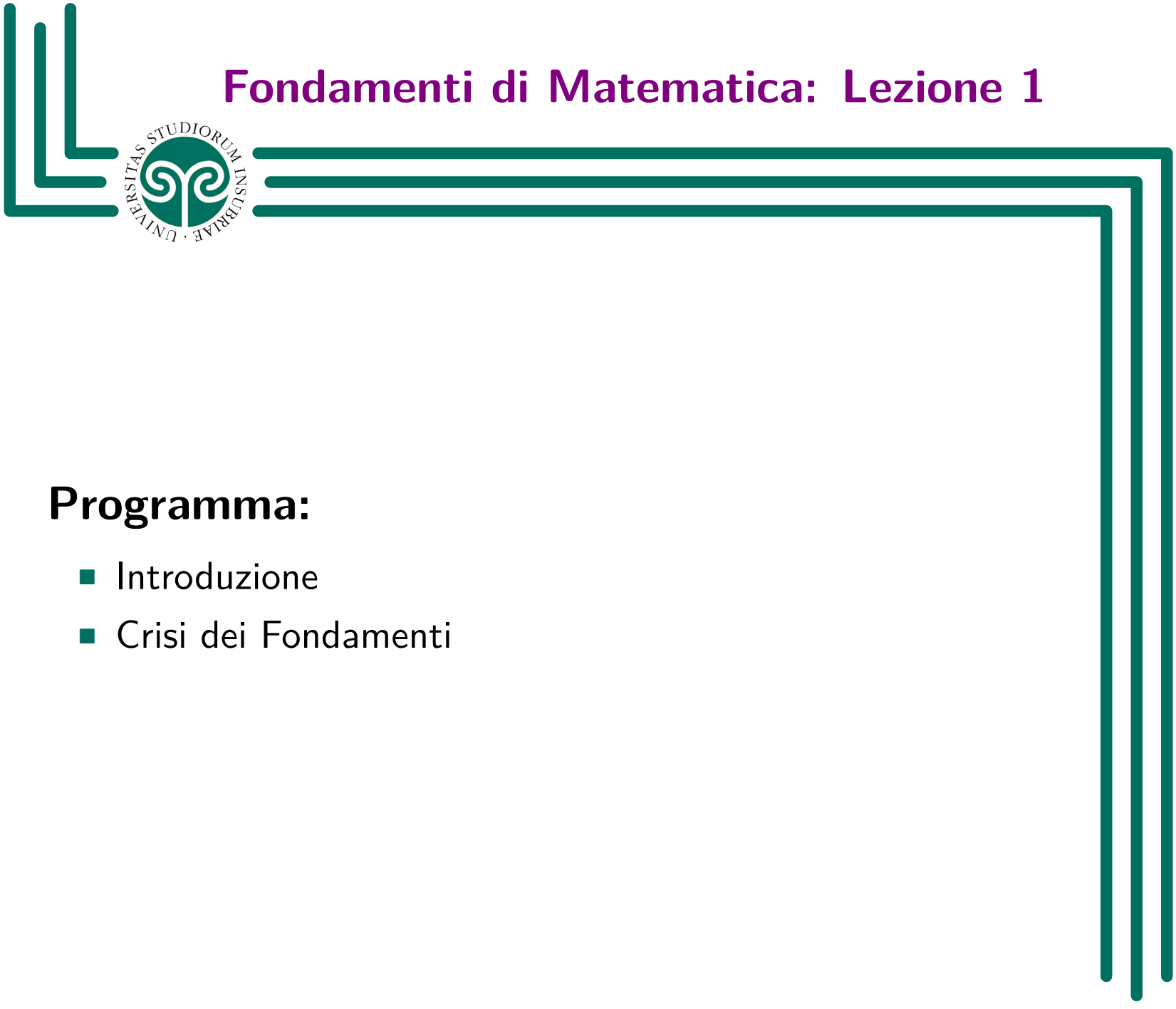
Fondamenti di Matematica

Dr Marco Benini (marco.benini@uninsubria.it)

Percorso Formazione Docenti — **A026-Matematica**

2026



Fondamenti di Matematica: Lezione 1

Programma:

- Introduzione
- Crisi dei Fondamenti

Introduzione

Lo scopo di questo ciclo di lezioni è introdurre la disciplina dei Fondamenti della Matematica.

In particolare, si vuole mettere in evidenza come questa disciplina fornisca un *metodo unificante* per guardare alla Matematica.

La conseguenza, molto pratica, è che tanti problemi matematici possono essere visti come istanze di un unico fenomeno, fornendo spunti e strumenti per la soluzione, pescando da ambiti apparentemente molto distanti.

Burocrazia

Il corso durerà si articolerà su quattro lezioni.

La lezione odierna illustrerà la crisi dei fondamenti e la ricerca di una soluzione da un punto di vista storico.

La seconda e la terza lezione verteranno sulla analisi di come le idee sviluppate nella prima lezione trovino applicazione nella Matematica.

La quarta lezione concluderà questo percorso e si chiuderà con una discussione in aula dei temi del corso.

Crisi dei Fondamenti

Per descrivere la Matematica serve dare per acquisite alcune nozioni di base. Queste nozioni traggono il loro fondamento dalla realtà.

I pilastri della Matematica nella seconda metà del '700 sono sintetizzabili:

- i numeri naturali, $\mathbb{N}$, e i numeri reali, $\mathbb{R}$, sono astrazioni dalla realtà e la loro concezione intuitiva, ovvero permettono di *contare* e *misurare*, è adeguata allo sviluppo della Matematica.
- esiste un solo spazio, quello Euclideo.
- gli insiemi, ovvero gli oggetti risultato dell'azione di *raggruppare*, sono un concetto intuitivo e pre-matematico.

L'assunto filosofico era che tutta la Matematica potesse essere costruita a partire da queste nozioni di base.

Crisi dei Fondamenti

Questo quadro tuttavia mostra delle evidenti crepe di natura metodologica.

In quel periodo storico, la Matematica esplora la *convergenza* delle *serie*, ottenendo risultati problematici.

Esempio 1. Si consideri

$$\sum_{i=1}^{\infty} \frac{1}{i} \ .$$

Questa serie è divergente: la sua somma è più grande di qualsiasi numero reale.

La dimostrazione viene fatta risalire a Nicole Oresme, matematico medievale vissuto attorno alla metà del 1300.

Crisi dei Fondamenti

Esempio 2. Prendiamo la serie

$$\sum_{i=0}^{\infty}(-1)^i$$

le cui somme parziali sono sempre 1 oppure 0. Dato che la sequenza $0,1,0,1,0,1,\ldots$ non converge come successione, la serie non ha limite.

Ma, $\sum_{i=0}^{\infty}(-1)^i = 1+\sum_{i=1}^{\infty}(-1)^i = 1-1+\sum_{i=2}^{\infty}(-1)^i = 0+\sum_{i=2}^{\infty}(-1)^i = \sum_{i=2}^{\infty}(-1)^i$.

Quindi $\sum_{i=0}^{\infty}(-1)^i = 0+\sum_{i=2}^{\infty}(-1)^i = 0+0+\sum_{i=4}^{\infty}(-1)^i = 0+0+0\ldots = 0$.

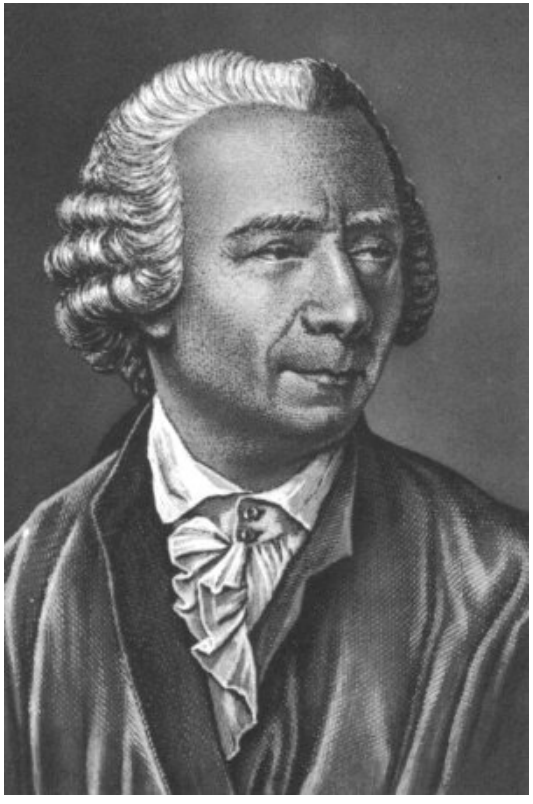
Perciò la serie ha limite e l'Analisi contiene una contraddizione interna.

Chiaramente, da qualche parte abbiamo commesso un errore.
Ma, al tempo, una serie **era considerata** una *somma infinita*, l'esito del processo di sommare tutti i termini.

Crisi dei Fondamenti

Esempio 3. Consideriamo

$$\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$$



che è noto come il *Problema di Basilea*, posto da Pietro Mengoli nel 1644 e risolto da Eulero nel 1735. Tuttavia, una dimostrazione rigorosa appare solo nel 1741.

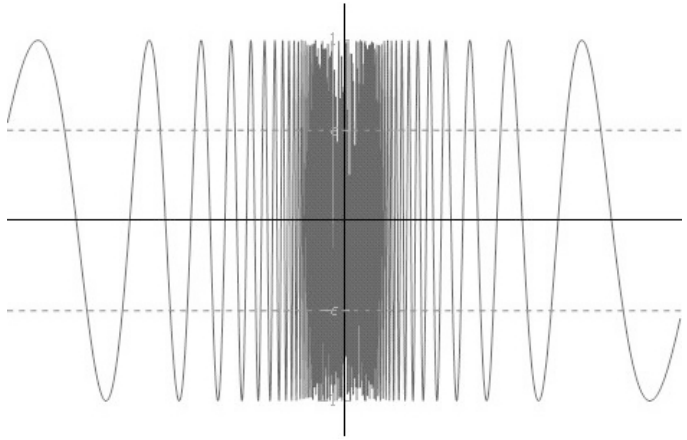
Questa serie è *convergente*. La dimostrazione originale di Eulero presuppone che le regole di manipolazione dei polinomi valgano anche per le serie, il che non è necessariamente vero.

Quindi, quali sono le operazioni ammissibili sulle serie?
E, soprattutto, se una serie non è una *somma infinita*, cos'è?

Crisi dei Fondamenti

Esempio 4. Prendiamo la funzione

$$f(x) = \sin \frac{1}{x}$$



La funzione è continua in 0?

In base alla *nostra* nozione di continuità, per ogni intorno aperto U di $f(0)$ possiamo trovare un intervallo aperto contenente 0 la cui immagine è U, quindi la funzione è continua in 0.

Ma la nozione intuitiva che la curva possa essere tracciata con un singolo tratto di matita è chiaramente falsa.

Crisi dei Fondamenti

Problemi come quelli illustrati comparivano sempre più frequentemente nello sviluppo dell'Analisi e minavano la certezza dei risultati: l'intuizione comune non trovava riscontro nei risultati apparentemente contraddittori.

Per questo motivo, a partire dall'inizio dell'800, si sviluppò un ponderoso sforzo per sistematizzare e formalizzare l'Analisi matematica, onde farla poggiare su solide fondamenta.

Senza entrare nei dettagli, in questo periodo vengono sviluppati in modo rigoroso i concetti di

- limite
- derivata
- integrale
- serie

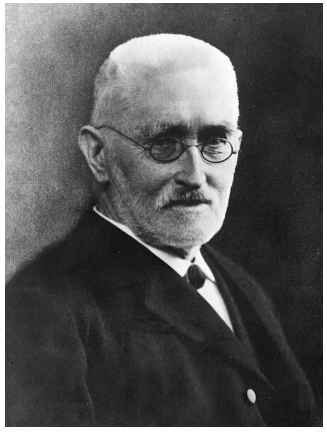
e le loro proprietà vengono analizzate e dimostrate su una base assiomatica e ipotetico-deduttiva, fornendo la necessaria base ai risultati precedenti.

