PALESTRA MATEMATICA DEL 3 E 10 NOVEMBRE 2003

MARCO MANETTI

Minicorso intensivo di geometria algebrica in 9 minilezioni e 33 e più esercizi.
Per gli studenti del ≥terzo anno del corso di Laurea in Matematica

INDICE

1. Come si risolve l'equazione di terzo grado?

Il nostro primo obiettivo è quello di trovare un metodo per risolvere per radicali l'equazione di terzo grado: lo faremo in due modi, il primo semplice ed elegante, il secondo un po' meno ma con il vantaggio di generalizzarsi facilmente alla risoluzione delle equazioni di quarto grado.

Consideriamo un polinomio $f(x) = x^3 + 3a_1x^2 + 3a_2x + a_3 \in \mathbb{C}[x]$ di terzo grado a coefficienti complessi. A meno di sostituire x con $x - a_1$ non è restrittivo supporre $a_1 = 0$ e quindi $f(x) = x^3 + 3a_2x + a_3$.
Sia $f'(x) = 3x^2 + 3a_2$ la derivata di f e consideriamo tre casi distinti:

1. $a_2 = 0$.
2. f ed f' hanno una radice in comune.
3. f ed f' non hanno radici in comune.

Il primo caso lo sappiamo risolvere. Nel secondo caso, dato che

$$f(x) - \frac{x}{3}f'(x) = 2a_2x + a_3$$

se $\alpha \in \mathbb{C}$ è una radice di f ed f', allora $2a_2\alpha + a_3 = 0$ e quindi $\alpha = -\dfrac{a_3}{2a_2}$.

Se f ed f' non hanno radici comuni, allora cerchiamo tre numeri complessi t, n, m tali che

$$x^3 + 3a_2x + a_3 = t(x - n)^3 + (1 - t)(x - m)^3,$$

ossia cerchiamo di risolvere il sistema

$$\begin{cases} tn + (1-t)m &= 0 \\ tn^2 + (1-t)m^2 &= a_2 \\ tn^3 + (1-t)m^3 &= -a_3 \end{cases}$$

Esercizio 1. Mostrare che se f ed f' non hanno radici in comune, allora non esiste alcuna soluzione del precedente sistema con $n = m$. △

Dato che non $n-m\neq 0$, possiamo ricavare il valore di t dalla prima equazione e sostituirlo nelle altre due; semplificando si ottiene

$$\begin{cases} \dfrac{m}{m-n} &= t \\ nm &= -a_2 \\ \dfrac{mn^3-nm^3}{m-n} &= -a_3 \end{cases}$$

Mettendo nella terza equazione $-a_2$ al posto di nm e semplificando si ottiene

$$\begin{cases} \dfrac{m}{m-n} &= t \\ nm &= -a_2 \\ n+m &= -\dfrac{a_3}{a_2} \end{cases}$$

Si tratta di un sistema di secondo grado simmetrico dal quale si può ricavare n, m e t. Le radici di f sono quindi le radici dell'equazione

$$\left(\frac{x-n}{x-m}\right)^3=\frac{t-1}{t}=\frac{n}{m}$$

che si calcolano esattamente e, fissate due radici cubiche $\sqrt[3]{m}$, $\sqrt[3]{n}$ di m e n rispettivamente, sono date dalla formula:

$$\alpha_i=\frac{m\sqrt[3]{n}-n\xi^i\sqrt[3]{m}}{\sqrt[3]{n}-\xi^i\sqrt[3]{m}},\qquad i=0,1,2$$

dove ξ è una radice primitiva cubica di 1.

Esercizio 2. Mostrare che, se f ed f' hanno radici in comune, allora la precedente equazione risolutiva degenera alla forma $\alpha_i=\dfrac{0}{0}$. △

2. Come facciamo a sapere se due polinomi hanno una radice in comune?

Ovviamente calcolando il loro massimo comune divisore tramite l'algoritmo della divisione Euclidea. Per future applicazioni vogliamo codificare questo algoritmo mediate formule universali.

Consideriamo due polinomi, il primo dei quali monico, $f=x^n+a_1x^{n-1}+\cdots+a_n$, $g=b_0x^m+\cdots+b_m$ a coefficienti in un campo $\mathbb{K}$. Indichiamo con $(f)\subset\mathbb{K}[x]$ l'ideale generato da f e con $V=\mathbb{K}[x]/(f)$ l'anello quoziente. Come spazio vettoriale su $\mathbb{K}$, V ha dimensione n ed ha come base le classi di $1,x,\dots,x^{n-1}$ (perché?).

Definizione 2.1. Il *risultante dell'eliminazione di x da f e g*, si indica con $R_x(f,g)$ ed è il determinante dell'applicazione lineare $g\colon V\to V$ indotta dalla moltiplicazione per g.

In altri termini, per ogni $j=0,\dots,n-1$ esistono unici un polinomio $h_j\in\mathbb{K}[x]$ ed n coefficienti $m_{0j},m_{1j},\dots$ tali che

$$x^jg=h_jf+\sum_{i=0}^{n-1}m_{ij}x^i$$

e $R_x(f,g)=\det(m_{ij})$ (perché?).

Il risultante dipende polinomialmente dai coefficienti a_i,b_j. Inoltre i coefficienti m_{ij} dipendono linearmente da g e quindi $R_x(f,g)$ è un polinomio omogeneo di grado n in $b_0,\dots,b_m$.

Lemma 2.2. *Siano f e g come sopra. Allora vale $R_x(f,g)=0$ se e soltanto se f e g hanno un fattore comune di grado positivo in x.*

Dimostrazione. Il risultante si annulla se e soltanto se l'applicazione $g\colon V \to V$ non è iniettiva, ossia se e soltanto se esiste un polinomio $h \neq 0$ di grado $< n$ tale che $hg \in (f)$, o per meglio dire se e soltanto se almeno uno dei fattori irriducibili di f divide g. □

Osserviamo che se $g = b_0$ è il polinomio costante, allora la matrice m_{ij} è diagonale con $m_{ii} = b_0$ per ogni i e quindi $R_x(f, g) = b_0^n$.

