Lezione 14 ottobre

Titolo nota 14/10/2020

Un po' di algebra: IL RISULTANTE

Sieno $\mathbb{K}$ un campo, $A = \mathbb{K}$, oppure $A = \mathbb{K}[x_1, \dots, x_n]$, per cui A è comunque un dominio a fattorizzazione unica.

Osservazione preliminare: Sia $M \in M(k \times k, A)$ una matrice $k \times k$ a coefficienti in A. Allora le righe di M sono dipendenti in A (cioè se esiste una combinazione lineare nulla non banale) $\iff \det M = 0$.

Dimostrazione: Se A è un campo lo sappiamo. In generale (cioè se A è un dominio di integrità), si procede così.
Se le righe di M sono dipendenti, la tesi segue facilmente dalla multilinearità del determinante rispetto alle righe: moltiplicando le righe per opportuni coefficienti non nulli e sommando si ottiene la riga nulla senza alterare il fatto che $\det M$ si annulli o no, da cui la freccia $\Longrightarrow$.
$\Longleftarrow$: Supponiamo $\det M = 0$. Allora $\det {}^t M = 0$
Consideriamo il sistema lineare ${}^t M \cdot v = 0$ (v è un k-upla di variabili in A). Ricordiamo che $A = \mathbb{K}[x_1, \dots x_n]$.
Cercando di risolvere il sistema con l'algoritmo di Gauss incontriamo il problema che vorremmo dividere per elementi non nulli di A (cosa sempre possibile se A è un campo).

Convenzionalmente di dividere per polinomi non nulli, il che equivale a considerare $A \subseteq B$, dove B è il campo delle funzioni razionali, cioè il campo delle frazioni $\frac{P}{q}$, $P, q \in \mathbb{K}[x_1, \dots x_n]$, $q \neq 0$.

Così facendo, poiché $\det M = 0$, si trova una soluzione non banale $v = \left(\frac{P_1}{q_1}, \dots, \frac{P_n}{q_n}\right)$ di ${}^t M \cdot v = 0$.

(le entrate di v stanno in B, non necessariamente in A).

Posto $w = q_1 \dots q_n \cdot v$ (cioè moltiplicando per tutti i denominatori) otteniamo una soluzione $w \in A^n \setminus \{(0,0,\dots 0)\}$ di ${}^t M w = 0$. Questa soluzione esprime una combinazione lineare nulla non banale delle colonne di ${}^t M$, cioè delle righe di M.

□

RISULTANTE

Siano $f, g \in A[X]$, con $\deg f = n$, $\deg g = m$.

Ad esempio, $f = 1 + 5x^2 + 6x^3$ se $A = \mathbb{Q}$, $n = 3$

$f = x_1^2 x_2 + x_1 x + x_2 x^2 + (x_1 - x_2^2 + x_1^3) x^3$

se $A = \mathbb{K}[x_1, x_2]$, $n = 3$

coefficienti di f

Dunque $f = a_0 + a_1 x + \dots + a_n x^n$, $a_n \neq 0$

$g = b_0 + b_1 x + \dots + b_m x^m$, $b_m \neq 0$.

La matrice di Sylvester di f, g è la matrice

$S(f,g) \in M(n+m, n+m, A)$ data da

$$S(f,g) = \begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & \dots & 0 \\ & \ddots & & & & & \\ 0 & \dots & a_0 & a_1 & \dots & & a_n \\ b_0 & \dots & & b_m & 0 & \dots & 0 \\ 0 & b_0 & \dots & & b_m & \dots & 0 \\ 0 & \dots & b_0 & \dots & & & b_m \end{pmatrix}$$

($n+1$ colonne per $a_0 \dots a_n$, $m-1$ colonne per gli zeri; m righe per i coefficienti di f, n righe per i coefficienti di g; $n-1$ zeri, $m+1$ coefficienti di g)

Il risultante di f, g è

$$R(f,g) = \det S(f,g) \in A$$

Teorema: Sono fatti equivalenti ($f, g \in A[x]$ non nulli):

1. $R(f,g) = 0$
2. f, g hanno un fattore irriducibile di grado positivo (in x) in comune
3. $\exists\, h, k \in A[x]$ NON NULLI con $\deg h < \deg f$, $\deg k < \deg g$ e $kf + hg = 0$.

