NULLSTELLENSATZ PER TUTTI

MARCO MANETTI

Dedicato alla memoria di Franco Conti

Il Nullstellensatz, detto anche **teorema degli zeri di Hilbert**, è la generalizzazione in più dimensioni del teorema fondamentale dell'algebra ed è uno dei risultanti più importanti di quel ramo della matematica noto come geometria algebrica. A dispetto del nome, per noi italiani molto esotico, e del fatto che nei testi di algebra e geometria oggi in circolazione viene dimostrato usando tecniche incomprensibili agli studenti non specializzati, il teorema degli zeri di Hilbert era e resta sostanzialmente un risultato di algebretta e di algebra lineare.
Il nostro obbiettivo è quello di riportare il teorema degli zeri in questo ambito. Probabilmente lo slogan "Nullstellensatz per tutti" è più da campagna elettorale che da libro di Matematica; in ogni modo, la mia fondata speranza è quella di aver prodotto una dimostrazione comprensibile da tutti quelli che hanno seguito il primo anno di corso in una Facoltà Scientifica.
Per studiare con soddisfazione queste pagine si richiede solamente un po' di volontà e la conoscenza di alcuni fatti elementari di algebra (principio di induzione, polinomi e algoritmo di divisione euclidea) e di algebra lineare (il determinante).

1. Di cosa stiamo parlando?

Consideriamo un polinomio di grado d

$$p(z) = a_0 z^d + a_1 z^{d-1} + \ldots + a_d,$$

con coefficienti $a_0, \ldots, a_d$ numeri complessi ed $a_0 \neq 0$. Una radice di $p(z)$ è un numero complesso u tale che $p(u) = a_0 u^d + a_1 u^{d-1} + \ldots + a_d = 0$. Enunciamo un ben noto risultato.

Teorema 1 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio a coefficienti complessi di grado $d \geq 1$ possiede radici.*

Se il polinomio $p(z)$ ha grado < 1, significa che è una costante, diciamo $p(z) = c$. In questo caso $p(z)$ può avere radici (se $c = 0$) oppure può non averne affatto (se $c \neq 0$). Un risultato equivalente al teorema fondamentale dell'algebra che contempla anche il caso dei polinomi di grado < 1 è il seguente:

Teorema 2. *Un polinomio $p(z)$ a coefficienti complessi non possiede radici se e solo se esiste un polinomio $q(z)$ tale che $p(z)q(z) = 1$.*

Infatti, se esiste un polinomio $q(z)$ tale che $p(z)q(z) = 1$, allora per ogni numero complesso u vale $p(u)q(u) = 1$ e quindi $p(u)$ non può essere uguale a 0. Viceversa, se $p(z)$ non ha radici allora $p(z)$ è una costante $c \neq 0$ e, ponendo $q(z)$ il polinomio costante c^{-1} si ha $p(z)q(z) = 1$.

Il passo successivo è quello di considerare un insieme finito di polinomi $p_1(z), \ldots, p_m(z)$ a coefficienti complessi. Una radice comune è un numero complesso u tale che $p_1(u) = \ldots = p_m(u) = 0$.

Teorema 3. *Un insieme finito $p_1(z),\dots,p_m(z)$ di polinomi a coefficienti complessi non possiede radici comuni se e solo se esistono polinomi $q_1(z),\dots,q_m(z)$ a coefficienti complessi tali che*

$$p_1(z)q_1(z)+\cdots+p_m(z)q_m(z)=1.$$

Ebbene, il Nullstellensatz è l'ulteriore generalizzazione del Teorema 3 ad insiemi di polinomi in un numero qualsiasi di variabili: vediamo che cosa significa.

