IL TEOREMA FONDAMENTALE DELL'ALGEBRA

Placido Longo (8/7/2010)

La storia del teorema fondamentale dell'Algebra sarebbe interessante di per sé, ma richiederebbe un impegno ed un'estensione impensabili per una dispensa.

Ad ogni modo, in estrema sintesi, la storia è questa.

Leonardo Fibonacci, pisano, accompagnando il padre nei suoi viaggi di commercio, soggiornò per qualche tempo in Algeria, ove prese contatto con l'Algebra, nata in ambiente islamico, e la importò in Europa. A quell'epoca erano noti i procedimenti di risoluzione delle equazioni di primo e secondo grado.

In Italia, durante il Rinascimento, si compirono progressi molto importanti: la formula di Cardano, per la risoluzione dell'equazione generale di terzo grado, e quella di Ludovico Ferrari, per quelle di quarto. Ogni tentativo di reperire formule simili per l'equazione di quinto grado fu inutile.

Gli sforzi degli algebristi italiani condussero anche all'"invenzione" dei numeri complessi, in origine col solo scopo di estrarre le radici di numeri negativi, che si incontravano applicando la formula di Cardano, anche quando le soluzioni erano tutte reali.

Due secoli più tardi, fu chiaro il perché non si riuscisse a trovare le formule risolutive per le equazioni algebriche dal quinto grado in su: Galois, la sera prima di venire ucciso in un duello, scrisse la dimostrazione del fatto che tali formule NON ESISTONO, nel caso generale (ovviamente $x^5=1$ è risolubile!).
Il problema algebrico era definitivamente chiuso: non è sempre possibile trasformare, utilizzando le identità algebriche elementari (permutare e associare addendi, mettere in evidenza, sommare e sottrarre, spostare ad un altro membro...) un'equazione generale di quinto grado in una di tipo "speciale" che utilizzi solo le "operazioni" $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$, $\sqrt[5]{\ }$, ossia le soluzioni delle rispettive equazioni "pure" $x^2=k$, $x^3=k$, $x^4=k$, $x^5=k$.

Dove sta allora il problema? Il problema consiste nel fatto che una cosa è che non esiste formula risolutiva, un'altra è che non esistano soluzioni! Il punto di vista rivoluzionario, che nei secoli successivi pervase l'intera Analisi Matematica, è di rimuovere del tutto a priori il problema della ricerca di formule risolutive (fra l'altro così complicate da essere di uso assai poco agevole!) ed occuparsi del seguente problema:

"Dato un polinomio, esistono punti in cui si annulla"?

Ciò fu GAUSS, il "princeps mathematicorum".
Una prima osservazione è che i polinomi costanti (non nulli) NON hanno zeri. Prenderemo dunque in considerazione solo polinomi NON costanti. Anche i polinomi non costanti, però,

hanno i loro problemi: $1+x^2$ NON ha zeri reali, ma ha zeri complessi $x = \pm i$.
La risposta fornita da C.F. GAUSS, dopo vent'anni di ripensamenti e quattro diverse dimostrazioni, fu semplice e formidabile:

TEOREMA (fondamentale dell'Algebra):

Ogni polinomio non costante a coefficienti in $\mathbb{C}$ ha zeri in $\mathbb{C}$.

Abbiamo già visto che un simile teorema è **FALSO IN $\mathbb{R}$.**
Osserviamo anche che il teorema non si occupa minimamente di come determinare tali soluzioni di $f(z)=0$, ma solo del fatto che esistono.
Osserviamo infine che se $f(z^*)=0$, allora f è divisibile per $(z-z_0)$ (Ruffini), e dunque, eseguita la divisione, si ottiene

$$f(z) = (z-z^*)\,q(z)$$

ove q (il quoziente della divisione) è un polinomio di grado diminuito di 1. Poiché f si annulla solo in z^* e in tutti i punti sui quali si annulla q (legge d'annullamento del prodotto) ne segue che, finché il grado di q non è zero (q costante) si può riapplicare il teorema di GAUSS al quoziente e, alla fine, fattorizzare f in fattori di primo grado (e una costante)

$$f(z) = A\,(z-z_1)(z-z_2)\cdots(z-z_n)$$

ove alcuni degli zeri $z_1 \ldots z_n$ possono o no coincidere. Dunque, ogni polinomio complesso può essere decomposto nel prodotto di

polinomi di grado uno e zero. La costante A risulta essere il coefficiente del termine d'ordine massimo.
La dimostrazione presentata (una delle tante), è basata sulla seguente linea di ragionamento, e su due risultati:

— Per ogni polinomio complesso $p(z)$ la funzione
$$f(z) = |p(z)|$$
ha minimo assoluto in $\mathbb{C}$.