Dim.: (1) $\Leftrightarrow$ (3) L'esistenza di $k = c_0 + \dots + c_{m-1}x^{m-1}$, $h = d_0 + \dots + d_{n-1}x^{n-1}$ come in (3) equivale al fatto che $kf + hg = 0$, cioè

(mi fermo a x^{m-1} perché $\deg k < \deg g$, nulla vieta $c_{m-1} = 0$.)

$$c_0 f + c_1 x f + \dots + c_{m-1} x^{m-1} f + d_0 g + d_1 x g + d_2 x^2 g + \dots + d_{n-1} x^{n-1} g = 0,$$

cioè che i polinomi

$$f, xf, x^2 f, \dots, x^{m-1} f, g, xg, x^2 g, \dots, x^{n-1} g$$

sono dipendenti in A. Poiché le coordinate di questi polinomi rispetto a $\{1, x, x^2, \dots, x^{m+n-1}\}$ sono proprio le righe di $S(f,g)$, che vogliamo essere dipendenti $\iff \det S(f,g) = 0$. Ciò prova ① $\iff$ ③

② $\Rightarrow$ ③ Se $f = p \cdot \bar{f}$, $g = p \cdot \bar{g}$, $\deg p > 0$ allora pongo $h = \bar{f}$ (poiché $\deg \bar{f} < \deg f$), $k = -\bar{g}$ e ho $kf + hg = -\bar{g} f + \bar{f} g$, che è nullo in quanto $p(-\bar{g} f + \bar{f} g) = (-p\bar{g}) \cdot f + (p\bar{f}) g = -gf + fg = 0$, $p \neq 0$ e A è un dominio di integrità.

③ $\Rightarrow$ ② Se $\exists\, h, k$ come in ③, ho $kf = -hg$, per cui $f \mid hg$. Ma $\deg f > \deg h$ per cui nella fattorizzazione in irriducibili di f deve comparire almeno un fattore di grado positivo che divide g. Quello è il fattore cercato.

Corollario: Siano $f, g \in \mathbb{K}[x]$. Allora se f, g hanno una radice in comune, $R(f,g) = 0$. Se $\mathbb{K} = \overline{\mathbb{K}}$

(cioè $\mathbb{K}$ alg. chiuso), vale il "se e solo se".

Dim.: Infatti, $R(f,g)=0 \iff f,g$ hanno un fattore irriducibile in comune, mentre f,g hanno una radice comune $\iff$ hanno un fattore di grado 1 (automaticamente irriducibile) in comune.

PROPRIETÀ del RISULTANTE

Sia $A=\mathbb{K}[x_0,x_1]$ e prendiamo $f\in\mathbb{K}[x_0,x_1,x_2]$, pensato come $f\in\mathbb{K}[x_0,x_1][x_2]=A[x_2]$.
Supponiamo f omogeneo di grado n (rispetto a x_0,x_1,x_2)
Analogamente, sia $g\in A[x_2]$ omogeneo (in $\mathbb{K}[x_0,x_1,x_2]$) di grado m.
Avremo

$$f = a_0(x_0,x_1)+a_1(x_0,x_1)x_2+a_2(x_0,x_1)x_2^2+\dots+a_n(x_0,x_1)x_2^n$$

$$g = b_0(x_0,x_1)+b_1(x_0,x_1)x_2+\dots+b_m(x_0,x_1)x_2^m$$

con $\deg a_i(x_0,x_1)=n-i$, $\deg b_j(x_0,x_1)=m-j$.

SPECIALIZZAZIONE: Dati $(a,b)\in\mathbb{K}^2$, sia $f_{a,b}\in\mathbb{K}[x_2]$, $f_{a,b}(x_2)=f(a,b,x_2)$, e analogamente $g_{a,b}\in\mathbb{K}[x_2]$, $g_{a,b}(x_2)=g(a,b,x_2)$.

Se $\deg f_{a,b}=\deg f$ e $\deg g_{a,b}=\deg g$, allora $R(f_{a,b},g_{a,b})=R(f,g)(a,b)$ (in $\mathbb{K}$),

cioè le operazioni di valutazione in (a,b,x_2) e calcolo del risultante commutano.

Infatti, se $\deg f_{a,b} = \deg f$ e $\deg g_{a,b} = \deg g$, $S(f_{a,b}, g_{a,b})$ si ottiene sostituendo $x_0 = a$ $x_1 = b$ nella matrice $S(f,g)$.

OMOGENEITÀ: Nelle ipotesi sopra (cioè f,g omogenei di gradi n,m), il polinomio $R(f,g) \in \mathbb{K}[x_0,x_1]$ è omogeneo di grado $n+m$.