Questa è l'Analisi che ancora oggi studiamo e usiamo.

Crisi dei Fondamenti







Gauss, Cauchy, Weierstrass, Riemann, Dedekind, Bolzano e molti altri sono tra i protagonisti di questa formalizzazione dell'Analisi, che portò anche a un approfondimento, generalizzazione e avanzamento grazie alla chiarezza e alla profondità delle idee di base.

Crisi dei Fondamenti

Un fatto evidente a posteriori, ma non ovvio a priori, è che le definizioni di base dell'Analisi matematica sono *errate* se non si dispone di una solida e adeguata definizione di *numero reale*.

Esempio 5. Se ragioniamo nello stile di Liebniz, $\lim_{n\to\infty}\frac{1}{n}$ e $\lim_{n\to\infty}\frac{1}{n^2}$ non possono essere il numero reale 0, ma piuttosto $0+\epsilon_1$ e $0+\epsilon_2$ con ϵ_1 e ϵ_2 due infinitesimi distinti (precisamente $\epsilon_2=\epsilon_1^2$) perché $1/n>0$ e $1/n^2>0$ per ogni $n\in\mathbb{N}$ e quindi il limite deve essere strettamente maggiore di 0 di un infinitesimo. Ovvero le successioni tendono a 0 da destra.

Ma è *necessario* che il limite sia esattamente 0 altrimenti

$$\lim_{n\to\infty}\left(\frac{1}{n^2}-\frac{1}{n}\right)\neq\left(\lim_{n\to\infty}\frac{1}{n^2}\right)-\left(\lim_{n\to\infty}\frac{1}{n}\right)=0+\epsilon_2-0-\epsilon_1\neq 0$$

ovvero l'operazione di limite non commuterebbe con la somma.

Crisi dei Fondamenti

Un modo per definire i numeri reali è *costruirli* a partire dai numeri razionali. Le due costruzioni più importanti sono mediante

- le *successioni di Cauchy*
- le *sezioni di Dedekind*

Una successione $\{a_i\}_{i\in\mathbb{N}}$ è *di Cauchy* se per ogni $\epsilon > 0$ esiste $n \in \mathbb{N}$ tale che $|a_j - a_i| < \epsilon$ per ogni $i, j \geq n$. Due successioni di Cauchy $\{a_i\}_{i\in\mathbb{N}}$ e $\{b_i\}_{i\in\mathbb{N}}$ sono equivalenti se $\{|a_i - b_i|\}_{i\in\mathbb{N}}$ è una successione di Cauchy. Quindi i numeri reali sono definiti come il quoziente delle successioni di Cauchy rispetto a questa nozione di equivalenza.

Si osservi che, ad esempio, una serie è definita come la successione delle sue somme parziali. Essa converge se e solo se tale successione è di Cauchy, e la sua somma è il numero rappresentato dalla successione.

Crisi dei Fondamenti

Una *sezione di Dedekind* è una partizione (A, B) dei numeri razionali tale che

- per ogni $a \in A$ e $b \in B$, $a < b$
- A non ha massimo

I numeri reali sono definiti come le sezioni di Dedekind dei razionali.

Osserviamo che questa costruzione significa che ogni sottoinsieme C limitato superiormente, ovvero tale che esista M per cui $c \leq M$ per ogni $c \in C$, ha un estremo superiore.

Le due costruzioni dei reali sono equivalenti solo sotto opportune ipotesi: ad esempio, solitamente, per costruire una successione di Cauchy da una sezione di Dedekind serve l'*assioma della scelta*.

Crisi dei Fondamenti

Dalle costruzioni precedenti deduciamo che

- da $\mathbb{N}$, l'insieme dei naturali, costruiamo l'insieme degli interi $\mathbb{Z}$
- da $\mathbb{Z}$ costruiamo l'insieme dei razionali, $\mathbb{Q}$
- da $\mathbb{Q}$ costruiamo l'insieme dei reali, $\mathbb{R}$

Gli ingredienti per eseguire queste costruzioni sono

- i numeri naturali
- gli insiemi

Quindi per avere i numeri reali in modo soddisfacente onde sviluppare l'Analisi solidamente e senza contraddizioni ci *basta* avere i naturali e gli insiemi.

Crisi dei Fondamenti

Giuseppe Peano in *Arithmetices principia, nova methodo exposita* del 1889 dette una formulazione dell'aritmetica, in particolare dei numeri naturali, che è al contempo estremamente semplice e potente.

Essa è basata sulla rappresentazione unaria e sul *principio di induzione*.

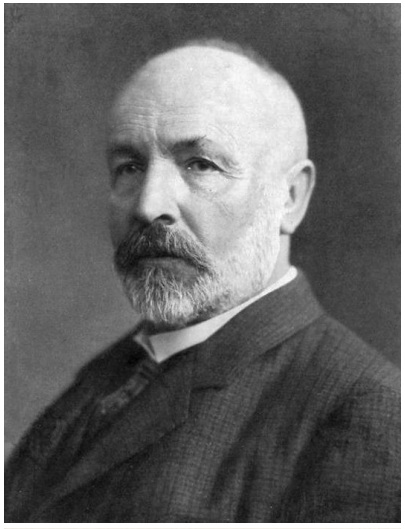
La costruzione dei naturali di Peano è essenzialmente linguistica e risolve in modo definitivo l'individuazione dei naturali, senza ricorrere a enti esterni alla esposizione formale.

Crisi dei Fondamenti

Tra il 1874 e il 1884 Georg Cantor sviluppò una parte fondamentale della teoria degli insiemi, mostrando come la nozione di *insieme infinito* non sia univoca: ad esempio $\mathbb{N}$ e $\mathbb{R}$ sono entrambi infiniti ma non ponibili in corrispondenza biunivoca.

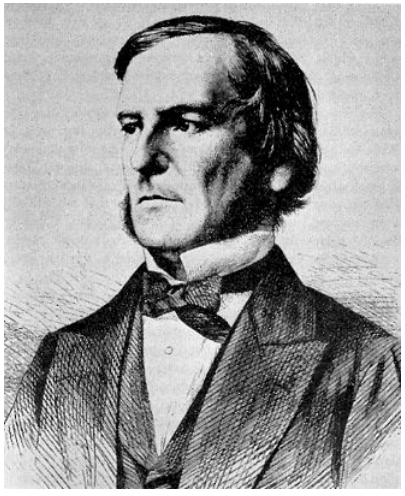
In altre parole, il concetto di insieme non è immediatamente ovvio, contrariamente all'idea comune. Usare gli insiemi come enti fondamentali richiede una loro disamina più approfondita.

Gottlob Frege tra la fine dell'800 e i primi del '900 sviluppò l'aritmetica in modo completamente rigoroso e formale a partire dalla teoria degli insiemi di Cantor.



Crisi dei Fondamenti

In realtà, il lavoro di Frege estende il lavoro di George Boole che diede una prima interpretazione del ragionamento matematico in termini insiemistici.



Il lavoro di Boole costituisce il punto di partenza di una nuova branca della Matematica, la *Logica*.

Il ragionamento matematico stesso divene oggetto di studio, attraverso strumenti matematici, estendendo e incorporando nella Matematica quanto fatto da Aristotele in poi in ambito filosofico.

La combinazione di logica e teoria degli insiemi sembra rispondere alle esigenze di una fondazione rigorosa dell'edificio della Matematica: un insieme di strumenti per descrivere l'intera disciplina a partire da pochi elementi primi indisputabili e perfettamente compresi.

Crisi dei Fondamenti

Questo promettente quadro venne messo in crisi da alcuni paradossi presenti nella teoria degli insiemi, che la rendono contraddittoria.

Il più famoso è dovuto a Bertrand Russell: se presumiamo di poter costruire l'insieme degli oggetti che soddisfano una determinata proprietà, allora possiamo costruire $R = \{x \mid x \notin x\}$. Ma $R \in R$ non può essere, così come $R \notin R$. Quindi R non è ammissibile come insieme, contraddicendo il fatto che debba esistere. Sfortunatamente l'intera fondazione di Frege usava questo *Principio di Comprensione* in modo essenziale, rendendo il suo tentativo fallimentare.

In realtà, paradossi simili, ad esempio quello dovuto a Cesare Burali-Forti, erano stati trovati qualche anno prima, all'interno della teoria degli insiemi di Cantor.

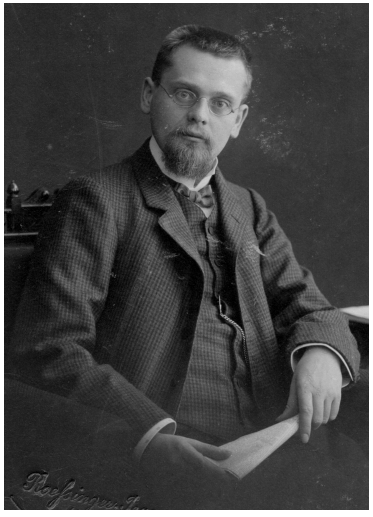
Crisi dei Fondamenti

Il *Programma di Hilbert*, messo a punto negli anni '20 del XX secolo, si ripromette di descrivere tutta la Matematica a partire da una base logica ben definita, utilizzando un numero minimo di assiomi elementari, attraverso metodi *finitistici*.

Il punto essenziale, per garantire solidità alla costruzione, è dimostrare all'interno del sistema stesso, l'assenza di contraddizioni.

È importante sottolineare come il principio di non-contraddizione è quello che, secondo la visione di Hilbert, renderebbe *vera* la Matematica.

Crisi dei Fondamenti



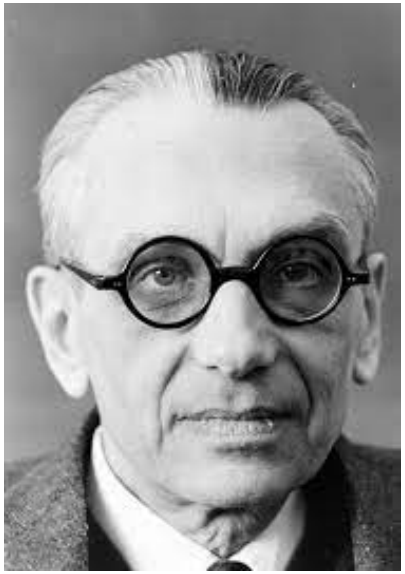
La teoria degli insiemi di Ernst Zermelo e Abraham Frækel, partendo da un piccolo insieme di assiomi, riesce a fornire gli strumenti per generare le strutture basilari della Matematica.

L'assioma di *regolarità* impedisce la formazione di insiemi contradditori, come quello che sottende il paradosso di Russell. Tuttavia, essa risulta una teoria altamente *tecnica*, che non rispecchia l'intuizione comune di cosa sia un insieme.

Essa, oggi, viene considerata la teoria degli insiemi di riferimento e, per molti versi, costituisce la teoria fondante della Matematica.

Crisi dei Fondamenti

Nel 1930, Kurt Gödel sviluppa i due *teoremi di incompletezza* che prendono il suo nome.



Il primo afferma che ogni sistema formale davvero scrivibile, sufficientemente potente e privo di contraddizioni interne contiene una affermazione necessariamente vera ma non dimostrabile. Per *sufficientemente potente* si intende che il sistema contiene, essenzialmente, la teoria dell'aritmetica.

Il secondo teorema afferma che per ogni teoria formale davvero scrivibile, sufficientemente potente e priva di contraddizioni interne, una della affermazioni indimostrabili è quella che codifica la sua consistenza.

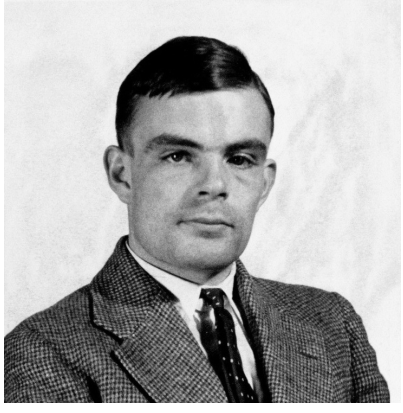
Questo risultato è la pietra tombale sul programma di Hilbert, che risulta semplicemente irrealizzabile.