Indichiamo con $\mathbb{C}$ il campo dei numeri complessi e consideriamo un intero positivo $n>0$. Per ogni n-upla di numeri naturali $i_0,\dots,i_n\geq 0$. La funzione

$$z_1^{i_1}\cdots z_n^{i_n}\colon \mathbb{C}^n\to\mathbb{C},\qquad z_1^{i_1}\cdots z_n^{i_n}(a_1,\dots,a_n)=a_1^{i_1}\cdots a_n^{i_n}$$

viene detta **monomio** di grado $d=i_0+\ldots+i_n$ nelle variabili $z_1,\dots,z_n$, dove, con un leggero abuso di notazione, si intende che $a^0=1$ per ogni numero complesso a. Osserviamo che la funzione che vale costantemente 1 è l'unico monomio di grado 0 e che gli n monomi di grado 1, $z_1,\dots,z_n$ non sono altro che il sistema di coordinate canoniche sullo spazio vettoriale $\mathbb{C}^n$.

Un **polinomio** $p(z_1,\dots,z_n)$ nelle variabili $z_1,\dots,z_n$ è una funzione $p\colon\mathbb{C}^n\to\mathbb{C}$ ottenuta per combinazione lineare a coefficienti complessi di un numero finito di monomi. Sono ad esempio polinomi in z_1,z_2 le funzioni z_1z_2-2 e $z_1^3+z_2^3$.
Notiamo che i polinomi possono essere tra loro sommati e moltiplicati e che somme e prodotti di polinomi sono ancora polinomi.

Teorema 4 (Nullstellensatz)**.** *Siano $p_1(z_1,\dots,z_n),\dots,p_m(z_1,\dots,z_n)$ polinomi a coefficienti complessi. L'insieme dei vettori $(a_1,\dots,a_n)\in\mathbb{C}^n$ tali che*

$$p_1(a_1,\dots,a_n)=\cdots=p_m(a_1,\dots,a_n)=0$$

è vuoto se e solo se esistono polinomi $q_1(z_1,\dots,z_n),\dots,q_m(z_1,\dots,z_n)$ tali che

$$p_1(z_1,\dots,z_n)q_1(z_1,\dots,z_n)+\cdots+p_m(z_1,\dots,z_n)q_m(z_1,\dots,z_n)=1.$$

Se $n=m=1$ allora il Nullstellensatz si riduce al teorema fondamentale dell'algebra.

2. Una prima generalizzazione.

Il Teorema 3 è una facile conseguenza della **divisione euclidea** tra polinomi, che andiamo a ricordare.
Sia $p(z)$ un polinomio monico di grado $d\geq 0$, cioè un polinomio della forma

$$p(z)=z^d+a_1z^{d-1}+\ldots+a_d$$

(monico significa che è uguale ad 1 il coefficiente della massima potenza di z che compare in p).
Se $q(z)=b_0z^s+b_1z^{s-1}+\cdots+b_s$, $b_0\neq 0$, è un qualsiasi polinomio di grado s allora esistono unici due polinomi $h(z),r(z)$ tali che:

(1) $q(z)-h(z)p(z)=r(z)$,
(2) se $s\geq d$ allora $h(z)$ ha grado $s-d$,
(3) $r(z)$ ha grado $<d$.

Dimostriamo esistenza ed unicità di h ed r:
Esistenza: Per induzione sul grado s di $q(z)$: se $s<d$ basta considerare $h(z)=0$ e $r(z)=q(z)$. Se $s\geq d$ osserviamo che il polinomio $q'(z)=q(z)-b_0z^{s-d}p(z)$ ha grado $<s$, per l'ipotesi induttiva esistono $h'(z),r(z)$ tali che $q'(z)-h'(z)p(z)=r(z)$

e quindi $q(z) - (b_0 z^{s-d} + h'(z))p(z) = r(z)$.
Come conseguenza abbiamo il seguente lemma:

Lemma 5. *Sia*

$$p(z) = a_0 z^d + a_1 z^{d-1} + \cdots + a_d, \qquad con \quad a_0 \neq 0,$$

un polinomio non nullo di grado d. Esistono allora al più d numeri complessi $u_1, \ldots, u_d$ tali che $p(u_i) = 0$.

