Per ben cominciare

A. Tonolo

30 settembre 2002

1 Gli insiemi numerici

Con il simbolo $\mathbb{N}$ si indica l'insieme dei numeri *naturali*; si tratta dei numeri

$$0, 1, 2, 3, \ldots$$

incontrati già alle scuole elementari. Nell'insieme $\mathbb{N}$ è possibile fare la somma, ma non la sottrazione: $3 - 7$ non è un numero naturale. Per poter fare le sottrazioni, si considera allora l'insieme $\mathbb{Z}$ dei numeri *interi*; si tratta dei numeri

$$\ldots -3, -2, -1, 0, 1, 2, \ldots.$$

Nell'insieme $\mathbb{Z}$ è possibile fare le moltiplicazioni, ma non le divisioni. Per poter fare le divisioni, si considera l'insieme $\mathbb{Q}$ dei numeri *razionali*; si tratta dell'insieme delle frazioni, ovvero dei numeri del tipo $\frac{a}{b}$ con a, b numeri interi. I numeri razionali possono anche essere descritti in altro modo: essi sono i numeri del tipo $a, b_1 b_2 b_3 \ldots$ con un numero finito di decimali (ad esempio $\frac{1}{2} = 0,5$) o periodici, ovvero con infiniti decimali ottenuti ripetendo una sequenza finita di numeri (ad esempio $\frac{13}{99} = 0,1313131313\ldots$). Sorge spontaneo ingrandire l'insieme dei numeri razionali considerando tutti i numeri del tipo $a, b_1 b_2 b_3 \ldots$ senza restrizioni su come devono comportarsi i decimali: otteniamo cosí l'insieme $\mathbb{R}$ dei numeri reali. Sono numeri reali non razionali il numero π, rapporto tra la semicirconferenza ed il raggio, oppure la radice $\sqrt{2}$. L'insieme dei numeri reali ha delle belle proprietà: si tratta, come del resto gli insiemi numerici precedentemente trattati, di un insieme *totalmente ordinato*, ovvero comunque dati due numeri reali r ed s sicuramente o $r \leq s$ oppure $s \leq r$. In piú rispetto ai razionali ha la proprietà seguente: comunque dato un insieme S di numeri reali inferiormente limitato, l'insieme

$$\{r \in \mathbb{R} : r \leq s,\ \forall s \in S\}$$

dei *minoranti* di S ha un elemento massimo. Tale elemento massimo è detto *estremo inferiore* di S, in breve $\inf S$. Analogamente, comunque dato un insieme T di numeri reali superiormente limitato, l'insieme

$$\{r \in \mathbb{R} : r \geq t,\ \forall t \in T\}$$

dei *maggioranti* di T ha un elemento minimo. Tale elemento minimo è detto *estremo superiore* di T, in breve $\sup T$.

L'insieme dei numeri reali non sempre è sufficiente. È ben noto che esistono polinomi di secondo grado a coefficienti reali che non possono essere scomposti nel prodotto di fattori lineari: ad esempio $x^2 + 1$. Questo corrisponde al fatto che esistono equazioni di secondo

grado (quelle con discriminante negativo) che non ammettono soluzioni. Per superare anche questo problema si introducono i numeri complessi. I numeri complessi sono del tipo

$$a + ib$$

dove a e b sono numeri reali, mentre i è la cosidetta *unità immaginaria*. È propio l'unità immaginaria i la novità rispetto ai numeri reali: i indica la radice $\sqrt{-1}$. Il numero reale a è detto parte reale di $a + ib$; il numero reale b è detto parte immaginaria di $a + ib$. Due numeri complessi coincidono se coincidono le loro parti reali ed immaginarie. I numeri del tipo $a + i0$ si scrivono semplicemente a; in questo modo i numeri reali sono particolari numeri complessi.

Come si sommano i numeri complessi? Raccogliendo l'unità immaginaria i:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Come si moltiplicano i numeri complessi? Raccogliendo l'unità immaginaria i, ricordando che $i \cdot i = i^2 = -1$:

$$(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

Dato un numero complesso $z = a+ib$, con $\overline{z}$ indichiamo il *coniugato* di z, ovvero il numero complesso $\overline{z} = a - ib$. Chiaramente

$$z \cdot \overline{z} = (a + ib)\overline{(a + ib)} = (a + ib)(a - ib) = a^2 + b^2$$

è un numero reale positivo. La radice quadrata di $z \cdot \overline{z}$ è detta modulo del numero complesso z.

Come si calcola l'inverso di un numero complesso $z = a + ib \neq 0$?

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{\overline{z}}{|z|^2} = \frac{a - ib}{a^2 + b^2}.$$

L'insieme dei numeri complessi si indica con il simbolo $\mathbb{C}$.

Fatti 1.0.1 (Teorema fondamentale dell'algebra). *Ogni polinomio a coefficienti complessi si fattorizza nel prodotto di fattori lineari.*

Esempio 1.0.2. Il polinomio $x^2 + 1$ che non sapevamo scomporre in ambito reale, risulta ora facilmente scomponibile:

$$x^2 + 1 = x^2 - (i)^2 = (x + i)(x - i).$$

L'unità immaginaria i ed il suo opposto $-i$ sono le radici dell'equazione $x^2 + 1 = 0$.

Nell'introdurre i numeri complessi peró, per la prima volta, nelle estensioni sin qui fatte, oltre a guadagnare qualcosa, perdiamo anche qualche proprietà: in particolare perdiamo ogni tipo di ordinamento. Per questo motivo, lungo tutto il corso dedicheremo la nostra attenzione tanto ai numeri reali che ai numeri complessi; a seconda del problema trattato, gli uni risulteranno piú utili degli altri.