Crisi dei Fondamenti

Un aspetto collaterale, ma decisamente importante nelle dimostrazioni di Gödel, è l'uso della nozione di *funzione calcolabile*.

Questa idea, estremamente feconda, porta più o meno nello stesso periodo, Alonzo Church e Alan Turing a formalizzare la nozione di *calcolabile*, e a sviluppare la Matematica necessaria al suo pieno trattamento.

È la nascita di una nuova disciplina, l'Informatica, che cambierà il mondo, come oggi ben sappiamo.



Crisi dei Fondamenti

Per dimostrare la consistenza dell'aritmetica di Peano è necessario, stante il risultato di Gödel, effettuare la prova in un sistema più potente.

Gerhard Gentzen sul finire degli anni '30 dimostra la consistenza dell'aritmetica usando l'aritmetica stessa, con un principio di induzione rafforzato: esso si estende oltre i numeri naturali e comprende anche una parte degli ordinali.

Questa tecnica, passando attraverso uno studio delle dimostrazioni formali come oggetto matematico, porta alla nascita della *Teoria della Dimostrazione*.

Crisi dei Fondamenti

Un caposaldo dei Fondamenti della Matematica nella visione di fine '700 era l'esistenza di un unico spazio: quello di Euclide.

A metà del XIX secolo, questa visione viene spazzata via con la nascita delle cosiddette *geometrie non-euclidee*. Sebbene i primi esempi mostrino delle strutture spaziali che soddisfano tutti gli assiomi di Euclide eccetto il *postulato delle parallele*, in breve, si riesce a mostrare che le geometrie alternative a quella classica sono ovunque, e assumono forme quanto mai diversificate.

Questi oggetti, all'inizio del XX secolo, assumono una importanza concreta straordinaria: grazie alla Teoria della Relatività Generale di Albert Einstein, l'universo in cui viviamo non è euclideo.

Il fondamento dello spazio unico è falso, anche nel mondo fisico.

Crisi dei Fondamenti

Tra la metà dell'800 e fino agli anni '20 del XX secolo, si sviluppa quindi una nozione di spazio più generale, che ricomprende le geometrie che man mano nascono.

Immaginando uno spazio come un insieme di punti dotato di struttura, il problema è individuare questa struttura. Spicca in questo senso lo studio di Henri Poincaré, che introdusse i concetti di *omotopia* e *omologia* per tentare di cogliere gli aspetti essenziali di uno spazio.

Successive generalizzazioni e raffinamenti condussero nel 1922 alla definizione odierna di *spazio topologico* dovuta a Kuratowski.

Crisi dei Fondamenti

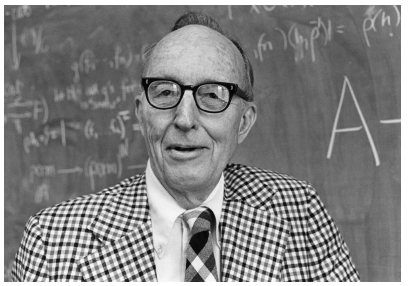
Sebbene la nozione di spazio topologico sia estremamente generale e, oggi, accettata come quella che meglio coglie l'essenza di cosa renda un insieme di punti uno spazio, per sviluppare la Matematica nelle sue varie branche, servono nozioni più specifiche.

Per questo motivo, parallelamente allo sviluppo della nozione di spazio topologico, appaiono anche i concetti fondamentali di *spazio metrico*, *spazio normato*, ma anche generalizzazioni della geometria analitica, che portarono alla algebrizzazione degli spazi attraverso gli *spazi vettoriali* su *campi* generici, e con uno sforzo ulteriore, ai *moduli* su *anelli*.

Questi sviluppi risultano imprescindibili per anche solo descrivere la Matematica del XX secolo, ma soprattutto quella contemporanea.

Crisi dei Fondamenti

La *geometria algebrica* e la *topologia algebrica*, che possiamo immaginare come lo studio delle strutture algebriche intrinseche agli spazi topologici e geometrici, entrarono in crisi attorno agli anni '30 del XX secolo.

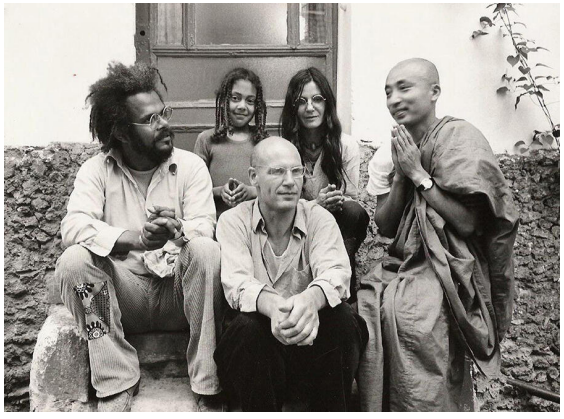


Semplicemente, gli strumenti matematici risultavano inadeguati per affrontare i problemi che si ponevano. Per costruire l'armamentario di strumenti necessari, MacLane e Eilenberg costruirono ex-novo la *Teoria delle Categorie*, che in primissima approssimazione possiamo immaginare come una generalizzazione profonda della teoria degli insiemi.

Essa è, in realtà, molto di più, e per certi versi costituisce la teoria fondativa della Matematica del XX secolo, così come la teoria degli insiemi fonda la Matematica del XIX.

Crisi dei Fondamenti

Alexandre Grothendieck introdusse un approccio completamente astratto al trattamento di problemi in geometria algebrica, culminando nella soluzione delle cosiddette congetture di Weil. Il suo lavoro usa la Teoria delle Categorie come fondativa nella sua visione della Matematica.



Il suo lavoro, e in particolare la nozione di *topos*, costituisce una delle più ardite generalizzazioni del concetto di spazio.

In modo estremamente informale, un topos di Grothendieck è al contempo, uno spazio totalmente astratto, una teoria degli insiemi, un sistema logico formale, una struttura algebrica complessa, e molto altro.

Crisi dei Fondamenti

Questa illustrazione, di necessità frettolosa e superficiale, della Crisi dei Fondamenti, ci mostra come gli enti fondamentali della Matematica siano stati oggetto di profonda analisi.

In un certo senso, questa analisi ha stravolto la concezione stessa della Matematica, generando nuove discipline e nuove branche.
Ha dato origine a un mondo matematico molto più vasto, ricco, complesso di quanto fosse alla fine del '700.

Un mondo che è ancora oggi in fase di studio.

Crisi dei Fondamenti

In particolare, tecniche estremamente generali e profonde sono state messe a punto per affrontare problemi difficili.

Solo per citare un paio di esempi maggiori, la prova di Andrew Wiles dell'ultimo teorema di Fermat, o la prova della congettura di Poincaré da parte di Grigori Perelman sarebbero inconcepibili senza tutto l'arsenale di strumenti cui abbiamo accennato.

Tuttavia, queste idee e strumenti non sono affatto confinati ai risultati più astrusi della Matematica contemporanea. Al contrario, le idee sin quì illustrate forniscono un punto di vista differente da cui guardare e descrivere anche le parti più elementari della Matematica, dando spunti per una sua trattazione certe volte più semplice, certe volte più unitaria.

Crisi dei Fondamenti

Questo corso proseguirà andando a vedere alcune delle tecniche accennate in questa lezione, tentando di calarle nella realtà della Matematica che viene tipicamente illustrata nelle scuole superiori.

Riferimenti

La Storia della Matematica così come illustrata è ben descritta nel secondo volume di Morris Kline, *Storia del pensiero matematico*, Einaudi.

Per alcuni aspetti della matematica più recente, vale la pena dare una occhiata al volumetto di Piergiorgio Odifreddi, *La matematica del Novecento*, Einaudi.

Nel corso di laurea magistrale in Matematica dell'Università degli Studi dell'Insubria viene tenuto un corso di Storia della Matematica il cui materiale didattico può essere di interesse:

`https://marcobenini.me/lectures/history-of-mathematics/`

Fondamenti di Matematica: Lezione 2

Programma:

- Logicismo
- Formalismo
- Costruttivismo

Logicismo

L'idea di Bertrand Russell è che la Matematica sia una branca della Logica.

Quest'idea è, dopo i risultati di Kurt Gödel, insostenibile. E, in ogni caso, non prende in considerazione l'aspetto precipuo dell'intuizione matematica che nasce dalla realtà e da una analisi dei problemi che prescinde dalla mera dimostrazione.

Tuttavia una parte tutt'altro che piccola della Matematica è, in effetti, descrivibile come prodotto dello sviluppo logico soggiacente.

Logicismo

Principio concreto

Far risaltare come poche nozioni accoppiate al ragionamento permettano di sviluppare matematica significativa

Logicismo

Teorema 6 (Fattorizzazione unica). *Ogni $n \in \mathbb{N}$ tale che $n \geq 2$ può essere scritto come prodotto di numeri primi in modo unico.*

Sebbene dimostrare questo teorema non sia difficile, la sua dimostrazione viene solitamente omessa nei corsi elementari.

Tuttavia esso rappresenta un semplice concetto: ogni numero naturale può essere scritto come 0, 1, oppure come un prodotto di numeri primi. E nel terzo caso, il prodotto è unico.
In altri termini, ogni numero naturale ha una *forma canonica* come prodotto di un sottoinsieme molto specifico di numeri.

Logicismo

Teorema 7 (Fattorizzazione unica). *Ogni $n \in \mathbb{N}$ tale che $n \geq 2$ può essere scritto come prodotto di numeri primi in modo unico*[1].

Dimostrazione. (i)

Supponiamo che $F = \{n \geq 2 \mid n \text{ non è fattorizzabile in primi}\}$ sia non vuoto. Poiché $\mathbb{N}$ è un buon ordinamento, F ha un minimo m.

Ma m non può essere primo, altrimenti sarebbe fattorizzabile banalmente come sé stesso. Quindi $m = ab$ con $a > 1$ e $b > 1$.
Poiché operiamo in $\mathbb{N}$, $a < m$ e $b < m$.

Quindi, per minimalità di m, $a \notin F$ e $b \notin F$, ovvero $a = \prod_i p_i$ e $b = \prod_j q_j$ con tutti i p_i e q_j primi. Perciò $m = \left(\prod_i p_i\right)\left(\prod_j q_j\right)$ e quindi è fattorizzabile.

Perciò F deve essere vuoto: tutti i numeri sono fattorizzabili in primi. ↪

[1] Dimostriamo il teorema non per verificare l'enunciato, ma per mostrare un esempio di ragionamento "logicista".

Logicismo

↪ Dimostrazione. (ii)

In modo analogo, supponiamo che l'insieme

$$D = \{n \geq 2 \mid n \text{ è fattorizzabile in due modi distinti}\}$$

sia non vuoto. Poiché $\mathbb{N}$ è un buon ordinamento, D ha un minimo d.

Quindi $d = \prod_{i=1}^{n} p_i$ e $d = \prod_{j=1}^{m} q_j$ con p_i e q_j primi e $p_i \neq q_j$ per qualche i e j.

Se $p_i = q_j$ per qualche i e j allora d/p_i sarebbe un numero più piccolo di d che ammette una doppia fattorizzazione. Pertanto, $p_i \neq q_j$ per ogni $i \neq j$.

Possiamo assumere senza perdere di generalità che $p_1 < q_1$.