Dimostrazione. Induzione su d, se $d = 0$ allora $p(z) = a_0$ e quindi non ci sono radici. Sia $d > 0$ e siano per assurdo $u_1, \ldots, u_{d+1}$ radici distinte di $p(z)$. Per l'esistenza della divisione euclidea possiamo scrivere $p(z) = (z - u_{d+1})h(z) + r(z)$ con $r(z)$ di grado < 1 cioè una costante, diciamo $r(z) = c$. Dato che $c = p(u_{d+1}) = 0$ ne segue che $u_2, \ldots, u_d$ sono radici di $h(z)$, il quale ha grado $< d$; abbiamo trovato una contraddizione. □

Unicità della divisione euclidea: Supponiamo di avere $q(z) = h_1(z)p(z) + r_1(z)$, $q(z) = h_2(z)p(z) + r_2(z)$; facciamo la differenza e otteniamo $(h_1(z) - h_2(z))p(z) + (r_1(z) - r_2(z)) = 0$. Il primo membro di tale uguaglianza è quindi un polinomio che si annulla su tutti i numeri complessi e per il lemma precedente deve essere il polinomio nullo. In particolare $h_1 = h_2$ (altrimenti il polinomio avrebbe grado $\geq d$) e $r_1 = r_2$.

Possiamo adesso fare un altro passo in avanti.

Teorema 6. *Un insieme finito $p_1(z), \ldots, p_m(z)$ di polinomi a coefficienti complessi non possiede radici comuni se e solo se esistono polinomi $q_1(z), \ldots, q_m(z)$ a coefficienti complessi tali che*

$$p_1(z)q_1(z) + \cdots + p_m(z)q_m(z) = 1.$$

Dimostrazione. Indichiamo con J l'insieme di tutti i polinomi che si possono scrivere come $p_1(z)q_1(z) + \cdots + p_m(z)q_m(z)$, al variare di $q_1(z), \ldots, q_m(z)$ tra i polinomi a coefficienti complessi.
Notiamo che se u è una radice comune a $p_1(z), \ldots, p_m(z)$ allora u è radice di ogni polinomio in J. Inoltre somma e differenza di polinomi in J appartiene ancora ad J e, se $p(z) \in J$ allora si ha $h(z)p(z) \in J$ per ogni polinomio $h(z)$.
Scegliamo un polinomio $p(z) \in J - \{0\}$ non nullo e di grado minimo tra quelli appartenenti a J. A meno di moltiplicare per un numero complesso non nullo non è restrittivo assumere $p(z)$ monico; sia d il suo grado. Se $d = 0$ allora $p(z) = 1$ e $p_1(z), \ldots, p_m(z)$ non hanno radici comuni. Se $d > 1$ proviamo che $p(z)$ divide $p_1(z), \ldots, p_m(z)$; seguirà che ogni radice di $p(z)$ è una radice comune di $p_1(z), \ldots, p_m(z)$.
Sia $i = 1, \ldots, m$ un indice fissato, per la divisione euclidea esiste un polinomio $h(z)$ tale che $r(z) = p_i(z) - h(z)p(z)$ ha grado $< d$. Essendo $r(z)$ un elemento di J deve essere $r = 0$ e quindi $p(z)$ divide $p_i(z)$. □

3. Come ti elimino una variabile.

Denotiamo con il simbolo $\mathbb{C}[z_1, \ldots, z_n]$ l'insieme dei polinomi nelle variabili $z_1, \ldots, z_n$. Chiameremo **polinomio nullo** quello corrispondente alla combinazione lineare nulla di monomi.

Lemma 7. *Un polinomio $p\colon \mathbb{C}^n \to \mathbb{C}$ è nullo se e solo se $p(a_1, \ldots, a_n) = 0$ per ogni $a_1, \ldots, a_n \in \mathbb{C}$.*

