NOZIONI DI BASE

MICHELE GRASSI

Note scritte per il primo anno del corso di laurea in Matematica del Dipartimento di Matematica dell'Università di Pisa, a.a. 2006-2007

1. Nozione di insieme

La nozione di insieme è usualmente considerata un *concetto primitivo* in matematica, ovvero un concetto che non si cerca di definire ma si prende come dato intuitivamente. Per procedere in modo rigoroso dovremmo però elencare le proprietà che ci aspettiamo che gli insiemi debbano soddisfare. Per i fini di questo corso sarà invece sufficiente la nozione intuitiva di insieme.
Notazione *Appartenenza di elementi ad insiemi* Quando l'elemento x appartiene all'insieme S, si scrive $x \in S$
Definizione *Uguaglianza e disuguaglianza di insiemi* Due insiemi sono uguali se e solo se contengono gli stessi elementi: in notazione matematica,

$$S = T \iff (\forall x \; x \in S \iff x \in T)$$

Quando due insiemi non sono uguali scriviamo $S \neq T$.
Notazione Per descrivere un insieme è necessario descrivere i suoi elementi. Quando questi elementi sono pochi, si possono semplicemente elencare. La notazione matematica per l'insieme formato dai numeri $2, 4$ e 6 è la seguente:

$$S = \{2, 4, 6\}$$

Si noti che gli elementi ripetuti vengono contati solo una volta, per cui $\{2, 4, 6\} = \{2, 2, 4, 6\}$.
Esempio
$\emptyset$ *l'insieme vuoto*
$\mathbb{N} = \{0, 1, 2, 3, ...\}$ (numeri naturali),
$\mathbb{Z} = \{-2, -1, 0, 1, 2, ...\}$ (numeri interi),
$\mathbb{Q} = \{0, 1, \frac{2}{5}, -\frac{7}{3}, ...\} = \{\frac{p}{q} \mid p \in \mathbb{Z}, \; q \in \mathbb{N}\}$ (numeri razionali)

Dato un insieme, possiamo individuare un certo numero di suoi elementi che soddisfano una qualche proprietà, e considerarli come elementi di un nuovo insieme, che sarà incluso in quello iniziale, nel senso che tutti i suoi elementi sono anche elementi di quello iniziale. In notazione matematica, diciamo che
Definizione S è incluso in T, e scriviamo $S \subset T$ quando vale quanto segue:

$$S \subset T \iff (\forall x \; x \in S \implies x \in T)$$

È chiaro che quando un insieme è incluso in un altro e a sua volta lo include, deve coincidere con esso. Questa affermazione ovvia può essere formalizzata in una proposizione matematica, che necessita di una dimostrazione rigorosa

Proposizione $S = T \iff S \subset T$ e $T \subset S$
Dimostrazione Dimostriamo prima che $S = T \implies S \subset T \wedge T \subset S$. Se $S = T$, per la definizione scritta prima sappiamo che deve valere $\forall x\ x \in S \iff x \in T$. Da questo seguono le due proprietà:

$$\forall x\ x \in S \implies x \in T,\ \forall x\ x \in T \implies x \in S$$

che dicono esattamente (per definizione) che $S \subset T$ e $T \subset S$.
Viceversa, supponiamo di sapere che $S \subset T \wedge T \subset S$. Allora per definizione questo vuol dire che