Sia $k = (q_1 - p_1)\prod_{j=2}^{m} q_j$. Poiché $0 < q_1 - p_1 < q_1$, $k < d$. ↪

Logicismo

↪ Dimostrazione. (iii)

Ma $k = \left(\prod_{i=1}^{m} q_j\right) - p_1 \prod_{j=2}^{m} q_j = \left(\prod_{i=1}^{n} p_i\right) - p_1 \prod_{j=2}^{m} q_j = p_1 \left(\left(\prod_{i=2}^{n} p_i\right) - \prod_{j=2}^{m} q_j\right)$.
Sia a una fattorizzazione in primi di $\left(\prod_{i=2}^{n} p_i\right) - \prod_{j=2}^{m} q_j$: quindi $k = p_1 a$.

Sappiamo che $p_1 \neq q_j$ per ogni $j \geq 1$.
Se fosse $q_1 - p_1 = p_1 x$ allora $q_1 = p_1(x+1)$ quindi q_1 non sarebbe primo, contro ipotesi.

Quindi ogni fattorizzazione di $q_1 - p_1$ non contiene p_1 tra i suoi fattori.
Sia b una fattorizzazione di $q_1 - p_1$. Pertanto $k = b \prod_{j=2}^{m} q_j$.
Ma questa fattorizzazione non contiene p_1 tra i suoi fattori.

Quindi k ha due fattorizzazione distinte, una che contiene p_1 e una che non lo contiene, e $k < m$, contraddicendo la minimalità di d. □

Logicismo

Applicando il ragionamento si possono ottenere facilmente conseguenze interessanti seppur di elementare dimostrazione.

Corollario 8. *Esistono infiniti numeri primi.*

Dimostrazione.
Supponiamo che i numeri primi siano finiti: $p_1, \ldots, p_N$.

Sia $P = 1 + \prod_{i=1}^{N} p_1$, il successore del prodotto di tutti i numeri primi.

Per il Teorema di Fattorizzazione Unica, $P = \prod_{j=1}^{m} q_j$ con q_j numeri primi. In particolare q_1 deve essere un numero primo.

Se fosse $q_1 = p_i$ per un qualche i, P deve essere divisibile per p_i. Ma tale divisione necessariamente ha resto 1, quindi P **non** è divisibile per p_i.

Quindi q_1 è un numero primo che non compare nella lista $p_1, \ldots, p_N$, contraddicendo l'ipotesi. □

Logicismo

Un'altra conseguenza elementare ma estremamente importante è che ogni frazione può essere ridotta *ai minimi termini*.

Consideriamo $f = \frac{p}{q}$. Per il Teorema di Fattorizzazione Unica, $p = \prod_{i=1}^{n} p_i$ e $q = \prod_{j=1}^{m} q_j$. Eliminando i fattori comuni ed eseguendo i prodotti otteniamo p' e q', rispettivamente.

Ne segue che $f = \frac{p'}{q'}$, che non è ulteriormente semplificabile.

È importante osservare che non solo abbiamo mostrato che ogni frazione *può* essere ridotta ai minimi termini, ma abbiamo anche fornito un *algoritmo* per effettuare questa operazione.

Logicismo

Consideriamo le espressioni aritmetiche sui naturali definite come:

- un numero n è una espressione
- se e_1 e e_2 sono espressioni allora anche $(e_1)+(e_2)$ e $(e_1)(e_2)$ sono espressioni
- nient'altro è un'espressione

Le espressioni aritmetiche così definite sono tante quante i numeri naturali.

Infatti, sia $2,3,5,7,11,13,\ldots$ la sequenza dei numeri primi. Definiamo la funzione c di conteggio per induzione sulla struttura delle espressioni:

- se e è un numero allora $c(e) = 2^e$
- se $e = (e_1)+(e_2)$ allora $c(e) = 3^{c(e_1)} \cdot 5^{c(e_2)}$
- se $e = (e_1)(e_2)$ allora $c(e) = 7^{c(e_1)} \cdot 11^{c(e_2)}$

Logicismo

Per il Teorema di Fattorizzazione unica la funzione c è iniettiva:
se $c(e_1) = c(e_2)$ allora $e_1 = e_2$.

Quindi ad ogni espressione corrisponde un numero naturale, ovvero l'immagine di c è un sottoinsieme proprio di $\mathbb{N}$.

Perciò le espressioni non sono di più dei numeri naturali.

Ma ogni numero naturale è una espressione, quindi le espressioni sono tante quante i numeri naturali.

Formalismo

L'idea del programma di Hilbert, da cui nasce la corrente della filosofia della Matematica nota come *formalismo*, è che la Matematica parli esclusivamente di *oggetti formali*.

Una teoria matematica è data fornendo un insieme di assiomi, e tale teoria descrive tutti e soli gli oggetti che soddisfano tali assiomi. In particolare, le proprietà che possiamo derivare nella teoria valgono per gli oggetti concreti che soddisfano gli assiomi.

Formalismo

Senza dubbio, l'approccio formalista ricorda molto dello studio della Matematica in tutti gli ambiti.
Però vale la pena rammentare anche i suoi aspetti critici:

- gli assiomi non sono un mero gioco, come il pensiero formalista suggerisce, ma dovrebbero riflettere un significato non formale.
- la consistenza interna di un sistema di assiomi è generalmente indimostrabile all'interno del sistema stesso.

La prima critica è quella cui siamo più interessati in questa lezione.
La Matematica viene sviluppata per rappresentare una realtà, e le teorie hanno senso quando siamo in grado di legarle ad un mondo di interesse.

In altri termini, non ci basta che una teoria sia priva di contraddizioni per attribuirle un significato o anche solo per considerarla degna di attenzione: deve parlare di qualcosa che, in un certo senso, c'è prima degli assiomi.

Formalismo

Principio concreto

Dare evidenza esplicita agli assiomi

Principio concreto

Fornire il significato degli assiomi di una teoria

Formalismo

La geometria di Euclide parte dai seguenti *postulati*:

- Congiungendo due punti qualsiasi si ottiene un segmento di retta
- Si può prolungare un segmento oltre i due punti estremi indefinitamente
- Dato un punto e una lunghezza, è possibile descrivere un cerchio
- Tutti gli angoli retti sono congruenti tra loro
- Se una retta che taglia altre due rette determina dallo stesso lato angoli interni la cui somma è minore di due angoli retti, prolungando le due rette, esse si incontreranno dalla parte dove i due angoli hanno somma minore di due retti.

Astrazione dal foglio di carta, matita, riga e compasso.
[Hilbert e *Gründlagen der Geometrie*]

Formalismo

Espressioni aritmetiche

- leggi fondamentali della somma, prodotto, sottrazione e divisione
- rappresentano i numeri razionali e le loro operazioni
- rappresentano polinomi e frazioni di polinomi

È importante rimarcare che lo stesso sistema di assiomi può avere più di un modello interessante.

Formalismo

Importanza dei controesempi.

La legge commutativa della somma, $a+b=b+a$ vale per tutti i numeri naturali, interi, razionali, reali e complessi.

Ma possiamo definire una operazione + sulle strighe di caratteri che soddisfa

- legge associativa: $a+(b+c)=(a+b)+c$
- esistenza dell'elemento neutro: $a+0=0+a=a$

ma **non** soddisfa la proprietà commutativa.

Ad esempio, la *concatenazione* di stringhe è associativa, e ha la stringa vuota come elemento neutro, ma chiaramente non è commutativa:

$$a+b=ab\neq ba=b+a \ .$$

Costruttivismo

La Matematica Costruttiva, introdotta da Brouwer come un approccio per evitare le contraddizioni alla radice, propone che ogni oggetto matematico venga costruito in modo *effettivo*, che generalmente significa che ogni oggetto possa essere calcolato:

- se dimostro $\exists x.P(x)$ allora devo anche esibire un valore t tale che $P(t)$
- se dimostro A o B allora devo far vedere in quali casi vale A e in quali B, esaustivamente

Esiste un chiaro legame diretto con la calcolabilità dei risultati dimostrati.

Costruttivismo

Un approccio costruttivo alla Matematica fornisce indubbi vantaggi

- le richieste sono naturali: se qualcosa esiste allora sono in grado di mostrarla; se è vero $A \vee B$, allora posso dire anche quando vale A e quando vale B.
- posso calcolare quanto dimostro: in un certo senso, la dimostrazione stessa è un algoritmo di calcolo.

Tuttavia, ciò avviene ad un prezzo che è ineludibile:

- non tutto è dimostrabile: vi sono risultati in cui dimostro che una entità esiste, ma non sono in grado di esibirla effettivamente.
- vi sono principi ovvi che non possono essere accettati e usati: ad esempio, il Terzo Escluso, $A \vee \neg A$.

Costruttivismo

Principio concreto

Preferire dimostrazioni costruttive quando c'è una alternativa

Principio concreto

Evidenziare come le dimostrazioni costruttive siano procedure di calcolo

Costruttivismo

Esempio 9. Esistono a a b numeri irrazionali tali che a^b è razionale.

Dimostrazione non costruttiva: poniamo $a = b = \sqrt{2}$.
Se a^b è razionale, l'asserto è dimostrato.

Altrimenti poniamo $a = \sqrt{2}^{\sqrt{2}}$ e $b = \sqrt{2}$.

Quindi $a^b = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$ che è razionale.

Nonostante la dimostrazione sia corretta, alla fine non sappiamo quale fra le due coppie individuate sia quella che soddisfa la proprietà richiesta.

Costruttivismo

Esempio 10. Esistono a a b numeri irrazionali tali che a^b è razionale.

Dimostrazione costruttiva: poniamo $a = \sqrt{2}$ e $b = \log_2 9$.
Sappiamo che a è irrazionale, ma anche b lo è: se $\log_2 9 = \frac{p}{q}$ con $p, q \in \mathbb{N}$ e $p \geq 1$, $q \geq 1$ allora

$$\begin{aligned} \frac{p}{q} &= \log_2 9 \\ p &= q \log_2 9 \\ p &= \log_2 9^q \\ 2^p &= 9^q \end{aligned}$$

il che è impossibile perché il lato sinistro è pari mentre quello destro è dispari.

$$a^b = \sqrt{2}^{\log_2 9} = 2^{\frac{1}{2}\log_2 9} = 2^{\log_2 \sqrt{9}} = \sqrt{9} = 3 \ .$$

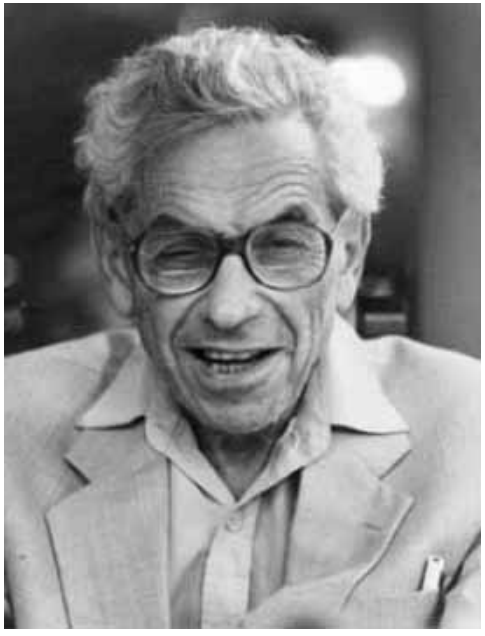
Costruttivismo

Principio 11 (Piccionaia). *Se n oggetti sono messi in r contenitori con $r < n$, allora almeno un contenitore contiene più di un oggetto.*

Questo principio è costruttivo: non dice quale contenitore contiene più di un oggetto, ma afferma che se esamininiamo i contenitori uno ad uno, esaustivamente, prima o poi troveremo un contenitore in cui sono presenti due o più oggetti.

In altre parole, grazie alla finitezza dei contenitori, l'algoritmo che ispeziona le scatole una ad una, è *corretto*, ovvero garantisce di trovare la scatola che contiene più di un oggetto.

Costruttivismo



Esempio 12. Sia $A \subseteq \{1, 2, \ldots, 2n\}$ con $|A| = n+1$.
Allora esistono a e b in A tali che a divide b.

Sia $x \in A$. Per il Teorema di Fattorizzazione Unica e per definizione di A, $x = 2^k y$ con $k \geq 0$ e y dispari tale che $1 \leq y \leq 2n-1$.
Pertanto, ci sono n possibili valori per y.

