Dispense su teoria degli insiemi e insiemi numerici

Emanuele Bottazzi* & Valentina Clamer†

Versione aggiornata al 11 novembre 2015‡

Indice

Avvertenze preliminari

Queste note raccolgono il materiale coperto nelle prime esercitazioni del corso di Geometria I (a.a. 2015/2016) per fisici e filosofi del dell'Università di Trento. Le note sono ancora in fase di elaborazione, ed è altamente probabile che nelle loro prime iterazioni contengano

*Dipartimento di Matematica, Università degli studi di Trento, emanuele.bottazzi@unitn.it.
†Dipartimento di Matematica, Università degli studi di Trento, v.clamer@unitn.it.
‡Eventuali versioni successive sono reperibili alla pagina `http://www.science.unitn.it/~bottazzi/geometria1516.html`.

diversi errori. Se ne trovate qualcuno, vi chiediamo la cortesia di segnalarcelo con una mail all'indirizzo `emanuele.bottazzi@unitn.it`, così che lo possiamo correggere.

Le sezioni che iniziano con la parola "Opzionale" sono di lettura facoltativa e non costituiscono materiale d'esame.

1 Teoria degli insiemi

1.1 Gli insiemi secondo Cantor e il paradosso di Russell

Il primo studioso che ha intuito l'importanza di occuparsi di cosa siano e come funzionino gli insiemi è stato Georg Cantor, un matematico tedesco vissuto nella seconda metà del 1800. Secondo l'idea originale di Cantor, un insieme si definisce come una "collezione di oggetti". Ad esempio: tutti i libri della biblioteca di scienze formano un insieme secondo la definizione di Cantor, così come anche tutti gli studenti del corso di Geometria I di Claudio Fontanari dell'anno accademico 2015/2016. Purtroppo, quest'idea così intuitiva e così attraente non funziona: se prendiamo la definizione di insieme data da Cantor, possiamo costruire degli insiemi che permettono di dimostrare contemporaneamente che una certa affermazione matematica è vera e falsa, cioè quella che i matematici chiamano una contraddizione.

La contraddizione più famosa della teoria degli insiemi di Cantor è il *paradosso di Russell*. Il paradosso di Russell si ottiene in questo modo: consideriamo l'insieme $P = \{\odot : \odot \notin \odot\}$ degli insiemi che non appartengono a se stessi. Per il principio del terzo escluso, o $P \in P$ o $P \notin P$. Supponiamo che $P \in P$: questo implica, per la proprietà che caratterizza gli elementi di P, che $P \notin P$. Se invece supponiamo che $P \notin P$, allora P soddisfa la proprietà che caratterizza gli elementi di P, e quindi $P \in P$. Concludiamo quindi che $P \in P \Leftrightarrow P \notin P$. Quindi dalla nozione intuitiva di insieme come collezione di oggetti deduciamo una contraddizione, che rende la teoria priva di interesse matematico[1].

1.2 Gli insiemi dopo Cantor

Dopo Cantor, sono state ideate molte "teorie assiomatiche degli insiemi", dove gli assiomi sono scelti in modo tale da evitare le contraddizioni note della teoria degli insiemi nella sua formulazione più ingenua. Nel passare dalle idee originali di Cantor alle nuove teorie, i matematici hanno avuto l'opportunità di capire meglio cosa siano gli insiemi, liberandosi dalle (poche) intuizioni sbagliate di Cantor. Eppure non si sa con certezza se le nuove teorie degli insiemi siano libere da contraddizioni: sorprendentemente, non è possibile dimostrare che una teoria matematica sia coerente, cioè priva di contraddizioni, e questo è un limite intrinseco a tutta la matematica. Infatti, con le tecniche matematiche conosciute non è neppure possibile dimostrare se l'aritmetica sia consistente[2][3].

In ogni caso, le nuove teorie degli insiemi vengono utilizzate assumendo implicitamente che siano coerenti. Nell'eventualità che al loro interno si scoprissero delle contraddizioni, probabilmente si cercherà di rimediare con teorie alternative che salvino i risultati coerenti e che eliminino quelli contraddittori.

[1] Secondo il principio logico dell'ex falso quodlibet (in formula: $\bot \to A$ per ogni A), che intuitivamente vuol dire che da una contraddizione è possibile dimostrare ogni affermazione matematica. Questo principio logico, all'apparenza bizzarro, ha un ruolo fondamentale nella matematica, e non è sacrificabile.

[2] Questo è, con un'approssimazione brutale, il contenuto del Secondo Teorema di Incompletezza di Gödel.

[3] In linea di principio, sarebbe invece possibile dimostrare che l'aritmetica è contraddittoria: per farlo, sarebbe sufficiente esibire la dimostrazione di un'affermazione e della sua negazione, raggiungendo così una contraddizione (sull'esempio del paradosso di Russell per la teoria degli insiemi secondo Cantor).

1.3 La teoria degli insiemi di Zermelo-Fraenkel

Per introdurre una teoria assiomatica si enunciano i suoi assiomi, cioè le regole che governano il comportamento degli oggetti di cui parla la teoria. Gli oggetti, però, non vengono definiti esplicitamente, ma vengono in qualche modo definiti implicitamente dagli assiomi. Quindi nel caso della teoria degli insiemi di Zermelo-Fraenkel (che di solito si abbrevia con la sigla ZF) non esiste una definizione esplicita di insieme: possiamo dire che un oggetto matematico è un insieme solo se riusciamo a dimostrare di poterlo "costruire" utilizzando gli assiomi della teoria. Questo è vero in particolare per le "collezione di oggetti": prima di concedere loro lo status di insieme dobbiamo dimostrare di poterle ottenere a partire dagli assiomi della teoria. Viceversa, ogni oggetto matematico (per quanto strano, bizzarro o inatteso) che possiamo costruire a partire dagli assiomi della teoria degli insiemi è un insieme, anche se magari sfida la nostra idea intuitiva di "collezione".