Dim.: $\mathrm{Ris}(f,g)(tx_0, tx_1) =$

$$\det \begin{pmatrix} a_0(tx_0,tx_1) & a_1(tx_0,tx_1) \dots & a_n(tx_0,tx_1) \dots 0 \dots 0 \\ & \dots & \\ b_0(tx_0,tx_1) & b_1(tx_0,tx_1) \dots & \end{pmatrix} =$$

$$= \det \begin{pmatrix} t^n a_0(x_0,x_1) & t^{n-1} a_1(x_0,x_1) \dots & a_n(x_0,x_1) \dots 0 \\ 0 & t^n a_0(x_0,x_1) \dots & 0 \\ & \dots & \\ t^m b_0(x_0,x_1) & t^{m-1} b_1(x_0,x_1) \dots & \\ 0 & t^m b_0(x_0,x_1) \dots & \end{pmatrix} \begin{matrix} \cdot t^m \\ \cdot t^{m-1} \\ \vdots \\ \cdot t^n \\ \cdot t^{n-1} \end{matrix}$$

Moltiplicando la i-esima riga degli a per t^{m-i} e la j-esima riga dei b per t^{n-i} il determinante risulta moltiplicato per $t^{m+(m-1)+\dots+1+n+(n-1)+\dots+1} =$

$= t^{\binom{m}{2}+\binom{n}{2}}$, per cui

$$t^{\binom{m}{2}+\binom{n}{2}} \cdot R(f,g)(t x_0, t x_1) =$$

$$\det \begin{pmatrix} t^{n+m} a_0 & t^{n+m-1} a_1 & \cdots & 0 \\ 0 & t^{n+m-1} a_0 & \cdots & \\ t^{n+m} b_0 & t^{n+m-1} b_1 & \cdots & \\ 0 & t^{n+m-1} b_0 & \cdots & \\ & & \ddots & \end{pmatrix} =$$

$$= t^{(n+m)+(n+m-1)+(n+m-2)+\cdots+1} \det \begin{pmatrix} a_0 & a_1 & \cdots \\ 0 & a_0 & a_1 \cdots \\ & & \ddots \end{pmatrix} =$$

$$= t^{\binom{n+m}{2}} R(f,g)(x_0, x_1).$$

Ricapitolando

$$t^{\binom{n}{2}+\binom{m}{2}} R(f,g)(t x_0, t x_1) = t^{\binom{n+m}{2}} R(f,g)(x_0, x_1)$$

$n \cdot m$

Dunque $R(f,g)(t x_0, t x_1) = t^{n \cdot m} R(f,g)(x_0, x_1)$, che implica (perché? Esercizio!) che $R(f,g)$ è omogeneo di grado $n \cdot m$.

TEOREMA DI BÉZOUT

(noto come Lemma di Bézout).

Sia $\mathbb{K}$ un campo infinito. Il lemma di Bezout ci dice "come" si intersecano due curve in $\mathbb{P}^2(\mathbb{K})$.

Lemma di Bézout: Siano C, D curve di $\mathbb{P}^2(\mathbb{K})$ di grado n, m rispettivamente. Allora:

① Se $\mathbb{K} = \overline{\mathbb{K}}$, $V(C) \cap V(D) \neq \emptyset$.

② Se $|V(C) \cap V(D)| > m \cdot n$, allora C e D hanno una componente irriducibile in comune.

In realtà, è possibile definire una nozione di molteplicità di intersezione tra curve in un punto p, denotata con $I(C, D, p)$, e, se C e D non hanno componenti comuni,

$$\sum_{p \in V(C) \cap V(D)} I(C, D, p) \leq m \cdot n,$$

con l'uguaglianza se $\mathbb{K} = \overline{\mathbb{K}}$.

Dim.: Siano $C = [f]$, $D = [g]$. Posso scegliere coordinate su $\mathbb{P}^2(\mathbb{K})$ in modo che $[0,0,1] \notin V(C) \cup V(D)$. (Se $\mathbb{K}$ è infinito, il complementare di una curva è sempre non vuoto, per cui $\exists$ un punto "fuori da" $C + D$).

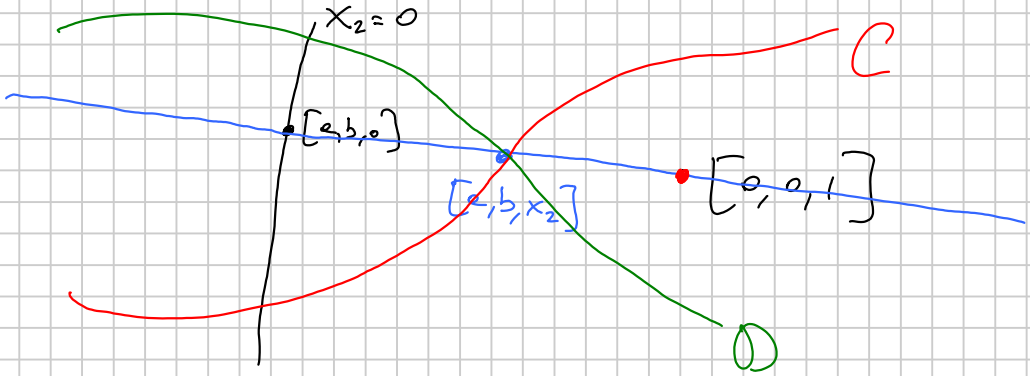
Questa condizione ci assicura che in f compare il monomio x_2^n (altrimenti in tutti i monomi di f compare x_0 o x_1 e perciò $f(0,0,1) = 0$). Perciò $\forall (a,b) \in \mathbb{K}^2$, $\deg f_{a,b} = \deg f$. Analogamente $\deg g_{a,b} = \deg g$, per cui $R(f,g)(a,b) = R(f_{a,b}, g_{a,b})$.