Quindi, per il principio della piccionaia, esistono due numeri $a, b \in A$ con $a < b$ della forma $a = 2^k m$ e $b = 2^h m$ per un qualche m. Perciò $b = 2^{h-k} a$.

[y è il numero di *scatole*.]

Costruttivismo

L'esempio precedente suggerisce un algoritmo per calcolare i due numeri. Supponiamo che A sia rappresentato da una lista ordinata.

Dapprima calcoliamo una lista B che sia costituita dalla fattorizzazione di ogni elemento di A come $2^k y$:

for $i := 1$ **to** $n+1$
    $y := A[i]$; $k := 0$
    while y pari
        $y :=$ y$/2$; $k := k+1$
    $B[i] := k$

Il suo costo computazionale è $O(n \log_2 n)$.

Costruttivismo

Quindi procediamo a calcolare una coppia (a, b) tali che a divida b:

for $i := 1$ **to** n
    for $j := i + 1$ **to** $n + 1$
        if $B[i] = B[j]$ **then**
            return $(A[i], A[j])$

L'algoritmo è corretto per la dimostrazione precedente.
La seconda parte ha un costo computazionale pari a $O(n^2)$.

Quindi il costo dell'algoritmo è $O(n \log_2 n) + O(n^2) = O(n^2)$.

Costruttivismo

Se sfruttiamo appieno la dimostrazione, otteniamo un algoritmo diverso: calcoliamo B come prima, e poi[2]

for $i := 1$ **to** $2n$ **step** 2
    $C[i] := []$
for $i := 1$ **to** $n+1$
    $C[B[i]] := i \circ C[B[i]]$
for $i := 1$ **to** $2n$ **step** 2
    if $\left|C[i]\right| > 1$ **then**
        return $(A[C[i][2]], A[C[i][1]])$

L'algoritmo è corretto per la dimostrazione precedente.
La seconda parte ha un costo computazionale pari a $O(n) + O(n) + O(n)$.

Quindi il costo dell'algoritmo è $O(n \log_2 n) + O(n) = O(n \log_2 n)$.

[2] dove $e \circ L$ aggiunge l'elemento e in testa alla lista L, e [] è la lista vuota.

Riferimenti

Sebbene vi sia abbondanza di testi specialistici, preferiamo suggerire i seguenti riferimenti più divulgativi:

- Piergiorgio Odifreddi, *Il diavolo in cattedra*, Einaudi.
- Richard Zach, *Hilbert's Program*, in Stanford Encyclopedia of Philosophy.
- *Intuitionism*, in Encyclopedia Britannica.

L'ultimo esempio è dovuto a Paul Erdős.

Fondamenti di Matematica: Lezione 3

Programma:

- Astrazione
- Calcolo
- Consistenza

Astrazione

Il termine *astrarre* viene utilizzato in Matematica per indicare due fenomeni:

- eliminare ciò che si ritiene non essenziale in una struttura
- immergere una struttura in un mondo più grande

Lo scopo dell'astrazione è rendere una struttura matematica di interesse con il minimo bagaglio concettuale indispensabile, e al contempo, facilitarne la comprensione e la manipolazione.

Questa spinta verso l'essenza serve anche per comprendere ciò che è davvero importante in una struttura.

Astrazione

Principio concreto

Astrarre per cogliere l'essenziale

Principio concreto

Astrarre per regolarizzare

Principio concreto

Astrarre per vedere in modo più profondo

Astrazione

Esempio 13. L'insieme dei numeri interi con la somma, $(\mathbb{Z}, +)$, è il prototipo del concetto algebrico di *gruppo*: un insieme con una operazione che sia associativa, dotata di elemento neutro e in cui ogni elemento ha un inverso.

Astraendo dagli interi ai gruppi possiamo cogliere l'essenziale della operazione di somma.

Questo ci consente di vedere altre strutture come simili agli interi, in quanto sono gruppi.

Ma ci permette di descrivere la medesima struttura in altri modi, potenzialmente interessanti.

La comprensione degli interi come un gruppo ci suggerisce anche l'esistenza di nuove strutture, che sono legate agli interi, ma ne differiscono profondamente.

Astrazione

Esempio 14. Se prendiamo la circonferenza in cui fissiamo un punto P, i percorsi da P a P con l'operazione di concatenazione formano un gruppo: l'elemento neutro è il percorso nullo, e l'inverso è il percorso in cui ci si muove nel verso opposto.

Chiamando 0 il percorso nullo, n con $n > 0$ il percorso che gira n volte attorno alla circonferenza in senso antiorario, e n con $n < 0$ il percorso che gira n volte attorno alla circonferenza in senso orario, questo gruppo è $(\mathbb{Z}, +)$.

Astrazione

Esempio 15. Una equazione polinomiale di grado n, $\sum_{i=0}^{n} a_i x^i = 0$ sui reali ha, al più, n radici.

Ci sono equazioni di secondo grado con due radici, come $x^2 - 4x + 3 = 0$ che ha radici $x = 1$ e $x = 3$, equazioni che hanno una soluzione doppia, come $x^2 - 2x + 1 = 0$, che ha soluzione $x = 1$, ma anche equazioni senza alcuna radice, come $x^2 + 2x + 2 = 0$.

Estendere le equazioni ai numeri complessi ha l'effetto di regolarizzare la situazione: tutte le equazioni di grado n hanno esattamente n soluzioni, risultato noto come il Teorema Fondamentale dell'Algebra.
Ad esempio $x^2 + 2x + 2 = 0$ ha soluzioni $x = -1 - i$ e $x = i - 1$.

Estendendo il dominio numerico su cui operiamo, perdiamo informazione ma acquisiamo regolarità. Stiamo *astraendo*, buttando via qualcosa che non ci interessa, per avere una struttura più semplice da trattare.

Astrazione

Esempio 16. Consideriamo due insiemi tali che $A \subseteq B$. La funzione $x \mapsto x$ da A in B è evidentemente iniettiva.

Se invertiamo il principio, ovvero se scriviamo $A \preceq B$ quando esiste una funzione iniettiva da A in B, stiamo effettuando una astrazione.

Se immaginiamo che una funzione iniettiva sia una *rinominazione* degli elementi di A negli elementi di B, stiamo *immergendo* A in B ignorando il nome degli elementi.

Questa idea ci permette di dimostrare che $|A| = |B|$ quando $A \preceq B$ e $B \preceq A$, il Teorema di Schröder-Bernstein, ma anche, se applicata in modo sistematico, di definire la categoria **Set**.

Astrazione

Esempio 17. Una *categoria* è una coppia $\left\langle O; \{\mathrm{Hom}(a,b)\}_{a,b\in O} \right\rangle$ con O una collezione di *oggetti* e $\mathrm{Hom}(a,b)$ la collezione delle *frecce* da a in b tale che:

- per ogni coppia $f : a \to b$ e $g : b \to c$ esiste una freccia $g \circ f : a \to c$
- la composizione è associativa
- per ogni oggetto $a \in O$, esiste $\mathrm{id}_a : a \to a$
- se $f : a \to b$ e $g : b \to a$ allora $f \circ \mathrm{id}_a = f$ e $\mathrm{id}_a \circ g = g$.

Possiamo pensare una categoria come un insieme O i cui oggetti siano collegati dalle frecce.

Astrazione

Esempio 18. Un insieme è una categoria in cui le uniche frecce siano le identità e la composizione è banale.

Un ordine è una categoria in cui via sia al più una freccia tra due oggetti: se esiste $f : a \to b$ allora $a \leq b$.

Un monoide è una categoria formata da un unico oggetto le cui frecce siano gli elementi del monoide.

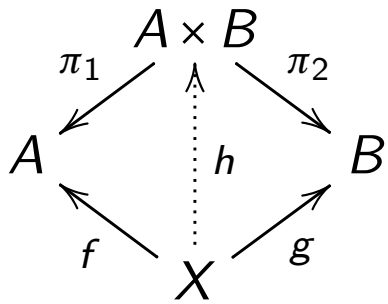
Una freccia $f : a \to b$ è un isomorfismo se esiste una freccia $g : b \to a$ tale che $f \circ g = \mathrm{id}_b$ e $g \circ f = \mathrm{id}_a$.

Un gruppo è un monoide in cui tutte le frecce siano isomorfismi.

Gli insiemi con le funzioni formano una categoria; i gruppi e i loro omomorfismi formano una categoria; gli spazi vettoriali e le funzioni lineari formano una categoria; gli spazi topologici e le funzioni continue formano una categoria; le varietà differenziabili e le funzioni differenziabili formano una categoria.

Astrazione

Esempio 19. Usualmente il prodotto Cartesiano $A \times B$ viene definito come l'insieme $\{(a, b) \mid a \in A \text{ e } b \in B\}$. Astraendo possiamo descrivere il prodotto Cartesiano mediante funzioni:

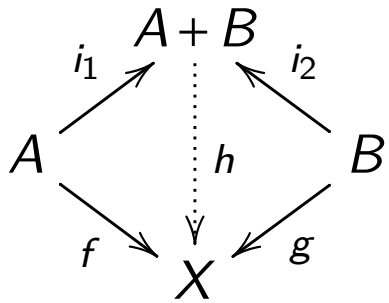


Il prodotto è un oggetto e una coppia di frecce π_1 e π_2 tali che, per ogni oggetto X e una coppia di frecce f e g come in figura, esiste una freccia h che fa commutare il diagramma.

Astrazione

Esempio 20. Nell categoria degli insiemi con le funzioni, il prodotto è l'usuale prodotto Cartesiano.
In un ordine il prodotto, se esiste, è il massimo dei minoranti.

La nozione duale, detta *coprodotto*,



definisce l'unione disgiunta nella categoria degli insiemi. In un ordine, definisce il minimo dei maggioranti.

Calcolo

Principio concreto

Ogni dimostrazione costruttiva è un algoritmo di calcolo

Calcolo

Teorema 21 (Bolzano). *Per ogni funzione* $f : \mathbb{R} \to \mathbb{R}$ *tale che*

- f *sia continua sull'intervallo* $[a, b]$
- $f(a) < 0 < f(b)$

esiste $c \in (a, b)$ *tale che* $f(c) = 0$.

Dimostrazione. (i)

Siano $a_0 = a$ e $b_0 = b$. Costruiamo le successioni $\{a_i\}_{i\in\mathbb{N}}$ e $\{b_i\}_{i\in\mathbb{N}}$, induttivamente: poniamo $d = (a_i + b_i)/2$,

- se $f(d) = 0$ allora $a_{i+1} = d$ e $b_{i+1} = d$;
- se $f(d) < 0$ allora $a_{i+1} = d$ e $b_{i+1} = b_i$;
- se $f(d) > 0$ allora $a_{i+1} = a_i$ e $b_{i+1} = d$;

Osserviamo che

$$0 \leq b_{+1} - a_{i+1} \leq \frac{b_i - a_i}{2} \leq \frac{b_0 - a_0}{2^{i+1}} \quad .$$

per induzione su i.

↪ Dimostrazione. (ii)

Pertanto

$$0 = \lim_{n\to\infty} 0 \le \lim_{n\to\infty} (b_n - a_n) \le \lim_{n\to\infty} \frac{b_0 - a_0}{2^n} = 0 \ ,$$

quindi $\lim_{n\to\infty}(b_n - a_n) = \lim_{n\to\infty} b_n - \lim_{n\to\infty} a_n = 0$, ovvero $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$. Sia $\{c_n\}_{n\in\mathbb{N}}$ con $c_n = (a_n + b_n)/2$.