$$\forall x\ x \in S \implies x \in T,\ \forall x\ x \in T \implies x \in S$$

da cui segue che $\forall x\ x \in S \iff x \in T$, che di nuovo per definizione vuol dire che $S = T$. □
Questa dimostrazione dovrebbe rendere chiara la differenza fra affermare "è chiaro" e "dimostrare". Molto spesso in matematica cose che sembrano "chiare" si rivelano non così chiare (o magari false) quando si prova a dimostrarle.
Definizione S è un *sottoinsieme proprio* di T se $S \subset T$ e $S \neq T$
Esempio $\{2, 3\} \subset \{2, 3, 5\}$ Quando vogliamo individuare degli elementi specifici di un insieme per definire un sottoinsieme, usando la proprietà P, usiamo la seguente notazione
Notazione $T = \{x \in S \mid x \text{ soddisfa } P\}$
Esempio $\{2, 3\} = \{x \in \{2, 3, 5\} \mid x \neq 5\}$
La notazione semplificata $\{x \mid x \text{ soddisfa } P\}$ si usa quando e' chiaro da dove prendiamo gli elementi x. Ad esempio, se stiamo parlando di numeri interi, possiamo scrivere $\{x \mid x \text{ è pari}\}$ invece del più corretto $\{x\ \in \mathbb{N} |\ x \text{ è pari}\}$.
Definizione Dati gli insiemi S, T, possiamo definire dei nuovi insiemi:
$S \cup T = \{x \mid x \in S\ \vee\ x \in T\}$ (unione di S e T)
$S \cap T = \{x \mid x \in S\ \wedge\ x \in T\}$ (intersezione di S e T) $S \setminus T = \{x \mid x \in S \wedge\ \notin T\}$ (differenza di S e T)
Esempio $\{1, 4, -3\} \cup \{4, 5, 7\} = \{1, 4, -3, 5, 7\}$ $\{1, 4, -3\} \cap \{4, 5, 7\} = \{1\}$), $\{1, 4, -3\} \cap \{5, 7\} = \emptyset$)
Teorema Dati gli insiemi R, S, T, valgono le seguenti proprietà:
a) (commutativa) $S \cap T = T \cap S$, $S \cup T = T \cup S$.
b) (associativa) $S \cap (T \cap U) = (S \cap T) \cap U$, $S \cup (T \cup U) = (S \cup T) \cup U$.
c) (distributiva) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$, $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
Dimostrazione a) Esercizio
b) Esercizio
c) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$: dimostriamo la doppia inclusione.
Dimostrazione di $R \cap (S \cup T) \subset (R \cap S) \cup (R \cap T)$: Sia $x \in R \cap (S \cup T)$. Allora deve essere $x \in R$ e $x \in S \cup T$. Quindi $x \in S$ o $x \in T$. Nel primo caso, $x \in R \cap S$, mentre nel secondo caso $x \in R \cap T$. Quindi $x \in (R \cap S) \cup (R \cap T)$.
Dimostrazione di $(R \cap S) \cup (R \cap T) \subset R \cap (S \cup T)$:Sia $x \in (R \cap S) \cup (R \cap T)$. Allora deve essere o $(R \cap S)$ oppure $x \in (R \cap T)$. Quindi si ha in ogni caso $x \in R$, e inoltre o $x \in S$ o $x \in T$, ovvero $x \in S \cup T$.
L'altra proprietà distributiva si dimostra in modo simile. La dimostrazione è lasciata come esercizio. □
Gli elementi di un insieme possono essere a loro volta insiemi.
Esempio $\{\mathbb{N}, \mathbb{Q}, \mathbb{Z}\}$ è un insieme con tre elementi.
Definizione Dato un insieme S, l'*insieme delle parti* di S, indicato con $\mathcal{P}(S)$, è

definito come

$$\mathcal{P}(S) = \{X \mid X \subset S\}$$

Esempio

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

Esempio Dato $i \in \mathbb{N}$, sia $T_i = \{x \in \mathbb{Z} \mid x = yi \text{ per qualche } y \in \mathbb{Z}\}$. Al variare di $i \in \mathbb{N}$ si ottengono sottoinsiemi diversi di $\mathbb{Z}$. Possiamo costruire allora l'insieme $\{T_i \mid i \in \mathbb{N}\}$, che contiene tutti i T_i come elementi. Si ha chiaramente che $\{T_i \mid i \in \mathbb{N}\} \subset \mathcal{P}(\mathbb{Z})$

Definizione Dato un insieme S i cui elementi sono a loro volta insiemi, definiamo:
$\bigcup S = \{x \mid \exists T \in S : x \in T\}$ (unione di S)
$\bigcap S = \{x \mid \forall T \in S : x \in T\}$ (intersezione di S)

Esempio Per ogni insieme X, si ha $\bigcup \mathcal{P}(X) = X$.