Esercizio 3. Sia f un polinomio monico di grado n. Provare che:

1. Se $g = x$, allora $R_x(f, g) = (-1)^n f(0) = (-1)^n a_n$.
2. $R_x(f, g_1 g_2) = R_x(f, g_1) R_x(f, g_2)$
3. Per ogni $a \in \mathbb{K}$ siano $f_a(x) = f(x + a)$, $g_a(x) = g(x + a)$. Allora $R_x(f_a, g_a) = R_x(f, g)$ (Sugg.: prendere come base di V i polinomi $(x + a)^i$).
4. Se $g(x) = b_0 \prod_{i=1}^m (x - \beta_i)$, allora $R_x(f, g) = (-1)^{nm} b_0^n \prod_{i=1}^m f(\beta_i)$.

△

Il risultante $R_x(f, f')$ prende il nome di *discriminante di* f e si indica $\Delta(f)$.

Esercizio 4. Mostrare che il discriminante del polinomio $x^3 - px - q$ è uguale a $27q^2 - 4p^3$. △

Esercizio 5. Sia $f \in \mathbb{C}[x]$ un polinomio monico a coefficienti complessi. Provare che f ha una radice multipla se e soltanto se $\Delta(f) = 0$. △

Esercizio 6. Sia $q \in \mathbb{C}[x_{11}, \ldots, x_{nn}]$ un polinomio non nullo in n^2 variabili. Dimostrare che esiste una matrice diagonalizzabile (a_{ij}) a coefficienti complessi tale che $q(a_{ij}) \neq 0$. △

3. Come si risolve l'equazione di quarto grado?

L'idea è, dato un polinomio monico $f(x)$ di grado n a coefficienti complessi, cercare un polinomio di secondo grado $g(x) = ax^2 + bx + c$ avente almeno una radice in comune con f. Se riusciamo nell'impresa, facciamo la divisione Euclidea $f = hg + r$ e proseguiamo come nel caso $n = 3$, $g = f'$ visto precedentemente.

Per impostare il problema in maniera algebrica consideriamo il polinomio

$$F(a, b, c) = R_x(f, ax^2 + bx + c)$$

e cerchiamo tre coefficienti a, b, c, non tutti nulli, tali che $F(a, b, c) = 0$.
La fregatura è che anche il polinomio F ha grado n e quindi non abbiamo fatto molta strada. Fortunatamente, nei casi $n = 3$ e $n = 4$ possiamo ricondurre il polinomio F ad un polinomio che sappiamo risolvere. Poniamo infatti $Q(a, b, c, t) = F(a, b, c+t)$; il polinomio Q è omogeneo di grado n e possiamo scrivere

$$Q = \sum_{i=0}^{n} Q_i(a, b, c) t^{n-i}$$

dove ogni Q_i è omogeneo di grado i. Notiamo incidentalmente che $Q(a, b, c, -t)$ è il polinomio caratteristico della moltiplicazione per $ax^2 + bx + c$ in $\mathbb{C}[x]/(f)$. Inoltre $Q(0, 0, c, t) = (c + t)^n$ e quindi $Q_i(0, 0, c) = \binom{n}{i} c^i$. In particolare si ha $Q_1(a, b, c) = \alpha' a + \beta' b + nc$ e quindi esistono $\alpha, \beta \in \mathbb{C}$ tali che $Q_1(a, b, c) = 0$ se e solo se $c = \alpha a + \beta b$.
Se $n = 3$, allora il polinomio $Q_2(a, b, \alpha a + \beta b)$ è omogeneo di grado 2 e sappiamo risolverlo; riusciamo quindi a trovare una terna (a, b, c), con a, b non entrambi nulli, tale che

$$Q(a, b, c, t) = t^3 + Q_3(a, b, c).$$

La quaterna $(a, b, c, t = -\sqrt[3]{Q_3(a, b, c)})$ annulla Q e quindi il polinomio $g(x) = ax^2 + bx + c + t$ ha grado 1 o 2 ed ha una radice in comune con f.
Se $n = 4$ si procede similmente; il polinomio $Q_3(a, b, \alpha a + \beta b)$ è omogeneo di grado 3 e sappiamo risolverlo per radicali. Esiste quindi una terna a, b, c, con a, b non entrambi nulli, tale che $Q = t^4 + Q_2(a, b, c)t^2 + Q_4(a, b, c)$.
Il polinomio Q è diventato biquadratico e sappiamo risolverlo per radicali.

Molti matematici si sono rotti le corna cercando trucchi simili per $n \geq 5$. Oggi sappiamo che tali trucchi non hanno effetto ed infatti, uno dei teoremi più importanti di *Teoria di Galois* afferma che *per ogni $n \geq 5$, non è possibile risolvere per radicali la generica equazione di grado n.*

Il polinomio $Q(a, b, c, t)$ viene detto il *Trasformato di Tschirnhausen* di f ed è stato apparentemente introdotto nel 1861 nell'ambito della *Teoria Algebrica degli Invarianti*.

4. Il teorema di Cayley-Hamilton.

Nella sua forma più generale, il teorema di Cayley-Hamilton recita come segue:

Teorema 4.1. *Sia $A = (a_{ij})$ una matrice quadrata a coefficienti in un anello commutativo R con unità e denotiamo con $p_A = \det(tI - A) \in R[t]$ il suo polinomio caratteristico. Allora vale $p_A(A) = 0$.*

Se R è un campo, allora il Teorema 4.1 si riconduce alla versione solitamente esposta nei corsi di algebra lineare. Daremo qui le tracce di due diverse dimostrazioni del teorema, lasciando al lettore il compito di completare i dettagli della sua preferita.