Poiché $a \le a_i \le c_i \le b_i \le b$ per ogni $i \in \mathbb{N}$,

$$\lim_{n\to\infty} a_n \le \lim_{n\to\infty} c_n \le \lim_{n\to\infty} b_n \ .$$

Poniamo $c = \lim_{n\to\infty} c_n$ che esiste e $c \in [a, b]$. ↪

Calcolo

↪ Dimostrazione. (iii)

Osserviamo che $f(a_n) < 0 < f(b_n)$ per ipotesi e costruzione. Quindi

$$f(c) = \lim_{n\to\infty} f(a_n) \leq 0 \leq \lim_{n\to\infty} f(b_n) = f(c)$$

per continuità, da cui $f(c) = 0$.

Per concludere, basti osservare che $c \neq a$ e $c \neq b$ per ipotesi, quindi $c \in (a, b)$. □

Calcolo

La dimostrazione precedente costruisce una sequenza di Cauchy $\{c_i\}_{i \in \mathbb{N}}$ che converge a c, il valore per cui $f(c) = 0$. Sebbene tale costruzione sia infinitaria, essa fornisce una approssimazione buona tanto quanto si desidera del valore di c.

Questa procedura è il cosiddetto Algoritmo di Bisezione.

Calcolo

Le istruzioni della CPU di un calcolatore comprendono solitamente le istruzioni aritmetiche di somma, sottrazione, prodotto e divisione sui numeri naturali.

Tuttavia, i numeri sono rappresentati in un numero di bit prefissato, diciamo 32. Inoltre, vi sono istruzioni per far scorrere i bit a sinistra e a destra.

La moltiplicazione produce un risultato a 64 bit, per cui vi sono generalmente due operazione di moltiplicazione: quella che produce i 32 bit inferiori e quella che produce i 32 bit superiori.

Infine, la divisione è costosa: mentre le altre istruzioni operano in tempo costante, la divisione richiede una iterazione che impiega un tempo variabile.

Calcolo

Teorema 22. *Se $n, d \in \mathbb{N}$ con $d \neq 0$ e $x \in \mathbb{R}$, $0 \leq x < 1/d$ allora*

$$\left\lfloor \frac{n}{d} + x \right\rfloor = \left\lfloor \frac{n}{d} \right\rfloor \ .$$

Dimostrazione.
Rammentiamo che $\lfloor x \rfloor = m \in \mathbb{N}$ con m tale che $m \leq x < m+1$. Chiaramente questa funzione è monotona.

$$\left\lfloor \frac{n}{d} \right\rfloor \leq \left\lfloor \frac{n}{d} + x \right\rfloor = \left\lfloor \frac{n+dx}{d} \right\rfloor \leq \left\lfloor \frac{n+1}{d} \right\rfloor \leq \left\lfloor \frac{n}{d} \right\rfloor + 1 \ .$$

Se la terza diseguaglianza è una uguaglianza, la seconda diseguaglianza è stretta, quindi

$$\left\lfloor \frac{n}{d} \right\rfloor \leq \left\lfloor \frac{n}{d} + x \right\rfloor < \left\lfloor \frac{n}{d} \right\rfloor + 1 \ ,$$

quindi il risultato segue per definizione di $\lfloor n/d \rfloor$. □

Calcolo

Esempio 23. Per dividere in modo efficiente $n \in \mathbb{N}$ per 3, $0 \le n < 2^{32}$ su un calcolatore usiamo il seguente algoritmo

$$
\begin{array}{ll}
M = 2863311531 & (M = (2^{33}+1)/3) \\
q = (Mn)^{\text{upper}} & (q = (Mn)/2^{32}) \\
q = q/2 & (q = (Mn)/2^{33}) \\
t = 3q & \\
r = n - t &
\end{array}
$$

q è il quoziente e r is resto. Infatti

$$q = \left\lfloor \frac{2^{33}+1}{3} \frac{n}{2^{33}} \right\rfloor = \left\lfloor \frac{n}{3} + \frac{n}{3 \cdot 2^{33}} \right\rfloor$$

poiché $0 \le n/(3 \cdot 2^{33}) < 1/3$, $q = \lfloor n/3 \rfloor$ e $r = n - 3q$.

Riferimenti

La maggior parte degli esempi sono presentazioni di risultati standard di Analisi, Analisi Numerica, e Algebra.

Come riferimento per la topologia algebrica, suggeriamo Allen Hatcher, *Algebraic Topology* , Cambridge University Press, Cambridge, 2002, disponibile anche online sulla pagina web dell'autore.

Tra i molti testi sulla teoria delle categorie, segnaliamo Robert Goldblatt, *Topoi: The Categorial Analysis of Logic*. Courier Corporation, 2013, anch'esso disponibile sulla home page dell'autore.

L'esempio sull'aritmetica dei calcolatori è tratto da Henry S. Warren, Jr. *Hacker's Delight*. Addison-Wesley, 2003.

Fondamenti di Matematica: Lezione 4

Programma:

- Consistenza
- Normalizzazione
- Forme Normali

- Discussione

Consistenza

Una teoria matematica T è detta essere *consistente* se non contiene una contraddizione. In altri termini, se non possiamo dimostrare una asserzione A e la sua negazione $\neg A$ al suo interno.

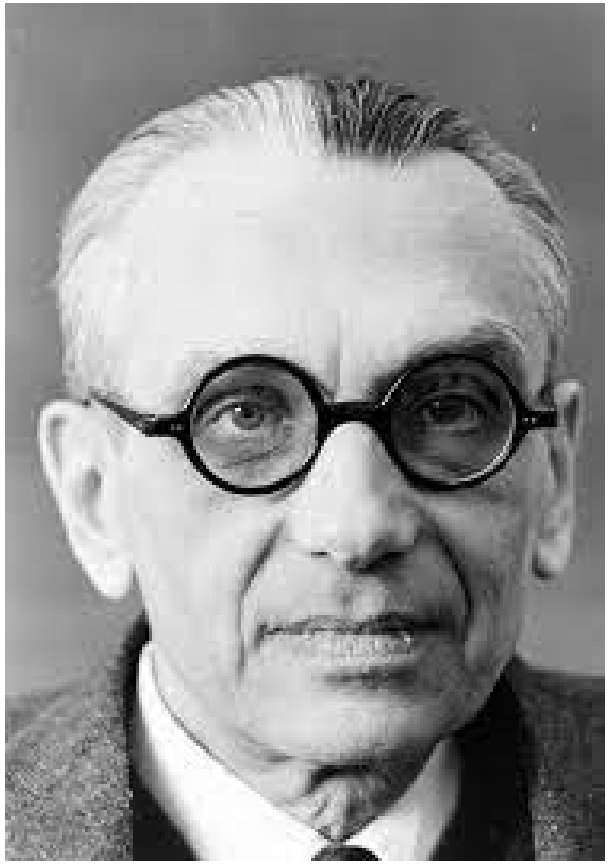
È chiaro che la consistenza di una teoria è una condizione necessaria: se proviamo una contraddizione, possiamo dedurre il falso e quindi possiamo derivare ogni cosa.

Una teoria inconsistente è priva di significato.

Consistenza

Se una teoria T è *abbastanza potente* allora non è possibile dimostrare la sua consistenza all'interno di T.

Ma è possibile dimostrare la consistenza di T in una teoria E che sia più potente ed estenda T.



Consistenza

Esempio 24. Possiamo definire i numeri naturali come $\mathbb{N} = \{x \in \mathbb{Z} \mid x \leq 0\}$.

Essendo $\mathbb{N}$ chiuso rispetto alla somma e al prodotto, e $0 \in \mathbb{N}$, in $\mathbb{N}$ valgono gli assiomi di Peano, per cui l'aritmetica di Peano, è consistente se l'aritmetica degli interi è consistente.

Consistenza

Poiché $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$,

- la consistenza della teoria dei numeri complessi implica la consistenza della teoria dei reali
- la consistenza della teoria dei numeri reali implica la consistenza della teoria dei razionali
- la consistenza della teoria dei numeri razionali implica la consistenza della teoria degli interi
- la consistenza della teoria dei numeri interi implica la consistenza della teoria dei naturali

La tecnica di *immersione* è il più semplice strumento per provare la consistenza di una teoria.

Consistenza

Esempio 25. Possiamo immergere l'aritmetica di Peano negli insiemi:

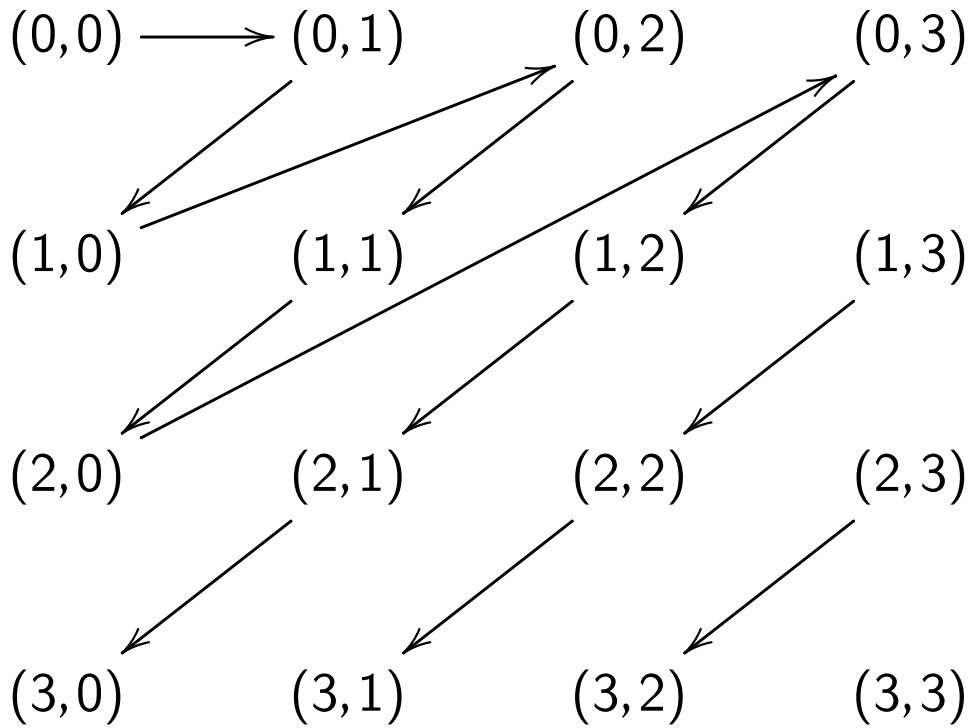
- $0 = \emptyset$
- $x + 1 = x \cup \{x\}$
- somma e prodotto ordinale
- somma e prodotto cardinale

Quindi l'aritmetica di Peano è consistente se la teoria degli insiemi è consistente.

Gran parte della matematica fino al XIX secolo è consistente se la teoria formale degli insiemi è consistente.

Consistenza

Esempio 26. $\mathbb{N} \simeq \mathbb{N} \times \mathbb{N}$: $x \mapsto (x,x)$; $(x,y) \mapsto \frac{(x+y)(x+y+1)}{2} + x$:



Quindi, con qualche cautela, la teoria dei razionali è consistente se e solo se lo è l'aritmetica di Peano.

Consistenza

Esempio 27. Allo stesso modo $\mathbb{R} \simeq \mathbb{R} \times \mathbb{R}$, quindi l'analisi complessa è consistente se e solo se l'analisi reale lo è.

Esempio 28. La geometria Euclidea è consistente se e solo se la geometria Cartesiana (o analitica) lo è, ovvero la consistenza della geometria Euclidea è conseguenza della consistenza della teoria di $\mathbb{R} \times \mathbb{R}$.

Normalizzazione

In certi sistemi formali, ogni dimostrazione può essere scritta in un modo canonico.

Il processo per trasformare una dimostrazione data in un'altra in forma canonica è detto *normalizzazione*.

Una dimostrazione del falso non può essere scritta in forma canonica, quindi tale dimostrazione non può esistere. Ne segue che il sistema formale è consistente.

Normalizzazione

La *proprietà della sottoformula* afferma che ogni asserzione presente in una dimostrazione formale è una sottoformula della conclusione oppure di una delle ipotesi.