Dimostrazione. Una implicazione è evidente. Viceversa se p è una combinazione lineare non nulla possiamo scrivere

$$p(z_1,\dots,z_n)=p_0(z_1,\dots,z_{n-1})z_n^d+p_1(z_1,\dots,z_{n-1})z_n^{d-1}+\cdots+p_d(z_1,\dots,z_{n-1})$$

per opportuni polinomi $p_0,\dots,p_d$ in $z_1,\dots,z_{n-1}$ non tutti nulli. Per induzione su n, esistono $a_1,\dots,a_{n-1}\in\mathbb{C}$ tali che i numeri $p_0(a_1,\dots,a_{n-1}),\dots,p_d(a_1,\dots,a_{n-1})$ non sono tutti nulli e quindi il polinomio

$$q(z)=p_0(a_1,\dots,a_{n-1})z_n^d+p_1(a_1,\dots,a_{n-1})z_n^{d-1}+\cdots+p_d(a_1,\dots,a_{n-1})$$

non è nullo. Esiste quindi $a_n\in\mathbb{C}$ tale che $p(a_1,\dots,a_n)=q(a_n)\neq 0$. □

Diremo che un polinomio p è **monico di grado** d in z_n se è possibile scrivere

$$p(z_1,\dots,z_n)=z_n^d+p_1(z_1,\dots,z_{n-1})z_n^{d-1}+\cdots+p_d(z_1,\dots,z_{n-1})$$

per opportuni polinomi $p_1,\dots,p_d$ nelle variabili $z_1,\dots,z_{n-1}$.

Con i polinomi monici in z_n come divisori, continua a valere la divisione euclidea: più precisamente, se $p(z_1,\dots,z_n)$ è un polinomio monico di grado d in z_n, per ogni $q(z_1,\dots,z_n)$ esistono, e sono unici, dei polinomi $h(z_1,\dots,z_n)$, $r_0(z_1,\dots,z_{n-1})$,…, $r_{d-1}(z_1,\dots,z_{n-1})$ tali che

$$q(z_1,\dots,z_n)-h(z_1,\dots,z_n)p(z_1,\dots,z_n)=\sum_{i=0}^{d-1}r_i(z_1,\dots,z_{n-1})z_n^i.$$

Come nel caso dei polinomi in una variabile si dimostra la divisione scrivendo

$$q(z_1,\dots,z_n)=\sum_{i=0}^{s}q_i(z_1,\dots,z_{n-1})z_n^i$$

e ragionando per induzione su s. Se $s<d$ si pone $r_i=q_i$, altrimenti si considera $q'=q-z_n^{s-d}q_sp$ che ha grado $<s$ rispetto alla variabile z_n.

Consideriamo adesso due polinomi $p(z_1,\dots,z_n)$ e $q(z_1,\dots,z_n)$, con p monico di grado d in z_n. Per la divisione euclidea esistono unici dei polinomi $h_i(z_1,\dots,z_n)$, $i=0,\dots,d-1$ e $r_{ij}(z_1,\dots,z_{n-1})$, $i,j=0,\dots,d-1$, tali che per ogni $i=0,\dots,d-1$ vale

$$z_n^iq(z_1,\dots,z_n)-h_i(z_1,\dots,z_n)p(z_1,\dots,z_n)=\sum_{j=0}^{d-1}r_{ij}(z_1,\dots,z_{n-1})z_n^j.$$

Denotiamo con $R(p,q)$ il determinante della matrice quadrata (r_{ij}). Chiameremo $R(p,q)$ il **risultante** di p e q.

In altri termini $R(p,q)\colon\mathbb{C}^{n-1}\to\mathbb{C}$ è la funzione che nel punto $(a_1,\dots,a_{n-1})\in\mathbb{C}^{n-1}$ assume come valore il determinante della matrice di coefficienti $r_{ij}(a_1,\dots,a_{n-1})$. Denotiamo con R^{ji} il determinante della matrice quadrata di ordine $d-1$, (r_{ab}), $a\neq i$, $b\neq j$, moltiplicato per $(-1)^{i+j}$. La regola di Laplace per il calcolo del determinante implica che

$$\sum_{i=0}^{d}R^{hi}r_{ij}=\begin{cases}R(p,q) & \text{se } h=j\\ 0 & \text{se } h\neq j\end{cases}$$

Da tale formula segue facilmente che $R(p,q)$ è un polinomio nelle variabili $z_1,\dots,z_{n-1}$. Infatti possiamo assumere per induzione su d che R^{0i} è un polinomio per ogni $i=0,\dots,d-1$. Ne segue che $R(p,q)=\sum_{i=0}^{d}R^{0i}r_{i0}$ è un polinomio.