Prima dimostrazione. Sia n l'ordine della matrice A, allora $M = R^n$ possiede una struttura di $R[t]$-modulo ponendo la moltiplicazione per t uguale all'azione dell'endomorfismo indotto dalla matrice A. Bisogna dimostrare che $p_A e_i = 0$ per ogni i, dove $e_1, \dots, e_n$ è la base canonica di M; osserviamo che in tale base si ha $te_j = \sum_i a_{ij} e_i$.

Consideriamo la matrice $B = b_{ij} = t\delta_{ij} - a_{ij}$ a coefficienti in $R[t]$; notiamo che $\det(B) = p_A$ e che B induce un morfismo di $R[t]$-moduli $B\colon M^n \to M^n$ con la regola del prodotto riga per colonne

$$(m_1, \dots, m_n) \mapsto (m_1, \dots, m_n)B, \qquad m_i \in M.$$

Per come abbiamo definito B, vale $(e_1, \dots, e_n)B = 0$.
Sia ora $\tilde{B}$ la matrice aggiunta di B, ossia la matrice di coefficienti $\tilde{b}_{ij} = (-1)^{i+j} \det B_{ji}$ dove B_{ji} è la sottomatrice di ordine $n-1$ ottenuta cancellando la riga j e la colonna i. Osserviamo che se B fosse invertibile, allora $\tilde{B}$ sarebbe uguale a $\det(B)B^{-1}$.
Dallo sviluppo di Laplace per il calcolo del determinante segue $B\tilde{B} = \det(B)I$ e quindi

$$(p_A e_1, \dots, p_A e_n) = (e_1, \dots, e_n) \det(B) I = (e_1, \dots, e_n) B\tilde{B} = 0\tilde{B} = 0.$$

Seconda dimostrazione. Per ogni n fissato, è sufficiente dimostrare il teorema per l'anello $\mathbb{Z}[x_{11}, \dots, x_{nn}]$ dei polinomi a coefficienti interi in n^2 variabili e la matrice X di coefficienti x_{ij}. Infatti per ogni anello R ed ogni matrice A a coefficienti $a_{ij} \in R$ esiste un unico omomorfismo di anelli $\phi\colon \mathbb{Z}[x_{ij}] \to R$ tale che $\phi(x_{ij}) = a_{ij}$; di conseguenza $\phi(X) = A$ e $\phi(p_X(X)) = p_A(A)$.
Sia $(y_{ij}) = p_X(X)$ e supponiamo per assurdo $y_{lk} \neq 0$ per qualche l, k. È allora possibile trovare un omomorfismo di anelli $\psi\colon \mathbb{Z}[x_{ij}] \to \mathbb{C}$ tale che $\psi(y_{lk}) \neq 0$ e tale che la matrice $\psi(X) \in M(n, n, \mathbb{C})$ sia diagonalizzabile. Infatti è sufficiente definire $\psi(x_{ij}) = a_{ij}$, dove a_{ij} è una n^2-upla di numeri complessi che non annulla né il polinomio y_{lk} né $\Delta(p_X)$, essendo $\Delta(p_X) \in \mathbb{Z}[x_{ij}]$ il discriminante del polinomio caratteristico di X. Dunque la matrice complessa $A = (a_{ij})$ ha tutti gli autovalori distinti (perché?), quindi diagonalizzabile e banalmente soddisfa l'equazione $p_A(A) = 0$.

Esercizio 7. Tappare i buchi lasciati nelle due dimostrazioni di Cayley-Hamilton. △

5. Il risultante, ripetutamente.

La definizione del risultante $R_x(f, g)$ data precedentemente si estende senza difficoltà quando i polinomi f e g sono a coefficienti in un anello commutativo con identità A. Siano infatti $f, g \in A[x]$ con $f = x^n + a_1 x^{n-1} + \cdots + a_n$ monico di grado $n > 0$.

Per ogni $j = 0, \dots, n-1$ esistono unici (perché?) un polinomio $h_j \in A[x]$ ed n coefficienti $m_{0j}, m_{1j}, \dots \in A$ tali che

$$x^j g = h_j f + \sum_{i=0}^{n-1} m_{ij} x^i.$$

Si definisce quindi $R_x(f,g) = \det(m_{ij}) \in A$.

Teorema 5.1. *Nelle notazioni precedenti esistono polinomi $F, G \in A[x]$ tali che $\deg F < \deg f = n$, $\deg G < \deg g$ e $R_x(f,g) = Fg + Gf$. In particolare $R_x(f,g) \in A \subset A[x]$ appartiene all'ideale generato da f e g.*

Dimostrazione. Sia $(\tilde{m}_{ij})$ la matrice aggiunta di (m_{ij}). Per lo sviluppo di Laplace del determinante si ha $\sum_j m_{ij}\tilde{m}_{j0} = \delta_{i0} R_x(f,g)$ e quindi

$$R_x(f,g) = \sum_{i,j} x^i m_{ij} \tilde{m}_{j0} = \sum_j (x^j g - h_j f)\tilde{m}_{j0} = Fg + Gf,$$

dove $F \in A[x]$ ha grado $< n$. Poiché f è monico, il grado di G deve essere uguale a $\deg F + \deg g - n$ e quindi $\deg G < \deg g$. □

Corollario 5.2. *Nelle notazioni precedenti, se A è un dominio di integrità e se f e g hanno un fattore comune di grado positivo in x allora $R_x(f,g) = 0$.*

Dimostrazione. Se h divide f e g, allora divide tutti gli elementi dell'ideale da essi generato. □

Corollario 5.3. *Nelle notazioni precedenti, se A è un dominio di integrità a fattorizzazione unica e $R_x(f,g) = 0$ allora f e g hanno un fattore comune di grado positivo in x.*

Dimostrazione. Per il Lemma 2.2, se il risultante si annulla, allora f e g hanno un fattore comune di grado positivo a coefficienti nel campo delle frazioni di A. Basta adesso applicare il lemma di Gauss. □