Esempio $\bigcup\{\{2,3\},\{3,4\}\} = \{2,3,4\}$.

Esempio $\bigcap\{\{2,3\},\{3,4\}\} = \{3\}$.

Esempio Prendendo $S = \{T_i \mid i \in \mathbb{N}\}$, si ha che $\bigcup S = \mathbb{Z}, \bigcap S = \{0\}$.

Dimostrazione Dato che $T_1 = \mathbb{Z}$, si ha che $\mathbb{Z} \subset \bigcup S$, e inoltre dato che $\forall i\ T_i \subset \mathbb{Z}$ deve anche essere $\bigcup S \subset \mathbb{Z}$. Unendo questi due fatti si ha che $\bigcup S = \mathbb{Z}$.
Supponiamo ora per assurdo che esista $x \in \bigcap S$, con $x > 0$. Si dovrebbe avere per definizione di intersezione che $\forall i\ x \in T_i$, e quindi in particolare $x \in T_{2x}$. Questo significherebbe però che esiste $y \in \mathbb{Z}$ con $x = 2xy$, e questo è assurdo. Se invece fosse $x \in \bigcap S$ con $x < 0$, si dovrebbe avere analogamente che $x \in T_{-2x}$, e quindi dovrebbe esistere $y \in \mathbb{Z}$ con $x = -2xy$ che è assurdo. Dato che chiaramente $0 \in \bigcap S$, ne segue che deve essere $\bigcap S = \{0\}$.

Definizione Una *funzione* con *dominio* A e *codominio* B è una regola per associare ad ogni elemento di A uno ed un solo elemento di B. In tal caso scriviamo $f : A \to B$. Se indichiamo con f una funzione, allora il suo dominio si indica con $Dom(f)$, il suo codominio si indica con $Cod(f)$, e il valore della funzione sull'elemento $x \in Dom(f)$ si indica con $f(x) \in Cod(f)$. Se $C \subset A$ e $f : A \to B$, allora f definisce una regola per associare ad ogni elemento di C uno ed un solo elemento di B, semplicemente pensando gli elementi di C come particolari elementi di A. In questo modo si ottiene una funzione da C a B, che si chiama *restrizione* di f a C e si indica con $f|_C$.

Esempio Dato $A = \mathbb{Z}$ e $B = \mathbb{N}$, definiamo $f(x) = x^2$. Con lo stesso simbolo $f(x) = x^2$ si può indicare anche $f|_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$, stavolta però la x varia solo in $\mathbb{N}$ e non in tutto $\mathbb{Z}$.

Definizione Una funzione f da un insieme A ad un insieme B si dice:
Iniettiva se $\forall x_1, x_2 \in A\ f(x_1) = f(x_2) \implies x_1 = x_2$
Surgettiva se $\forall y \in B\ \exists x \in A\ :\ f(x) = y$.
Bigettiva se è sia iniettiva che bigettiva.

Esempio La funzione dell'esempio precedente non è ne surgettiva ne iniettiva, dato che non tutti i naturali sono quadrati (ad esempio 2 non lo è), e $f(x) = f(-x)$ per ogni $x \in \mathbb{Z}$. La sua restrizione $f|_{\mathbb{N}}$ è iniettiva, ma non surgettiva. Se definiamo $D = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : x = y^2\}$, allora possiamo pensare sia f che $f|_{\mathbb{N}}$ come funzioni a valori in D. In questo caso f è surgettiva, e $f|_{\mathbb{N}}$ è bigettiva.