La teoria degli insiemi di ZF, oltre a parlare di insiemi, utilizza altri due concetti: l'*uguaglianza*, indicata con il simbolo "=" e l'*appartenenza*, indicata con il simbolo "$\in$". La relazione di uguaglianza, che pure vuole esprimere un concetto intuitivamente famigliare, rispetta tutte (e sole) le regole che verranno elencate negli assiomi, e nessuna sua proprietà può essere utilizzata senza prima essere dimostrata a partire dagli assiomi. Il caso dell'appartenenza, invece, è un po' più delicato: formalmente, i matematici dicono solo che è una relazione binaria, e poi la usano negli altri assiomi senza spiegarne il significato. Anche se un formalista messo all'angolo non darà mai una definizione esplicita del significato dell'appartenenza, nessuno discute sull'idea intuitiva che se $\star \in \spadesuit$ allora "$\star$ è un elemento di $\spadesuit$" (allo stesso modo in cui Claudio Fontanari è un elemento dell'insieme dei professori dell'Università di Trento o in cui Le Due Trinità appartiene all'insieme dei quadri conservati alla National Gallery di Londra).

Ed ora, finalmente, vediamo quali sono gli assiomi di ZF.

1.3.1 Assioma di esistenza

Esiste un insieme.

Senza questo assioma, potrebbero anche non esistere insiemi, e quindi ZF sarebbe completamente inutile.

1.3.2 Assioma di uguaglianza

Se $\diamond \in A \Leftrightarrow \diamond \in B$ (i.e. se ogni elemento di A è anche un elemento di B e viceversa), allora $A = B$.

Questo assioma è necessario per regolamentare l'uguaglianza tra insiemi. Il comportamento dell'uguaglianza dipende dal comportamento dell'appartenenza: se noi decidessimo per qualche strano motivo che "insieme" vuol dire "persona" ed "appartiene" vuol dire "è genitore di", questo assioma direbbe che "se due persone hanno gli stessi genitori, allora sono uguali".

1.3.3 I sottoinsiemi

Diciamo che A è un sottoinsieme di B, in simboli $A \subseteq B$, quando $* \in A \Rightarrow * \in B$ (i.e. ogni elemento di A è anche un elemento di B). Attenzione: questo non è un assioma, bensì una definizione che ci fa comodo per abbreviare la formula "$* \in A \Rightarrow * \in B$".

1.3.4 Assioma della coppia

Se A e B sono due insiemi, allora $C = \{A, B\}$ è un insieme.

Si può pensare a questo assioma come a una "regola" per costruire nuovi insiemi. Ad esempio: l'assioma di esistenza ci dice che esiste un insieme $\surd$. Usando l'assioma della coppia (dove $A = B = \surd$, dato che $\surd$ è l'unico insieme che abbiamo), otteniamo un insieme C i cui unici elementi sono $\surd$ e $\surd$. Dato che $\surd = \surd$, concludiamo che C contiene un unico elemento, cioè l'insieme $\surd$.

Di solito, per convenzione si usa indicare gli elementi di un insieme tra parentesi graffe e separati da una virgola. Il nostro insieme C costruito sopra sarebbe quindi l'insieme $C = \{\surd\}$ che è quasi sempre diverso da $\surd$[4]. A questo punto, utilizzando l'assioma della coppia possiamo ottenere gli insiemi:

$$\{\{\{\surd\}\}\};\ \{\surd, \{\surd\}\};\ \{\surd, \{\surd, \{\surd\}\}\}$$

e tantissimi altri. È interessante osservare che questi insiemi hanno al massimo due elementi: il terzo insieme dell'elenco qui sopra, ad esempio, ha come unici elementi l'insieme $\surd$ e l'insieme $\{\surd, \{\surd\}\}$. A sua volta, quest'ultimo insieme ha come elementi l'insieme $\surd$ e l'insieme $\{\surd\}$.

Per costruire insiemi con più di due elementi, abbiamo bisogno di un altro assioma.

1.3.5 Assioma dell'unione

Se A è un insieme, allora è un insieme anche

$$\{🔊 :\ \text{esiste un insieme } ★ \in A \text{ tale che } 🔊 \in ★\}.$$

Questo nuovo insieme di solito si indica con il simbolo $\bigcup_{★ \in A} ★$.

Ad esempio, a partire da due insiemi T e Q possiamo, grazie all'assioma della coppia, costruire l'insieme $\{T, Q\}$. Applicando l'assioma dell'unione all'insieme $\{T, Q\}$, otteniamo l'insieme

$$\{♠ : ♠ \in T \text{ o } ♠ \in Q\} = T \cup Q$$

1.3.6 Assioma di comprensione

Se A è un insieme e P è una proprietà, allora è un insieme anche

$$B = \{♠ : ♠ \in A \text{ e soddisfa } P(♠)\}.$$

Per essere precisi, dovremmo chiarire cosa si intende per "proprietà": intuitivamente, le proprietà insiemistiche sono proprietà matematiche degli insiemi, come ad esempio "avere esattamente due elementi". Una proprietà non insiemistica è "essere comprensibile", quindi la collezione di tutti gli insiemi comprensibili che appartengono ad un insieme dato non esiste.

La formula $♣ \notin ♣$, invece, è una proprietà insiemistica. Nella teoria degli insiemi secondo Cantor, questa formula ci ha permesso di dedurre l'inconsistenza della teoria mediante il paradosso di Russel. In ZF, possiamo invece dimostrare che la collezione di tutti gli insiemi non è un insieme.

[4] L'unica eccezione è data dal caso in cui $\surd = \{\surd\}$.

