

IL TEOREMA FONDAMENTALE DELL'ALGEBRA

ANDREA FERRETTI

Date: 22 febbraio 2010.

Vogliamo raccogliere qui alcune dimostrazioni di quello che è noto con il pomposo nome di Teorema fondamentale dell'algebra. L'enunciato è molto semplice ed è noto a tutti i matematici:

Teorema (fondamentale dell'algebra). *Il campo \mathbb{C} dei numeri complessi è algebricamente chiuso. In altre parole ogni polinomio non costante a coefficienti in \mathbb{C} ammette una radice complessa.*

Corollario. *Ogni polinomio $f \in \mathbb{C}[x]$ si spezza come prodotto di fattori lineari:*

$$f(x) = \lambda(x - x_1) \cdots (x - x_n),$$

per opportuni $\lambda, x_i \in \mathbb{C}$, eventualmente coincidenti.

Però forse non è nota a tutti la varietà di modi diversi in cui questo risultato può essere dimostrato. Gli argomenti che daremo sono dovuti a diversi matematici, ma fra di essi si distingue Gauß, che ha dato una prima dimostrazione del teorema nella sua tesi di dottorato e nel corso della sua carriera ne ha trovate altre tre. Storicamente, però la prima dimostrazione (quasi) completa è dovuta a D'Alembert, che ha presentato un argomento simile al nostro primo approccio. Nella letteratura sono presenti altri approcci alla dimostrazione; abbiamo evitato di dare più versioni sostanzialmente equivalenti di una stessa dimostrazione, tranne nel caso in cui una delle versioni fosse sostanzialmente elementare.

Parlando del Teorema fondamentale dell'algebra non si può evitare di citare il libro di Fine e Rosenberger ([FR97]). In quel caso lo scopo è didattico: gli autori usano il Teorema fondamentale dell'algebra come pretesto per insegnare vari strumenti di topologia, analisi complessa e algebra. Questo articolo ha invece lo scopo di raccogliere una varietà di dimostrazioni diverse e, a differenza del libro, non è autocontenuto. Il background necessario per leggere le diverse dimostrazioni varia; è comunque utile avere una minima familiarità con le funzioni olomorfe (ad esempio dai primi capitoli di [Lan99] o [Car95]), il gruppo fondamentale ([Hat02, cap. 1]) e un po' di teoria dei campi. Un'inesauribile fonte di dimostrazioni e commenti sul Teorema fondamentale dell'algebra è l'American Mathematical Monthly, dal quale abbiamo attinto per diversi approcci.

1. DIMOSTRAZIONI ELEMENTARI

In questa sezione presentiamo gli argomenti che non richiedono conoscenze di analisi complessa, algebra o topologia. Tutto quello che è richiesto è di un primo corso in analisi (oltre che, ovviamente, un po' di familiarità con i numeri complessi). In realtà le dimostrazioni di questa sezione consistono in versioni semplificate di argomenti più concettuali che compariranno più avanti. Ad esempio la prima dimostrazione, dovuta a D'Alembert, presenta in forma elementare lo stesso ragionamento della dimostrazione III.

Lemma 1. *Sia $f(x) \in \mathbb{C}[x]$ un polinomio non costante. Allora*

$$\lim_{|z| \rightarrow +\infty} |f(z)| = +\infty.$$

In altre parole un polinomio non costante è coercivo.

Dimostrazione. Sia

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

Prendendo il valore assoluto e raccogliendo un termine $|z|^n$ troviamo

$$|f(z)| = |z|^n \left| a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n} \right|.$$

Per $|z| \rightarrow +\infty$ troviamo che $\frac{a_k}{z^{n-k}} \rightarrow 0$ per $k > 0$, perciò

$$\lim_{|z| \rightarrow +\infty} |f(z)| = \lim_{|z| \rightarrow +\infty} |a_n| |z|^n = +\infty.$$

□

Teorema fondamentale dell'algebra I. Sia $f(x) \in \mathbb{C}[x]$ non costante. Il lemma precedente ci garantisce l'esistenza di $R > 0$ tale che $|f(z)| > M := f(0)$ per $|z| > R$. Dunque

$$\inf_{z \in \mathbb{C}} |f(z)| = \inf_{z \in \overline{B(0,R)}} |f(z)|.$$

Poiché la palla $\overline{B(0,R)}$ è un compatto, $|f|$ ammette minimo su \mathbb{C} (questa è la parte mancante nell'argomento originale di D'Alembert). Sia z_0 un punto di minimo per $|f|$: vogliamo vedere che $f(z_0) = 0$.

L'argomento, in modo informale, è il seguente. Possiamo sviluppare f intorno a z_0 ; salvo il termine costante il comportamento qualitativo di f intorno a un punto è lo stesso di una potenza (quella che corrisponde al termine di grado più basso in questo sviluppo). Ma una potenza è surgettiva nell'intorno dello 0, perciò ci possiamo spostare di poco da z_0 in modo che $|f(z)| < |f(z_0)|$.

Non è difficile rendere rigoroso tutto questo. Supponiamo per assurdo che $|f(z_0)| > 0$ e scriviamo

$$f(z) = f(z_0) + \sum_{j=k}^n a_j (z - z_0)^j,$$

dove $k \geq 1$ è scelto in modo che $a_k \neq 0$. Scegliamo $h \in \mathbb{C}$ in modo che $a_k h^k = -f(z_0)$, e poniamo $z = z_0 + \varepsilon h$, con $\varepsilon > 0$ e piccolo. Indicando

$$g(z) = \sum_{j=k+1}^n a_j (z - z_0)^j,$$

si ricava

$$|f(z)| \leq |f(z_0) + \varepsilon^k a_k h^k| + |g(z)| \leq (1 - \varepsilon^k) |f(z_0)| + \varepsilon^{k+1} \left| \sum_{j=k+1}^n a_j h^j \varepsilon^{j-k-1} \right|.$$

Se ε è scelto abbastanza piccolo questo valore è minore di $|f(z_0)|$, assurdo. □

La prossima dimostrazione, tratta da [Bur06], richiede il teorema di Fubini per integrali in due variabili, ma per il resto è altrettanto elementare della precedente.

Teorema fondamentale dell'algebra II. Sia $f(z)$ un polinomio non costante, e supponiamo per assurdo che non si annulli; possiamo allora considerare $g = 1/f$, che è una funzione razionale definita su tutto \mathbb{C} . Indichiamo con g' la derivata formale di g , ovvero

$$g'(z) = -\frac{f'(z)}{f(z)^2}.$$

Scrivendo $z = \rho e^{i\theta}$ la regola per la derivazione di funzioni composte dà

$$\begin{cases} \frac{\partial}{\partial \rho} g(\rho e^{i\theta}) = e^{i\theta} g'(\rho e^{i\theta}) \\ \frac{\partial}{\partial \theta} g(\rho e^{i\theta}) = i\rho e^{i\theta} g'(\rho e^{i\theta}), \end{cases}$$

da cui si ricava

$$\frac{\partial}{\partial \rho} g(\rho e^{i\theta}) = \frac{1}{i\rho} \frac{\partial}{\partial \theta} g(\rho e^{i\theta}). \quad (1)$$