Definizione Date due funzioni $f : A \to B$ e $g : B \to A$, diciamo che g è *inversa* di f se vale che

$$\forall x \in A\ g(f(x)) = x\ \forall y \in B\ f(g(y)) = y$$

Quando per una data funione f esiste una g che è inversa di f, diciamo che f è *invertibile*.
Proposizione Una funzione è invertibile se e solo se è bigettiva. In questo caso, la sua inversa è unica
Dimostrazione Esercizio □

2. Principio del buon ordinamento e principio di induzione

Principio del buon ordinamento *Ogni insieme non vuoto di numeri naturali contiene un elemento minimo*
Il principio del buon ordinamento è equivalente al seguente
Principio di induzione *Sia S un insieme di numeri naturali con le seguenti proprietà:*
a) $1 \in S$
b) Se $x \in S$, allora $x + 1 \in S$.
Allora $S = \mathbb{N}$.
Teorema Il principio di induzione ed il principio del buon ordinamento sono equivalenti.
Dimostrazione Dimostriamo che il principio di induzione implica il principio del buon ordinamento:
Sia $S \subset \mathbb{N}$, $S \neq \emptyset$, e prendiamo $T = \{n \in \mathbb{N} \mid \forall t \in S \; n < t\}$ Si dimostra allora che $1 \in T$ e $x \in t \implies x + 1 \in T$, e quindi per il principio di induzione $T = \mathbb{N}$, contraddicendo $S \neq \emptyset$.
Viceversa, dimostriamo che il principio del buon ordinamento implica il principio di induzione:
Sia S un insieme di numeri naturali tale che $1 \in S$ e se $x \in S$, allora $k + 1 \in S$. Vogliamo dimostrare che $S = \mathbb{N}$ usando il principio del buon ordinamento. Supponiamo per assurdo che $S \neq \mathbb{N}$. Allora $T = \mathbb{N} \setminus S \neq \emptyset$. T ammette quindi un minimo, chiamiamolo m. Deve esssere $m > 1$, perche' $1 \in S$ per ipotesi. Ma allora si ha che $m - 1 \in \mathbb{N}$, e inoltre $m - 1 \notin T$ perchè m è il minimo di T e $m - 1 < m$. Deve essere quindi $m-1 \in S$, e quindi per ipotesi $m = (m-1)+1 \in S$, assurdo. □

Per definire una espressione $F(n)$ che dipende da $n \in \mathbb{N}$, possiamo usare un metodo induttivo, nel senso che definiamo $F(1)$ e poi diamo un modo per dire quanto vale $F(n + 1)$ sapendo quanto vale $F(n)$. In questo modo l'insieme S degli $n \in \mathbb{N}$ per cui $F(n)$ è definito contiene 1, e se contiene n allora contiene $n + 1$. Per il principio di induzione, deve essere $S = \mathbb{N}$, e quindi abbiamo definito $F(n)$ per tutti gli N.
Esempio Potenza di un numero razionale: $F(n) = x^n$ per un qualche (fissato) $x \in \mathbb{Q}$. Definiamo $F(1) = x$, e $F(n + 1) = xF(n)$. In altre parole, per definire x^n diciamo che $x^1 = x$, e $x^{n+1} = x(x^n)$. È chiaro che in questo modo definiamo x^n er tutti gli $n \in \mathbb{N}$.
Esempio Simbolo di sommatoria: $F(n) = \sum_{i=1}^{n} f(i)$, per qualche funzione $f = f(i)$ nota.
Definiamo $F(1) = f(1)$, e $F(n + 1) = F(n) + f(n + 1)$. Questa è una buona definizione per induzione, e la funzione F che si ottiene si indica con $\sum_{i=1}^{n} f(i)$.
Usando il principio di induzione si possono fare le cosiddette dimostrazioni per induzione, in cui si dimostrano in genere (ma non esclusivamente) proprietà di quantità che sono stade a loro volta definite in modo induttivo. Vediamo di seguito

due esempi.