Teorema 1.1. *La collezione* $\Omega = \{\star : \star = \star\}$ *(i.e. la collezione di tutti gli insiemi) non è un insieme.*

Dimostrazione. Supponiamo per assurdo[5] che Ω sia un insieme. L'assioma di comprensione ci garantisce che

$$\Xi = \{\star : \star \in \Omega \text{ e soddisfa } \star \notin \star\}$$

è un insieme. Ragionando come nel paradosso di Russel, otteniamo nuovamente la contraddizione $\Xi \notin \Xi \Leftrightarrow \Xi \in \Xi$. La contraddizione è stata dedotta a partire dall'ipotesi che Ω sia un insieme: lo schema della dimostrazione per assurdo ci permette di concludere che questa ipotesi è falsa, cioè che Ω non è un insieme. □

1.3.7 Assioma dell'insieme delle parti

Se A è un insieme, allora è un insieme anche

$$\{B : B \subseteq A\}.$$

Questo insieme si chiama l'*insieme delle parti*[6] di A, e si indica con $\mathcal{P}(A)$. Osserviamo che nel nome "l'insieme delle parti" si usa l'articolo determinativo: il motivo è che, usando l'assioma dell'uguaglianza, si può dimostrare che l'insieme delle parti di un insieme dato è unico.

1.3.8 Assioma dell'esistenza di un insieme infinito

Esiste un insieme che soddisfa:

1. $\varnothing \in A$**;**
2. **se** $\heartsuit \in A$**, allora anche** $\{\heartsuit\} \in A$**.**

Senza questo assioma, nessuno ci garantirebbe che dentro la teoria ci siano insiemi infiniti. L'assioma dell'esistenza di un insieme infinito non solo ci dice che esiste (almeno) un insieme infinito, ma chiede anche che questo insieme abbia una forma ben precisa. Il motivo è che questo insieme all'apparenza un po' bizzarro è in realtà molto significativo.

1.4 Altre operazioni insiemistiche

1.4.1 Sottrazione

Anche tra gli insiemi è definita un'operazione di sottrazione. Se ★ e 🎤 sono insiemi, allora

$$★ \setminus 🎤 = \{\star \in ★ : \star \notin 🎤\}$$

è un insieme, costruito a partire da ★ utilizzando l'assioma di comprensione con la proprietà $P(\star) = \star \notin 🎤$.

La differenza tra insiemi non è commutativa, i.e. in generale $♠ \setminus ♣ \neq ♣ \setminus ♠$. Questo si può facilmente dimostrare esibendo un controesempio.

[5] La dimostrazione per assurdo si può sintetizzare nella seguente inferenza logica: $(\neg A \to \bot) \to A$. In altre parole: se dall'ipotesi che A sia falsa (i.e. assumendo $\neg A$) deduciamo una contraddizione, allora A è vera. Questa tecnica dimostrativa si basa sul principio del terzo escluso (in formula: $A \vee \neg A$, cioè o A è vera o A è falsa, e non ci sono ulteriori alternative) che è rifiutato dai matematici costruttivisti. Per i costruttivisti continua a valere l'implicazione $(\neg A \to \bot) \to \neg\neg A$, ma per loro non è vero che $\neg\neg A$ sia equivalente ad A.

[6] In inglese invece è il *power set*.

1.4.2 Prodotto cartesiano

Siano Γ e Θ due insiemi non vuoti. Possiamo costruire il prodotto cartesiano $\Gamma \times \Theta = \{(g, t) : g \in \Gamma, t \in \Theta\}$ di coppie ordinate in cui il primo elemento appartiene a Γ e il secondo appartiene a Θ. Anche in questo caso si può dimostrare che $\Gamma \times \Theta$ è veramente un insieme, ma la dimostrazione è abbastanza macchinosa e non aiuta ad illuminare la definizione.

1.5 Funzioni

Coming soon.

2 I numeri naturali

2.1 Cosa sono i numeri?

La domanda che dà il titolo a questa sezione è onesta, ed è un velato invito ad una riflessione personale.

Euclide, il famoso autore degli Elementi di geometria, vissuto intorno al 300 avanti Cristo, prima di iniziare lo studio dell'aritmetica (la "scienza dei numeri") dà queste definizioni:

1. unità è ciò secondo cui ciascun ente è detto uno;
2. numero è una pluralità composta da unità.

Secondo (una possibile interpretazione di) Euclide, un numero è quasi come una misura: fissata l'unità di riferimento, che chiama unità (possiamo pensare all'unità di Euclide come all'1), un numero è un composto di unità. È interessante, anche se forse un po' pedante, osservare che secondo la definizione di Euclide 1 non è un numero.

Anche se magari non siamo totalmente soddisfatti dalla definizione di Euclide, una quantità strabiliante di persone ne deve essere rimasta affascinata, dato che l'idea di numero secondo Euclide è sopravvissuta fino al Settecento, quando per la prima volta nella storia della matematica iniziano ad affermarsi delle definizioni alternative. La più notevole è data da Newton: "per numero, invece di una moltitudine di unità, noi intendiamo il rapporto astratto di una quantità con un'altra dello stesso tipo, assunta come unità"[7].

Le definizioni di numero di Euclide e di Newton indubbiamente colgono diversi aspetti dell'idea che abbiamo dei numeri. Sono definizioni esaustive, cioè descrivono completamente che cosa siano i numeri? E ancora, come possiamo usare queste definizioni nella pratica matematica?