Fissati due raggi $r < R$, integriamo la (1) sul rettangolo $[-\pi, \pi] \times [r, R]$; applicando il teorema di Fubini si trova

$$\begin{aligned} \int_{-\pi}^{\pi} [g(Re^{i\theta}) - g(re^{i\theta})] d\theta &= \int_{-\pi}^{\pi} \int_r^R \frac{\partial}{\partial \rho} g(\rho e^{i\theta}) d\rho d\theta = \\ &= \int_r^R \int_{-\pi}^{\pi} \frac{1}{i\rho} \frac{\partial}{\partial \theta} g(\rho e^{i\theta}) d\theta d\rho = \int_r^R \frac{1}{i\rho} [g(\rho e^{-i\pi}) - g(\rho e^{i\pi})] d\rho = 0. \end{aligned} \quad (2)$$

Per $R \rightarrow \infty$ si ha $f(Re^{i\theta}) \rightarrow 0$ uniformemente in θ , grazie alla stima del lemma di coercività. Perciò passando al limite nella (2) si trova $g(0) = 0$, assurdo. \square

2. ANALISI COMPLESSA

Il settore che più naturalmente si presta ad apportare dimostrazioni del Teorema fondamentale dell'algebra è certamente quello dell'analisi complessa. In questo ambito troveremo quattro diversi modi di provare il risultato. A meno di indicazioni diverse, le dimostrazioni di questa sezione sono prese da [Lan99].

Lemma 2. *Sia U un aperto di \mathbb{C} . Una funzione olomorfa $f: U \rightarrow \mathbb{C}$ è aperta nell'intorno dei punti in cui non è localmente costante.*

Dimostrazione. Consideriamo un punto $z_0 \in U$. Se $f'(z_0) \neq 0$ la tesi segue dal teorema della funzione inversa. Supponiamo invece che $f'(z_0) = 0$; a meno di traslazioni possiamo avere $z_0 = f(z_0) = 0$. Sviluppiamo f in serie di potenze come

$$f(z) = \sum_{j=k}^{\infty} a_j z^j,$$

dove $k \geq 1$ è il minimo indice per cui $a_k \neq 0$. Raccogliendo a_k possiamo scrivere $f(z) = a_k(1 + h(z))$ con h olomorfa intorno a 0 e nulla nell'origine. Poiché la funzione z^k è invertibile nell'intorno di 1 possiamo prendere una radice k -esima olomorfa di $1 + h(z)$ per z sufficientemente vicino a 0. Ne segue che

$$f(z) = a_k(g(z))^k = (bg(z))^k,$$

dove g è una funzione olomorfa, $g(0) = 0$ e $b^k = a_k$. Confrontando lo sviluppo di Taylor di g con quello di f si trova che $g'(0) \neq 0$, così g è aperta nell'intorno dell'origine. Ma allora f è composizione di due funzioni aperte, perciò è aperta essa stessa. \square

Corollario (Principio del massimo). *Sia $U \subset \mathbb{C}$ un aperto connesso e $f: U \rightarrow \mathbb{C}$ olomorfa. Se $|f|$ assume massimo su U , allora f è costante.*

Dimostrazione. Sia $z_0 \in U$ un punto di massimo; possiamo supporre che $f(z_0) \neq 0$. Poiché il valore assoluto è una funzione aperta lontano da 0, il lemma precedente

ci dice che f è localmente costante nell'intorno di z_0 . Questo mostra che la controimmagine di $f(z_0)$ è un insieme aperto, e anche chiuso per la continuità di f . Essendo U connesso, segue che f è costante su U . \square

Teorema fondamentale dell'algebra III. Sia $f \in \mathbb{C}[x]$ un polinomio non costante, e supponiamo che f non si annulli in nessun punto di \mathbb{C} . Allora la funzione $1/f: \mathbb{C} \rightarrow \mathbb{C}$ è olomorfa e non costante. D'altra parte abbiamo visto nella prima dimostrazione, come conseguenza del lemma di coercività che $|f|$ ammette minimo su \mathbb{C} , ovvero $|1/f|$ ammette massimo. Il principio del massimo ci dà allora l'assurdo cercato. \square

Un'altra dimostrazione del Teorema fondamentale dell'algebra parte dalle stime di Cauchy per i coefficienti dello sviluppo in serie di una funzione olomorfa. Ricordiamo che la dimostrazione che ogni funzione olomorfa (cioè che ammetta una derivata complessa) è localmente sviluppabile in serie di potenze dà come sottoprodotto un'espressione esplicita per i coefficienti dello sviluppo. Più precisamente sia f olomorfa su un'aperto $U \supset B(z_0, r_0)$, e sia $r < r_0$. Allora f si esprime con una serie di potenze $f(z) = \sum a_j(z - z_0)^j$ sulla palla $B(z_0, r)$, dove i coefficienti a_j sono dati da

$$a_j = \frac{1}{2\pi i} \int_{\partial B(z_0, r)} \frac{f(z)}{z^{j+1}} dz.$$

Una conseguenza immediata di questo è il seguente

Corollario (stime di Cauchy). Sia $f: B(0, R) \rightarrow \mathbb{C}$ olomorfa, $r < R$. Sia

$$f(z) = \sum a_j z^j$$

lo sviluppo di f in 0. Allora $|a_j| \leq \frac{M_r}{r^j}$, dove $M_r = \sup_{|z|=r} |f(z)|$.

Corollario (Liouville). Sia $f: \mathbb{C} \rightarrow \mathbb{C}$ olomorfa e limitata. Allora f è costante.

Dimostrazione. Essendo f olomorfa, possiamo prenderne lo sviluppo in serie in 0, $\sum a_j z^j$. Questa serie di potenze ha raggio di convergenza infinito, perché f è definita ovunque, e coincide con la funzione. Le stime di Cauchy mostrano che

$$|a_j| \leq \frac{M_r}{r^j} \leq \frac{M}{r^j},$$

dove $M = \sup_{\mathbb{C}} |f|$, perciò $a_j = 0$ per ogni $j > 0$. \square

Come conseguenza abbiamo la terza dimostrazione.

Teorema fondamentale dell'algebra IV. Sia $f(z)$ un polinomio che non si annulla su \mathbb{C} . Allora $1/f$ è una funzione olomorfa definita su \mathbb{C} . Dal lemma di coercività segue che $1/f$ è limitata, perciò costante per il teorema di Liouville. \square

L'integrale di Cauchy sulla circonferenza dà un'ulteriore dimostrazione diretta del Teorema fondamentale.

Teorema fondamentale dell'algebra V. Ci basta dimostrare che ogni polinomio reale ha una radice complessa. Infatti se $p(x) \in \mathbb{C}[x]$, il polinomio $p(x)\overline{p(x)}$ è reale, dunque ha una radice (z_0). Questa può essere una radice di p (nel qual caso abbiamo la tesi) oppure una radice di \bar{p} , nel qual caso \bar{z}_0 è una radice di p .