Lemma 8. *Nelle notazioni precedenti esistono due polinomi $f, g \in \mathbb{C}[z_1, \ldots, z_n]$ tali che*

$$R(p, q) = fq - gp.$$

Dimostrazione. Abbiamo visto che $\sum_{i=0}^{d-1} R^{0i} r_{i0} = R(p, q)$ e $\sum_{i=0}^{d-1} R^{0i} r_{ij} = 0$ se $j > 0$. Vale allora

$$\begin{aligned} R(p,q) &= \sum_{j=0}^{d-1} \left(\sum_{i=0}^{d-1} R^{0i} r_{ij} \right) z_n^j = \sum_{i=0}^{d-1} R^{0i} \left(\sum_{i=0}^{d-1} r_{ij} z_n^j \right) \\ &= \sum_{i=0}^{d-1} R^{0i} (z_n^i q - h_i p) = \left(\sum_{i=0}^{d-1} R^{0i} z_n^i \right) q - \left(\sum_{i=0}^{d-1} R^{0i} h_i \right) p = fq - gp. \end{aligned}$$

□

Lemma 9. *Nelle notazioni precedenti, se esiste un vettore $(a_1, \ldots, a_{n-1}) \in \mathbb{C}^{n-1}$ tale che $q(a_1, \ldots, a_{n-1}, z_n)$ è identicamente uguale ad 1, allora $R(p, q)(a_1, \ldots, a_{n-1}) = 1$.*

Dimostrazione. La dimostrazione è puramente concettuale e non richiede alcun conto. L'unicità della divisione euclidea implica che, per $i < d$ fissato, il polinomio

$$\sum_{j=0}^{d-1} r_{ij}(a_1, \ldots, a_{n-1}) z_n^j$$

coincide con il resto della divisione di $z_n^i q(a_1, \ldots, a_{n-1}, z_n)$ per $p(a_1, \ldots, a_{n-1}, z_n)$ e quindi, essendo per ipotesi $z_n^i q(a_1, \ldots, a_{n-1}, z_n) = z_n^i$, vale

$$\sum_{j=0}^{d-1} r_{ij}(a_1, \ldots, a_{n-1}) z_n^j = z_n^i$$

e la matrice $(r_{ij}(a_1, \ldots, a_{n-1}))$ è la matrice identità. □

4. Ideali

Viene spontanea l'idea di utilizzare il risultante per impostare una dimostrazione del Teorema 4 per induzione su n, essendo il caso $n = 1$ esattamente il Teorema 3. Questo approccio funziona bene a condizione di lavorare con gli ideali in $\mathbb{C}[z_1, \ldots, z_n]$ anziché con le m-uple di polinomi.

Un sottoinsieme $I \subset \mathbb{C}[z_1, \ldots, z_n]$ si dice un **ideale** quando sono soddisfatte le condizioni:

(1) se $f, g \in I$ allora $f + g \in I$.
(2) se $f \in I$, $h \in \mathbb{C}[z_1, \ldots, z_n]$ allora $fh \in I$.

Ad esempio 0 e $\mathbb{C}[z_1, \ldots, z_n]$ sono ideali. Più in generale, se $p_1, \ldots, p_m$ sono polinomi in $\mathbb{C}[z_1, \ldots, z_n]$, allora l'insieme J di tutte le espressioni $p_1 q_1 + \ldots + p_m q_m$, al variare di $q_1, \ldots, q_m \in \mathbb{C}[z_1, \ldots, z_n]$, è un ideale.
Se ne deduce che il Teorema 4 è una conseguenza immediata del seguente Teorema 10

Teorema 10. *Sia $J \subset \mathbb{C}[z_1, \ldots, z_n]$ un ideale: esiste un vettore $(a_1, \ldots, a_n) \in \mathbb{C}^n$ tale che $p(a_1, \ldots, a_n) = 0$ per ogni $p \in J$ se e solo se $1 \notin J$.*