Supponiamo che $\pi \colon \vdash \bot$ sia in forma canonica. L'ultimo passo della dimostrazione π deve avere una conclusione che è sottoformula di una delle ipotesi, ma non ve ne è alcuna, o della conclusione, la cui unica sottoformula è $\bot$. Quindi π è una dimostrazione $\pi' \colon \bot$ conclusa da una eliminazione del falso per dedurre $\bot$. Ma L'ultimo passo non può comparire in una prova canonica, quindi π non esiste.

Normalizzazione

Una tecnica correlata alla normalizzazione è la *cut-elimination*: ogni prova π può essere trasformata in una dimostrazione π' che non usi la regola di taglio

$$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\,\text{Cut}$$

Questo significa che la prova π' è *diretta*: non usa lemmi aggiuntivi come A.

In un sistema formale in cui vale la cut-elimination ogni dimostrazione può essere effettuata senza ricorrere a lemmi esterni alla prova.
In altri termini, tutta l'informazione necessaria a dimostrare la conclusione è contenuta nelle ipotesi.

Normalizzazione

Esempio 29. $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. La dimostrazione di Gauss:

$$\begin{array}{cccccccc} & 0 & +1 & +2 & \cdots & +n-2 & +n-1 & +n \\ + & n & +n-1 & +n-2 & \cdots & +2 & +1 & +0 \\ = & n & +n & +n & \cdots & +n & +n & +n \end{array}$$

quindi $2\sum_{i=0}^{n} i = n(n+1)$.

Normalizzazione

Esempio 30. $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. Una dimostrazione canonica: per induzione su n

- se $n = 0$ allora $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$.
- se $n = m+1$ allora

$$\begin{aligned}\sum_{i=0}^{n} i &= m+1+\sum_{i=0}^{m} i \\ &= m+1+\frac{m(m+1)}{2} \\ &= \frac{m^2+3m+2}{2} = \frac{(m+1)(m+2)}{2} \\ &= \frac{n(n+1)}{2} \ .\end{aligned}$$

Forme normali

Fissato un insieme O di oggetti, le *forme normali* di O sono un sottoinsieme $N \subseteq O$ tale che:

- esiste una mappa $f : O \to N$ che trasforma ogni oggetto in una forma normale;
- gli elementi di N sono interessanti.

La mappa f è la *normalizzazione*.

Le forme normali hanno un grado di arbitrarietà, ma devono fornire un sottoinsieme dotato di qualche caratteristica matematica rilevante.

Forme normali

È utile ma non necessario che le forme normali siano uniche: in altre parole, la mappa f, in generale, è una relazione e non una funzione.

Il concetto di forma normale non è unico: allo stesso insieme di oggetti O possono essere associate più forme normali distinte, ovvero più sottoinsiemi N_1, N_2, ... differenti che siano forme normali.

Ogni forma normale rappresenta un modo matematicamente rilevante di guardare gli oggetti.

Forme normali

Esempio 31. Prendiamo le espressioni polinomiali in una variabile su $\mathbb{C}$ come oggetti: possiamo definire le forme normali come

$$\sum_{i=0}^{n} a_i x^i \quad .$$

La normalizzazione consiste nel trasformare una espressione polinomiale, ad esempio $3(x+5)(x^2+2)$ in una forma normale: $3x^3+15x^2+6x+30$.

In questo caso, ogni espressione ha una forma normale unica.

Forme normali

Esempio 32. Allo stesso insieme di oggetti possiamo associare un secondo sottoinsieme di forme normali:

$$\prod_{i=0}^{n}(x - r_i) \ .$$

La normalizzazione consiste nel calcolo delle radici.

La forma normale è unica.

Forme normali

Osserviamo che i due esempi precedenti danno forme normali interessanti:

- ogni espressione polinomiale può essere espressa come un polinomio (prima forma normale),
- ogni polinomio di grado n possiede n radici (seconda forma normale).

Quindi il Teorema Fondamentale dell'Algebra, visto in questa ottica, è un risultato di normalizzazione.

Se prendiamo il campo $\mathbb{R}$, la seconda rappresentazione non è una forma normale: mentre tutte le espressioni polinomiali possono essere scritte come polinomi, non tutti i polinomi di grado n hanno n radici.

Forme normali

Questo modo di vedere

- suggerisce concetti e risultati
- aiuta e orienta il calcolo
- amplia la comprensione degli oggetti studiati

Coda

A conclusione del corso presentiamo un insieme di esempi *difficili* che illustrano le tecniche illustrate.

Gli esempi sono stati scelti perché:

- sono spiegabili nell'ambito della matematica delle scuole superiori;
- sono concreti;
- usano la matematica per ottenere risultati non evidenti.

Algoritmi di ordinamento

Uno degli argomenti classici di Informatica è dato dagli algoritmi di ordinamento:

> Dato un vettore (array) A di n elementi e una relazione d'ordine, trovare una permutazione di A in cui $A[i] \leq A[j]$ per ogni $1 \leq i \leq j \leq n$.

Algoritmi di ordinamento

Per tradizione vengono dapprima presentati algoritmi “naturali”, che risolvono il problema ma sono relativamente inefficienti, e poi vengono presentati algoritmi efficienti ma più sofisticati.

Il “campione” tra gli algoritmi efficienti è **heapsort**.
Esso, nel caso peggiore, esegue in $O(n \log_2 n)$ passi di computazione.

Algoritmi di ordinamento

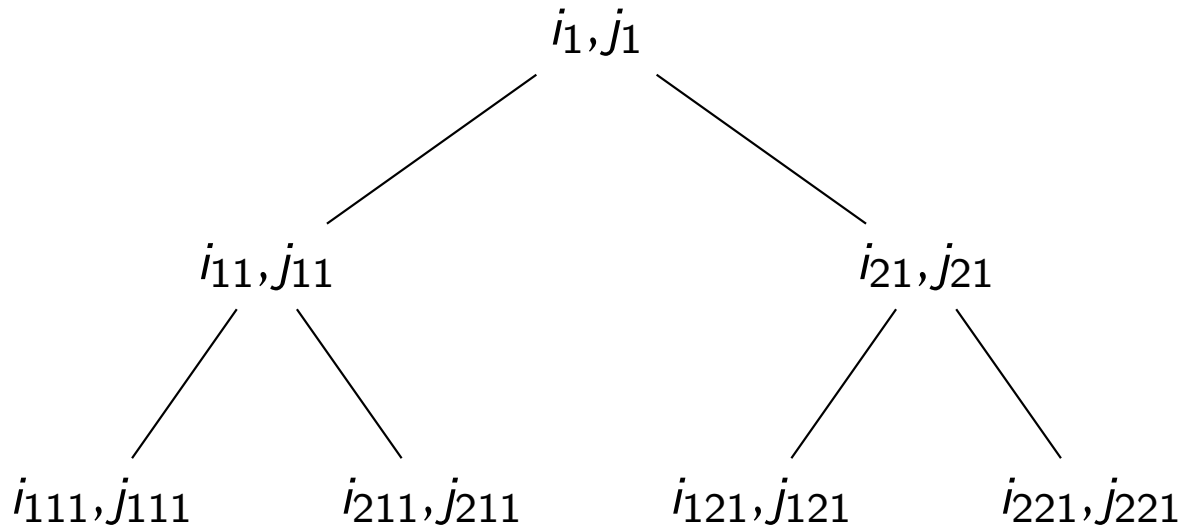
A questo punto, la presentazione lascia cadere una frase

> Non è possibile trovare un algoritmo per confronto che operi in un tempo inferiore a $O(n \log_2 n)$ passi.

Perché?

Alberi di decisione

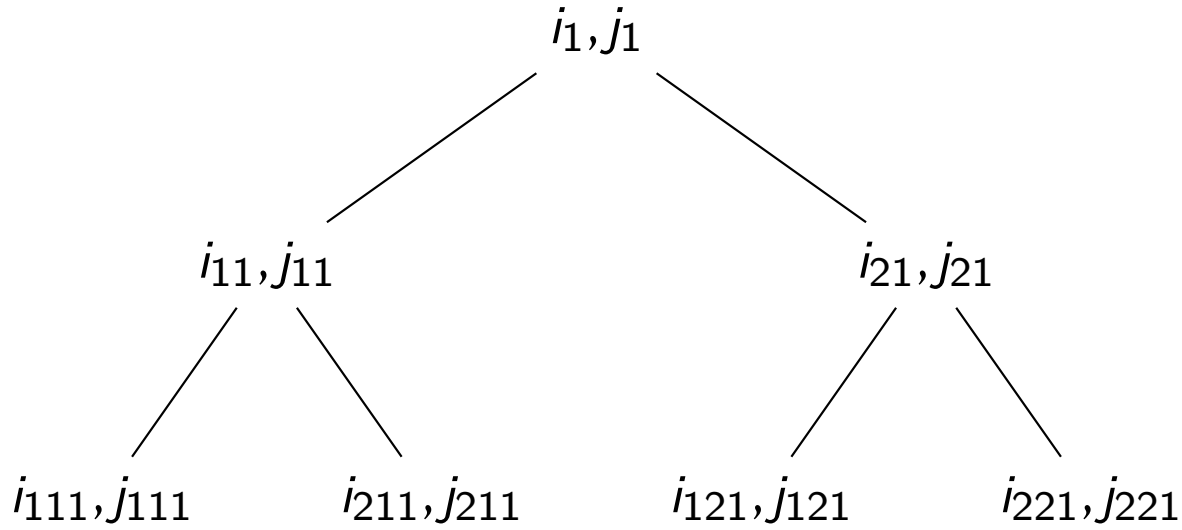
Un algoritmo per confronto, inizierà confrontando due elementi $A[i_1]$ e $A[j_1]$: se $A[i_1] \leq A[j_1]$ continuerà confrontando altri due elementi $A[i_{11}]$ e $A[j_{11}]$, altrimenti confronterà $A[i_{21}]$ e $A[j_{21}]$. E così via.



In mezzo a questi confronti l'algoritmo effettuerà delle operazioni per costruire l'array ordinato. Supponiamo, ragionevolmente, che queste operazioni richiedano un tempo costante.

Alberi di decisione

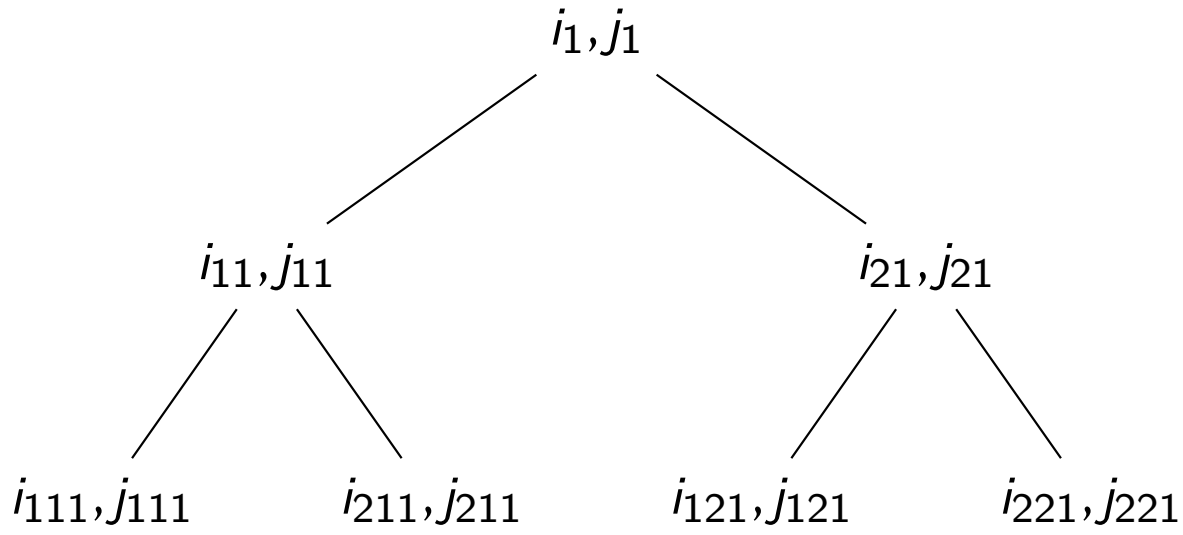
Ogni ramo di questo albero rappresenta una esecuzione del nostro algoritmo su un dato array A. Quando si raggiunge la foglia, l'algoritmo avrà costruito la permutazione ordinata di A.



