SUL CONTARE

CARLANGELO LIVERANI

1. Un linguaggio

Una parte della diffoltà della matematica risiede nel fatto che essa usa un linguaggio suo, in parte differente dal linguaggio naturale che usiamo ogni giorno. In particolare, può capitare che parole del linguaggio comune siano usate con una differente accezione in matematica. Tuttavia ogni parola in matematica è precisamente definita in termini di parole già note o dei termini *primitivi* della teoria. Quando si legge un testo di matematica bisogna sempre essere allerti alla possibiltà che una parola sia usata in senso *tecnico* e in tal caso è buona norma domandarsi: che cosa significa?

In questo corso si utilizzeranno alcuni rudimenti del linguaggio logico ed insiemistico. Poichè tale elementi del linguaggio matematico sono di uso abbastanza comune nelle scuole inferiori, essi saranno considerati noti. Tuttavia, forse è meglio ricapitolare il minimo che verrà usato nel corso.

Per *insieme* intenderò una collezione di oggetti (o elementi), poichè tutti gli insiemi trattati nel corso saranno alquanto concreti ed esenti da problemi (tipicamente sottoinsiemi dei numeri reali) ignorerò tranquillamente la distinzione tra insiemi e classi necessaria per non incorrere in contraddizioni.[1]

Con $x \in A$ si intende *l'elemento x appartiene all'insieme A*. Con $A \subset B$ si intende *l'insieme A è contenuto nell'insieme B*, piú precisamente *per ogni x se $x \in A$ allora $x \in B$* o, piú sinteticamente, $\forall x(x \in A \to x \in B)$.

Esempio 1.1. *Se $A = \{1, 2, 3\}$ e $B = \{1, 2, 3, 5\}$ allora $1 \in A$ e $A \subset B$. Attenzione però: un insieme può anche essere un elemento di un'altro insieme. Per esempio se $C = \{1, 2, 3, 5, \{1, 2, 3\}\}$ allora $A \subset C$ ma anche $A \in C$ mentre $B \subset C$ ma $B \notin C$, cioè B* non è un elemento di C.

Due insiemi A, B si dicono uguali se $A \subset B$ e $B \subset A$. Abbiamo poi l'unione di due insiemi $A \cup B = \{x : x \in A$ oppure $x \in B\}$, ovvero *l'insieme di tutti gli elementi x tali che x appartiene ad A oppure a B, o ad entrambi*, e l'intersezione $A \cap B = \{x : x \in A$ e $x \in B\}$.[2] L'insieme vuoto $\emptyset$, cioè un buffo insieme che non

Date: Rome, October 11, 2003.

[1]Essenzialmente le classi sono collezioni di oggetti e gli insiemi classi che appartengono ad altre classi. Abbastanza sorprendentemente se si ammette che ogni classe può appartenere ad un'altra classe (e quindi ogni classe è un insieme) si incorre in una contraddizione.

[2]Si noti la possibilità di definire un insieme specificando una proprietà a cui i suoi elementi debbono soddisfare. In realtà questo modo di definire un insieme può generare paradossi se usato indiscriminatamente, per ovviare a questo pericolo in generale occorrerebbe sviluppare una teoria assiomatica degli insiemi (approssimativamente, il punto è che una proprietà determina sempre una classe, che poi essa sia o meno un insieme è una cosa che va dimostrata) che però esula dagli scopi del presente corso, anche perchè non veramente necessaria per il tipo di proprietà a cui saremo interessati.

contiene alcun elemento.[3] Inoltre abbiamo l'insieme potenza $\mathcal{P}(A) = \{x : x \subset A\}$, cioè *l'insieme di tutti i sottoinsiemi di A*.