2 Il binomio di Newton

Ricordo a tutti, anche se probabilmente è superfluo, come si calcola la m-esima potenza di un binomio:

$$(x + y)^m = \sum_{k=0}^{m} \left(\begin{array}{c} m \\ k \end{array} \right) x^{m-k} y^k,$$

dove il *coefficiente binomiale* $\left(\begin{array}{c} m \\ k \end{array} \right)$ indica $\dfrac{m!}{(m-k)!k!}$. Il fattoriale $m!$ del numero naturale m è il numero $m \cdot (m-1) \cdot \ldots \cdot 2 \cdot 1$; per definizione si pone $0! = 1$.

3 Relazioni tra insiemi e funzioni

Sia X un insieme. Con il simbolo $\in$ si indica la relazione di appartenenza, pertanto $X = \{x \in X\}$. Con il simbolo $\emptyset$ si indica l'insieme vuoto, ovvero l'insieme che non ha alcun elemento. Un insieme Y è detto *sottoinsieme* dell'insieme X se

$$z \in Y \Rightarrow z \in X;$$

in tal caso scriveremo $Y \subseteq X$.

Siano Y e Z due sottoinsiemi diun insieme X. Diciamo *intersezione di Y e Z* il seguente sottoinsieme di X:

$$Y \cap Z = \{x \in X : x \in Y \text{ e } x \in Z\}.$$

$Y \cap Z$ è il piú grande sottoinsieme di X contenuto tanto in Y quanto in Z. Diciamo *unione di Y e Z* il seguente sottoinsieme di X:

$$Y \cup Z = \{x \in X : x \in Y \text{ o } x \in Z\}.$$

$Y \cup Z$ è il piú piccolo sottoinsieme di X contenente tanto Y quanto Z.

Dati due insiemi Y e Z con il simbolo $Y \times Z$ indichiamo il *prodotto cartesiano* di Y e Z, ovvero l'insieme delle coppie ordinate (y, z) ove $y \in Y$ e $z \in Z$.

Siano X e Y due insiemi non vuoti. Una funzione $f : X \to Y$ è una legge che associa ad ogni elemento x dell'insieme X uno ed un solo elemento dell'insieme Y; tale elemento viene indicato con $f(x)$ e detto *immagine* di x tramite f. L'insieme X è detto dominio della funzione f, l'insieme Y è detto codominio della funzione f. Diciamo *immagine* della funzione f il sottoinsieme $\operatorname{Im} f$ del codominio formato dalle immagini degli elementi del dominio:

$$\operatorname{Im} f = \{f(x) : x \in X\} \subseteq Y.$$

Una funzione $f : X \to Y$ è *iniettiva* se elementi distinti del dominio hanno immagini distinte, ovvero

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Si osservi che la proprietà

$$f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2,$$

ben lungi dall'essere equivalente all'iniettività o alla sua negazione, è verificata da ogni funzione, iniettiva o non iniettiva.

Una funzione $f : X \to Y$ è *suriettiva* se ogni elemento del codominio è immagine di qualche elemento del dominio, ovvero

$$\operatorname{Im} f = Y.$$

Una funzione è biiettiva se è iniettiva e suriettiva.

4 Principio di induzione

In questa sezione presentiamo una tecnica di dimostrazione estremamente potente. Proprio per la sua straordinaria utilità deve essere ben imparata, ben utilizzata e ben giustificata. Nelle righe seguenti dimostriamo che tale tecnica è corretta.

Sia $P(m)$ una proposizione nella variabile naturale m (ad esempio "$2m + 1 < m^2$"). Se per un opportuno naturale m_0 si ha

1. $P(m_0)$ è vera,

2. per ogni $l \geq m_0$, se è vera $P(l)$ allora è vera anche $P(l+1)$,

allora per ogni $m \geq m_0$ si ha che $P(m)$ è vera. Infatti: sia $F \subseteq \mathbb{N}$ il sottoinsieme dei numeri naturali $k \geq m_0$ tali che $P(k)$ è falsa:

$$F := \{k \in \mathbb{N} : k \geq m_0,\ P(k) \text{ è falsa}\}.$$

Vogliamo dimostrare che $F = \emptyset$. Procediamo per assurdo: se $F \neq \emptyset$, allora esiste in F un numero naturale f piú piccolo di tutti gli altri. Certamente, visto che per 1 $P(m_0)$ è vera, $f > m_0$; quindi $f - 1 \geq m_0$ non appartiene ad F, pertanto $P(f-1)$ è vera. Per 2, essendo $P(f-1)$ vera, anche $P(f)$ è vera: contraddizione!

Esempio 4.0.3. Consideriamo la proposizione $P(m) := 2m + 1 < m^2$; chiaramente $P(1)$ e $P(2)$ sono false. Peró $P(3)$ è vera; vediamo ora che se $l \geq 3$, $P(l)$ vera implica $P(l+1)$ vera:

$$2(l+1) + 1 = 2l + 2 + 1 = (2l+1) + 2;$$

per ipotesi induttiva (cosí si dice!) $2l + 1 < l^2$, pertanto

$$2(l+1) + 1 = (2l+1) + 2 < l^2 + 2;$$

essendo $l^2 + 2 < l^2 + 2l + 1$, si conclude $2(l+1) + 1 < (l+1)^2$, ovvero $P(l+1)$ è vera. Questo basta per concludere che per ogni $m \geq 3$ si ha $2m + 1 < m^2$.