Dal punto di vista della matematica moderna (cioè circa dal 1900 ad oggi), l'unica risposta definitiva ed esaustiva alla domanda "cosa sono i numeri?" è analoga a quella che abbiamo visto per gli insiemi: per un matematico, i numeri naturali sono quegli "oggetti matematici" di cui parla una buona teoria assiomatica dell'aritmetica. Una tra le più potenti ed eleganti di queste teorie è stata ideata poco più di un secolo fa da Giuseppe Peano, un matematico e filosofo italiano famoso in tutto il mondo scientifico. Peano è stato il primo ad aver elencato con rigore e precisione le proprietà essenziali dei numeri naturali, invece che di cercare di esprimerli mediante una definizione. Inoltre, le proprietà che lui ha individuato, cioè gli assiomi della sua teoria, si sono rivelati corretti (cioè esprimono solo proprietà che ci aspettiamo che i numeri naturali soddisfino) e completi (cioè sono

[7] "Per numerum non tam multitudinem unitatum, quam abstractam quantitatis cuiusvis ad aliam eiusdem generis quantitatem, quae pro unitate habetur, rationem intelligimus."

sufficienti ad esprimere tutte le proprietà che ci aspettiamo che i naturali soddisfino). In confronto, Euclide non è riuscito a fare altrettanto bene con la sua geometria!

2.2 L'aritmetica di Peano

Questa teoria, che abbrevieremo con la sigla PA, presenta alcune differenze rispetto a quella di ZF: in PA si parlerà di "numeri", che saranno gli oggetti della teoria, e poi di una operazione particolare, che Peano indica con la parola "successore" e che noi indicheremo con la lettera s. La funzione "successore", in qualche modo, vorrebbe essere la funzione che "aggiunge uno" al numero a cui si applica. Tra i numeri, è evidenziato un elemento particolare, in qualche modo privilegiato rispetto agli altri: il numero "0". Questi sono i tre enti primitivi della teoria, e giocheranno un ruolo di rilievo negli assiomi di PA. Ecco i cinque assiomi:

2.2.1 Primo assioma dello zero

0 è un numero.

Questo assioma è analogo all'assioma dell'esistenza di un insieme in ZF: serve per garantirci che la teoria parlerà effettivamente di qualcosa. Come mai allora non dire semplicemente "esiste un numero"? Il numero 0, in realtà, ha un ruolo diverso da tutti gli altri numeri, quindi è utile metterlo subito in rilievo e dargli un nome.

2.2.2 Assioma del successore

Se n è un numero, $s(n)$ è un numero.

Questo assioma si può interpretare come una regola che ci permette di costruire nuovi numeri a partire da numeri dati: quindi, partendo da 0, avremo ad esempio che $s(0)$ è un numero, $s(s(0))$ è un numero, ed anche $s(s(s(s(s(s(s(0)))))))$ è un numero. Dato che quest'ultimo è abbastanza arduo da leggere, semplifichiamo la notazione in questo modo: battezzeremo con il simbolo 1 il numero $s(0)$, con il simbolo 2 il numero $s(s(0)) = s(1)$, e così via:

$$\begin{array}{ccl} 1 & = & s(0) \\ 2 & = & s(1) = s(s(0)) \\ 3 & = & s(2) = s(s(1)) = s(s(s(0))) \\ \vdots & \vdots & \vdots \\ n & = & \underbrace{s(s(\dots s}_{n \text{ volte}}(0)\dots)) \end{array}$$

È importante sottolineare che 1, 2 e tutte le altre cifre che abbiamo usato sopra sono solo dei *simboli* con cui indichiamo i *numeri* $s(0)$, $s(s(0))$ e tutti gli altri numeri costruiti a partire da 0 ed usando la funzione successore. Solo dopo aver introdotto questa convenzione, siamo autorizzati a dire che 37 è un numero, dato che per noi 37 coincide con $\underbrace{s(s(\dots s}_{37 \text{ volte}}(0)\dots))$.[8]

2.2.3 Iniettività del successore

Se $m \neq n$, allora $s(m) \neq s(n)$.

Anche se non sappiamo ancora bene cosa faccia di preciso la funzione "successore", questo assioma le impedisce di comportarsi in modo bizzarro. Ad esempio, se sappiamo già che $0 \neq s(0)$, grazie a questo assioma possiamo dedurre che $s(0) \neq s(s(0))$.

[8] Una domanda provocatoria: chi è questo 37?

Avendo a disposizione solo i primi tre assiomi della teoria, però, non possiamo decidere se la formula $0 \neq s(0)$ è vera o falsa. Da un lato, sappiamo che nei numeri naturali come li conosciamo la formula $0 \neq s(0)$ è vera. Dall'altro, possiamo considerare un mondo dove esiste solo lo 0 e dove vale la formula $0 = s(0)$. In questo mondo, i tre assiomi precedenti sono verificati: 0 è un numero, il successore di un numero è un numero, ed infine numeri diversi hanno successori diversi, dato che non esistono due numeri diversi[9].

Per uscire da questa situazione imbarazzante, abbiamo bisogno di un altro assioma.

2.2.4 Secondo assioma dello zero

$0 \neq s(n)$ per ogni numero n.

Grazie a questo assioma, possiamo finalmente dimostrare che $0 \neq s(0)$, cioè $0 \neq 1$. Poi, con un po' di lavoro, possiamo dimostrare anche che $1 \neq 2$, e così via. Osserviamo però che ci manca ancora un assioma per ottenere i numeri naturali per come li conosciamo. Infatti, se ci limitiamo a questi quattro assiomi, nulla impedisce che i numeri naturali abbiano una struttura simile a questa[10]:

$$\underbrace{0 \xrightarrow{s} 1 \xrightarrow{s} 2 \xrightarrow{s} \dots}_{\mathbb{N}} \qquad \underbrace{\dots \xrightarrow{s} -\mathfrak{1} \xrightarrow{s} \mathfrak{0} \xrightarrow{s} \mathfrak{1} \xrightarrow{s} \dots}_{\cong \mathbb{Z}}$$

dove $0 \neq \mathfrak{0}$, $1 \neq \mathfrak{1}$ e così via.

2.2.5 Schema di induzione

Se A soddisfa le proprietà

1. $0 \in A$**;**
2. **se** $n \in A$**, allora anche** $s(n) \in A$**;**

allora A è l'insieme di tutti i numeri.