Proposizione $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Dimostrazione Faremo una *dimostrazione per induzione*: Sia $\subset \mathbb{N}$ l'insieme dei numeri naturali per cui l'affermazione "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$" è vera. Vogliamo dimostrare che $S = \mathbb{N}$. Intanto $1 \in S$, perche' l'affermazione per $n = 1$ è semplicemente $1 = 1$. Supponiamo di sapere che $n \in S$, e cerchiamo di dimostrare che $n+1 \in S$. In effetti $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1)$ che è uguale, per ipotesi induttiva, a $\frac{n(n+1)}{2} + (n+1)$. Quest'ultima espressione è però chiaramente

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

□

Proposizione Per qualunque numero (razionale) $x \neq 1$ e qualunque $n \in \mathbb{N}$, vale $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$

Dimostrazione Dimostriamo il teorema per induzione su n. Per $n = 1$ la proposizione dice che $\sum_{i=0}^{1} x^i = \frac{1-x^2}{1-x}$, e questo si verifica direttamente, osservando che $\sum_{i=0}^{n} x^i = 1 + x$ per definizione (usiamo la convenzione $x^0 = 1$.

Supponiamo di sapere la proposizione per $n = h$, e dimostriamola per $n = h + 1$. Vogliamo dimostrare che $\sum_{i=0}^{h+1} x^i = \frac{1-x^{h+2}}{1-x}$. Per definizione di sommatoria sappiamo che

$$\sum_{i=0}^{h+1} x^i = \sum_{i=0}^{h} x^i + x^{h+1}$$

Per ipotesi induttiva, questo si può riscrivere:

$$\sum_{i=0}^{h} x^i + x^{h+1} = \frac{1 - x^{h+1}}{1 - x} + x^{h+1}$$

e una semplice manipolazione algebrica di questa espressione la rende uguale a $\frac{1-x^{h+2}}{1-x}$. Per il principio di induzione, abbiamo dimostrato la tesi del teorema. □

3. Insiemi finiti ed insiemi numerabili

Definizione Un insieme X si dice *finito* se esiste una funzione bigettiva da X ad un insieme di numeri naturali del tipo $\{1, ..., n\} = \{x \in \mathbb{N} \mid x \leq n\}$ per qualche $n \in \mathbb{N}$

Definizione Un insieme X si dice *numerabile* se esiste una funzione bigettiva da X a $\mathbb{N}$.

Esempio L'insieme $\mathbb{Z}$ è numerabile.

Dimostrazione Costruiamo una funzione bigettiva $f : \mathbb{N} \to \mathbb{Z}$ nel modo seguente: $f(x) = \frac{x}{2}$ se x è pari, e $f(x) = -\frac{x-1}{2}$ se x è dispari. Si verifica facilmente che f è bigettiva, e quindi $\mathbb{Z}$ è numerabile. □

Esempio L'unione di due insiemi numerabili o di un insieme numerabile ed un insieme finito è numerabile.

Dimostrazione Supponiamo che S_1 sia numerabile e S_2 sia finito, e sia $X = S_1 \cup S_2$. Sostituendo S_2 con $S_2 \setminus S_1$ possiamo assumere che $S_1 \cap S_2 = \emptyset$. Sia $f : S_1 \to \mathbb{N}$ bigettiva, e supponiamo che $S_2 = \{y_1, ..., y_n\}$ per quanche $n \in \mathbb{N}$ (se $S_2 = \emptyset$ non c'e' nulla da dimostrare, dato che in questo caso $S_1 = X$). Definiamo una nuova funzione $h : X \to \mathbb{N}$ in questo modo: $h(y_i) = i$ per $i = 1, .., n$, e $h(x) = f(x) + n$ se