Dimostrazione. Dimostriamo il teorema per induzione su n, essendo il caso $n = 0$ banalmente verificato. Supponiamo quindi vero il teorema per polinomi in $n-1$ variabili.
L'enunciato è ovvio se $1 \in J$ oppure se $J = 0$; assumiamo quindi $J \neq 0$, $1 \notin J$ e proviamo che esiste un vettore $(a_1, \ldots, a_n)$ che annulla tutti gli elementi di J.
Dimostriamo preliminarmente tale fatto sotto l'ulteriore ipotesi che J contenga un polinomio p_0 monico di grado $d > 0$ in z_n; vedremo in un secondo momento in che modo tale ipotesi aggiuntiva può essere rimossa.
Consideriamo l'intersezione $I = J \cap \mathbb{C}[z_1, \ldots, z_{n-1}]$, si tratta di un ideale di $\mathbb{C}[z_1, \ldots, z_{n-1}]$, $1 \notin I$ e, per il Lemma 8, I contiene tutti i risultanti $R(p_0, q)$, al variare di $q \in J$.
Per l'ipotesi induttiva esiste un vettore $(a_1, \ldots, a_{n-1})$ che annulla tutti gli elementi di I. Denotiamo con $u_1, \ldots, u_s \in \mathbb{C}$, $s \leq d$, le radici del polinomio $p_0(a_1, \ldots, a_{n-1}, z_n) \in \mathbb{C}[z_n]$ e proviamo che esiste un indice j tale che $(a_1, \ldots, a_{n-1}, u_j)$ annulla tutti gli elementi di J. Se cosi non è, esistono $p_1, \ldots, p_s \in J$ tali che $p_j(a_1, \ldots, a_{n-1}, u_j) \neq 0$ per ogni j. Gli $s+1$ polinomi $p_j(a_1, \ldots, a_{n-1}, z_n)$, $j = 0, \ldots, s$ non hanno radici comuni e quindi, per il Teorema 3 esistono $h_0, \ldots, h_s \in \mathbb{C}[z_n]$ tali che

$$\sum_{j=0}^{s} h_j(z_n) p_j(a_1, \ldots, a_{n-1}, z_n) = 1.$$

Interpretando gli h_j come polinomi in $z_1, \ldots, z_n$ e ponendo $q = \sum h_i p_i \in J$ si ha, per il Lemma 9, $q(a_1, \ldots, a_{n-1}, z_n) = 1$ e quindi $R(p_0, q)(a_1, \ldots, a_{n-1}) = 1$ in contraddizione con il fatto che $R(p_0, q) \in I$.
Vediamo adesso in che modo possiamo rimuovere la condizione che J contenga un polinomio monico in z_n. Osserviamo per correttezza che tale ipotesi non è sempre verificata, non è soddisfatta ad esempio dall'ideale di tutti i polinomi in $\mathbb{C}[z_1, z_2]$ divisibili per z_1.
Se J contiene un polinomio monico di grado positivo in una qualche variabile z_i, $i = 1, \ldots, n$ il problema si risolve semplicemente permutando gli indici. Tuttavia questo può non bastare.
Si consideri a titolo di esempio l'ideale $J \subset \mathbb{C}[z_1, z_2]$ di tutti i polinomi che sono divisibili per $g = z_1 z_2 - 1$. Nessun polinomio di J è monico rispetto ad una variabile. Possiamo ovviare all'inconveniente con il cambio di coordinate $z_1 = x + y$, $z_2 = x - y$; il polinomio g diventa $x^2 - y^2 - 1$ che è monico di grado 2 in x.
Il trucco appena visto si può generalizzare e dimostrare che a meno di un cambio lineare di coordinate ogni ideale non nullo contiene un polinomio monico nella variabile z_n; si può ragionare nel modo seguente.
Sia $f \colon \mathbb{C}^n \to \mathbb{C}^n$ un'applicazione lineare invertibile, se $p \colon \mathbb{C}^n \to \mathbb{C}$ è un polinomio, la funzione

$$f^*p \colon \mathbb{C}^n \to \mathbb{C}, \qquad f^*p(a_1, \ldots, a_n) = p(f(a_1, \ldots, a_n))$$