2.3 Opzionale: definizioni ricorsive di somma e prodotto su $\mathbb{N}$

Mediante l'operazione successore e sfruttando lo schema di induzione si possono *definire* le usuali operazioni di somma e prodotto, ed è possibile *dimostrare* le loro proprietà a partire dalle definizioni. I lettori interessati possono approfondire questo argomento ad esempio in [2].

Senza scendere dettagli: per ogni $n \in \mathbb{N}$, $n+m$ si definisce per induzione su m in questo modo:

1. (Base dell'induzione) $n + 0 = n$;
2. (Passo induttivo) $n + s(m) = s(n + m)$,

mentre il prodotto si definisce sempre per induzione su m in questo modo:

1. (Base dell'induzione) $n \cdot 0 = 0$;
2. (Passo induttivo) $n \cdot s(m) = (n \cdot m) + n$.

[9] Quest'ultima affermazione è una variante particolarmente rilevante dell'ex falso quodlibet.
[10] Esistono anche esempi molto più complicati.

Dopo aver dato queste definizioni bisognerebbe dimostrare che queste operazioni godono delle proprietà alle quali siamo abituati fin da bambini: sono entrambe commutative, associative, e il prodotto è distributivo rispetto alla somma. Come si può intuire, tutte le dimostrazioni vengono effettuate per induzione. Questa tecnica dimostrativa è talmente rilevante da meritare un paragrafo tutto per sé.

2.4 Le dimostrazioni per induzione

Lo schema di induzione ci mette a disposizione una tecnica dimostrativa estremamente potente: la dimostrazione per induzione. La dimostrazione per induzione consiste nel seguente argomento: sia P una proprietà dei numeri naturali per cui valgono le due ipotesi

1. $P(0)$ è vera;
2. a partire dall'ipotesi che $P(n)$ sia vera possiamo dedurre che anche $P(n+1)$ è vera;

allora, per lo schema di induzione possiamo concludere che $\{x \in \mathbb{N} : P(x)\} = \mathbb{N}$, cioè è vera $\forall n \in \mathbb{N},\ P(n)$.

In particolare, una dimostrazione per induzione di basa su due pilastri fondamentali: la *base dell'induzione*, cioè la verifica che vale $P(0)$, e il *passo induttivo*, cioè la dimostrazione che $P(n)$ implica $P(n+1)$. Se uno di questi due passi manca, allora la dimostrazione non è completa (e quindi non corretta).

Due varianti notevoli di dimostrazioni per induzione:

a. sia $k \in \mathbb{N}$ e P una proprietà dei numeri naturali per cui valgono le due ipotesi

   (1') $P(k)$ è vera;

   (2) a partire dall'ipotesi che $P(n)$ sia vera possiamo dedurre che anche $P(n+1)$ è vera;

   allora, per lo schema di induzione possiamo concludere che $\{x \in \mathbb{N} : P(x)\} = \{x \in \mathbb{N} : x \geq k\}$, cioè è vera $\forall n \geq k\ P(n)$.

b. sia P una proprietà dei numeri naturali per cui valgono le due ipotesi

   (1) $P(0)$ è vera;

   (2') a partire dall'ipotesi che $P(0), P(1), \ldots, P(n-1)$ e $P(n)$ siano vere possiamo dedurre che anche $P(n+1)$ è vera;

   allora, per lo schema di induzione possiamo concludere che $\{x \in \mathbb{N} : P(x)\} = \mathbb{N}$, cioè è vera $\forall n \in \mathbb{N},\ P(n)$.

Vediamo un semplice esempio.

Teorema 2.1. $\forall n \in \mathbb{N},\ n \geq 1,\ \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Dimostrazione. In questo caso la dimostrazione per induzione ci chiede di partire da $P(1)$. Verifichiamo quindi $P(1)$, cioè che $\sum_{i=1}^{1} i = \frac{n(1+1)}{2}$. Questo è vero, dato che $\sum_{i=1}^{1} i = 1 = \frac{1*2}{2}$.

Per dimostrare il passo induttivo, supponiamo ora che valga $P(n)$ con $n > 0$ qualsiasi, e a partire da quest'ipotesi dimostriamo $P(n+1)$. Valutiamo dunque $\sum_{i=1}^{n+1} i$. Abbiamo la catena di uguaglianze

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

come volevamo dimostrare. Osserviamo esplicitamente che la seconda uguaglianza è vera grazie all'ipotesi induttiva (tutte le altre invece sono semplici conti).

Dato che abbiamo verificato sia la base dell'induzione ($P(0)$) sia il passo induttivo ($P(n)$ implica $P(n+1)$), concludiamo che, per induzione, $\forall n > 0,\ P(n)$ è vera. □

2.4.1 Dimostrazioni per induzione sbagliate (in costruzione)

Quando o manca la base dell'induzione o il passo induttivo non è dimostrato correttamente, lo schema di induzione fallisce in modo spettacolare. Vediamo qualche esempio.

Teorema 2.2 (Palesemente falso)**.** $\forall n \in \mathbb{N},\ n > 0$*,* n *è pari.*

Dimostrazione (palesemente sbagliata). Verifichiamo il passo induttivo: supponiamo che $1, 2, \ldots, n$ siano pari e dimostriamo che anche $n+1$ è pari. Dato che sia 1 sia n sono pari, abbiamo $1 = 2k$ e $n = 2t$ per qualche $t, k \in \mathbb{N}$, da cui deduciamo che anche $n + 1 = 2t + 2k = 2(t + k)$ è pari.

