

.....

cosí proseguendo costruiamo le due classi contigue $C_1 = \{1, 1, 4, 1, 41, 1, 414, 1, 4142, ...\}$ di approssimazioni per difetto di $\sqrt{2}$ e $C_2 = \{2, 1, 5, 1, 42, 1, 415, 1, 4143, ...\}$ di approssimazioni per eccesso per $\sqrt{2}$. Si nota che a differenza di prima non esiste una periodicitá nelle cifre decimali delle approssimazioni per difetto, quindi l'elemento separatore $\sqrt{2}$ non sará un numero razionale.

Definizione di classi contigue. Due classi H_1 ed H_2 composte di numeri razionali si dicono **contigue** se soddisfano:

- $\forall h_1 \in H_1;\ \ \forall h_2 \in H_2 \Longrightarrow h_1 < h_2$;
- $\forall \epsilon \in \mathbf{Q}^+\ \ \exists h_2 \in H_2\ \ \exists h_1 \in H_1\ \mid\ h_2 - h_1 < \epsilon$.

Teorema 5.4.1 *Date due classi contigue C_1 e C_2 esiste ed è unico l'elemento separatore α che definisco* **numero reale**. *Esso puó essere razionale o irrazionale.*

(Il numero α si puó rappresentare considerando una sua approssimazione per difetto (in C_1), con un errore piccolo a piacere, prolungata con dei puntini, ad esempio $\sqrt{2} = 1,414213.....$).

Per indicare che il numero α è individuato dalle classi contigue C_1 e C_2 useremo il simbolo $\alpha = (C_1; C_2)$. Definiamo in maniera piú rigorosa **numero reale** la coppia $(C_1; C_2)$ di classi contigue di cui α è l'unico elemento separatore.

Osservazione 5.4.2 *Si puó dimostrare che presi comunque due numeri reali α_1 ed α_2 con $\alpha_1 < \alpha_2$ esiste sempre un numero reale α tale che $\alpha_1 < \alpha < \alpha_2$. Ció si esprime dicendo che l'insieme* **R** *è* **continuo.**

Inoltre presi comunque due numeri reali α_1 ed α_2 con $\alpha_1 < \alpha_2$ esiste sempre un numero razionale q tale che $\alpha_1 < q < \alpha_2$. Ció si esprime dicendo che i numeri razionali sono **densi** *nei reali. Nonostante ció i razionali, che sono una infinitá numerabile, sono molti meno degli irrazionali che hanno la potenza del continuo.*

Operazioni con i numeri reali.

Diremo che due numeri reali $\alpha = (A_1, A_2), \beta = (B_1, B_2)$ sono **uguali** quando ogni numero di A_1 è $\leq$ di ciascun numero di B_2 e ogni numero di B_1 è $\leq$ di ciascun numero di A_2. Valgono le proprietá riflessiva, simmetrica e transitiva.

Due numeri reali $\alpha = (A_1, A_2), \beta = (B_1, B_2)$ che non siano uguali si dicono **disuguali**. Piú particolarmente se $\alpha \neq \beta$ si dice che α è **maggiore** di β, quando vi è qualche numero di A_1 maggiore di qualche numero di B_2. Invece si dice che α è **minore** di β quando vi è qualche numero di A_2 minore di qualche numero di B_1. Per $>$ e $<$ vale la proprietá transitiva.

Si chiama **somma** di due numeri reali $\alpha = (A_1, A_2), \beta = (B_1, B_2)$ il numero reale $(A_1 + B_1, A_2 + B_2)$.

Il numero reale $(-B_1, -B_2)$ è l'opposto del numero $\beta = (B_1, B_2)$ e si denota con $-\beta$.

Si chiama **prodotto** di due numeri reali $\alpha = (A_1, A_2), \beta = (B_1, B_2)$ il numero reale (A_1B_1, A_2B_2).

Il numero reale $(1/B_2, 1/B_1)$ è l'inverso di β e si denota con $1/\beta$.

Infine proviamo l'unicitá dell'elemento di separazione di due classi contigue.

Sia $\alpha = (A_1, A_2)$. Se per assurdo le due classi A_1, A_2 avessero un altro elemento separatore $\alpha_1 > \alpha$ allora per ogni $h \in A_1$ e per ogni $k \in A_2$ risulta:

$$h < \alpha < \alpha_1 < k$$

e quindi $k - h > \alpha_1 - \alpha$. La relazione precedente dice che la differenza tra due numeri qualsiasi rispettivamente di A_1 e A_2 è sempre maggiore di $\alpha_1 - \alpha$ e ció è assurdo per la proprietá dell'avvicinamento indefinito delle classi contigue.