Un altro modo di costruire nuovi insiemi partendo da insiemi dati è il prodotto Cartesiano. Dati due insiemi A e B si dice loro prodotto, e si scrive $A \times B$, l'insieme $\{(a, b) : a \in A,\, b \in B\}$. Per (a, b) si intende la coppia ordinata (a, b), cioè (a, b) è, in generale, diverso da (b, a). In particolare, $A \times B$ e $B \times A$ sono, in generali, diversi. Si noti che dati tre insiemi, A, B, C, $(A \times B) \times C$ e $A \times (B \times C)$ sono naturalmente *isomorfi*[4] dove l'isomorfismo è stabilito dalla corrispondenza $((a, b), c) \to (a, (b, c))$. È quindi naturale sopprimere le parentesi. Dato un insieme A si può dunque farne "il quadrato" cioè $A^2 := A \times A$ o, piú in generale, l'ennesima potenza, cioè $A^n := A \times \cdots \times A$, n volte. Per ragioni che appariranno ovvie tra un secondo si usa anche scrivere $A^{\{1,\dots,n\}}$.

Una funzione F tra due insiemi A e B si scrive $F : A \to B$ ed è semplicemente una regola tale che ad ogni $x \in A$ associa un unico elemento di B che viene appunto chiamato $F(x) \in B$.[5] Una funzione si dice *suriettiva* se per ogni $y \in B$ esiste $x \in A$ tale che $y = F(x)$ (scritto brevemente $\forall y \in B\ \exists x \in A : y = F(x)$) cioè ogni elemento di B è l'immagine, attraverso F, di un qualche elemento di A. Una funzione di dice *iniettiva* se $F(x) = F(y) \to x = y$ cioè un elemento di B non può essere l'immagine di due diversi elementi di A. L'insieme A si dice *dominio* della funzione F e $F(A) = \{F(x) : x \in A\}$ si dice *codominio*. Finalmente, una funzione suriettiva ed iniettiva si dice *biunivoca*. Se la funzione $F : A \to B$ è biunivoca allora essa determina univocamente una funzione $F^{-1} : B \to A$ tale che $\forall a \in A\ \ F^{-1}(F(a)) = a$ e $\forall b \in B\ \ F(F^{-1}(b)) = b$. Tale funzione è detta *funzione inversa* ed è chiaramente una funzione biunivoca tra B ed A.

Considereremo inoltre dato (e noto) l'insieme (infinito) dei numeri naturali $\mathbb{N} = \{0, 1, 2, \dots\}$.

Lemma 1.2. *Per ogni insieme A e $n \in \mathbb{N}$ gli insiemi $A^{\{1,\dots,n\}}$ e $\{f : \{1, \dots, n\} \to A\}$ possono essere messi in corrispondenza biunivoca.*[6]

Proof. Dato un elemento $\bar a = (a_1, \dots, a_n) \in A^n$ possiamo definire la funzione $f_{\bar a}(i) = a_i$, $i \in \{1, \dots, n\}$. D'altro canto per ogni funzione $f : \{1, \dots, n\} \to A$ possiamo definire la n-nupla ordinata $a_f := (f(1), \dots, f(n))$. Chiaramente, $a_{f_{\bar a}} = \bar a$. Possiamo dunque definire la corrispondenza biunivoca $F : A^n \to \{f : \{1, \dots, n\} \to A\}$, $F(\bar a) = f_{\bar a}$. □

Tramite la funzione F costruita nella dimostrazione del Lemma 1.2 possiamo dunque identificare i due insiemi. Abbiamo cosí una definizione alternativa di $A^{\{1,\dots,n\}}$. Il vantaggio di tale definizione è che ora A^B è ben definito per tutti gli insieme A e B, cioè $A^B = \{f : B \to A\}$.

[3] L'esistenza di tale insieme, come di altri che stiamo definendo, è in realtà un assioma nella teoria assiomatica degli insiemi il che significa che piace tanto ai matematici che non hanno alcuna intenzione di farne a meno.

[4] Questo significa che possono essere posti in *corrispondenza biunivoca*, si veda più sotto per una definizione precisa.