— Per ogni polinomio complesso non costante, se $p(z^*) \neq 0$ allora esiste $\bar{z} \in \mathbb{C}$ tale che
$$|p(z^*)| > |p(\bar{z})|$$

Il teorema di GAUSS segue da questi due risultati perché, detto z^* un punto di minimo assoluto di $|p(z)|$ su $\mathbb{C}$ deve risultare $|p(z^*)| = 0$ (e quindi $p(z^*) = 0$): se così non fosse, per il secondo risultato si avrebbe, per qualche $\bar{z}$
$$|p(\bar{z})| < |p(z^*)|$$
contro l'ipotesi che z^* sia di minimo assoluto per $|p(z)|$.
Le prossime due sezioni sono dedicate a stabilire questi due risultati.

NOTA: secondo altri, fu Niels Abel a provare la non esistenza di formule risolutive. Morì giovanissimo anch'egli (di malattia) e patì, come Galois, le angherie di Cauchy.

Se p è un polinomio in $\mathbb{C}$,
allora $|p|$ ha minimo in $\mathbb{C}$.

Il primo risultato da stabilire riguarda il comportamento di polinomi non costanti all'infinito.

LEMMA: Se $p : \mathbb{C} \to \mathbb{C}$ è non costante, allora

$$\lim_{z \to \infty} p(z) = \infty$$

Dim. Posto $p(z) = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \dots + \alpha_1 z + \alpha_0$, $\alpha_n \neq 0$ si ha

$$p(z) = z^n \left(\alpha_n + \frac{\alpha_{n-1}}{z} + \dots + \frac{\alpha_{n-k}}{z^k} + \dots + \frac{\alpha_0}{z^n} \right)$$

Poiché $z \to \infty \Rightarrow z^k \to \infty$ per ogni k intero strettamente positivo e $f \to \infty \Rightarrow \frac{1}{f} \to 0$, ne segue che il termine in parentesi tende a $\alpha_n \neq 0$, mentre $z^n \to \infty$, da cui $p(z)$ diverge.

Dimostrazione del teorema

È immediato per i polinomi costanti: ogni punto è di minimo.
Fissato ad arbitrio $z_0 \in \mathbb{C}$, se $p(z_0) = 0$ abbiamo già provato il teorema (ed anche il teorema di Gauss) perché

$$|p(z)| \geq 0 = |p(z_0)|$$

Se, invece, risulta $p(z_0) \neq 0$, allora segue dalla divergenza di p all'infinito che, scelto $\varepsilon = |p(z_0)| > 0$, si ha che esiste $\delta > 0$ tale che

$$|p(z)| > \varepsilon = |p(z_0)|$$

per ogni z tale che $|z| > \delta$. A causa della disuguaglianza stretta precedente, $|z_0| \leq \delta$.

Sia ora $f(z) = |p(z)|$ e si consideri la sfera chiusa (e limitata) $\overline{B}(0,\delta)$. La funzione f è continua (perché composta di funzioni continue) su un compatto (la sfera $\overline{B}(0,\delta)$) e dunque, per il teorema di Weierstrass, ha massimo e minimo.
Sia z^* un punto di minimo di f su $\overline{B}(0,\delta)$.
Si ha subito, per ogni $z \in \overline{B}(0,\delta)$

$$|p(z)| = f(z) \geq f(z^*) = |p(z^*)|$$

Se invece è $z \notin \overline{B}(0,\delta)$, e cioè $|z| > \delta$, ricordando che $z_0 \in \overline{B}(0,\delta)$, si ottiene

$$|p(z)| \geq \varepsilon = |p(z_0)| \geq |p(z^*)|$$

e dunque

$$|p(z)| \geq |p(z^*)| \qquad \forall z \in \mathbb{C}.$$

▨

La proprietà di divergenza all'infinito, che permette di restringere la ricerca del minimo ad un insieme chiuso e limitato sul quale essa è assicurata dal teorema di Weierstrass, viene (in altro contesto) chiamata di COERCIVITÀ!

$\boxed{\text{Se } p(z) \text{ è non costante, e } p(z^*) \neq 0, \text{ allora esiste } \bar{z} \in \mathbb{C} \text{ tale che } |p(\bar{z})| < |p(z^*)|}$

Poiché $p(z^*) \neq 0$, si può definire un nuovo polinomio

$$q(w) = \frac{1}{p(z^*)}\, p(z^* + w)$$

Il polinomio q ha lo stesso grado di p, perché sviluppando tutte le potenze $(z^* + w)^m$ si ottiene sempre il termine w^m, ed inoltre $q(0) = 1$.
Riordinando q per potenze crescenti di w si otterrà

$$q(w) = 1 + \alpha_1 w + \alpha_2 w^2 + \dots + \alpha_m w^m + \dots + \alpha_n w^n$$

Poiché q ha lo stesso grado di p, esso è NON costante, e dunque esisterà almeno un coefficiente fra gli $\alpha_1 \dots \alpha_n$ non nullo. Sia k il minimo intero (non nullo) per cui $\alpha_k \neq 0$ e dunque, in realtà,

$$q(w) = 1 + \alpha_k w^k + w^{k+1}\, \tilde{q}(w) \qquad (*)$$

ove $\tilde{q}(w)$ è il polinomio che si ottiene raccogliendo w^{k+1} fra tutti i termini di grado strettamente maggiore di k.