Sia dunque per assurdo $f(x)$ un polinomio a coefficienti reali di grado $n > 0$, e supponiamo che f non si annulli in \mathbb{C} . In particolare f ha segno costante su \mathbb{R} , dunque

$$\int_0^{2\pi} \frac{1}{f(2\cos\vartheta)} d\vartheta \neq 0.$$

Allo stesso tempo questo integrale è pari a

$$\frac{1}{i} \int_{|z|=1} \frac{1}{zf(2\Re z)} dz$$

Sulla circonferenza $|z| = 1$ abbiamo $2\Re z = z + \bar{z} = z + z^{-1}$, perciò, posto $g(z) = z^n f(z + z^{-1})$, l'integrale si può riscrivere come

$$\frac{1}{i} \int_{|z|=1} \frac{z^{n-1}}{g(z)} dz.$$

Per costruzione g è un polinomio; osserviamo che $g(z) \neq 0$ per $z \neq 0$, mentre $g(0)$ è pari al primo coefficiente di f , ed è perciò non nullo. Di conseguenza la funzione nell'integrale è olomorfa sul disco unitario, e l'integrale sul bordo è nullo, assurdo. \square

L'ultima dimostrazione in questo ambito usa uno strumento più raffinato, che permette di contare esattamente il numero di zeri di una funzione olomorfa. Sia $f: U \mapsto \mathbb{C}$ olomorfa, $z_0 \in U$, e consideriamo una palletta sufficientemente piccola $B(z_0, r)$ centrata in z_0 , su cui f ammette uno sviluppo

$$f(z) = \sum_{j=0}^{\infty} a_j (z - z_0)^j.$$

Se k è il più piccolo intero per cui $a_k \neq 0$, diciamo che z_0 è uno zero di molteplicità k per f . In questo caso raccogliendo il termine $(z - z_0)^k$ possiamo scrivere $f(z) = (z - z_0)^k g(z)$ dove g è una funzione olomorfa non nulla su $B(z_0, r)$.

Lemma 3. *Sia $f: U \mapsto \mathbb{C}$ olomorfa, V un aperto con bordo regolare tale che $\bar{V} \subset U$. Supponiamo che $f|_{\partial V}$ non si annulli. Allora il numero di zeri di f in V (contati con molteplicità) è pari a*

$$\frac{1}{2\pi i} \int_{\partial V} \frac{f'(z)}{f(z)} dz. \quad (3)$$

Dimostrazione. Sia $z_0 \in U$ uno zero di ordine k per f , e sia r un raggio abbastanza piccolo. Sulla palla $B(z_0, r)$ possiamo scrivere $f(z) = (z - z_0)^k g(z)$, dove g non si annulla sulla palla. Ne segue che

$$\frac{f'(z)}{f(z)} = \frac{k}{z - z_0} + \frac{g'(z)}{g(z)}.$$

L'integrale sul bordo del secondo addendo è nullo, perché g'/g è olomorfa sulla palla; l'integrale del primo addendo è invece $2k\pi i$, perciò il teorema è vero per $V = B(z_0, r)$.

L'integrale in (3) è invariante per omotopia di cammini contenuti nell'insieme $\{z : f(z) \neq 0\}$. Decomponiamo V in un'unione numerabile di quadrati che si intersechino solo sul bordo, in modo che ogni quadrato contenga al più uno zero di f . Il teorema è vero per ciascuno dei quadrati, e sommando si ottiene la tesi per V . \square

Teorema (Rouché). *Siano $f, g: U \mapsto \mathbb{C}$ olomorfe, V un aperto con bordo regolare tale che $\overline{V} \subset U$. Supponiamo che per $z \in \partial V$ valga*

$$|f(z) - g(z)| < |g(z)|. \quad (4)$$

Allora f e g hanno su V lo stesso numero di zeri, contato con molteplicità.

Dimostrazione. Dalla (4) segue in particolare che f e g non si annullano su ∂V . In particolare possiamo calcolarne il numero di zeri usando il lemma 3. Ci basta perciò dimostrare che

$$\int_{\partial V} \frac{f'(z)}{f(z)} dz - \int_{\partial V} \frac{g'(z)}{g(z)} dz = 0.$$

Osserviamo a questo scopo che derivando si ricava l'uguaglianza

$$\frac{(f/g)'(z)}{(f/g)(z)} = \frac{f'(z)}{f(z)} - \frac{g'(z)}{g(z)};$$

pertanto ci basta mostrare che

$$\int_{\partial V} \frac{(f/g)'(z)}{(f/g)(z)} dz = 0.$$

Sia $\gamma(z)$ una parametrizzazione del cammino δV . Allora

$$\int_{\partial V} \frac{(f/g)'(z)}{(f/g)(z)} dz = \int_{S^1} \frac{(f/g)'(\gamma(z))}{(f/g)(\gamma(z))} \gamma'(z) dz = \int_{((f/g) \circ \gamma)(S^1)} \frac{1}{z} dz = 0,$$

dove l'ultima uguaglianza segue dal fatto che il cammino $((f/g) \circ \gamma)(S^1)$ è contenuto in $B(1, 1)$, essendo $|(f/g)(z) - 1| < 1$ su ∂V . \square

Come corollario otteniamo un'altra dimostrazione.

Teorema fondamentale dell'algebra VI. Sia $f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ un polinomio monico non costante. La stima fatta nel lemma di coercività ci dice che, se R è abbastanza grande,

$$|a_{n-1}z^{n-1} + \dots + a_0| < |z^n|$$

per $|z| = R$. Il teorema di Rouché, applicato con $V = B(0, R)$, $g(z) = z^n$, ci dice che f ha su V lo stesso numero di zeri di z^n , cioè n . \square

3. ENTRA IN BALLO LA TOPOLOGIA

Dopo l'analisi complessa vediamo come la topologia fornisca vari approcci per dimostrare il Teorema fondamentale dell'algebra. Il concetto più utile in questo campo sarà quello di grado, per mappe da S^1 in S^1 e da S^2 in S^2 (S^2 comparirà come varietà complessa $\mathbb{P}^1\mathbb{C}$).

Ricordiamo ([Hat02, cap. 1]) che, data una funzione continua $f: S^1 \mapsto S^1$, è definito il suo grado, che è un numero intero, ed è semplicemente l'elemento corrispondente a $[f]$ tramite l'identificazione $\pi_1(S^1) = \mathbb{Z}$. In particolare il grado di una funzione è invariante per omotopia, ed è nullo se e solo se la funzione è omotopa a costante.

Teorema fondamentale dell'algebra VII. Sia $f(z)$ un polinomio mai nullo, per semplicità monico. Restringendo il dominio di f ad una circonferenza centrata in 0 otteniamo una funzione continua da S^1 in $\mathbb{C} \setminus \{0\}$; a meno di riscalare in arrivo possiamo fare sì che il codominio sia ancora S^1 . Più precisamente poniamo, per $z \in S^1$,

$$f_t(z) = \frac{f(tz)}{|f(tz)|}.$$

Le f_t sono una famiglia di funzioni continue da S^1 in S^1 tra loro omotope; in particolare hanno tutte lo stesso grado. D'altronde f_0 è costante, perciò il suo grado è 0. Supponiamo ora per assurdo che f abbia grado positivo, diciamo $f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$. Ragionando come nel lemma di coercività possiamo trovare $t > 0$ tale che se $|z| = t$ si abbia $|z|^n > |a_{n-1}z^{n-1} + \dots + a_0|$. In particolare $z^n + s(a_{n-1}z^{n-1} + \dots + a_0)$ è non nullo per ogni $s \in [0, 1]$. Possiamo così definire, per $s \in [0, 1]$,

$$g_s(z) = \frac{z^n + s(a_{n-1}z^{n-1} + \dots + a_0)}{|z^n + s(a_{n-1}z^{n-1} + \dots + a_0)|}.$$

Le g_s sono funzioni continue da tS^1 in S^1 , e sono tutte omotope tra loro. Inoltre per $z \in S^1$, $g_1(tz) = f_t(z)$. Da questo si deduce che $g_0(tz)$ ha grado 0 il che è assurdo, perché $g_0(tz) = z^n$ ha grado $n > 0$. \square

Una piccola variante di questa dimostrazione utilizza una tecnica simile a quella del teorema di punto fisso di Brower in dimensione 2. Si tratta di un adattamento di [Lei05].