è ancora un polinomio. Infatti, se f è rappresentata dalla matrice (f_{ij}), si ha $f^* z_i = \sum_j f_{ij} z_j$ e quindi

$$f^*p(z_1, \ldots, z_n) = p\left(\sum_j f_{1j} z_j, \ldots, \sum_j f_{nj} z_j \right).$$

Notiamo inoltre che f^* commuta con le operazioni di somma e prodotto, cioè

$$f^*(p+q) = f^*p + f^*q, \qquad f^*(pq) = (f^*p)(f^*q)$$

e quindi se $J \subset \mathbb{C}[z_1, \ldots, z_n]$ è un ideale allora anche $f^*(J)$ è un ideale. L'applicazione $f^* \colon \mathbb{C}[z_1, \ldots, z_n] \to \mathbb{C}[z_1, \ldots, z_n]$ è invertibile con inversa $(f^{-1})^*$; inoltre $f^*1 = 1$ ed un vettore u annulla tutti gli elementi di $f^*(J)$ se e solo se $f(u)$ annulla tutti gli

elementi di J. In conclusione possiamo affermare che se il teorema degli zeri vale per un ideale J allora vale anche per tutti gli ideali $f^*(J)$ al variare di f tra le applicazioni lineari invertibili.
Basta quindi dimostrare che, per ogni ideale $J \neq 0$ esiste una f come sopra tale che l'ideale $f^*(J)$ contiene un polinomio monico di grado positivo in z_n. Prendiamo un qualsiasi polinomio non nullo $q \in J$ e scriviamo $q = q_0 + q_1 + \cdots + q_d$, dove q_i è una combinazione lineare di monomi di grado i e $q_d \neq 0$.
Per il Lemma 7 esiste un vettore $u \in \mathbb{C}^n$ tale che $q_d(u) \neq 0$. A meno di moltiplicare q per una costante non nulla possiamo supporre $q_d(u) = 1$. Se $d = 0$ allora $1 \in J$ e non c'è nulla da dimostrare; se $d > 0$ allora necessariamente $u \neq 0$ ed esiste $f\colon \mathbb{C}^n \to \mathbb{C}^n$ lineare invertibile tale che $f(0, \ldots, 0, 1) = u$, ovvero u coincide con l'ultimo vettore colonna della matrice che rappresenta f. Proviamo che f^*q è un polinomio monico di grado d in z_n. Infatti ogni f^*q_i è una combinazione lineare di monomi di grado i e possiamo scrivere

$$f^*q_d(z_1, \ldots, z_n) = a_0(z_1, \ldots, z_{n-1})z_n^d + a_1(z_1, \ldots, z_{n-1})z_n^{d-1} + \cdots + a_d(z_1, \ldots, z_{n-1})$$

dove ogni a_i è una combinazione lineare di monomi di grado i. Basta quindi dimostrare che la costante a_0 è uguale a 1, per fare questo valutiamo f^*q_d nel punto $(0, \ldots, 0, 1)$ e otteniamo