Esercizio 8. Trovare l'errore nella seguente dimostrazione di 5.3: Se $R = 0$ allora, per il Teorema 5.1 si ha $Fg + Gf = 0$ e quindi f divide Fg. Poiché F ha grado $< n$ almeno un fattore irriducibile di f deve dividere g. △

6. Esercizi

Esercizio 9. Siano A un anello commutativo con identità e $n, m \in \mathbb{N}$ fissati. Per ogni coppia di polinomi $f, g \in A[x]$, $f(x) = a_0 x^n + \cdots + a_n$, $g(x) = b_0 x^m + \cdots + b_m$ di gradi $\le n$ e $\le m$ rispettivamente. Si dice matrice di Sylvester di f e g la seguente matrice quadrata di ordine $n + m$

$$S_{n,m}(f,g) = \begin{pmatrix}
a_0 & a_1 & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot & a_n & & & \\
 & a_0 & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & a_n & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & a_0 & a_1 & a_2 & \cdots & \cdot & \cdot & \cdot & \cdots & a_n \\
b_0 & b_1 & \cdots & \cdot & b_m & & & & & & & \\
 & b_0 & \cdots & \cdot & \cdot & b_m & & & & & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & & & & & \\
 & & & b_0 & b_1 & b_2 & \cdots & b_m & & & & \\
 & & & & b_0 & b_1 & \cdots & \cdot & b_m & & & \\
 & & & & & b_0 & \cdots & \cdot & \cdot & b_m & & \\
 & & & & & & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & & & & & b_0 & b_1 & b_2 & \cdots & b_m
\end{pmatrix}$$

Dimostrare che se $a_0 = 1$, allora $\det S_{n,m}(f,g) = R_x(f,g)$. Dedurre che se anche $b_0 = 1$, allora $R_x(f,g) = (-1)^{nm} R_x(g,f)$. △

Il risultante $R(f,g)$ di due polinomi omogenei $f,g\in A[x,y]$ di gradi n,m si definisce come il determinante della matrice di Sylvester associata, dove $f(x)=a_0x^n+a_1x^{n-1}y+\cdots+a_ny^n$, $g(x)=b_0x^m+\cdots+b_my^m$.

Esercizio 10. Provare che due polinomi omogenei $f,g\in\mathbb{K}[x,y]$, con $\mathbb{K}$ campo, hanno un fattore comune se e solo se $R(f,g)=0$. △

Esercizio 11. Consideriamo il generico polinomio monico di grado n $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ e indichiamo $\Delta(f)\in\mathbb{Z}[a_1,\dots,a_n]$ il suo discriminante. Dimostrare:

1. $\Delta(f)$ è un polinomio di grado $2n-2$ (Sugg.: si considerino le due forme binarie $p=a_0x^n+\cdots+a_ny^n$, $q=\dfrac{\partial p}{\partial x}$ e provare che a_0^2 non divide $R(p,q)$.)
2. Siano $\alpha_1,\dots,\alpha_n$ le radici, contate con molteplicità, di f in una opportuna estensione di $\mathbb{Z}[a_1,\dots,a_n]$. Dimostrare che
$$\Delta(f)=\prod_{i\neq j}(\alpha_i-\alpha_j).$$
3. Siano $a\in\mathbb{C}$ e $g(x)\in\mathbb{C}[x]$ un polinomio monico di grado $n-2$ tale che $g(a)\neq 0$. Provare che $\delta(t)=\Delta(((x-a)^2+t)g(x))$ ha una radice semplice per $t=0$.
4. Dimostrare che $\Delta(f)$ non è una potenza di un polinomio in $\mathbb{C}[a_1,\dots,a_n]$.

△

Esercizio 12. Sia A una matrice $n\times n$ invertibile su di un campo $\mathbb{K}$. Dimostrare che si può trovare un polinomio $p\in\mathbb{K}[x]$ di grado $<n$ tale che $A^{-1}=p(A)$. △

Esercizio 13. Sia $S(f,g)$ la matrice di Sylvester di due forme binarie f,g di gradi n,m. Provare che se f,g hanno un fattore comune di grado r allora la dimensione del nucleo di $S(f,g)$ è almeno r. △

Esercizio 14. Siano $f,g,q\in\mathbb{K}[x]$ polinomi monici senza fattori comuni di gradi n,n,m con $m<n$. Si provi che $R(f+\lambda q,g+\mu q)\in\mathbb{K}[\lambda,\mu]$ è un polinomio di grado $\leq n$. (Sugg.: non è restrittivo supporre $\mathbb{K}$ algebricamente chiuso, si considerino allora gli omomorfismi $\mathbb{K}[\lambda,\mu]\to\mathbb{K}[t]$ dati da $\lambda\to at$, $\mu\to bt$, al variare di $a,b\in\mathbb{K}$.) △

Esercizio 15. (Lemma di Gauss rivisitato)
Sia S un dominio a fattorizzazione unica e $M\in M(n,m,S)$ una matrice a coefficienti in S. Diremo che M è *primitiva* se i determinanti delle sottomatrici quadrate di ordine massimo non sono tutti nulli e non hanno fattori comuni. Diremo che un vettore $a\in S^n=M(n,1,S)$ è primitivo se è primitivo come matrice. Provare:

1. $M\in M(n,m,S)$ è primitiva se e solo se per ogni irriducibile $f\in S$, detto F il campo delle frazioni di $S/(f)$, l'immagine di M in $M(n,m,F)$ ha rango massimo.
2. Se M come sopra è primitiva e $m\leq n$, allora l'applicazione $M\colon S^m\to S^n$ è iniettiva e manda vettori primitivi in vettori primitivi. È vero il viceversa?
3. Sia $m>0$ un intero fissato. Un polinomio $\sum_{i=0}^n a_it^i\in S[t]$ è primitivo se e solo se la matrice
$$M=(M_{ij}=a_{i-j})=\begin{pmatrix}a_0&a_1&\cdots&a_n&0&\cdots&0\\0&a_0&\cdots&\cdot&a_n&\cdots&0\\\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\end{pmatrix}\in M(m,n+m,S)$$
è primitiva.
4. Dedurre il lemma di Gauss classico (ossia che il prodotto di polinomi primitivi è primitivo) dai punti precedenti.