Poiché $[0,0,1] \notin V(C) \cup V(D)$ in particolare $[0,0,1] \notin V(C) \cap V(D)$, per cui tutti i punti di $V(C) \cap V(D)$ sono della forma $[a,b,c]$ con $(a,b) \neq (0,0)$. Fissiamo $(a,b) \in \mathbb{K}^2 \setminus \{0\}$. Allora $\exists x_2 \in \mathbb{K}$ t.c. $[a,b,x_2] \in V(C) \cap V(D) \iff f(a,b,x_2) = g(a,b,x_2) = 0$

$\iff f_{a,b}(x_2) = g_{a,b}(x_2) = 0 \iff f_{a,b}, g_{a,b}$ hanno una radice in comune $\Longrightarrow$ $R(f_{a,b}, g_{a,b}) = 0 \iff$

$\Longleftarrow$ se $\mathbb{K} = \overline{\mathbb{K}}$

$\iff R(f,g)(a,b) = 0 \iff [a,b] \in \mathbb{P}^1(\mathbb{K})$ è una "radice proiettiva" del polinomio omogeneo $R(f,g)(x_0,x_1)$.



Si danno 2 casi: Se $R(f,g) = 0$ come polinomio in $\mathbb{K}[x_0,x_1]$, allora f e g hanno un fattore comune, per cui C e D hanno una componente in comune ($\mathbb{K} = \overline{\mathbb{K}}$, $V(C) \cap V(D) \neq \emptyset$), per cui il teorema è dimostrato.

Altrimenti, $R(f,g)$ è omogeneo di grado $m \cdot n$ non nullo. Se $\mathbb{K} = \overline{\mathbb{K}}$, allora $\exists$ una soluzione $(a,b) \neq (0,0)$

per cui $\mathrm{Ris}(f,g)(a,b)=0$, per cui $\exists x_2$ con

$[a,b,x_2] \in V(C)\cap V(D) \Rightarrow V(C)\cap V(D)\neq\emptyset$.

Ciò mostra ①.

Vediamo ②. Distinguiamo due casi, a seconda che $|V(C)\cap V(D)|$ sia finita o no. $\exists x_2 \in \mathbb{K}$ t.c. $[a,b,x_2]\in V(C)\cap V(D) \iff (a,b)$ annulla il polinomio omogeneo non nullo $\mathrm{Ris}(f,g)$. Poiché tale polinomio ha grado $n\cdot m$, esso ha al più $n\cdot m$ "soluzioni proiettive", per cui se $V(C)\cap V(D)$ è infinito necessariamente $\exists (\bar a,\bar b)\neq(0,0)$ tale che $\exists$ infiniti valori di x_2 per cui $[\bar a,\bar b,x_2]\in V(C)\cap V(D)$. Ciò vuol dire che la retta $\bar b x_0 - \bar a x_1 = 0$ interseca $V(C)\cap V(D)$ in infiniti punti. Abbiamo visto che se una retta r interseca una curva E in k punti, $k>\deg E$, allora r ne è una componente irriducibile

Dunque la retta $\bar b x_0 - \bar a x_1 = 0$ è componente sia di C sia di D, che hanno perciò una componente in comune, come voluto.

Se $V(C)\cap V(D)=\{P_1,\dots P_k\}$ è finito,

scelgo $P \notin C + D + \sum_{\substack{i,j \\ i\neq j}} L(P_i,P_j)$

(cioè P non è allineato con coppie di punti di $V(C)\cap V(D)$).

Scelgo coordinate tali che $P = [0:0:1]$ e ripeto tutto il procedimento. Ora, per costruzione, $\forall (a,b) \neq (0,0)$ esiste al più un solo $x_2 \in \mathbb{K}$ con $[a, b, x_2] \in V(C) \cap V(\mathcal{D})$, perché se ne esistessero 2, chiamo P_{i_1} e P_{i_2}, avremmo $P_{i_1}, P_{i_2}, [0;0,1]$ allineati. Dunque ogni radice proiettiva di $Ris(f,g)$ corrisponde al più un punto di $V(C) \cap V(\mathcal{D})$, per cui tali punti sono al massimo $m \cdot n$.

□.