Osservazione 5.4.3 *Se ho due classi contigue l'elemento di separazione è unico, viceversa dato un numero reale questo puó essere individuato da piú di una coppia di classi contigue.*

Un altro metodo per definire i numeri reali è quello dovuto a Cantor - Meray che utilizza le successioni di Cauchy.

Definizione 5.4.4 *Si dice che una successione $\{a_n\}$ di numeri razionali* **converge** *a un numero razionale a se:*

$$\forall \epsilon \in \mathbf{Q}^+ \ \ \exists n_0 | \ \forall n \geq n_0 \ \textit{risulti} \ |a_n - a| < \epsilon$$

e si scrive $lim a_n = a$.

Teorema 5.4.5 *Una successione convergente in* $\mathbf{Q}$ *ammette un unico limite.*

Definizione 5.4.6 *Una successione* $\{a_n\}$ *di numeri razionali è* **di Cauchy** *se*

$$\forall \epsilon \in \mathbf{Q}^+ \ \ \exists n_0 | \ \forall n_1, n_1 \geq n_0 \ \textit{risulti} \ |a_{n_1} - a_{n_2}| < \epsilon$$

Sussite la seguente proposizione:

Proposizione 5.4.7 *Se una successione di razionali è convergente in* $\mathbf{Q}$ *allora essa è di Cauchy.*

Della precedente proposizione non vale il vicevera in quanto esistono in $\mathbf{Q}$ successioni di Cauchy che non sono convergenti in $\mathbf{Q}$.

Tale fatto si esprime dicendo che $\mathbf{Q}$ non è completo.

(Ad esempio la successione $1, 1, 4, 1, 41, 1, 414, 1, 4142, ...$ in $\mathbf{Q}$ è di Cauchy ma non convergente).

Si puó costruire un nuovo insieme $\mathbf{R}$, che chiameremo numeri reali, in cui ogni successione di Cauchy è convergente. Pertanto l'insieme dei numeri reali è **completo.** Inoltre $\mathbf{R}$ contiene un sottoinsieme isomorfo a $\mathbf{Q}$.

Per effettuare tale costruzione consideriamo la seguente relazione di equivalenza tra le successioni di Cauchy di $\mathbf{Q}$.

Definizione 5.4.8 *Due successioni di Cauchy* $\{a_n\}$ *e* $\{b_n\}$ *si dicono* **equivalenti** *se la loro differenza* $\{a_n - b_n\}$ *converge a zero. E si scrive*

$$\{a_n\} \rho \{b_n\} \iff lim(a_n - b_n) = 0$$

Poichè ρ è una relazione di equivalenza, l'insieme delle successioni di Cauchy di $\mathbf{Q}$ resta ripartito in classi di equivalenza. Denotiamo con $\mathbf{R}$ l'insieme quoziente cosí ottenuto. Pertanto diremo **numero reale** ogni classe costituita da tutte le successioni di Cauchy tra loro equivalenti, che denoteremo con $\alpha = [\{a_n\}]$.

Sia $\alpha = [\{a_n\}]$, dove $\{a_n\}$ è una successione di Cauchy di $\mathbf{Q}$. Se la successione $\{a_n\}$ era convergente a un numero razionale a allora identificheremo $\alpha = [\{a_n\}]$ con a che quindi è un numero razionale.

Se invece $\{a_n\}$ era di Cauchy ma non convergente in $\mathbf{Q}$ allora diremo che $\alpha = [\{a_n\}]$ è un numero **irrazionale**. In tal caso possiamo rappresentare α con un elemento della successione $\{a_n\}$ seguito da puntini.

Da quanto detto segue che i razionali sono contenuti nei reali. Si puó dimostrare che nei reali ogni successione di Cauchy è convergente.