△

Esercizio 16. Sotto quali condizioni sul campo $\mathbb{K}$ è vero il seguente risultato? *Sia A una matrice $n\times n$ a coefficienti in $\mathbb{K}$ tale che*
$$\text{Traccia}(A)=\text{Traccia}(A^2)=\cdots=\text{Traccia}(A^n)=0.$$
Allora A è nilpotente. △

Esercizio 17. Siano A, B matrici quadrate di ordine $n \geq 2$ a coefficienti in $\mathbb{C}$. Se B ha tutti gli autovalori distinti, provare che $A + sB$ non è diagonalizzabile per al più $n(n-1)$ valori di $s \in \mathbb{C}$. Verificare direttamente la stima nel caso

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Assumendo $AB = BA$ oppure A, B triangolari superiori, come si può migliorare il risultato? △

7. La Topologia di Zariski.

Da ora in poi, salvo avviso contrario, denoteremo con $\mathbb{K}$ un campo algebricamente chiuso.

Esercizio 18. Provare che $\mathbb{K}$ contiene infiniti elementi. △

Ricordiamo che, dare una topologia su di un insieme X, significa dare una famiglia $\mathcal{C}$ di sottoinsiemi di X, detti i *chiusi di* X che soddisfa gli assiomi:

1. $\emptyset, X \in \mathcal{C}$.
2. Unione finita di elementi di $\mathcal{C}$ appartiene ancora a $\mathcal{C}$.
3. Intersezione arbitraria di elementi di $\mathcal{C}$ appartiene ancora a $\mathcal{C}$.

Gli *aperti* di una topologia su X sono i sottoinsiemi complementari $X - A$, al variare di A tra i chiusi.

Sia $n \geq 0$ un intero fissato; per ogni sottoinsieme $E \subset \mathbb{K}[x_1, \dots, x_n]$ si definisce il *luogo di zeri* di E come

$$V(E) = \{(a_1, \dots, a_n) \in \mathbb{K}^n \mid f(a_1, \dots, a_n) = 0 \text{ per ogni } f \in E\}.$$

Se $E = \{f_1, \dots, f_m\}$ è un sottoinsieme finito scriveremo talvolta $V(f_1, \dots, f_m)$ al posto di $V(E)$.

Le seguenti proprietà sono di immediata verifica:

1. $V(0) = \mathbb{K}^n$, $V(1) = \emptyset$.
2. Se $E \subset H$, allora $V(H) \subset V(E)$.
3. Dati E, H sottoinsiemi di $\mathbb{K}[x_1, \dots, x_n]$, vale $V(E) \cup V(H) = V(EH)$, dove per EH si intende l'insieme di tutti i prodotti fg al variare di $f \in E$, $g \in H$.
4. Data una famiglia qualsiasi $\{E_\alpha\}$, vale $V(\cup E_\alpha) = \cap V(E_\alpha)$.

Quindi i luoghi di zeri $V(E)$ sono i chiusi di una topologia su $\mathbb{K}^n$ che viene detta *Topologia di Zariski.*

Esercizio 19. I sottoinsiemi finiti di $\mathbb{K}^n$ sono chiusi di Zariski. Più in generale, le unioni finite di sottospazi affini sono chiusi. △

Non tutti i sottoinsiemi di $\mathbb{K}^n$ sono chiusi, ad esempio un sottoinsieme proprio di $\mathbb{K}$ è un chiuso di Zariski se e solo se è finito (perché?).

Appare chiaro che diversi sottoinsiemi $E, H \subset \mathbb{K}[x_1, \dots, x_n]$ possono dare luogo allo stesso chiuso di Zariski $V(E) = V(H)$. Conviene quindi scegliere, per ogni chiuso X un rappresentante $E_X \subset \mathbb{K}[x_1, \dots, x_n]$ tale che $V(E_X) = X$ e l'unico modo ragionevole di fare ciò è il seguente.

Dato un qualsiasi sottoinsieme chiuso $X \subset \mathbb{K}^n$ si definisce

$$I(X) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a) = 0 \text{ per ogni } a \in X\}.$$

Valgono le proprietà:

1. $I(\emptyset) = \mathbb{K}[x_1, \dots, x_n]$, $I(\mathbb{K}^n) = 0$.
2. Se $X \subset Y$, allora $I(Y) \subset I(X)$.
3. Dato un chiuso $X \subset \mathbb{K}^n$ ed un sottoinsieme $E \subset \mathbb{K}[x_1, \dots, x_n]$, vale $E \subset I(X)$ se e soltanto se $X \subset V(E)$.
4. Per ogni sottoinsieme chiuso $X \subset \mathbb{K}^n$ vale $X = V(I(X))$.
5. $I(X)$ è un ideale.

Le prime tre proprietà elencate seguono immediatamente dalla definizione. Poiché ogni elemento di $I(X)$ si annulla su X è chiaro che $X \subset V(I(X))$. Viceversa, essendo X chiuso si ha $X = V(E)$ e per il punto 3 vale $E \subset I(X)$. Di conseguenza $V(I(X)) \subset V(E) = X$.

In particolare, ogni chiuso di Zariski è il luogo di zeri di un ideale. Inoltre, se E è un sottoinsieme di $\mathbb{K}[x_1, \dots, x_n]$ e denotiamo con (E) l'ideale generato, allora E, (E) hanno lo stesso luogo di zeri, $V(E) = V((E))$ anche se in generale (E) è strettamente contenuto in $I(V(E))$.