[5] Più precisamente, una funzione $F : A \to B$ è un sottoinsieme di $A \times B$ tale che $(x, y) \in F$ e $(x, z) \in F$ implica $y = z$. Dunque in F esiste una sola coppia ordinata il cui primo termine è x, il secondo termine di tale coppia è appunto chiamato $F(x)$.

[6] Si noti che l'insieme di tutte le funzioni tra A e B è, per definizione, un elemento dell'insieme $\mathcal{P}(A \times B)$. Si tratta dunque di uno degli oggetti che abbiamo assunto essere definibili senza problemi.

Gli insiemi possono essere finiti o infiniti, tuttavia per dare un significato preciso a questa affermazione occorre dire che si intende per *finito* o *infinito*. A questo scopo è utile chiarire che significa dire che due insiemi hanno *lo stesso numero di elementi*.

Definitione 1.3. *Diremo che due insiemi A e B hanno lo stesso numero di elementi o che hanno* la stessa cardinalità *se esiste una funzione biunivoca $F : A \to B$.*[7]

2. uno due tre ...

Cerchiamo di familiarizzarci con le conseguenze della definizione 1.3.

Esercizio 2.1. *Si mostri che se A e B hanno la stesa cardinalità e se B e C hanno la stessa cardinalità allora A e C hanno la stessa cardinalità.*

Definitione 2.2. *Diremo che un insieme ha $n \in \mathbb{N}$ elementi se ha la medesima cardinalità dell'insieme $\{1, 2, \dots, n\} \subset \mathbb{N}$.*[8]

Tale definizione è sensata, ma per accertarcene occorre fare il seguente esercizio che richiede un attimo di meditazione.

Esercizio 2.3. *Si mostri che un insieme non può avere sia n che m elementi, per $n \neq m$. (Suggerimento: per assurdo. Se non fosse vero esisterebbero, per l'Esercizio 2.1, $n, m \in \mathbb{N}$, $n > m$, tali che gli insiemi $\{1, 2, \dots, n\}$ e $\{1, 2, \dots, m\}$ sono in corrispondenza biunivoca. Da questo si deduca che lo stesso deve valere per $n - 1$ e $m - 1$. Per fare questo si mostri che se un insieme ha n elementi e se ne toglie uno allora l'insieme rimanente ha $n - 1$ elementi.*[9] *Iterando l'argomento ci si riduce a $n - m + 1 > 1$ e 1, cosa assurda.)*

Fino ad ora tutto sembra alquanto banale, anche se la spiegazione di che si intende per contare può sembrare piuttosto strana, tuttavia sembra coincidere con la nostra intuizione. Va comunque notato che si possono avere problemi un poco piú interessanti di quello dell'esercizio 2.1.

Lemma 2.4. *Per ogni insieme A, gli insiemi $\mathcal{P}(A)$ e $\{0, 1\}^A$ hanno lo stesso numero di elementi.*

Proof. Definiamo la funzione $F : \mathcal{P}(A) \to \{0, 1\}^A$ nel modo seguente: per ogni $B \subset A$ sia $F(B)$ la funzione che vale 1 in B e zero fuori, cioè, per ogni $a \in A$,

$$F(B)(a) = \begin{cases} 1 & \text{se } a \in B \\ 0 & \text{se } a \notin B \end{cases}$$

A volte $F(B)$ è chiamata la *funzione caratteristica* di B. Chiaramente F è biunivoca e questo conclude la dimostrazione. □

[7] Infatti, se ne esiste una, di solito ne esisteranno molte altre.

[8] Ovviamente, diremo che l'insieme vuoto ha zero elementi.

[9] Puó sembrare pazzesco che si debba dimostrare una cosa del genere, ma bisogna ricordare che, in questo contesto, *avere n elementi* non ha necessariamente nulla a che fare col solito significato intuitivo ma ha il preciso significato specificato nella definizione 2.2. Che questo significato sia consistente col significato intuitivo che abbiamo di questo concetto è esattamente quello che stiamo verificando in questo momento.