È possibile che una esecuzione confronti più volte la stessa coppia di elementi, ed è possibile che due elementi non vengano mai confrontati.

Alberi di decisione

Facendo variare l'array A ma tenendo fissa la sua lunghezza n, un algoritmo di ordinamento **deve** poter generare tutte le permutazioni degli indici.



Quindi il numero ℓ delle foglie dell'albero deve essere maggiore o uguale al numero delle permutazioni di A.

Alberi di decisione

Pertanto, $n! \leq \ell$.

Noi siamo interessati a conoscere il tempo di calcolo. Questo, nelle nostre ipotesi, non può essere inferiore al numero di confronti nel corso di una esecuzione dell'algoritmo.

Nel caso peggiore, il tempo di esecuzione sarà *proporzionale* all'*altezza* h dell'albero.

Essendo l'albero binario, sappiamo che $\ell \leq 2^h$.

Stima di h

Sappiamo $n! \leq \ell \leq 2^h$.
Quindi $\log_2(n!) \leq \log_2 \ell \leq h$.

Vogliamo confrontare $\log_2(n!)$ con $n \log_2 n$, al crescere di n.
Quindi, asintoticamente, vogliamo stimare

$$\lim_{n \to \infty} \frac{\log_2(n!)}{n \log_2 n}$$

Stima di h

Ricordiamo l'*approssimazione di Stirling*:

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + O(n^{-1})\right)$$

Quindi

$$\begin{aligned}\log_2(n!) &= \frac{1}{2}\log_2(2\pi n) + (n\log_2 n - n\log_2 e) + \log_2\left(1 + O(n^{-1})\right) \\ &= (\frac{1}{2}\log_2(2\pi) + \frac{1}{2}\log_2 n) + (n\log_2 n - n\log_2 e) + \log_2\left(1 + O(n^{-1})\right)\end{aligned}$$

Ma questo significa

$$\frac{\log_2(n!)}{n\log_2 n} = \left(\frac{\log_2(2\pi)}{2n\log_2 n} + \frac{1}{2n}\right) + \left(1 - \frac{\log_2 e}{\log_2 n}\right) + \frac{\log_2\left(1 + O(n^{-1})\right)}{n\log_2 n}$$

Stima di h

$$\frac{\log_2(n!)}{n\log_2 n} = \frac{\log_2(2\pi)}{2n\log_2 n} + \frac{1}{2n} + 1 - \frac{log_2 e}{\log_2 n} + \frac{\log_2\left(1+O(n^{-1})\right)}{n\log_2 n}$$

Quindi

$$\lim_{n\to\infty} \frac{\log_2(n!)}{n\log_2 n} = 0+0+1-0+\lim_{n\to\infty} \frac{\log_2(1+kn^{-1})}{n\log_2 n} = 1+0=1$$

poiché il numeratore dell'ultima frazione tende a $\log_2 1 = 0$ e il denominatore tende a ∞.

Stima di h

Quindi, se esistesse un algoritmo di ordinamento per confronto che operi nel tempo h, allora esso eseguirebbe almeno $\log_2(n!)$ passi nel caso peggiore, che è una quantità comunque proporzionale a $n \log_2 n$, asintoticamente.

Sinteticamente, il miglior algoritmo di ordinamento per confronto, non può operare in meno di $O(n \log_2 n)$ passi nel caso peggiore.
Ed esiste un algoritmo che raggiunge questo limite ottimale.

Votazioni

In queste slides vogliamo presentare il teorema di GIbbard-Sattherwaite, che riguarda un risultato sorprendente sui sistemi di voto.

Supponiamo di avere un numero n di elettori e 3 candidati (in realtà il teorema funziona anche con un numero superiore).

Ogni elettore esprime l'ordine di preferenza dei tre candidati.

La votazione mira a stabilire il candidato vincente.

Quello che vogliamo analizzare è la possibilità di definire un meccanismo di voto **equo**.

Voto equo

Un meccanismo di elezione equo soddisfa tre criteri:

1. **unanimità**: se un candidato è indicato come primo da tutti gli elettori, allora vince
2. **nessun dittatore**: un elettore è detto *dittatore* se chiunque indichi al primo posto nella propria lista di preferenze, questi vince. Richiediamo che il meccanismo di voto non permetta la presenza di un dittatore.
3. **monotonicità**: sia Γ una votazione che dichiari X come vincitore. Se Δ è una seconda votazione in cui, nella lista di preferenze di ogni elettore, se X viene prima di Y in Γ, allora X viene prima di Y anche in Δ.
   In questo caso, diremo che Δ è *consistente* con Γ.
   Richiediamo che se X vince le elezioni Γ, allora vince anche le elezioni Δ, per ogni votazione Δ consistente con Γ.

Inversione

Siano Γ e Δ due votazioni che differiscono solo per il voto dell'elettore i: in Γ, il candidato X è immediatamente prima del candidato Y, mentre in Δ, X e Y sono scambiati.

Diciamo che Δ è una (X, Y)-*inversione* di Γ e Γ è una (Y, X)-inversione di Δ.

Un lemma ausiliario

Lemma 33. *Sia X il vincitore della votazione Γ. Sia Δ una (X, Y)-inversione di Γ. Se il meccanismo di voto è equo allora il vincitore di Δ è X oppure Y.*

Dimostrazione.
Supponiamo che il vincitore di Δ sia Z diverso sia da X che da Y. La (Y, X)-inversione di Δ è Γ.
Ma l'insieme dei candidati sotto Z in ogni lista di preferenze in Γ è lo stesso che in Δ, quindi per monotonicità, il vincitore di Γ è Z.
Ma questo è in contraddizione con l'ipotesi. Quindi il vincitore non può essere che uno tra X e Y. □

Un risultato sorprendente

Teorema 34. *Non esiste nessun meccanismo di elezione equo.*

La prova mostra che, se il meccanismo di voto rispetta i criteri di unanimità e monotonicità, allora deve esistere un dittatore, il cui voto determina, da solo, l'esito dell'elezione.

Dimostrazione

Fissiamo due candidati generici A e B.

Sia Γ_0 una votazione in cui ogni elettore pone A in cima alla propria lista di preferenze e B in fondo.
Per il criterio di unanimità, il vincitore sarà A.

Ora muoviamo il candidato B appena sotto il candidato A nella lista dell'elettore 1. Per monotonicità, il vincitore sarà ancora il candidato A.

Adesso scambiamo A e B nella lista di preferenze dell'elettore 1. Per il lemma, il vincitore sarà A oppure B.

Dimostrazione

Se il vincitore fosse A, ci muoviamo al secondo elettore e effettuiamo lo stesso procedimento.

Ad un certo punto, necessariamente, arriviamo all'elettore i in cui lo scambio tra A e B determina un cambio di vincitore.

Chiameremo questo elettore i il *pivot*.

Il pivot deve esistere perché, se continuassimo fino all'ultimo elettore, avremmo una votazione in cui tutti gli elettori indicano B come primo della propria lista, quindi B deve essere il vincitore per unanimità.

Dimostrazione

Chiamiamo Γ_1 la votazione modificata come sopra **senza scambiare** A e B nella lista del pivot.

E chiamiamo Γ_2 la votazione in cui abbiamo effettuato lo scambio di A e B nella lista del pivot.

Definiamo la votazione Γ_{2a} come quella che si ottiene muovendo A in fondo alla lista delle preferenze di ogni elettore **prima** del pivot, e muovendo il candidato A appena prima del candidato B nella lista di preferenze di ogni elettore **dopo** il pivot.

Osserviamo che in Γ_{2a} il candidato B è preferito ad ogni candidato cui B è sopra anche in Γ_2.
Quindi, per monotonicità, B è il vincitore della votazione Γ_{2a}.

Dimostrazione

Modifichiamo in modo analogo Γ_1 per ottenere la votazione Γ_{1a}: muoviamo A in fondo alla lista delle preferenze di ogni elettore **prima** del pivot, e muovendo il candidato A appena prima del candidato B nella lista di preferenze di ogni elettore **dopo** il pivot.

Osserviamo che Γ_{1a} e Γ_{2a} differiscono soltanto per il voto del pivot. In particolare Γ_{2a} è la (A, B)-inversione di Γ_{1a}. Quindi, per il lemma, il vincitore di Γ_{1a} è A oppure B.

Supponiamo sia B. Dato che l'insieme dei candidati sotto B in Γ_1 è lo stesso dei candidati sotto B in Γ_{1a}, il vincitore di Γ_1 dovrebbe essere B per monotonicità, mentre è A. Contraddizione.

Quindi il vincitore di Γ_{1a} è A.

Dimostrazione

Prendiamo un candidato X che non sia A o B. Costruiamo una votazione Γ_3 muovendo gli elementi delle liste di preferenze in Γ_{1a} in modo tale che:

- per ogni elettore **prima** del pivot, gli ultimi tre candidati nella lista di preferenze sono, nell'ordine X, B, A.
- i primi tre candidati nella lista del pivot sono A, X, B.
- per ogni elettore **dopo** il pivot gli ultimi tre candidati sono X, A, B.

Osserviamo che nessun candidato sotto A in Γ_{1a} si muove sopra A in Γ_3. Quindi il vincitore di Γ_3 è A per monotonicità.

Dimostrazione

Infine, nella votazione Γ_3, per ogni elettore **dopo** il pivot scambiamo A con B. Chiamiamo questa votazione Γ_4.

Osserviamo che in Γ_4, A è in fondo alla lista di preferenze di ogni elettore **eccetto** il pivot, in cui A è in cima.

Partendo da Γ_3, stiamo attuando una (A, B)-inversione su ogni elettore dopo il pivot. Ad ogni passo, per il lemma, il vincitore è ancora A, oppure B. Quindi il vincitore di Γ_4 è necessariamente A oppure B.

Dimostrazione

Osserviamo che X è sopra B in ogni lista di preferenza in Γ_4. Quindi se muoviamo X in cima alla lista di preferenza di ogni elettore, ottenendo Γ_5, l'insieme dei candidati sotto B rimane immutato.

Supponiamo che il vincitore di Γ_4 sia B. Quindi, per monotonicità, il vincitore di Γ_5 deve essere B.

Ma X è in cima alla lista di preferenze di ogni elettore in Γ_5, quindi X è il vincitore di Γ_5. Contraddizione.

Quindi il vincitore di Γ_4 è A.

Dimostrazione

In Γ_4 permutiamo in ogni modo possibile tutti i candidati eccetto A nelle liste di preferenza di ogni elettore eccetto il pivot.

Osserviamo che i candidati sotto A restano immutati poiché A è in fondo alla lista di ogni elettore eccetto il pivot.

Quindi A è il vincitore di ogni votazione così ottenuta per monotonicità.

Lo stesso avviene se facciamo risalire A in una qualsiasi lista di preferenza. E anche se permutiamo in un modo qualsiasi la lista del pivot pur di mantenere A in cima.

In ogni votazione dove A è in cima alla lista del pivot, A vince.

Dimostrazione

Ma A e B sono candidati generici: invece di A prendiamo un qualsiasi candidato C e un D diverso da C nel ruolo di B.

Possiamo ripetere lo stesso identico ragionamento, ottenendo lo stesso pivot e lo stesso esito.

Quindi il pivot è un dittatore.

Riferimenti

Normalizzione, eliminazione del taglio e altri risultati simili sono l'argomento di studio della *Teoria della Dimostrazione*. Un riferimento è Sara Negri, Jan Von Plato, *Structural proof theory*. Cambridge University Press, 2001.

Palazzo Davanzati, Firenze

Marco Benini 2025–26