Lemma 4. Sia $D \subset \mathbb{C}$ il disco unitario chiuso e $f: D \rightarrow D$ continua. Supponiamo che $f(S^1) \subset S^1$ e che $\deg(f|_{S^1}) \neq 0$. Allora f è surgettiva.

Dimostrazione. Chiaramente $f(S^1) \supset S^1$. Supponiamo allora che f non sia surgettiva e prendiamo $z_0 \in \mathring{D}$ che non sia nell'immagine. Costruiamo una funzione continua $g: D \rightarrow S^1$ nel modo seguente: $g(z)$ è il punto in cui la semiretta di origine z_0 e passante per $f(z)$ incontra la circonferenza unitaria (in particolare $f|_{S^1} = g|_{S^1}$). g induce un omomorfismo $g_*: \pi_1(D) \rightarrow \pi_1(S^1)$; per la semplice connessione di D otteniamo

$$[f|_{S^1}] = [g|_{S^1}] = g_*([\text{id}_{S^1}]) = 0 \in \pi_1(S^1),$$

il che contraddice l'ipotesi che $f|_{S^1}$ abbia grado non nullo. \square

Teorema fondamentale dell'algebra VIII. Scegliamo un omeomorfismo $h': [0, +\infty[\rightarrow [0, 1[$ (ad esempio $h'(t) = \frac{2}{\pi} \arctan(t)$) e definiamo un omeomorfismo $h: \mathbb{C} \rightarrow \mathring{D}$ ponendo, in coordinate polari, $h(\rho e^{i\theta}) = h'(\rho) e^{i\theta}$. In pratica tutto quello che ci serve è un omeomorfismo tra \mathbb{C} e \mathring{D} che conservi l'argomento. Prendiamo ora un polinomio monico $p(z)$ di grado $n > 0$, e definiamo la funzione $f: D \rightarrow D$

$$f(z) = \begin{cases} p(h^{-1}(z)) & \text{se } z \in \mathring{D} \\ z^n & \text{se } z \in S^1. \end{cases}$$

La dimostrazione del lemma di coercività mostra che f è continua su tutto D . Per il lemma precedente f è surgettiva, in particolare esiste $z \in \mathring{D}$ con $f(z) = 0$, e dunque $h^{-1}(z)$ è una radice di p . \square

Per la terza dimostrazione useremo ancora il concetto di grado, ma ci fa più comodo avere il punto di vista della geometria differenziale ([Mil97]). Siano M ed N varietà lisce, connesse, compatte, di dimensione n , e sia $f: M \mapsto N$ una mappa regolare. Chiameremo un punto $p \in M$ regolare se $df_p: T_p M \mapsto T_{f(p)} N$ è un isomorfismo. Diremo che $q \in N$ è un valore regolare se le sue controimmagini sono tutti punti regolari.

Osserviamo che se $p \in M$ è un punto regolare, allora il teorema della funzione inversa ci dice che f è un diffeomorfismo locale intorno a p . In particolare le controimmagini di un valore regolare sono punti isolati; essendo M compatta sono in numero finito. Dato un valore regolare $q \in N$, indichiamo con $g(q)$ la cardinalità della controimmagine. In questo modo resta definita una funzione localmente costante da un aperto di N in \mathbb{N} . Nel caso in cui M e N siano orientabili e f mantenga l'orientazione si può mostrare che g è in realtà una funzione costante, e il valore di questa costante è detto grado di f .

Teorema fondamentale dell'algebra IX. Sia f un polinomio non costante. Possiamo vedere f come funzione da \mathbb{C} in \mathbb{C} , ed estendere f ad una funzione $\mathbb{P}^1 \mathbb{C} \mapsto \mathbb{P}^1 \mathbb{C}$ ponendo $f(\infty) = \infty$. Il lemma di coercività ci dice l'estensione di f è continua; in realtà il cambio di variabile $z \mapsto 1/z$ mostra che è una funzione liscia su tutto $\mathbb{P}^1 \mathbb{C}$. Un punto $z \in \mathbb{C}$ è regolare se e solo se $f'(z) \neq 0$. Poiché gli zeri della derivata di f sono in numero finito, l'insieme dei valori regolari è connesso, perciò g è costante. Dunque tutti i valori regolari sono l'immagine di esattamente k valori, per un opportuno k . Da questo segue che $k > 0$. Inoltre i valori che non sono regolari sono nell'immagine di f per definizione. Dunque f è surgettivo, in particolare assume il valore 0. \square

La dimostrazione seguente invece utilizza solo concetti elementari di topologia generale. Tuttavia è necessario assumere un risultato di algebra commutativa, ovvero una forma del lemma di Hensel per l'anello delle serie convergenti. Innanzitutto introduciamo un po' di notazione. L'anello delle serie formali in n indeterminate sarà indicato con $\mathbb{C}[[X_1, \dots, X_n]]$, mentre il sottoanello dato dalle serie con raggio di convergenza non nullo verrà indicato $\mathbb{C}\{X_1, \dots, X_n\}$. Diremo che $p(X, T) \in \mathbb{C}\{X_1, \dots, X_n, T\}$ è uno pseudopolinomio se è un polinomio monico nella variabile T (in particolare $p(X, T) \in \mathbb{C}\{X_1, \dots, X_n\}[T]$). L'anello delle serie convergenti, pur non essendo completo, soddisfa il

Lemma 5 (Hensel). *Sia $p(X, T)$ uno pseudopolinomio di grado N in T , e sia p_0 il polinomio $p_0(T) = p(0, T)$. Supponiamo che valga la fattorizzazione $p_0 = h_0 k_0$ in $\mathbb{C}[T]$, con h_0 e k_0 privi di fattori comuni, rispettivamente di gradi a e b . Allora esistono e sono unici due pseudopolinomi h e k di gradi a e b tali che $p = hk$ e $h(0, T) = h_0(T)$, $k(0, T) = k_0(T)$.*

Vediamo come questo ci possa aiutare a dimostrare il Teorema fondamentale dell'algebra. Dato $a = (a_0, \dots, a_{n-2}) \in \mathbb{C}^{n-1}$ indichiamo con p_a il polinomio

$$p_a(z) = z^n + a_{n-2}z^{n-2} + \dots a_0.$$

Indichiamo poi $V = \{a \in \mathbb{C}^{n-1} : p_a = rs \text{ con } r, s \text{ di grado positivo senza fattori comuni}\}$ e $W = \{a \in \mathbb{C}^{n-1} : p_a \text{ è irriducibile}\}$.

Lemma 6. *V è contenuto nella parte interna di $\mathbb{C}^{n-1} \setminus W$.*

Dimostrazione. Sia $a \in V$ e poniamo $\phi(x, t) = p_{a+x}(t)$. Per ipotesi $\phi(0, t)$ è il prodotto di due polinomi di grado positivo primi fra loro; per il lemma di Hensel troviamo due pseudopolinomi r ed s , degli stessi gradi, e tali che $\phi(x, t) = r(x, t)s(x, t)$. Le serie r ed s hanno raggio di convergenza non nullo, perciò se x è abbastanza piccolo, $p_{a+x}(t)$ si fattorizza, cioè $a + x \notin W$. \square

Teorema fondamentale dell'algebra X. A meno di effettuare un cambio di variabile lineare, ogni polinomio monico di grado n è della forma p_a , per un opportuno $a \in \mathbb{C}^{n-1}$. Dimostriamo dunque che ogni polinomio p_a è prodotto di fattori lineari. Per fare questo utilizziamo un'induzione su n ; la tesi è che $W = \emptyset$. Utilizzando la connessione di $\mathbb{C}^{n-1} \setminus \{0\}$ ci basta vedere che V e W sono aperti disgiunti, e che $V \cup W = \mathbb{C}^{n-1} \setminus \{0\}$, visto che V è ovviamente non vuoto.