Esercizio 20. Provare che i sottoinsiemi $\mathbb{K}^n_f = \{a \in \mathbb{K}^n \mid f(a) \neq 0\}$ formano, al variare di $f \in \mathbb{K}[x_1, \dots, x_n]$, una base di aperti della topologia di Zariski, provare cioè che ogni aperto è unione, possibilmente infinita, di aperti del tipo $\mathbb{K}^n_f$. △

Esercizio 21. Provare che la topologia di Zariski non è di Hausdorff. △

Esercizio 22. Sia $\pi\colon \mathbb{K}^n \to \mathbb{K}^{n-1}$ la proiezione sulle prime coordinate. Mostrare che per ogni aperto di Zariski $U \subset \mathbb{K}^n$, l'insieme $\pi(U)$ è ancora aperto.
(Sugg.: se $f(x_1, \dots, x_n) = \sum_i f_i(x_1, \dots, x_{n-1})x_n^i$, mostrare che $\pi(\mathbb{K}^n_f) = \cup_i \mathbb{K}^{n-1}_{f_i}$.) △

8. Andare Preparare Proiettare.

Esercizio 23. Sia V uno spazio vettoriale su di un campo F. Dimostrare che se F possiede almeno $n+1$ elementi, allora V non può essere unione di n sottospazi affini propri. In particolare uno spazio vettoriale su di un campo infinito non può essere unione finita di sottospazi affini propri. (Sugg.: per induzione su n sia per assurdo $V = \cup_{i=1}^n V_i$, a meno di traslazioni possiamo supporre $0 \in V_n$. Se $V_n \subset V_i$ per qualche $i < n$ OK, altrimenti siano $v \in V_n - \cup_{i=1}^{n-1}(V_n \cap V_i)$, $h \in V - V_n$ e consideriamo la retta affine $\overline{vh} = \{tv + (1-t)h \mid t \in F\}$. Esiste allora un indice i tale che $\overline{vh}$ interseca V_i in almeno due punti.) △

Ricordiamo che con $\mathbb{K}$ intendiamo un campo algebricamente chiuso e quindi infinito.

Lemma 8.1. *Siano $I \subset \mathbb{K}[x_1, \dots, x_n]$ un ideale e $X \subset \mathbb{K}^n$ un sottoinsieme finito tale che $X \cap V(I) = \emptyset$. Allora esiste un polinomio $g \in I$ tale che $g(x) \neq 0$ per ogni $x \in X$.*

Dimostrazione. Scriviamo $X = \{p_1, \dots, p_s\}$, poiché $p_i \notin V(I)$ per ogni i, esistono $f_1, \dots, f_s \in I$ tali che $f_i(p_i) \neq 0$ per ogni i. Ne segue che

$$H_i = \{(a_1, \dots, a_s) \in \mathbb{K}^s \mid \sum_j a_j f_j(p_i) = 0\}$$

è un sottospazio vettoriale proprio. Basta quindi prendere $g = \sum b_i f_i$ per una qualsiasi n-upla di costanti $(b_1, \dots, b_n) \notin \cup_i H_i$. □

Lemma 8.2. (Lemma di Preparazione)
Sia $f \in \mathbb{K}[x_1, \dots, x_n]$ un polinomio non nullo di grado $d \geq 0$. Allora

1. *L'aperto $\mathbb{K}^n_f = \{a \in \mathbb{K}^n \mid f(a) \neq 0\}$ è non vuoto.*
2. *Esiste un cambio lineare di coordinatei $x_i = \sum a_{ij} y_j$, $\det(a_{ij}) \neq 0$, ed una costante non nulla $c \in \mathbb{K}$ tale che il polinomio $f(y_1, \dots, y_n)/c$ è monico di grado d nella variabile y_n.*

Dimostrazione. [1] Per induzione assumiamo l'asserto vero per polinomi in $\mathbb{K}[x_1, \dots, x_{n-1}]$ e scriviamo $f = \sum f_i x_n^i$ con i polinomi $f_i \in \mathbb{K}[x_1, \dots, x_{n-1}]$ non tutti nulli. Sia $a \in \mathbb{K}^{n-1}$ tale che $f_0(a), f_1(a), \dots$ non siano tutti nulli. Allora il polinomio $f(a, x_n)$ non è nullo in $\mathbb{K}[x_n]$ ed ha al più un numero finito di radici.
[2] Sia f_d la componente omogenea di grado d di f. Per il punto 1) esiste un punto $a \in \mathbb{K}^n$ tale che $f_d(a) \neq 0$ e scegliamo un sistema di coordinate $y_1, \dots, y_n$ tale che il punto a corrisponda a $(0, 0, \dots, 0, 1)$. Nel nuovo sistema di coordinate il polinomio $f(0, \dots, 0, y_n)$ ha grado d e basta quindi prendere come costante $c = f_d(0, \dots, 0, 1)$. □

Vogliamo adesso studiare il comportameto dei chiusi di Zariski rispetto alle proiezioni su sottospazi di $\mathbb{K}^n$. Vediamo prima cosa succede in un esempio concreto.

Consideriamo l'iperbole $X = V(xy-1) \subset \mathbb{K}^2$ e sia $\pi\colon \mathbb{K}^2 \to \mathbb{K}^1$ la proiezione sulla prima coordinata. Si vede immediatamente che $\pi(X) = \mathbb{K} - \{0\}$ non è un chiuso di Zariski. Similmente se facciamo la proiezione sulla seconda coordinata.
Però, se prima si effettua un cambio lineare di ccordinate $x = au+bv$, $y = cu+dv$, $ad-bc \neq 0$ si trova che $X = V(bdv^2 + vu(ad+bc) + acu^2 - 1)$ e, se $bd \neq 0$, allora la proiezione sul primo asse coordinato di X è $\mathbb{K}^1$ che è quindi chiuso. Abbiamo quindi sperimentato che *la generica proiezione di X su di un sottospazio è un chiuso.*

Lemma 8.3. (Lemma di Proiezione) *Siano $\mathbb{K} = \overline{\mathbb{K}}$ un campo algebricamente chiuso, $J \subset \mathbb{K}[x_1, \dots, x_n]$ un ideale: denotiamo $J^c = J \cap \mathbb{K}[x_1, \dots, x_{n-1}]$ e sia $\pi\colon \mathbb{K}^n \to \mathbb{K}^{n-1}$ la proiezione sulle prime coordinate.*
Se esiste un polinomio $f \in J$ monico di grado positivo rispetto a x_n allora $\pi(V(J)) = V(J^c)$.