5.5 I numeri complessi

Il sistema dei numeri reali ha un'evidente limitazione che consiste in questo: l'equazione $x^2 = -1$ non ha soluzione in $\mathbf{R}$. Si puó rimediare a questa limitazione aggiungendo ai reali ulteriori numeri e formando il sistema $\mathbf{C}$ dei numeri complessi. Esso è algebricamente chiuso, ossia ogni equazione a coefficienti in $\mathbf{C}$ ha soluzioni in $\mathbf{C}$, pertanto non è ulteriormente ampliabile come abbiamo fatto per passare da $\mathbf{N}$ a $\mathbf{Z}$, da $\mathbf{Z}$ a $\mathbf{Q}$, da $\mathbf{Q}$ a $\mathbf{R}$ e da $\mathbf{R}$ a $\mathbf{C}$.

Consideriamo il prodotto cartesiano $\mathbf{R} \times \mathbf{R}$ che denotiamo con $\mathbf{C}$ e definiamo in esso una somma e un prodotto:

$$(a, b) + (c, d) = (a + b, c + d)$$
$$(a, b)(c, d) = (ac - bd, ad + bc).$$

$(0, 0)$ è l'elemento neutro per la somma, $(1, 0)$ è l'elemento neutro per il prodotto, l'opposto di (a, b) è $(-a, -b)$ e l'inverso di ogni elemento non nullo (a, b) risulta $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}$.

L'applicazione $a \leftrightarrow (a, 0)$ è un isomorfismo tra $\mathbf{R}$ e il sottoinsieme $\{(a, 0)|a \in \mathbf{R}\}$ di $\mathbf{C}$.

Per ogni numero complesso $z = (a, b)$ definiamo **coniugato** di z il numero complesso $\overline{z} = (a, -b)$.

Osserviamo che $(0, 1)^2 = (0, 1)(0, 1) = (-1, 0) \leftrightarrow -1$ pertanto $(0, 1)$ è soluzione dell'equazione $x^2 = -1$. Chiamiamo $(0, 1)$ l'unitá immaginaria e denotiamola con i; abbiamo $i^2 = -1$. Inoltre risulta

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1) = x + iy.$$

Rappresentazione trigonometrica.

$$x + iy \leftrightarrow (x, y)$$

Se $P(x, y)$ è un punto del piano cartesiano e θ è l'angolo tra OP e l'asse delle ascisse risulta

$$x = rcos\theta; \qquad y = rsen\theta$$

ove $r = \sqrt{x^2 + y^2}$ da cui

$$z = x + iy = r(cos\theta + isen\theta)$$

$$z_1 = r_1(cos\theta_1 + isen\theta_1), z_2 = r_2(cos\theta_2 + isen\theta_2)$$

allora

$$z_1 z_2 = r_1 r_2(cos(\theta_1 + \theta_2 + isen(\theta_1 + \theta_2)$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(cos(\theta_1 - \theta_2 + isen(\theta_1 - \theta_2)$$

Teorema 5.5.1 (La formula di De Moivre) *Se n è un intero positivo allora*

$$[r(cos\theta + sen\theta)]^n = r^n(cosn\theta + isenn\theta)$$

Le radici n-esime di un numero complesso $z = r(cos\theta + isen\theta)$ sono

$$\sqrt[n]{(z)} = \{\sqrt[n]{r}(cos(teta/n + 2k\pi/n) + isen(teta/n + 2k\pi/n)\}$$

con $k = 0, 1, \ldots, n-1$.

Le radici n-esime dell'unitá $1 = cos0 + isen0$ sono:

$$\sqrt[n]{(1)} = \{(cos(2k\pi/n) + isen(2k\pi/n)\}$$

e posto $\rho = cos2\pi/n + isen2\pi/n$ possono essere scritte come

$$\sqrt[n]{(1)} = \{1, \rho, \rho^2, \rho^{n-1}.\}$$

Radici primitive dell'unitá

Una radice n-esima dell'unitá , z è detta **primitiva** se per ogni $m < n$ risulta $z^m = 1$. Ad esempio considerate le radici seste dell'unitá $1, \rho, \rho^2, \rho^3, \rho^4, \rho^5$ sono radici primitive dell'unitá ρ e ρ^5 in quanto $(\rho^5)^m \neq 1$ per ogni $m < 6$, mentre tutte le altre non sono primitive.