Per vedere che $V \cup W = \mathbb{C}^{n-1} \setminus \{0\}$ utilizziamo l'ipotesi induttiva. Se $a \notin W$, p_a ha una fattorizzazione non banale $p_a = rs$, e per induzione sappiamo che r ed s sono prodotto di fattori lineari. Se inoltre $a \notin V$, non possono comparire fattori lineari distinti, perciò $p_a(T) = (T - b)^n$. Da questo si ricava $nb = 0$, cioè $b = 0$, e infine $a = 0$.

A questo punto sappiamo che V e W sono complementari in $\mathbb{C}^{n-1} \setminus \{0\}$, e dal lemma 6 segue che V è contenuto nella propria parte interna, cioè è un aperto.

Vediamo infine che W è aperto. Consideriamo il chiuso di $\mathbb{C}^{n-1} \times \mathbb{P}^1\mathbb{C}$ dato da

$$H = \left\{ (a, [t_0 : t_1]) \in \mathbb{C}^{n-1} \times \mathbb{P}^1\mathbb{C} : t_0^n + \sum a_i t_0^i t_1^{n-i} = 0 \right\}.$$

Essendo $\mathbb{P}^1\mathbb{C}$ compatto, la proiezione $\pi : \mathbb{C}^{n-1} \times \mathbb{P}^1\mathbb{C} \rightarrow \mathbb{C}^{n-1}$ è una mappa propria; dunque $\pi(H)$ è chiuso. Ma $\pi(H)$ è proprio il complementare di W , che dunque è aperto. \square

4. DIMOSTRAZIONI ALGEBRICHE

Come abbiamo visto finora, il nome di Teorema fondamentale dell'algebra non è del tutto azzeccato per un risultato che esprime sostanzialmente proprietà analitiche o topologiche del piano complesso. D'altra parte è chiaro che non può esistere una dimostrazione puramente algebrica di questo risultato, che si basa alla fine sulla completezza di \mathbb{R} . In questo paragrafo illustreremo però alcune dimostrazioni che si basano perlopiù su tecniche algebriche.

In particolare le dimostrazioni di questo paragrafo sono indipendenti da tecniche analitiche, salvo per due risultati di analisi elementare. È sufficiente assumere i due seguenti fatti, che si provano entrambi applicando il teorema del valore intermedio.

- i) Un numero reale è non negativo se e solo se è un quadrato;
- ii) ogni polinomio a coefficienti reali di grado dispari ha una radice reale.

Teorema fondamentale dell'algebra XI. Per mostrare che \mathbb{C} è algebricamente chiuso vediamo che ogni sua estensione finita di Galois è l'estensione banale \mathbb{C}/\mathbb{C} .

Per prima cosa mostriamo che ogni estensione K/\mathbb{C} ha grado una potenza di 2. Per vedere questo ci basta vederlo per l'estensione K/\mathbb{R} , e poiché ogni estensione di \mathbb{R} è contenuta in un'estensione normale, possiamo supporre che K/\mathbb{R} sia di Galois. Indichiamo con k il grado, e con G il gruppo di Galois dell'estensione. Scriviamo infine $k = 2^h d$, con d dispari. Il teorema di Silow ci garantisce l'esistenza di un sottogruppo $H < G$ di ordine 2^h ; a questo è associato per corrispondenza di Galois un'estensione L/\mathbb{R} di grado d . Per il teorema dell'elemento primitivo possiamo scrivere $L = \mathbb{R}[\alpha]$. Se $f \in \mathbb{R}[X]$ è il polinomio minimo di α su \mathbb{R} , allora f è

irriducibile. Poiché f ha grado dispari, ammette una radice reale, perciò si deve avere $d = 1$ per l'irriducibilità.

A questo punto mostriamo che ogni estensione normale di \mathbb{C} è data da \mathbb{C} stesso. Sia K/\mathbb{C} un'estensione normale con gruppo di Galois G , e supponiamo per assurdo che sia non banale. Abbiamo visto che G è un 2-gruppo; pertanto ammette un sottogruppo di indice 2. Tramite la corrispondenza di Galois otteniamo un'estensione di grado 2 di \mathbb{C} . Ci basta perciò vedere che ogni tale estensione è banale, o equivalentemente che ogni numero complesso ammette una radice quadrata.

Sia $a + ib \in \mathbb{C}$ e cerchiamo una radice quadrata della forma $x + iy$. Esplicitamente si tratta di risolvere

$$\begin{cases} a = x^2 - y^2 \\ b = 2xy. \end{cases} \quad (5)$$

Da queste si trova $\sqrt{a^2 + b^2} = x^2 + y^2$ ($a^2 + b^2$ è positivo, dunque ammette una radice reale), o anche

$$\begin{cases} x^2 = \frac{\sqrt{a^2 + b^2} + a}{2} \\ y^2 = \frac{\sqrt{a^2 + b^2} - a}{2}. \end{cases}$$

Dall'ultimo sistema si ricavano x ed y , osservando che i numeri a secondo membro sono positivi. Per una scelta opportuna dei segni si possono invertire i passaggi e vedere che vale la (5). \square

Una seconda dimostrazione sulle stesse linee (tratta da [FR97]) non usa direttamente la corrispondenza di Galois. Il punto di partenza è l'espressione dei polinomi simmetrici (cioè invarianti per permutazione delle indeterminate) come polinomi nelle funzioni simmetriche elementari. Date le indeterminate x_1, \dots, x_n , la funzione simmetrica elementare k -esima è per definizione il polinomio

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \cdots x_{i_k}.$$

In particolare la prima funzione simmetrica è la somma e l' n -esima è il prodotto delle indeterminate.

Teorema. *Sia K un campo. L'omomorfismo di anelli*

$$K[y_1, \dots, y_n] \longmapsto K[x_1, \dots, x_n]$$

che manda y_i nella funzione simmetrica $\sigma_i(x_1, \dots, x_n)$ è iniettivo, con immagine l'anello dei polinomi simmetrici in x_1, \dots, x_n . In particolare ogni polinomio simmetrico è un polinomio in $\sigma_1, \dots, \sigma_k$, e l'anello dei polinomi simmetrici è isomorfo ad un anello di polinomi.

A noi basta però una forma più debole di questo teorema, che si presta ad essere dimostrata tramite la teoria di Galois.