Quindi abbiamo dimostrato per induzione che $\forall n \in \mathbb{N},\ n > 0$, n è pari. □

Osservazione 2.3. *Ovviamente il teorema precedente è falso. Invece, la dimostrazione del passo induttivo* è corretta! *Infatti l'ipotesi induttiva è utilizzata a dovere. Qual è dunque il problema della dimostrazione? Semplicemente non abbiamo verificato la base dell'induzione, che è falsa (infatti* 1 *non è pari)!*

3 I numeri interi

È noto fin dall'Ottocento che, a partire dai numeri naturali, è possibile *definire* tutti gli altri insiemi numerici. Leopold Kronecker ha riassunto quest'idea con le affascinanti parole: "Dio ha creato i numeri naturali; tutto il resto è opera dell'uomo". Vediamo quindi come si costruiscono i vari insiemi numerici a partire dai naturali. È importante osservare che, nel costruire questi nuovi numeri, non dobbiamo partire dal nulla: da una parte, abbiamo i numeri naturali introdotti nella sezione precedente, e dall'altra abbiamo delle idee intuitive delle proprietà che desideriamo siano soddisfatte dai nuovi numeri che vogliamo definire.

Vediamo questo modo di procedere con un esempio concreto. In $\mathbb{N}$ non possiamo eseguire liberamente le sottrazioni: infatti $n - m$ non è definito se $n < m$. Per ovviare a questo problema, vogliamo costruire un nuovo insieme numerico dove effettuare le sottrazioni senza vincoli. Questo insieme sarà l'insieme dei numeri interi, che sarà costituito dai numeri positivi e dai numeri negativi.

Come costruirlo a partire dai naturali? L'idea fondamentale è la seguente: ogni numero intero $n-m$ sarà rappresentato da una coppia di numeri naturali (n, m). Quindi iniziamo a considerare l'insieme $\mathbb{N} \times \mathbb{N}$, i cui elementi sono coppie di numeri naturali. Un'osservazione: la coppia (n, m) rappresenta il numero $n - m$, quindi se $n \geq m$ allora (n, m) coinciderà con un numero naturale (che sarà un intero non negativo), e se $n < m$ allora (n, m) sarà un nuovo numero (che sarà un intero negativo).

Inoltre, la rappresentazione di un numero intero $n-m$ non è unica: oltre a (n, m), anche $(n + k, m + k)$ rappresenta $n - m$ per ogni numero naturale k. Quello che si fa per ovviare a questo inconveniente è quello di *identificare*, ovvero di considerare come un unico elemento, tutte le coppie (n, m) e (n', m') che rappresentano lo stesso numero intero. Dato che nei numeri naturali non è definita la sottrazione, non possiamo esprimere la condizione di "rappresentare lo stesso numero intero" mediante la formula $n - m = n' - m'$, ma dobbiamo

usare una formulazione equivalente che richieda solamente l'uso della somma: diciamo che $(n, m) \sim (n', m')$ (i.e. sono equivalenti) se vale l'uguaglianza $n + m' = n' + m$.

A questo punto, definiamo l'insieme dei numeri interi come l'insieme $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, che è l'insieme di coppie di numeri naturali identificati secondo la relazione di equivalenza $\sim$.

Su questo insieme, dobbiamo definire le operazioni di somma a partire dalle operazioni sui numeri naturali. Per distinguere le operazioni, chiamiamo $+_{\mathbb{Z}}$ e $\cdot_{\mathbb{Z}}$ la somma e il prodotto che vogliamo definire su $\mathbb{Z}$, mentre $+$ e $\cdot$ indicheranno le solite operazioni su $\mathbb{N}$.

È semplice verificare che una scelta vincente per definire la somma è

$$(n, m) +_{\mathbb{Z}} (n', m') = (n + n', m + m')$$

Infatti, se calcoliamo esplicitamente otteniamo

$$n - m + n' - m' = (n + n') - (m + m')$$

che è proprio rappresentato dalla coppia $(n + n', m + m')$.

Per quel che riguarda la moltiplicazione, svolgendo i conti si ottiene che una buona definizione è

$$(n, m) \cdot_{\mathbb{Z}} (n', m') = (n \cdot n' + m \cdot m', n \cdot m' + n' \cdot m).$$

L'unico passaggio ulteriore, che noi non faremo, è quello di verificare che ognuna di queste definizioni è indipendente dalla particolare coppia scelta per rappresentare i numeri interi, cioè che se $(n, m) \sim (a, b)$ e $(n', m') \sim (a', b')$, allora

$$(n, m) +_{\mathbb{Z}} (n', m') \sim (a, b) +_{\mathbb{Z}} (a', b') \text{ e } (n, m) \cdot_{\mathbb{Z}} (n', m') \sim (a, b) \cdot_{\mathbb{Z}} (a', b').$$

Si può facilmente dimostrare che queste operazioni estendono la somma e il prodotto su $\mathbb{N}$. Per questo motivo, ometteremo l'ornamento $_{\mathbb{Z}}$ e le indicheremo semplicemente mediante i simboli $+$ e $\cdot$. Inoltre, nella pratica quotidiana non useremo mai la scrittura $(2, 9)$ per indicare il numero -7, ma indicheremo i numeri interi con la solita notazione in uso fin dalle scuole elementari.

3.1 La regola dei segni

Dimostriamo la regola dei segni usando la definizione del prodotto. Ricordiamo che se $a \in \mathbb{Z}$ e $a > 0$, allora a è rappresentato dalla coppia $(a, 0)$. Se $a < 0$, allora a è rappresentato dalla coppia $(0, |a|)$, dove $|a|$ è il valore assoluto di a.

- $a, b > 0$. Abbiamo $(a, 0)(b, 0) = (ab + 0, a \cdot 0 + 0 \cdot b) = (ab, 0)$, che è positivo.
- $a, b < 0$. Abbiamo $(0, |a|)(0, |b|) = (0 + |a||b|, 0 \cdot |b| + |a| \cdot 0) = (|a||b|, 0)$, che è positivo.
- $a > 0, b < 0$ (il caso $a < 0, b > 0$ si ottiene applicando la proprietà commutativa del prodotto su $\mathbb{Z}$). Abbiamo $(a, 0)(0, |b|) = (a \cdot 0 + 0 \cdot |b|, a|b| + 0 \cdot 0) = (0, a|b|)$, che è negativo.