Tra le altre cose il lemma precedente chiarisce perchè $\mathcal{P}(A)$ è chiamato l'insieme *potenza*.

Tuttavia, le vere sorprese giungono quando si cerca di applicare tali concetti agli insiemi infiniti (di cui al momento abbiamo una sola istanza: $\mathbb{N}$).

Esempio 2.5. *Si consideri l'insieme $\mathbb{N}_* = \{1, 2, \dots\} \subset \mathbb{N}$. Tale insieme ha un elemento in meno dei naturali (lo zero) e quindi ci si potrebbe aspettare che la sua cardinalità sia inferiore. Invece se si considera $F : \mathbb{N}_* \to \mathbb{N}$ definita da $F(n) = n-1$ si ha chiaramente un funzione biunivoca tra $\mathbb{N}_*$ e $\mathbb{N}$. Dunque, per definizione, $\mathbb{N}_*$ e $\mathbb{N}$ hanno lo stesso numero di elementi!*

Esempio 2.6. *Si consideri l'insieme $\mathbb{N}_p = \{0, 2, 4, \dots, 2n, \dots\}$ dei numeri pari. Di nuovo si potrebbe pensare che contenga la metà degli elementi di $\mathbb{N}$, cioè che la sua cardinalità sia inferiore. Eppure, applicando la definizione e considerando la funzione $F(n) = 2n$ si ottiene che $\mathbb{N}_p$ e $\mathbb{N}$ hanno la stesa cardinalità.*

Queste stranezze hanno a lungo lasciato perplessi i matematici, fino a quando non ci si è rassegnati alla constatazione che l'infinito è un concetto controintuitivo e si sono usate le sue peculiarità proprio per definirlo.

Definitione 2.7. *Un insieme A si dice* infinito, *se esiste un suo sottoinsieme proprio (cioè $B \subset A$ ma $B \neq A$) con la stessa cardinalità di A.*

Vediamo che una tale definizione non fa danni.

Esercizio 2.8. *Se A è un insieme finito (cioè non è infinito) allora ogni suo sottoinsieme è finito. (Suggerimento: per assurdo. Si supponga che esistano $C \subset B \subset A$ tali che C può essere messo in corrispondenza biunivoca con B e si costruisca un sottoinsieme C_1 che può essere messo in corrispondenza con A.)*

Esercizio 2.9. *Per ogni $n \in \mathbb{N}$ l'insieme $A_n := \{0, 1, \dots, n\}$ è finito. (Suggerimento: per assurdo si supponga che esista $n \in \mathbb{N}$ tale che A_n è infinito. Sia $B \subset A_n$ in corrispondenza biunivoca con A_n tramite la funzione F. Si tolga da A il piú grande elemento che non è contenuto in B, diciamo k, e si tolga da B l'elemento $F^{-1}(k)$. Si mostri che in tal modo segue che anche A_{n-1} è infinito. Continuando in tale modo si ottiene che A_0 è in corrispondenza biunivoca con un suo sottoinsieme proprio, insensato visto che l'unico sottoinsieme proprio è $\emptyset$.)*

Dunque con la definizione 2.7 gli insiemi finiti sono quelli che ci aspettiamo mentre quelli infiniti godono delle strane patologie di cui agli esempi 2.5, 2.6 In realtà, patologie anche peggiori sono possibili.