Teorema. *Sia K un campo, $f \in K(x_1, \dots, x_n)$ una funzione razionale simmetrica. Allora f è una funzione razionale in $\sigma_1, \dots, \sigma_k$*

Dimostrazione. Indicando con S il campo delle funzioni razionali simmetriche, abbiamo l'inclusione di campi

$$K(\sigma_1, \dots, \sigma_n) \subset S \subset K(x_1, \dots, x_n).$$

Consideriamo il polinomio

$$p(x) = \prod_{i=1}^n (x - x_i) = x^n - \sigma_1(x_1, \dots, x_n)x^{n-1} + \dots + (-1)^n \sigma_n(x_1, \dots, x_n).$$

La seconda espressione mostra che è a coefficienti in $K(\sigma_1, \dots, \sigma_n)$, mentre la prima espressione mostra che il suo campo di spezzamento è esattamente $K(x_1, \dots, x_n)$. Pertanto possiamo limitare il grado dell'estensione

$$[K(x_1, \dots, x_n) : K(\sigma_1, \dots, \sigma_n)] \leq (\deg p)! = n!.$$

Il gruppo delle permutazioni su n elementi \mathfrak{S}_n agisce su $K(x_1, \dots, x_n)$ permutando le indeterminate, e il campo lasciato invariato è per definizione S . Perciò abbiamo un omomorfismo iniettivo

$$\mathfrak{S}_n \longmapsto \text{Aut}(K(x_1, \dots, x_n), S).$$

Il gruppo degli automorfismi $\text{Aut}(K(x_1, \dots, x_n), S)$ ha al più tanti elementi quante sono le immersioni di $K(x_1, \dots, x_n)$ nella chiusura algebrica di S che lasciano fisso S , e questo numero è pari al grado dell'estensione (l'uguaglianza vale se e solo se l'estensione è di Galois). Di conseguenza

$$n! = \#\mathfrak{S}_n \leq \#\text{Aut}(K(x_1, \dots, x_n), S) \leq [K(x_1, \dots, x_n) : S].$$

Confrontando i gradi si ricava che l'inclusione $K(\sigma_1, \dots, \sigma_n) \subset S$ è in realtà un'uguaglianza. Per inciso, dalla dimostrazione abbiamo anche ottenuto che l'estensione $K(x_1, \dots, x_n)/S$ è di Galois, con gruppo di Galois \mathfrak{S}_n . \square

Corollario. *Sia K un campo e $g(x, x_1, \dots, x_n) \in K[x, x_1, \dots, x_n]$ un polinomio simmetrico in x_1, \dots, x_n . Sia $f(x) \in K[x]$ con radici (in una chiusura algebrica) $\alpha_1, \dots, \alpha_n$. Allora $g(x, \alpha_1, \dots, \alpha_n) \in K[x]$.*

Dimostrazione. A priori g è un polinomio a coefficienti nella chiusura algebrica di K . Però i suoi coefficienti sono polinomi simmetrici (a coefficienti in K) in $\alpha_1, \dots, \alpha_n$. Il teorema precedente ci dice che questi coefficienti sono funzioni razionali in $\sigma_1(\alpha_1, \dots, \alpha_n), \dots, \sigma_n(\alpha_1, \dots, \alpha_n)$, che sono i coefficienti di f ; pertanto sono elementi di K . \square

Da questi risultati sui polinomi simmetrici deduciamo un'altra dimostrazione

Teorema fondamentale dell'algebra XII. Abbiamo già osservato che ci basta dimostrare la tesi per un polinomio reale. Sia dunque $f(x)$ un polinomio a coefficienti reali, di grado n . Scomponiamo $n = 2^k d$, dove d è dispari, e mostriamo la tesi per induzione su k . Se $k = 0$ abbiamo un polinomio di grado dispari a coefficienti reali, che ha una radice reale.

Per il passo induttivo, siano $\alpha_1, \dots, \alpha_n$ le radici di f in un campo di spezzamento. Dato un intero h consideriamo il polinomio

$$g(x) = \prod_{i < j} (x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)).$$

g è un polinomio simmetrico negli α_i , pertanto il lemma ci dice che è a coefficienti reali. Il grado di g è

$$\binom{n}{k} = 2^{k-1}d(2^k d - 1).$$

Per ipotesi induttiva g ha almeno una radice complessa, cioè per opportuni i, j il termine $\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}$.

Questo può essere fatto per ogni scelta di h intero; poiché abbiamo un numero finito di coppie troviamo h_1 e h_2 distinti tali che per la stessa scelta di i, j si abbia $\alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}$ e $\alpha_i + \alpha_j + h_2\alpha_i\alpha_j \in \mathbb{C}$. Per differenza si ricava che il prodotto $\alpha_i\alpha_j \in \mathbb{C}$, e di nuovo per differenza anche la somma. A questo punto possiamo ricavare α_i e α_j come radici di un'equazione di secondo grado a coefficienti complessi. Ma le soluzioni di un'equazione di secondo grado in \mathbb{C} stanno a loro volta nei complessi: infatti queste si esprimono tramite la formula risolutiva, e la radice quadrata di un numero complesso è ancora in \mathbb{C} (abbiamo visto nella dimostrazione precedente come questo segua dalla seconda delle nostre assunzioni analitiche). Con questo l'induzione è completata. \square

Derksen, in [Der03] dà una dimostrazione geniale basata sull'algebra lineare. Osserviamo innanzitutto che l'enunciato del Teorema fondamentale dell'algebra può essere ripafrasato dicendo che ogni matrice a coefficienti complessi ha un autovalore. Chiaramente la forma standard del teorema, applicata al polinomio caratteristico della matrice, implica questo enunciato. Viceversa supponiamo che ogni matrice abbia un autovalore, e sia

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

un polinomio a coefficienti complessi. Definiamo la matrice compagna di p come

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & 1 & & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Allora A ammette p come polinomio caratteristico, perciò p ha una radice, corrispondente ad un autovalore di A .

Teorema fondamentale dell'algebra XIII. La dimostrazione fa riferimento più volte ad un enunciato piuttosto complesso. Sia K un campo (\mathbb{R} o \mathbb{C}) e siano d ed r due interi. Indichiamo con $\mathcal{P}(K, d, r)$ il seguente enunciato:

Sia V uno spazio vettoriale su K di dimensione non multipla di d , e siano A_1, \dots, A_r endomorfismi di V che commutano fra loro. Allora gli A_i ammettono un autovettore comune.

Dividiamo la dimostrazione in vari passi.

- i) *Mostriamo che $\mathcal{P}(K, d, 1)$ implica $\mathcal{P}(K, d, r)$ per ogni r , per induzione su r .* Assumiamo dunque $\mathcal{P}(K, d, r-1)$ e prendiamo r endomorfismi A_1, \dots, A_r di V che commutano. Dimostriamo che ammettono un autovettore comune tramite una seconda induzione, stavolta su n .

Il caso $n = 1$ è banale. L'ipotesi $\mathcal{P}(K, d, 1)$ ci garantisce che A_r ha un autovettore in V , con autovalore λ . Indichiamo

$$\begin{aligned} W &= \text{Ker}(A_r - \lambda \text{id}) \\ Z &= \text{Im}(A_r - \lambda \text{id}); \end{aligned}$$

l'ipotesi che gli endomorfismi commutino garantisce che W e Z siano mandati in se stessi da A_1, \dots, A_{r-1} . Se $W = V$, un qualsiasi autovettore comune per