Corollario 5.5.2 *Le radici n-esime primitive dell'unitá sono quelle tra $1, \rho, \rho^2, \rho^3, \rho^4, \rho^5$ che hanno esponenti primi con n*

5.6 Numeri algebrici e trascendenti

Definizione 5.6.1 *Un numero reale o complesso è* **algebrico** *se è soluzione di un'equazione algebrica $F(x) = 0$, cioè di un polinomio intero a coefficienti razionali eguagliato a zero.*

Un numero reale o complesso è **trascendente** *se non è algebrico ossia se non esiste alcuna equazione algebrica $F(x) = 0$ di cui egli è soluzione.*

I numeri razionali m/n sono tutti algebrici perchè radici dell'equazione del tipo $mx = n$.

Sono algebriche tutte le radici n-esime di numeri razionali e le loro somme come ad esempio $\sqrt[3]{5}$ che è soluzione di $x^3 = 5$. Sono algebrici anche i radicali doppi come ad esempio $\sqrt{1 + \sqrt{2}}$ che è soluzione di $x^4 - 2x^2 - 1 = 0$.

Definizione 5.6.2 *Chiamasi* **equazione canonica** *relativa ad un numero algebrico l'equazione algebrica di grado minimo di cui esso è radice e* **grado** *del numero algebrico quello della sua equazione canonica.*

Esempio 5.6.3 *Per* $\sqrt{2}$ *il polinomio minimo è* $x^2 - 2 = 0$ *è il suo grado è due.*

Se considero le radice seste dell'unitá $1, \rho, \rho^2, \rho^3, \rho^4, \rho^5$ *allora le radici primitive dell'unitá* ρ *e* ρ^5 *hanno come polinomio minimo* $z^6 = 1$ *e quindi hanno grado sei;* ρ^2 *verifica* $z^6 = 1$ *ovviamente, ma ha come polinomio minimo* $z^3 = 1$ *e quindi ha grado tre.*

In generale le radici n*-esime* $\neq 1$ *dell'unitá con* n *primo sono tutte numeri algebrici di grado* n*.*

I numeri razionali sono algerici di primo grado; gli irrazionali quadratici sono algebrici di secondo grado.

Se a è un numero algebrico di grado n, le altre $n-1$ radici della sua equazione canonica si dicono i suoi coniugati.

Sussiste il seguente

Teorema 5.6.4 *L'insieme dei numeri algebrici reali è numerabile.*

Dim. Indicata con $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ l'equazione canonica di un numero algebrico a definiamo sua **altezza** il numero $H = (n-1) + |a_0| + |a_1| + \cdots + |a_n|$. Allora, poichè fissata l'altezza H il numero delle equazioni algebriche a coefficienti interi, aventi per altezza H è finito sará possibile ordinare i numeri algebrici reali per altezza crescente e quelli di data altezza secondo l'ordine naturale crescente (omettendo eventualmente quelli che precedentemente si sono giá incontrati); in tal modo il teorema è dimostrato. □

Esempio 5.6.5 *Per* $H = 1$ *si ha la sola equazione* $x = 0$*, per* $H = 2$ *si hanno* $2x = 0, x + 1 = 0, x - 1 = 0, x^2 = 0$*.*

Pertanto l'insieme dei numeri reali si divide in:

- razionali: che sono tutti algebrici ed in quantitá numerabile;
- irrazionali che si dividono in:
  - irrazionali algebrici che sono in quantitá numerabile;
  - irrazionali trascendenti che sono in quantitá continua.

Da ció segue che quasi tutti i numeri reali sono trascendenti.

E' stato dimostrato che i numeri $e, \pi, log2, e^\pi, 2^{\sqrt{2}}$ sono trascendenti.

Teorema 5.6.6 (di Lindemann) *Se $a_1, a_2, \ldots, a_n$ sono numeri algebrici, tanto reali che complessi, e $c_1, c_2, \ldots, c_n$ sono numeri interi relativi non tutti nulli è sempre*

$$c_1 e^{a_1} + c_2 e^{a_2} + \cdots + c_n e^{a_n} \neq 0$$

Utilizzando il teorema di Lindemann si puó dimostrare la trascendenza di:

- *il numero e è trascendente.* Infatti e non puó soddisfarre alcuna equazione algebrica a coefficienti interi della forma

  $$c_1 e^n + c_2 e^{n-1} + \cdots + c_n = 0$$

  per il teorema di Lindemann essendo $n, n-1, \ldots, 1$ algebrici.

- *il numero π è trascendente.* Infatti essendo $e^{i\pi} + 1 = 0$ ne segue che $i\pi$ è trascendente, altrimenti sarebbe contraddetto il teorema di Lindemann, poichè i è algebrico allora π è trascendente.