Dimostrazione. Se $(a_1, \dots, a_n) \in V(J)$, allora $f(a_1, \dots, a_n) = 0$ per ogni $f \in J^c$ e quindi $(a_1, \dots, a_{n-1}) \in V(J^c)$.
Proviamo adesso che $\pi\colon V(J) \to V(J^c)$ è surgettiva: si consideri un punto $a = (a_1, \dots, a_{n-1}) \in V(J^c)$ e supponiamo per assurdo che $\pi^{-1}(a) \cap V(J) = \emptyset$. Denotiamo $X = \pi^{-1}(a) \cap V(f)$, poiché i punti di X sono in bigezione con le radici del polinomio monico $f(a_1, \dots, a_{n-1}, x_n) \in \mathbb{K}[x_n]$, si ha che X è un insieme finito, $X \cap V(J) = \emptyset$ e quindi esiste $g \in V(J)$ tale che $X \cap V(g) = \emptyset$ o equivalentemente tale che i due polinomi $f(a_1, \dots, a_{n-1}, x_n), g(a_1, \dots, a_{n-1}, x_n) \in \mathbb{K}[x_n]$ non hanno radici in comune.
Dunque, $R(f,g)(a_1, \dots, a_{n-1}) \neq 0$, dove $R(f,g)$ è il risultante dell'eliminazione di x_n da f e g. D'altra parte $R(f,g)$ appartiene all'ideale generato da f e g e quindi appartiene a J^c e questo provoca una contraddizione. □

Esercizio 24. Provare che il lemma di proiezione è falso se $\mathbb{K} = \mathbb{R}$, anche se continua ad essere vero che $\pi(V(J))$ è chiuso nella topologia della distanza euclidea. △

9. Il teorema degli zeri di Hilbert.

Siamo adesso in grado di dimostare agevolmente il:

Teorema 9.1. (degli zeri di Hilbert[1], forma debole) *Se $\mathbb{K}$ è un campo algebricamente chiuso e $J \subset \mathbb{K}[x_1, \dots, x_n]$ è un ideale, allora vale $V(J) = \emptyset$ se e solo se $1 \in J$.*

Dimostrazione. L'enunciato è ovvio se $1 \in J$ oppure se $J = 0$. Supponiamo quindi $0 \neq J \neq \mathbb{K}[x_1, \dots, x_n]$ e proviamo che $V(J)$ è non vuoto.
Se $n = 1$, allora l'ideale J è principale, diciamo $J = (f)$, e dunque $V(J)$ è l'insieme delle radici di f. Siccome f non è invertibile deve avere grado positivo e quindi possiede radici.
Se $n > 1$ ragioniamo per induzione e supponiamo il teorema vero in $\mathbb{K}^{n-1}$. Sia $f \in J$ un polinomio di grado $m > 0$. Per il Lemma di Preparazione 8.2, a meno di effettuare un cambio lineare di coordinate e di moltiplicare f per una costante possiamo supporre che f sia un polinomio monico di grado m rispetto a x_n. Consideriamo l'ideale $J^c = J \cap \mathbb{K}[x_1, \dots, x_{n-1}]$; per l'ipotesi induttiva $V(J^c) \neq \emptyset$, detta quindi $\pi\colon \mathbb{K}^n \to \mathbb{K}^{n-1}$ la proiezione sulle prime $n-1$ coordinate, per il Lemma 8.3 vale $\pi(V(J)) = V(J^c)$ e quindi $V(J) \neq \emptyset$. □

Corollario 9.2. *Siano $f, g \in \mathbb{K}[x_1, \dots, x_n]$ con f irriducibile e $\mathbb{K}$ campo algebricamente chiuso. Allora vale $V(f) \subset V(g)$ se e soltanto se f divide g.*

Dimostrazione. Se f divide g e $x \in V(f)$, allora $f(x) = 0$, $g(x) = 0$ e quindi $x \in V(g)$. Viceversa, supponiamo per assurdo che $V(f) \subset V(g)$ e che $g \notin (f)$. Consideriamo l'ideale $J \subset \mathbb{K}[x_1, \dots, x_n, t]$ generato dai polinomi $f, gt-1$. Un punto $(a_1, \dots, a_{n+1}) \in \mathbb{K}^{n+1}$ appartiene a $V(J)$ se e soltanto se $f(a_1, \dots, a_n) = 0$ e $g(a_1, \dots, a_n)a_{n+1} = 1$; segue pertanto dalla

[1]Poiché è il teorema ad essere di Hilbert e non gli zeri sarebbe più appropriato chiamarlo teorema di Hilbert degli zeri. Per intimorire gli studenti viene spesso chiamato (in tedesco) *Nullstellensatz*

condizione $V(f)\subset V(g)$ che $V(J)=\emptyset$ e quindi, per il teorema degli zeri $1\in J$.
Abbiamo quindi una relazione del tipo

$$(\sum_{i=0}^{r} a_i t^i)f-(\sum_{i=0}^{s} b_i t^i)(gt-1)=1,\qquad a_i,b_i\in\mathbb{K}\,[x_1,\dots,x_n].$$