- A_1, \dots, A_{r-1} è autovettore anche per A_r . Altrimenti W e Z sono entrambi sottospazi propri di V . Poiché $\dim W + \dim Z = \dim V$, d non divide $\dim W$ oppure non divide $\dim Z$. In entrambi i casi, per ipotesi induttiva, A_1, \dots, A_r hanno un autovettore comune dentro W (rispettivamente Z).
- ii) *Vale $\mathcal{P}(\mathbb{R}, 2, r)$ per ogni r .* Dal passo precedente segue che è sufficiente mostrare $\mathcal{P}(\mathbb{R}, 2, 1)$; questo è vero perché ogni polinomio reale di grado dispari ha una radice reale.
- iii) *Vale $\mathcal{P}(\mathbb{C}, 2, r)$ per ogni r .* Come sopra ci basta verificare che è vera $\mathcal{P}(\mathbb{C}, 2, 1)$. Sia dunque n dispari e sia $A: \mathbb{C}^n \mapsto \mathbb{C}^n$ un endomorfismo. Applichiamo il risultato del passo precedente allo spazio vettoriale reale V delle matrici n times n hermitiane, cioè

$$V = \{B \in \mathcal{M}_{n \times n}(\mathbb{C}) : B^* = B\}.$$

V ha dimensione reale n^2 , perché ogni matrice hermitiana B è determinata una volta fissate le $n(n-1)/2$ entrate complesse sopra la diagonale e le n entrate reali sulla diagonale; in particolare V ha dimensione dispari. Definiamo due endomorfismi di V ponendo

$$L_1(B) = \frac{AB + BA^*}{2}$$

$$L_2(B) = \frac{AB - BA^*}{2i}.$$

È una verifica immediata che se B è hermitiana anche $L_1(B)$ e $L_2(B)$ lo sono, e che L_1 ed L_2 commutano. Per il passo precedente L_1 ed L_2 hanno un autovettore comune, cioè esiste una matrice hermitiana B tale che $L_1(B) = \lambda B$, $L_2(B) = \mu B$, con $\lambda, \mu \in \mathbb{R}$. Ne segue che

$$AB = (L_1 + iL_2)B = (\lambda + i\mu)B,$$

dunque una colonna non nulla di B dà luogo ad un autovettore per A .

- iv) *Mostriamo per induzione su k che vale $\mathcal{P}(\mathbb{C}, 2^k, r)$.* La base dell'induzione consiste nel passo precedente. Supponiamo dunque valido $\mathcal{P}(\mathbb{C}, 2^{k-1}, r)$; come sopra ci è sufficiente vedere che vale $\mathcal{P}(\mathbb{C}, 2^k, 1)$.

Sia A un endomorfismo di \mathbb{C}^n , dove n non è divisibile per 2^k . Se n non è divisibile per 2^{k-1} la tesi segue per ipotesi induttiva, dunque supponiamo che 2^{k-1} divida n . Sia V il \mathbb{C} -spazio vettoriale delle matrici antisimmetriche:

$$V = \{B \in \mathcal{M}_{n \times n}(\mathbb{C}) : B^T = -B\}.$$

Stavolta V ha dimensione complessa $n(n-1)/2$, dunque $\dim_{\mathbb{C}} V$ non è divisibile per 2^{k-1} . Definiamo due endomorfismi di V ponendo

$$L_1(B) = AB - BA^T$$

$$L_2(B) = ABA^T.$$

Per $\mathcal{P}(\mathbb{C}, 2^{k-1}, 2)$ L_1 ed L_2 hanno un autovettore comune, ovvero esiste una matrice antisimmetrica B tale che $L_1(B) = \lambda B$, $L_2(B) = \mu B$, con $\lambda, \mu \in \mathbb{C}$. Ne segue che

$$\mu B = ABA^T = A(AB - \lambda B).$$

Se \mathbf{v} è una colonna non nulla di B si ha

$$(A^2 - \lambda A - \mu \text{id})\mathbf{v} = 0. \tag{6}$$

Abbiamo visto come dall'ipotesi che ogni numero reale non negativo sia un quadrato segua che ogni numero complesso ha una radice quadrata. Possiamo allora fattorizzare la (6) come

$$(A - \alpha \text{id})(A - \beta \text{id})\mathbf{v} = 0,$$

dove α e β sono le soluzioni dell'equazione di secondo grado

$$x^2 - \lambda x - \mu = 0.$$

Se $(A - \beta \text{id})\mathbf{v} = 0$, allora \mathbf{v} è autovettore per A con autovalore β , altrimenti $(A - \beta \text{id})\mathbf{v}$ è autovettore per A con autovalore α .

- v) *Ogni matrice quadrata a coefficienti complessi ha un autovettore.* Questo segue banalmente da $\mathcal{P}(\mathbb{C}, 2^k, r)$, applicato con k sufficientemente grande.

□

5. STRUTTURE DI ALGEBRA SU \mathbb{R}^n

Un altro approccio è quello di studiare in generale le conseguenze dell'esistenza di una struttura di algebra su \mathbb{R}^n , e mostrare un'algebra di dimensione finita su \mathbb{R} può essere un campo solo nei casi in cui sia \mathbb{R} stesso oppure \mathbb{C} . In particolare da questo segue il Teorema fondamentale dell'algebra, perché \mathbb{C} non ammette estensioni finite, ed è dunque algebricamente chiuso. La prima dimostrazione che diamo compare in [dSOS05].

Lemma 7. *Ogni sottogruppo discreto di \mathbb{R}^n è isomorfo a \mathbb{Z}^k per un opportuno $k \leq n$, generato da k vettori e_1, \dots, e_k linearmente indipendenti.*

Dimostrazione. Induzione su n . Iniziamo dal caso $n = 1$, e sia $G < \mathbb{R}$ un sottogruppo discreto non banale. Osserviamo che $t = \inf\{x > 0 : x \in G\}$ è un elemento di G . Se così non fosse potremmo scegliere elementi $x_1, x_2 \in G$ positivi e minori di $2t$; $|x_1 - x_2|$ sarebbe allora un elemento di G inferiore a t . Mostriamo ora che $G = \mathbb{Z}t$. Se $x \in G$, sottraendo a x un opportuno multiplo di t otteniamo un elemento $y \in G$ non negativo e minore di t ; per costruzione si ha $y = 0$, cioè $x \in \mathbb{Z}t$.

Per il passo induttivo consideriamo un sottogruppo discreto $G < \mathbb{R}^n$ non banale. Prendiamo $v \in G$ e consideriamo il sottogruppo $g \cap \mathbb{R}v$. Per il caso $n = 1$ questo è ciclico, generato da un vettore e_1 . Mostriamo ora che $G' = G/\mathbb{Z}e_1$ è un sottogruppo discreto di $\mathbb{R}^n/\mathbb{R}e_1$. Supponiamo infatti di avere nel quoziente una successione di elementi $y_i \in G'$ che tendono a $y \in G'$. Solleviamo ciascun y_i ad un rappresentante x_i , e prendiamo un rappresentante x di y . Allora per opportuni n_i la successione $x_i + n_i e_1$ tende a x , contro l'assunzione che G sia discreto. Per ipotesi induttiva G' è generato da opportuni vettori f_2, \dots, f_k per un opportuno $k \leq n$. Se e_2, \dots, e_k sono vettori rappresentanti di f_2, \dots, f_k , allora e_1, e_2, \dots, e_k sono linearmente indipendenti, e $G = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_k$. □

Teorema fondamentale dell'algebra XIV. Supponiamo che \mathbb{C} non sia algebricamente chiuso. Allora ammette un'estensione finita di campi K/\mathbb{C} . Come spazio vettoriale K è isomorfo a \mathbb{R}^n per un opportuno $n > 2$, perciò ci basterà mostrare che \mathbb{R}^n non ammette una struttura di campo. Supponiamo che invece ne ammetta una: data l'usuale norma $|\cdot|$ su \mathbb{R}^n definiamo la norma

$$\|x\| = \sup_{|y| \leq 1} |x \cdot y|.$$

In termini di questa norma definiamo le funzioni esponenziale e logaritmo:

$$\begin{aligned}\exp(x) &= \sum_{n=0}^{\infty} \frac{x^n}{n!} \\ \log(x) &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.\end{aligned}$$