Da $(*)$, per la disuguaglianza triangolare in $\mathbb{C}$, segue

$$|q(w)| \leq |1 + \alpha_k w^k| + |w|^{k+1}\, |\tilde{q}(w)|$$

L'idea della dimostrazione è di scegliere $\overline{w}$ in modo che $\alpha_k w^k$ sia reale, negativo, e di modulo minore di 1.

Perché $\alpha_k w^k$ sia reale e negativo dovrà essere

$$\arg(\alpha_k w^k) = \pi$$

e cioè

$$\pi = \arg \alpha_k + \arg w^k = \arg \alpha_k + k \arg w$$

e infine

$$\theta \equiv \arg w = \frac{\pi - \arg \alpha_k}{k}$$

Volendo poi avere $|\alpha_k w^k| \leq 1$, basta scegliere

$$|w| \leq \frac{1}{|\alpha_k|^{1/k}}$$

In definitiva, per ogni $\overline{w} = \rho e^{i\theta}$, con $\rho \leq \frac{1}{|\alpha_k|^{1/k}}$ e $\theta = \frac{\pi - \arg \alpha_k}{k}$, essendo $\alpha_k \overline{w}^k$ reale, negativo e di modulo minore di 1 risulta

$$|1 + \alpha_k \overline{w}^k| = 1 - |\alpha_k| |\overline{w}|^k$$

da cui

$$|q(\overline{w})| \leq 1 - |\overline{w}|^k \left[|\alpha_k| - |\overline{w}| |\tilde{q}(\overline{w})| \right]$$

Facendo ora tendere $|\overline{w}|$ a zero, mantenendone l'argomento costantemente uguale a θ, si ottiene che il termine in parentesi quadra tende a $|\alpha_k|$ (> 0 per come k è stato definito) da cui, per il teorema della permanenza del segno, esso mantiene lo stesso segno strettamente positivo del limite $|\alpha_k|$ per tutti i $\bar{w} \neq 0$, di argomento uguale a θ e modulo, già in partenza minore di $1/|\alpha_k|^{1/k}$, abbastanza piccolo. Ne segue che, per tali $\bar{w}$

$$\underbrace{|\bar{w}|^k}_{>0}\Big[\underbrace{|\alpha_k| - |\bar{w}||\tilde{q}(\bar{w})|}_{\to |\alpha_k| > 0}\Big] > 0$$

e, di conseguenza,

$$|q(\bar{w})| < 1$$

Ricordando la definizione di q, ne segue

$$|p(z^* + \bar{w})| < |p(z^*)|$$

e la tesi, scegliendo

$$\tilde{z} = z^* + \bar{w}$$

∎

L'impiego del teorema della permanenza del segno consente di concludere che $|q|$ si comporta, per w di norma piccola, come

$$1 + \alpha_k w^k$$

e la caratteristica di $\mathbb{C}$ (non presente in $\mathbb{R}$) che consente di concludere la prova è quella di poter forzare a piacere l'argomento di $\alpha_k w^k$! Per un polinomio reale con k pari e $\alpha_k > 0$ non si può evitare che $\alpha_k w^k$ sia positivo (è esattamente ciò che accade a $p(x) = 1 + x^2$!). Su $\mathbb{C}$, invece, c'è una libertà molto maggiore.

NOTE CONCLUSIVE

A che serve, in definitiva, un teorema di esistenza di soluzioni, senza sapere come calcolarle?
La risposta è meno ovvia di quanto non possa apparire e, vista la fatica notevole che essi richiedono, di solito, per stabilirli, è necessario soffermarsi sulla questione.
I discorsi che stiamo per fare sono comuni anche ad altri celebri teoremi d'esistenza, primo fra tutti quello per le soluzioni delle equazioni differenziali.
Un approccio non solo realistico, ma anche teoricamente corretto al problema non può prescindere dal fatto che già le formule risolutive