Esercizio 2.10. *Si mostri che gli insiemi $\mathbb{N}$ ed $\mathbb{N} \times \mathbb{N}_*$ hanno lo stesso numero di elementi. (Suggerimento: si provi con la funzione $F : \mathbb{N} \times \mathbb{N}_* \to \mathbb{N}$ definita da $F((p, q)) = p + 1 + \sum_{i=0}^{p+q}(i + 1)$).*[10]

Si noti che l'insieme dei numeri razionali può essere considerato come contenuto in $\mathbb{N} \times \mathbb{N}_*$, infatti ad ogni $(p, q) \in \mathbb{N} \times \mathbb{N}_*$ si può associare il numero razionale $\frac{p}{q}$. Ovviamente tale funzione non è iniettiva ma questo significa solo che il numero

[10]La funzione è ottenuta considerando gli insiemi $G_n = \{(p, q) \in \mathbb{N} \times \mathbb{N}_* : p + q = n\}$, chiaramente $\cup_{n\in\mathbb{N}} G_n = \mathbb{N} \times \mathbb{N}_*$. A questo punto si contano prima gli elementi in G_0, poi in G_1 e cosi via, in ogni G_i, invece, gli elementi sono contati secondo l'ordine di p crescente.

degli elementi di $\mathbb{N} \times \mathbb{N}_*$ è maggiore od uguale a quello di $\mathbb{Q}$, ma poichè $\mathbb{N} \subset \mathbb{Q}$ è chiaro che $\mathbb{N}$ e $\mathbb{Q}$ hanno lo stesso numero di elementi.[11]

A questo punto si potrebbe pensare che tutti gli insiemi infiniti hanno la stessa cardinalità e dunque, in un qualche senso, esiste un solo tipo di infinito. Anche questo risulta essere falso.

Lemma 2.11. *Per ogni insieme A la cardinalità di $\mathcal{P}(A)$ è sempre maggiore della cardinalità di A.*

Proof. Ragionando per assurdo, supponiamo che il lemma sia falso e che quindi esista una funzione biunivoca $F : A \to \mathcal{P}(A)$. In tal caso definiamo l'insieme $B = \{x \in A : x \notin F(x)\}$. Chiaramente $B \subset A$ e dunque $B \in \mathcal{P}(A)$. Esisterà perció un unico elemento $z \in A$ tale che $F(z) = B$. A questo punto possiamo ottenere una contraddizione chiedendoci se $z \in B$ oppure no. Infatti se $z \in B$ allora, per definizione di B, $z \notin F(z) = B$. Dunque deve essere $z \notin B$. Ma se $z \notin B$ allora $z \notin F(z)$ e, per la definizione di B, $z \in B$, assurdo. □

Ciò significa che il numero degli elementi di $\mathcal{P}(\mathbb{N})$ è strettamente maggiore di quello di $\mathbb{N}$. Si noti che $\{0,1\}^{\mathbb{N}}$ può essere interpretato come la collezione di stringhe infinite $(a_0, a_1, \dots, a_n, \dots)$, dove $a_i \in \{0,1\}$ per ogni $i \in \mathbb{N}$. Ognuna di tali stringhe può essere pensata come l'espansione binaria di un numero reale nell'intervallo $[0,1]$, tuttavia diverse stringhe possono corrispondere allo stesso numero (ad esempio $(1,0,0,\dots)$ e $(0,1,1,1,\dots)$ corrispondono entrambi al numero uno, come vedremo nel proseguo del corso). Si può comunque dimostrare che solo un numero numerabile di stringhe sono problematiche e dunque la cardinalità di $[0,1]$ coincide con quella di $\mathcal{P}(\mathbb{N})$.

Per concludere vorrei mettere in guardia contro la possibile impressione che contare insiemi finiti sia una banalità. In realtà contare può essere un problema assai difficile,[12] di solito occorre una qualche idea molto astuta su come organizzare il conteggio per venirne a capo. Allo scopo di capire meglio il problema facciamoci una semplice domanda: per gli insiemi finiti quanto è grande l'insieme potenza?