4 I numeri razionali

Per definire i numeri razionali, si procede in modo simile a quanto abbiamo visto nella definizione dei numeri interi. L'esigenza che ci spinge a definire i numeri razionali a partire dagli interi è quella di poter effettuare le divisioni per ogni numero $q \neq 0$. Anche questa

volta rappresentiamo un numero p/q mediante una coppia di elementi $(p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Il primo numero della coppia esprimerà il dividendo, mentre il secondo il divisore.

Ancora una volta, il primo passo da compiere è identificare quelle coppie (p, q) e (p', q') che individuano lo stesso numero. Si verifica facilmente che porta al risultato desiderato identificare le coppie che verificano l'uguaglianza $p \cdot q' = p' \cdot q$.

Per quel che riguarda le operazioni, definire il prodotto è molto semplice:

$$(p, q) \cdot_{\mathbb{Q}} (p', q') = (p \cdot p', q \cdot q').$$

La somma, invece, va trattata con più attenzione: come ci è stato insegnato a scuola, non possiamo sommare due frazioni a meno che non abbiano lo stesso denumeratore. Quindi, si può verificare che la scelta giusta per la somma è questa:

$$(p, q) +_{\mathbb{Q}} (p', q') = (p \cdot q' + p' \cdot q, q \cdot q').$$

Anche in questo caso, si dovrebbe dimostrare che la definizione delle operazioni è indipendente dalla particolare scelta delle coppie, e che le usuali proprietà di somma e prodotto sono verificate.

Ancora una volta, nella pratica si usano indicare i numeri razionali o sotto forma di frazioni o sotto forma di numeri decimali finiti o periodici, mentre l'insieme di tutti i numeri razionali viene indicato con il simbolo $\mathbb{Q}$, e le operazioni con i simboli $+$ e $\cdot$.

4.1 $\sqrt{2}$ è irrazionale

Il campo dei numeri razionali, pur avendo molte proprietà algebriche, non esaurisce l'insieme di tutti i numeri di cui la matematica può parlare. Un esempio particolarmente interessante, già noto agli antichi Greci, è dato da $\sqrt{2}$. La dimostrazione dell'irrazionalità di $\sqrt{2}$ è molto semplice e d'effetto. Prima di affrontarla, introduciamo un risultato preliminare.

Lemma 4.1. *Se $p \in \mathbb{N}$ e p^2 è pari, allora anche p è pari.*

Dimostrazione. Effettuiamo la dimostrazione per contronominale[11]: supponiamo che p sia dispari e dimostriamo che p^2 è dispari. Grazie all'ipotesi che p è dispari, possiamo scrivere $p = 2k + 1$ con $k \in \mathbb{N}$. Con un semplice calcolo, otteniamo $p^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Quindi p^2 è dispari, e questo completa la dimostrazione. □

Teorema 4.2 (Euclide)**.** $\sqrt{2} \notin \mathbb{Q}$.

Dimostrazione. Supponiamo per assurdo che

$$\sqrt{2} = \frac{p}{q} \in \mathbb{Q}. \tag{1}$$

Inoltre possiamo supporre che $p, q \in \mathbb{N}$ non abbiano fattori comuni, i.e. che $\mathrm{MCD}(p, q) = 1$. Elevando al quadrato entrambi i membri della 1, otteniamo

$$2q^2 = p^2 \tag{2}$$

[11] La dimostrazione per contronominale è espressa dalla seguente equivalenza: $(A \to B) \leftrightarrow (\neg B \to \neg A)$. Quindi per dimostrare l'implicazione $A \to B$ possiamo dimostrare $\neg B \to \neg A$, e viceversa. L'ordine delle implicazioni è cruciale: di solito non è vero che $(A \to B) \leftrightarrow (\neg A \to \neg B)$. Per comodità, ci si può ricordare l'esempio classico: "tutti i corvi sono neri" è equivalente a "se un oggetto non è nero, allora non è un corvo", e non a "tutti i non corvi sono non neri".

In particolare, p^2 è pari e, per il lemma precedente, anche p è pari, i.e. $p = 2k$ per qualche $k \in \mathbb{N}$. Sostituendo $p = 2k$ nell'uguaglianza 2 otteniamo $2q^2 = 4k^2$, che implica che anche q^2 è pari. Di conseguenza anche q è pari, ma questo contraddice l'ipotesi che $\mathrm{MCD}(p, q) = 1$. Concludiamo che $\sqrt{2} \notin \mathbb{Q}$, come volevamo. □

Si può dimostrare che molti altri numeri sono irrazionali: ad esempio $\sqrt{p}$ per ogni primo $p \in \mathbb{N}$, e[12], π[13].

5 Numeri reali

Coming soon.

6 Numeri complessi

Storicamente, l'insieme dei numeri complessi è stato introdotto a partire dall'esigenza di risolvere equazioni di secondo grado come

$$x^2 = -r, \ r > 0 \tag{3}$$

che non ha soluzioni nell'insieme dei numeri reali, poiché il prodotto di qualsiasi numero reale per se stesso è sempre positivo (come si può dedurre ad esempio dalla regola dei segni 3.1).