$$a_0 = f^*q_d(0, \ldots, 0, 1) = q_d(f(0, \ldots, 0, 1)) = q_d(u) = 1.$$

Questo conclude la dimostrazione. □

5. Das is nicht mathematische - das ist theologie!

Questa frase, divenuta celebre, fu pronunciata da Gordan, algebrista leader nella Germania del 1890, in riferimento al lavoro del giovane Hilbert, lavoro in cui venivano enunciati e dimostrati due tra i più importanti teoremi di algebra, quelli che oggi vengono chiamati il **teorema della base** ed il teorema degli zeri.
Nella monografia di Hilbert, questi due risultati erano preparatori alla sua dimostrazione del teorema di finitezza degli invarianti, teorema che generalizzava e semplificava enormemente quello che Gordan aveva fatto venti anni prima.
Il motto stizzoso di Gordan era motivato, oltre che dall'invidia professionale, dal fatto che le dimostrazioni di Hilbert non erano costruttive, si limitavano a dimostrare l'esistenza di certi oggetti ma non davano nessun algoritmo utile alla loro descrizione esplicita.
Il teorema della base di Hilbert afferma che, per ogni ideale J di $\mathbb{C}[z_1, \ldots, z_n]$ esiste un insieme finito di polinomi $p_1, \ldots, p_m \in J$ tali che J coincide con l'insieme di tutte le espressioni $p_1q_1 + \cdots + p_mq_m$ al variare di $q_1, \ldots, q_m \in \mathbb{C}[z_1, \ldots, z_n]$. Quindi, in virtù del teorema della base, i Teoremi 4 e 10 sono perfettamente equivalenti.
L'enunciato dato da Hilbert del teorema degli zeri comprendeva al suo interno sia il teorema della base sia quella che oggi viene detta **forma forte del teorema degli zeri**, una ulteriore generalizzazione del Teorema 4 che recita così:

Teorema 11 (Hilbert; vedi [3])**.** *Sia J un ideale di $\mathbb{C}[z_1, \ldots, z_n]$ e denotiamo con $V(J) \subset \mathbb{C}^n$ l'insieme dei vettori che annullano tutti gli elementi di J. Esiste allora un intero $d > 0$, dipendente da J, tale che se $f \in \mathbb{C}[z_1, \ldots, z_n]$ si annulla su $V(J)$ allora $f^d \in J$.*

Omettiamo la, seppur semplice ed elementare, dimostrazione di questo teorema come conseguenza del Teorema 10 e del teorema della base: la si può trovare scritta quasi ovunque (vedi ad esempio [1], [4], [5] e [6]).

Il lettore attento si sarà accorto che nella dimostrazione del teorema degli zeri non è stata usata nessuna proprietà dei numeri complessi, oltre ovviamente a quella di essere un campo algebricamente chiuso: considerando al posto di $\mathbb{C}$ un qualsiasi campo algebricamente chiuso i Teoremi 10 e 11 continuano ad essere validi.
Per finire, alcuni commenti sulla bibliografia. Citare tutti i libri che contengono dimostrazioni del Nullstellensatz sarebbe un'impresa titanica; ci limitiamo quindi ad una lista parziale ma significativa. I testi [1], [4], [5] e [6] sono manuali introduttivi alla geometria algebrica, dove si possono trovare le più svariate applicazioni alla geometria dei teoremi di Hilbert. Il libro [3] non è ovviamente stato scritto da Hilbert, che nel 1993 non era più in grado di dedicarsi alla Matematica terrena, ma è la revisione degli appunti presi a lezione da uno studente dei corsi che Hilbert teneva all'Università di Gottinga nel decennio 1890-1900. Il libro di Herstein [2] contiene tutto quello che serve per la comprensione di queste note (e molto di più).

Riferimenti bibliografici

[1] W. Fulton: *Algebraic Curves: an introduction to algebraic geometry.* Benjamin (1969).
[2] I.N. Herstein: *Algebra.* Editori Riuniti (1982).
[3] D. Hilbert: *Theory of algebraic invariants.* Cambridge Univ. Press (1993).
[4] M. Manetti: *Corso introduttivo alla Geometria Algebrica.* Appunti dei corsi tenuti dai docenti della Scuola Normale Superiore (1998) 1-247.
[5] M. Reid: *Undergraduate algebraic geometry.* Cambridge Univ. Press (1988).
[6] I.R. Shafarevich: *Basic algebraic geometry.* Springer-Verlag (1972).

Dipartimento di Matematica Guido Castelnuovo,
Università di Roma "La Sapienza",
Piazzale Aldo Moro 5, I-00185 Roma, Italy.
URL: `http://www.mat.uniroma1.it/people/manetti/`
E-mail address: `manetti@mat.uniroma1.it`