$x \in S_1$. La funzione h è una bigezione fra X e $\mathbb{N}$, e quindi X è numerabile.
Se invece S_1, S_2 sono entrambi numerabili, sia di nuovo $X = S_1 \cup S_2$. Se $S_2 \setminus S_1$ è finito ci possiamo ricondurre alla dimostrazione precedente, quindi possiamo assumere che $S_1 \cap S_2 = \emptyset$ e sia S_1 che S_2 sono numerabili. Costruiremo ora una bigezione fra X e $\mathbb{Z}$, e questo basterà per concludere la dimostrazione perchè abbiamo già visto che $\mathbb{Z}$ è numerabile. Siano $f_1 : S_1 \to \mathbb{N}$ e $f_2 : S_2 \to \mathbb{N}$ due bigezioni (che esistono percè entrambi gli insiemi sono numerabili). Definiamo $h : X \to \mathbb{Z}$ in questo modo: se $x \in S_1$, $h(x) = f_1(x)$; se $x \in S_2$, $h(x) = 1 - f_2(x)$. La h così costruita è una bigezione (esercizio). □

Esercizio L'insieme $\mathbb{N} \times \mathbb{N}$ delle coppie di numeri naturali è numerabile.

Proposizione Un sottoinsieme di un insieme numerabile o è finito o è numerabile.

Dimostrazione Possiamo chiaramente assumere che il nostro insieme X sia un sottoinsieme di $\mathbb{N}$, visto che è sottoinsieme di un insieme numerabile. Supponiamo che X non sia finito, e costruiamo una funzione bigettiva da $\mathbb{N}$ a X. La definizione è ricorsiva, e procede come segue:

$$f(1) = min(X),\ f(n+1) = min(X \setminus \{f(1), ..., f(n)\})$$

I minimi esistono per il principio del buon ordinamento, che si applica ad ogni passaggio in quanto se per qualche n fosse $X \setminus \{f(1), ..., f(n)\} = \emptyset$ vorrebbe dire che X è finito, e stiamo assumento il contrario. Per costruzione f è iniettiva, e vale $f(n) < f(n+1)$ per tutti gli n. La funzione f è anche surgettiva in quanto $f(n) \geq n$ per tutti gli n (esercizio) e $X \setminus \{f(1), ..., f(n)\} \subset \{m \in \mathbb{N} \mid m > f(n)\}$, e quindi un qualunque $x \in X$ dovrà comparire come $f(n)$ per qualche $n \leq x$ (esercizio). □

Esempio L'insieme $\mathbb{Q}^+$ dei numeri razionali positivi è numerabile.

Dimostrazione L'insieme $\mathbb{Q}^+$ è in bigezione con l'insieme delle coppie di numeri naturali (p, q) primi fra loro, tramite la funzione

$$f : \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid \text{il massimo comun divisore di } p, q \text{ è } 1\} \to \mathbb{Q}^+$$

data da $f(p, q) = \frac{p}{q}$. Dato che $\mathbb{Q}^+$ non è chiaramente un insieme finito, la dimostrazione si conclude applicando la proposizione precedente e l'esercizio precedente. □

Teorema Un insieme A qualsiasi non può essere in bigezione con il suo insieme delle parti

Dimostrazione Supponiamo per assurdo il contrario della tesi, cioè che esista $f : A \to \mathcal{P}(A)$ funzione bigettiva.
Definiamo allora il seguente sottoinsieme B di A:

$$B = \{x \in A \mid x \notin f(x)\}$$

l'insieme degli elementi di A che non appartengono alla propria immagine tramite f. L'insieme B appartiene a $\mathcal{P}(A)$ e quindi dato che f è bigettiva dovrà essere l'immagine di un qualche $c \in A$: $B = f(c)$. L'elemento c, appartenendo ad A, sara' in B o nel suo complementare in A; d'altra parte,

$$c \in B \implies c \notin f(c) \implies c \notin B \text{ assurdo}$$
$$c \notin B \implies c \in f(c) \implies c \in B \text{ assurdo}$$

e quindi in entrambi i casi abbiamo un assurdo. □

Corollario L'insieme delle parti di $\mathbb{N}$ è infinito ma non numerabile