Per poter sperare di risolvere equazioni come la 3, invece di definire un nuovo insieme numerico come abbiamo fatto per costruire numeri interi e razionali, utilizziamo un metodo leggermente diverso. Definiamo i numeri complessi come i numeri della forma $\mathbb{C} = \{a + \heartsuit b : a, b \in \mathbb{R}\}$ e definiamo su $\mathbb{C}$ la somma e il prodotto come se gli elementi di $\mathbb{C}$ fossero polinomi in $\heartsuit$. Inoltre, imponiamo che valga l'uguaglianza $\heartsuit^2 = -1$. Con questa nuova uguaglianza, il prodotto si può esprimere facilmente in questo modo:

$$(a + \heartsuit b) \cdot (c + \heartsuit d) = ac - bd + (ad + bc)\heartsuit.$$

Gli elementi di $\mathbb{C}$ sono chiamati numeri complessi, e di solito il numero $\heartsuit$, che si chiama anche unità immaginaria, si indica con il simbolo i. Si verifica facilmente che $(\mathbb{C}, +, \cdot, 0, 1)$ è un anello commutativo. In realtà, $\mathbb{C}$ ha una struttura algebrica più ricca.

Teorema 6.1. $(\mathbb{C}, +, \cdot, 0, 1)$ *è un campo.*

Dimostrazione (opzionale). Dato che $\mathbb{C}$ è un anello commutativo, ci basta dimostrare che ogni elemento diverso da 0 ha un inverso moltiplicativo. Se $x \in \mathbb{C}$ si può scrivere come $a \in \mathbb{R}$, allora è facile verificare che il numero reale a^{-1} è l'inverso moltiplicativo di a anche nel senso dei numeri complessi. Se invece $x = a + ib$ con $b \neq 0$, ci piacerebbe dire che $1/(a + ib)$ è l'inverso moltiplicativo di x. Se dimostriamo che esistono $c, d \in \mathbb{R}$ tali per cui vale l'uguaglianza $c + id = 1/(a + ib)$, allora possiamo concludere che $\mathbb{C}$ è un campo. Con un po' di conti, otteniamo

$$\frac{1}{a + ib} = \frac{1}{a + ib} \cdot \frac{a - ib}{a - ib} = \frac{a - ib}{a^2 - (ib)^2} = \frac{a - ib}{a^2 + b^2}.$$

A questo punto, per la nostra ipotesi $b \neq 0$, abbiamo $a^2 + b^2 > 0$ (e ovvamente $a^2 + b^2 \in \mathbb{R}$). Quindi $1/(a+ib) = a/(a^2+b^2)+(-b/(a^2+b^2))i$, ed in particolare è un numero complesso. □

[12] La prima dimostrazione è di Eulero nel 1737.

[13] La prima dimostrazione è del 1761, ad opera del matematico (e fisico, filosofo, astronomo) svizzero Johann Heinrich Lambert.

Abbiamo introdotto nei numeri complessi la radice quadrata di un numero negativo per poter risolvere delle equazioni come la 3. In realtà, che con questa aggiunta otteniamo molto di più di quello che speravamo. Infatti, si può dimostrare che nel campo dei numeri complessi ogni polinomio di grado n ha almeno una radice. Questo a sua volta implica l'enunciato più famoso del Teorema Fondamentale dell'Algebra, cioè che un polinomio di grado n ha esattamente n radici, non necessariamente distinte. Purtroppo, nessuna dimostrazione di questo teorema è accessibile al primo anno di una qualsiasi facoltà scientifica, quindi non la possiamo riportare qui. Ironicamente, le dimostrazioni coinvolgono tutte degli strumenti analitici, e quindi non sono particolarmente algebriche.

6.1 Piccole cose utili

Definizione 6.2 (Parte reale e parte immaginaria)**.** *Per sfruttare i numeri complessi, è comodo definire le funzioni di parte reale e parte immaginaria di un numero complesso. Se $\clubsuit \in \mathbb{C}$ è $x = a + ib$, allora la parte reale di $\clubsuit$ è a e la parte immaginaria di $\clubsuit$ è b. Di solito queste funzioni si indicano con $a = Re(\clubsuit)$ e $b = Im(\clubsuit)$.*

Definizione 6.3 (Il coniugato di un numero complesso)**.** *Il coniugato di un numero complesso $z = a + ib$ si denota con $\bar{z}$ ed è definito come $\bar{z} = a - ib$.*

L'operazione di complesso coniugato ha alcune proprietà interessanti. Ad esempio,

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

Questo ci permette di calcolare i quozienti tra generici numeri complessi. Se $z_1, z_2 \in \mathbb{C}$ e $z_2 \neq 0$, allora

$$\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{z_2\bar{z}_2} = \frac{z_1\bar{z}_2}{|z_2|^2}.$$

Questo è lo stesso trucco che abbiamo usato per dimostrare che $\mathbb{C}$ è un campo.

Si può verificare facilmente che $z + \bar{z} = 2Re(z)$ e $z - \bar{z} = 2iIm(z)$.

L'operazione $z \mapsto \bar{z}$ è un'involuzione, cioè è invertibile e coincide con la sua inversa. Quindi $\bar{\bar{z}} = z$.

Inoltre valgono le seguenti proprietà: $\overline{z + z'} = \bar{z} + \overline{z'}$ e $\overline{z \cdot z'} = \bar{z} \cdot \overline{z'}$[14].

6.2 Rappresentazione cartesiana dei numeri complessi

Coming soon.

6.3 Rappresentazione esponenziale dei numeri complessi

Coming soon.

[14] Se $(A, +_a, \cdot_a, 0_a, 1_a)$ e $(B, +_b, \cdot_b, 0_b, 1_b)$ sono anelli, una funzione $f : A \to B$ che verifica le proprietà

- $f(x +_a y) = f(x) +_b f(y)$ e
- $f(x \cdot_a y) = f(x) \cdot_b f(y)$

si chiama omomorfismo di anelli. Se A e B sono campi e f ha le proprietà sopra elencate, allora f è un omomorfismo di campi. Se $A = B$ e f è biettiva, allora è un isomorfismo.

Riferimenti bibliografici

[1] Keith Devlin, *The joy of sets*, 1993 Springer-Verlag New York, Inc.

[2] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R.Remmert, *Numbers*, reperibile alla pagina `http://www.maths.ed.ac.uk/~aar/papers/numbers`.