Assumiamo adesso che f non divida g e proviamo che $b_i\in(f)$ per ogni i. Infatti per ogni $i\geq 0$, identificando i coefficienti di t^{i+1} dei due membri della relazione si ottiene

$$a_{i+1}f+b_{i+1}=b_i g$$

ed assumendo per induzione decrescente su i che f divida b_{i+1} si ha che f divide $b_i g$. Essendo f irriducibile deve necessariamante dividere b_i.
Dunque $b_0\in(f)$ e quindi $1=a_0f+b_0\in(f)$ che è una contraddizione. □

Esercizio 25. Siano $f,g\in\mathbb{K}\,[x_1,\dots,x_n]$ due polinomi di secondo grado. Provare che $V(f)=V(g)$ se e soltanto se f e g differiscono per una costante moltiplicativa. Il risultato continua a valere per polinomi di terzo grado? △

Esercizio 26. Siano $f,g\in\mathbb{K}\,[x_1,\dots,x_n]$ due polinomi. Provare che $V(f)\subset V(g)$ se e soltanto se ogni fattore irriducibile di f divide g. △

Esercizio 27. (Difficile) Sia $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ il generico polinomio monico di grado n e indichiamo $\Delta(f)\in\mathbb{Z}[a_1,\dots,a_n]$ il suo discriminante. Dimostrare che $\Delta(f)$ è irriducibile. △

10. A cosa servono i radicali?

Il termine radicale nel titolo si riferisce al radicale di un ideale.

Definizione 10.1. Sia I un ideale di un anello commutativo A. Il *radicale di* I è definito come

$$\sqrt{I}=\{f\in A\mid f^n\in I \text{ per qualche } n\geq 0\}.$$

Il radicale di un ideale è ancora un ideale, infatti se $f,g\in\sqrt{I}$ e $f^n,g^m\in I$, allora per ogni $a\in A$ vale $(af)^n=a^nf^n\in I$ e

$$(f+g)^{n+m}=\sum_i \binom{n+m}{i} f^i g^{n+m-i}\in I.$$

Esercizio 28. Provare che in un dominio a fattorizzazione unica vale $f\in\sqrt{(g)}$ se e soltanto se ogni fattore irriducibile di g divide f. △

Consideriamo adesso un ideale $J\subset\mathbb{K}\,[x_1,\dots,x_n]$; dato che $J\subset\sqrt{J}$ vale $V(\sqrt{J})\subset V(J)$. D'altra parte, se $f\in\sqrt{J}$, allora $f^n\in J$ per qualche $n>0$; quindi $f(x)^n=f^n(x)=0$ per ogni $x\in V(J)$ e questo prova che $V(J)=V(\sqrt{J})$.
Vale quindi la relazione $\sqrt{J}\subset I(V(J))$ per ogni ideale J. Se il campo $\mathbb{K}$ non è algebricamente chiuso in generale $\sqrt{J}\neq I(V(J))$, si consideri ad esempio $\mathbb{K}=\mathbb{R}$, $n=1$ e $J=(x^2+1)$ allora $V(J)=\emptyset$ e $I(V(J))=\mathbb{R}[x]\neq\sqrt{J}$.

Teorema 10.2. (degli zeri di Hilbert (1892), forma forte) *Se* $\mathbb{K}$ *è algebricamente chiuso allora per ogni ideale* $J\subset\mathbb{K}\,[x_1,\dots,x_n]$ *vale* $\sqrt{J}=I(V(J))$.

Dimostrazione. Bisogna dimostare che se $f\in\mathbb{K}\,[x_1,\dots,x_n]$ e $f(p)=0$ per ogni $p\in V(J)$ allora $f^n\in J$ per $n>>0$. Per semplicità notazionale scriveremo $f\equiv g$ se $f-g\in J$.
Con un trucco già visto consideriamo l'ideale $H\subset\mathbb{K}\,[x_1,\dots,x_n,t]$ generato da J e $ft-1$. Il luogo di zeri di H in $\mathbb{K}^{n+1}$ è l'insieme vuoto e quindi esistono $g_1,\dots,g_m\in J$ ed una relazione

$$\sum_{i,j} a_{ij}t^i g_j-(\sum_{i=0}^{s} b_i t^i)(ft-1)=1,\qquad a_{ij},b_i\in\mathbb{K}\,[x_1,\dots,x_n].$$

che, guardando i coefficienti delle potenze di t si traduce nell'insieme di congruenze

$$b_0 \equiv 1, \qquad b_i f \equiv b_{i+1}.$$

Risolvendo si ottiene $b_i \equiv f^i$ per ogni $i > 0$ e basta osservare che $b_i = 0$ per i sufficientemente grande. □

Esercizio 29. Sia $Y \subset \mathbb{K}^3$ l'unione dei tre piani coordinati e $X \subset \mathbb{K}^3$ l'unione dei tre assi coordinati. Provare che $I(Y) = (xyz)$ e che $I(X) = (xy, yz, zx)$. (Sugg.: se $f \in I(X)$ considerare $f(x, y, z) - f(0, y, z) - f(x, 0, z) - f(x, y, 0)$.) △

11. Esercizi.

Esercizio 30. Provare che $\mathbb{C}^n$ è compatto nella topologia di Zariski. △

Esercizio 31. Dimostrare che, se $\mathbb{K}$ è un campo algebricamente chiuso, allora gli ideali massimali di $\mathbb{K}[x_1, \ldots, x_n]$ sono tutti e soli gli ideali $I(p)$, al variare di $p \in \mathbb{K}^n$. Esiste dunque una bigezione naturale fra $\mathbb{K}^n$ e l'insieme degli ideali massimali di $\mathbb{K}[x_1, \ldots, x_n]$. △

Esercizio 32. Calcolare la dimensione dello spazio vettoriale dei polinomi omogenei di grado d in $n + 1$ variabili. △

Esercizio 33. Sia $f \in \mathbb{C}[x, y]$ un polinomio con la proprietà che $(a_1, a_2) \in V(f)$ se e solo se $(a_2, a_1) \in V(f)$. Provare che $f(y, x) = \pm f(x, y)$. △

Dipartimento di Matematica "G. 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