Lemma 2.12. *Per ogni insieme A di cardinalità n, l'insieme $\mathcal{P}(A)$ ha cardinalità 2^n.*

Proof. Il lemma è banale per $A = \emptyset$. Per le altre posibiltà useremo il risultato del Lemma 2.4 e cercheremo di contare gli elementi dell'insieme $\{0,1\}^A$. Organizziamo il conteggio attraverso la seguente identità algebrica: per ogni due numeri α_0, α_1 si ha[13]

$$(\alpha_0 + \alpha_1)^n = \sum_{f \in \{0,1\}^A} \prod_{i \in A} \alpha_{f(i)}. \tag{1}$$

Utilizzando tale formula con $\alpha_0 = \alpha_1 = 1$ si ottiene

$$2^n = (1+1)^n = \sum_{f \in \{0,1\}^A} \prod_{i \in A} 1 = \sum_{f \in \{0,1\}^A} 1.$$

[11] Ovviamente, dire che un insieme A ha una cardinalità maggiore o uguale di un insieme B significa semplicemente che esiste $C \subset A$ con la stessa cardinalità di B.

[12] È il soggetto di una intera branca della matematica: la combinatorica.

[13] Dimostrarla equivale a capire cosa si è scritto ed è un esercizio molto utile. La si dimostri prima per $A = \{1, 2, \dots, n\}$ e poi per un generico insieme A con n elementi. Per la cronaca $\sum_{i \in \{1,\dots,n\}} \beta_i := \beta_1 + \beta_2 + \cdots + \beta_n$ e $\prod_{i \in \{1,\dots,n\}} \beta_i := \beta_1 \beta_2 \cdots \beta_n$.

Poichè l'ultima espressione è semplicemente la somma di uno per ogni elemento di $\{0,1\}^A$ è chiaro che la somma da esattamente la cardinalità di $\{0,1\}^A$ e dunque di $\mathcal{P}(A)$. □

A qualcuno la formula (1) può sembrare assai complessa, ci si può chiedere se sia possibile scriverla in maniera piú semplice. La risposta è positiva ma richiede di risolvere un altro problema di conteggio.

Sia $B_k = \{f \in \{0,1\}^A : \sum_{i\in A} f(i) = k\}$,[14] chiaramente $\{0,1\}^A = \cup_{k=0}^n B_k$, dunque possiamo scrivere[15]

$$(\alpha_0+\alpha_1)^n = \sum_{k=0}^n \sum_{f\in B_k} \prod_{i\in A} \alpha_{f(i)} = \sum_{k=0}^n \sum_{f\in B_k} \alpha_1^n \alpha_0^{n-k} = \sum_{k=0}^n \#B_k \alpha_1^n \alpha_0^{n-k}.$$

Esercizio 2.13 (Binomio di Newton)**.** *Per ogni due numeri a, b vale*[16]

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

(Suggerimento: per contare gli elementi di B_k si devono contare tutti i possibili modi in cui si possono scegliere k elementi tra n (sono gli elementi su cui f varrá uno). Per farlo, prima si sceglie chi è il primo elemento (n possibilità) poi chi è il secondo ($n-1$ possibilità, visto che un elemento è già stato scelto e non si può scegliere nuovamente), e cosí via. Questo da $n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$ possibiltà. Però, così facendo, abbiamo scelto lo stesso insieme un mucchio di volte, infatti se lo stesso insieme viene scelto in un ordine diverso nulla cambia, mentre noi lo abbiamo contato di nuovo. Quante volte abbiamo contato lo stesso insieme? Ovviamente $k!$.)

Dipartimento di Matematica, Università di Roma (Tor Vergata), Via della Ricerca Scientifica, 00133 Roma, Italy, liverani@mat.uniroma2.it

[14] Cioè B_k è l'insieme di tutti i sottoinsiemi di A con cardinalità k.

[15] Dato un insieme finito A, per $\#A$ si intende il numero di elementi di A.

[16] Per $\binom{n}{k}$ si intende $\frac{n!}{k!(n-k)!}$ mentre $k! := 1\cdot 2\cdot 3\cdots n = \prod_{i=1}^n i$.