$$x = -\frac{b}{a} \qquad x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

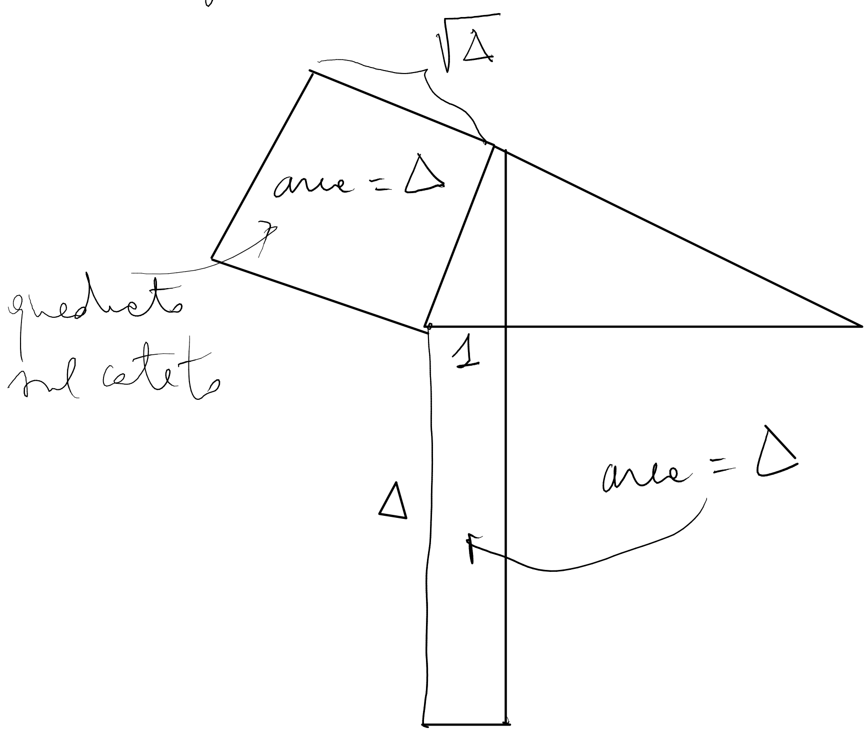
delle equazioni di I e II grado sono, nella stragrande maggioranza dei casi, almeno altrettanto approssimate — non "esatte" — di quanto non lo sia un procedimento di bisezione, ai fini del calcolo delle radici.

$$\frac{1}{3} = 0,333\ldots3\ldots$$

$$1-\sqrt{2} = -0,4142\ldots\ldots$$

La parte "esatta" (algebrica) del processo di risoluzione è la riduzione dell'equazione originaria (completa) ad

altre "pure" ($\sqrt{k}$ = soluzione positiva di $x^2=k$).
Una volta arrivati a $[-b\pm\sqrt{\Delta}]/2a$, se Δ non è un quadrato perfetto il simbolo $\sqrt{\Delta}$ non è nulla di "esatto" e nasconde un'approssimazione.
Non a caso i Greci penalizzarono l'aritmetica a favore della Geometria. Per la radice quadrata, il teorema di Euclide fornisce la costruzione:



Anche gli Antichi ebbero i loro problemi: non esiste una simile costruzione per la radice cubica (come l'oracolo di Apollo mise in chiaro).

Una volta accettato il principio che "esatto" e "approssimato" sono concetti largamente criticabili, i teoremi di esistenza entrano prepotentemente in gioco, offrendo la base teorica sulle quali edificare la costruzione di algoritmi di risoluzione approssimata.

l'esistenza dell'estremo superiore, e cioè la teoria dei numeri reali, fornisce il necessario supporto teorico alla convergenza dello algoritmo di bisezione per il calcolo degli zeri, ad esempio.

Occasionalmente, il favore viene reso. Una delle dimostrazioni del teorema di esistenza (senza unicità) di Peano per equazioni e sistemi differenziali del I ordine in forma normale è basata sull'algoritmo di Eulero di soluzioni approssimate e su un teorema di compattezza (Ascoli-Arzelà) che permette di provare la convergenza di tali approssimazioni, oltre ad un'altra messe dottrina di concetti e risultati: la trasformazione in equazione integrale, la convergenza uniforme e le sue proprietà rispetto agli integrali e la continuità, il buon comportamento delle funzioni equilipschitziane rispetto al teorema di Ascoli-Arzelà ... una discreta fatica, pienamente giustificata dalla portata dei risultati.

Un altro esempio, perfino più lampante, è costituito dalla teoria dei sistemi di equazioni differenziali lineari: teoria puramente algebrica, non appena si sappia provare che un sistema lineare a coefficienti continui su $\mathbb{R}$ ha soluzione <u>unica</u> in $\mathbb{R}$.

Non è possibile entrare qui nei dettagli, né accennare a tutte le applicazioni alla Geometria Analitica e all'Algebra Lineare del teorema di Gauss (si pensi alla storia molto diversa del teorema spettrale su $\mathbb{R}$ e su $\mathbb{C}$).

Forse si dice abbastanza dichiarando che è il primo dei teoremi della Matematica di oggi ad essere stato dimostrato.