La prima serie converge assolutamente su \mathbb{R}^n , mentre la seconda converge su $\{x \in \mathbb{R}^n : \|x - 1\| < 1\}$. Entrambi questi fatti seguono dall'usuale convergenza per la serie dell'esponenziale e del logaritmo, una volta osservato che $\|x \cdot y\| \leq \|x\| \|y\|$. Dalle definizioni si ricavano subito le usuali proprietà dell'esponenziale:

$$\begin{aligned}\exp(0) &= 1 \\ \exp(x + y) &= \exp(x) \cdot \exp(y) \\ \exp(-x) &= \exp(x)^{-1}.\end{aligned}$$

Nell'ipotesi che \mathbb{R}^n sia un campo, $\mathbb{R}^n \setminus \{0\}$ risulta essere un gruppo rispetto alla moltiplicazione, e $\exp: \mathbb{R}^n \mapsto \mathbb{R}^n \setminus \{0\}$ un omomorfismo. Inoltre se x è abbastanza vicino a 0 e y vicino a 1, si ha $\log \exp(x) = x$ e $\exp \log(y) = y$. In particolare ne segue che l'immagine di \exp contiene un intorno di 0; essendo un omomorfismo ne segue che l'immagine è aperta. $\exp(\mathbb{R}^n)$ è dunque un sottogruppo aperto, perciò anche chiuso (perché complementare dell'unione delle sue classi laterali, che sono a loro volta aperte). Essendo $\mathbb{R}^n \setminus \{0\}$ connesso segue che \exp è surgettiva.

Inoltre $\ker(\exp)$ è un sottogruppo discreto di \mathbb{R}^n , di nuovo perché \exp è un omomorfismo tra un intorno di 0 e un intorno di 1. Per il lemma precedente il nucleo di \exp è isomorfo a \mathbb{Z}^k per un opportuno $k \leq n$, generato da k vettori e_1, \dots, e_k linearmente indipendenti. Passando al quoziente otteniamo un isomorfismo

$$(S^1)^k \times \mathbb{R}^{n-k} \cong \mathbb{R}^n / \ker(\exp) \mapsto \mathbb{R}^n \setminus \{0\}.$$

Per concludere ci basta vedere che $(S^1)^k \times \mathbb{R}^{n-k}$ e $\mathbb{R}^n \setminus \{0\}$ non sono omeomorfi. Vediamo innanzitutto il gruppo fondamentale: $\pi_1((S^1)^k \times \mathbb{R}^{n-k}) = \pi_1(S^1)^k \cong \mathbb{Z}^k$, mentre $\pi_1(\mathbb{R}^n \setminus \{0\}) = \pi_1(S^{n-1}) = 0$, essendo $n > 2$. Pertanto si trova $k = 0$, ed \exp dà un isomorfismo tra \mathbb{R}^n e $\mathbb{R}^n \setminus \{0\}$. Ma nemmeno questi due spazi sono omeomorfi, poiché \mathbb{R}^n è contraibile, mentre $H^{n-1}(\mathbb{R}^n \setminus \{0\}) = H^{n-1}(S^{n-1}) \cong \mathbb{Z}$. \square

Il secondo approccio è simile, e consiste sostanzialmente in una riscrittura della dimostrazione del teorema di Gelfand-Mazur in un caso molto particolare. Supponiamo di avere un'algebra A di dimensione finita su \mathbb{C} . Come nella dimostrazione precedente possiamo introdurre su A una norma $\|\cdot\|$ che verifichi

$$\|x \cdot y\| \leq \|x\| \|y\|.$$

Dato $x \in \mathbb{C}^n$ definiamo il suo spettro

$$\sigma(x) = \{\lambda \in \mathbb{C} : x - \lambda e \text{ non è invertibile}\},$$

Dove $e = \text{id}_A$. Con questi preliminari possiamo dimostrare che se A è un campo, necessariamente $A = \mathbb{C}$, provando così il Teorema fondamentale dell'algebra.

Teorema fondamentale dell'algebra XV. Ci basta dimostrare che $\sigma(x)$ è non vuoto per ogni $x \in A$. Infatti se $\lambda \in \sigma(x)$, allora $x - \lambda e$ non è invertibile per definizione. Essendo A un campo, $x - \lambda e = 0$, cioè $x = \lambda e$ e A ha dimensione 1 su \mathbb{C} .

Supponiamo per assurdo che $\sigma(x) = \emptyset$ e definiamo la funzione risolvente

$$R_x: \mathbb{C} \mapsto A$$

$$\lambda \mapsto (\lambda e - x)^{-1}.$$

La funzione risolvente è olomorfa, ammettendo uno sviluppo locale in serie di potenze: se $\lambda_0 \in \mathbb{C}$ allora

$$(\lambda e - x)^{-1} = (\lambda_0 e - x + (\lambda - \lambda_0)e)^{-1} = (\lambda_0 e - x)^{-1} \sum_{i=0}^{\infty} [(\lambda - \lambda_0)(\lambda_0 e - x)^{-1}]^i$$

ogniqualevolta $|\lambda - \lambda_0| < \|(\lambda_0 e - x)^{-1}\|$. Inoltre se $\lambda > 2\|x\|$ allora possiamo stimare

$$\|(e - \lambda^{-1}x)^{-1}\| \leq \sum_{i=0}^{\infty} \left(\frac{\|x\|}{\lambda}\right)^i < 2,$$

perciò

$$\|R_x(\lambda)\| = \frac{1}{\lambda} \|(e - \lambda^{-1}x)^{-1}\| < \frac{2}{\lambda},$$

cosicché R_x tende a 0 per $\lambda \rightarrow \infty$. Se $\sigma(x) = \emptyset$, allora R_x dovrebbe essere costante per il teorema di Liouville, e dunque identicamente nulla, assurdo. \square

RIFERIMENTI BIBLIOGRAFICI

- [Bur06] R. B. BURCKEL, *Fubinito (immediately) implies FTA*, American Mathematical Monthly (2006), **113**, 344–347.
- [Car95] HENRI CARTAN, *Elementary theory of analytic functions of one or several complex variables*, Dover books on mathematics, Dover Publications Inc., 1995.
- [Der03] H. DERKSEN, *The fundamental theorem of algebra and linear algebra*, American Mathematical Monthly (2003), **110**, 620–623.
- [dSOS05] J. C. DE SOUSA OLIVEIRA SANTOS, *Another proof of the fundamental theorem of algebra*, American Mathematical Monthly (2005), **112**, 76–78.
- [FR97] B. FINE E G. ROSENBERGER, *The fundamental theorem of algebra*, Springer-Verlag, 1997.
- [Hat02] ALLEN HATCHER, *Algebraic topology*, Cambridge University Press, 2002, <http://www.math.cornell.edu/~hatcher/AT/ATpage.html>.
- [Lan99] SERGE LANG, *Complex analysis (fourth edition)*, Graduate Texts in Mathematics, **103**, Springer, 1999.
- [Lei05] G. LEIBMAN, *A nonstandard proof of the fundamental theorem of algebra*, American Mathematical Monthly (2005), **112**, 705–712.
- [Mil97] JOHN W. MILNOR, *Topology from the differentiable viewpoint*, Princeton Landmarks in Mathematics, Princeton University Press, 1997.

E-mail address: a.ferretti@sns.it