Appunti per Geometria e Algebra Computazionale 2-2. Il risultante

Corso di Laurea in Matematica, Università di Firenze, 2019/20

Giorgio Ottaviani

7 aprile 2020

Fattore a comune tra polinomi

Teorema

Sia R un UFD. Siano F, G polinomi in $R[x]$ di gradi rispettivamente $f, g > 0$.

$$\left.\begin{array}{c} F, G \quad \textit{hanno un fattore} \\ \textit{irriducibile di grado } > 0 \\ \textit{in comune} \end{array}\right\} \iff \left\{\begin{array}{c} \exists \quad A, B \\ \textit{di gradi risp. } g-1, f-1 \\ \textit{tali che } AF + BG = 0 \end{array}\right.$$

Dimostrazione.

$\Longrightarrow$ Sia $F = af_1$, $G = ag_1$. Poniamo $A := g_1$, $B := -f_1$. Allora abbiamo $Af + Bg = g_1 af_1 - f_1 ag_1 = 0$. Se *deg* A, *deg* B sono minori di quanto è richiesto basta moltiplicare A e B per lo stesso fattore.

$\Longleftarrow$ Per ipotesi $AF = -BG$. Quindi ogni fattore irriducibile di G divide A oppure F. Siccome *deg* $A = g - 1$ allora esiste un fattore irriducibile di G che divide F, come volevamo. $\square$

L'introduzione del risultante è adesso semplice. Il problema è di trovare condizioni per cui due polinomi $F, G \in R[x]$ hanno un fattore in comune.

Si considera come incognite i coefficienti dei due polinomi:

$A := a_0x^{g-1} + \ldots + a_{g-2}x + a_{g-1}$,

$B := b_0x^{f-1} + \ldots + b_{f-2}x + b_{f-1}$

e si pone la condizione

$$AF + BG = 0. \tag{0.1}$$

Questo è un sistema lineare con $f + g$ incognite e $f + g$ equazioni. Il determinante della matrice del sistema (0.1) *è per definizione il risultante di F e G.*

Posto $F := f_0x^f + \ldots$, $G := g_0x^g + \ldots$ il sistema (0.1) diventa:

$$\begin{array}{llll}
a_0 f_0 + & b_0 g_0 & = 0 & \text{coeff. di } x^{f+g-1} \\
a_0 f_1 + a_1 f_0 & b_0 g_1 + b_1 g_0 & = 0 & \text{coeff. di } x^{f+g-2} \\
\vdots & \vdots & \vdots & \\
a_{g-1} f_f + & b_{f-1} g_g & = 0 & \text{coeff. di} x^0
\end{array}$$

e la sua matrice è

$$\begin{pmatrix} f_0 & & & & g_0 & & & \\ f_1 & f_0 & & & g_1 & g_0 & & \\ \vdots & & \ddots & & \vdots & & \ddots & \\ f_f & & & f_0 & g_g & & & g_0 \\ & & \ddots & & & & \ddots & \\ & & & f_f & & & & g_g \end{pmatrix}$$

James Joseph Sylvester (1814-1897)

Definizione di risultante

Per comodità di scrittura si scrive il risultante come il determinante della matrice trasposta, cioè si pone:

Definizione

$$Res(f,g,x) := \det \begin{vmatrix}
f_0 & f_1 & \dots & f_f & & & & & \\
 & f_0 & \ddots & & \ddots & & & & \\
 & & \ddots & \ddots & & \ddots & & & \\
 & & & f_0 & f_1 & \dots & f_f & & \\
g_0 & g_1 & \cdots & \cdots & g_g & & & & \\
 & g_0 & \ddots & & & \ddots & & & \\
 & & \ddots & \ddots & & & \ddots & & \\
 & & & \ddots & \ddots & & & \ddots & \\
 & & & & g_0 & g_1 & & & g_g
\end{vmatrix}$$

La proprietà principale del risultante

Teorema

Sia R un UFD.

$$\left.\begin{array}{c} f, g \in R[x] \textit{ hanno} \\ \textit{un fattore in comune di grado } \geq 1 \end{array}\right\} \iff Res(f, g, x) = 0$$

Dimostrazione.

- $\Longrightarrow$ Se fosse $Res(f, g, x) \neq 0$ allora consideriamo il sistema $AF + BG = 0$ (0.1) nel campo dei quozienti di R. Dalla teoria dei sistemi lineari l'unica soluzione di (0.1) è quella nulla.
- $\Longleftarrow$ Nel campo dei quozienti esiste una soluzione di (0.1) non nulla. Moltiplicando per il denominatore comune si trova una soluzione a coefficienti in R.

$\square$

Esempio

Siano

$$F = x^2 - 4x + 3$$

$$G = x^2 - 6x + 5$$

che hanno a comune il fattore $x - 1$. *Infatti*

$$Res(f, g, x) = \begin{vmatrix} 1 & -4 & 3 & \\ & 1 & -4 & 3 \\ 1 & -6 & 5 & \\ & 1 & -6 & 5 \end{vmatrix} = 0$$

Il risultante di due polinomi F e G rispetto alla variabile x è implementato in Macaulay2 con il comando $\mathrm{resultant}(F, G, x)$, mentre la matrice che appare nella definizione di risultante può essere ricavata con $\mathrm{sylvesterMatrix}(F, G, x)$.

Esercizio

Esercizio

Verificare se i polinomi $x^5 + x + 1$ *e* $x^4 + x^3 + 1$ *hanno una radice in comune.*

Definizione

$Discr(f) := Res(f, f', x)$ si dice il discriminante di f. È implementato in Macaulay2 col comando $\mathrm{discriminant}(f, x)$.

Il discriminante del polinomio monico $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ é nullo se e solo se f ha una radice doppia (nel proprio campo di spezzamento).
Esempi. Se $f = ax^2 + bx + c$ allora $Discr(f) = a(4ac - b^2)$. Se $f = x^3 + px + q$ allora $Discr(f) = -(4p^3 + 27q^2)$

Teorema

Dati $p, q \in R[x]$ esistono due polinomi $A, B \in R[x]$ tali che $Ap + Bq = Res(p, q, x)$

Dimostrazione.

Se $Res(p, q, x) = 0$ la tesi è ovvia prendendo $A = q$ e $B = -p$. Se $Res(p, q, x) \neq 0$ scriviamo il sistema lineare (analogo di (0.1)) $\tilde{A}p + \tilde{B}q = 1$ con incognite $\tilde{A}$, $\tilde{B}$. Si trova un sistema lineare quadrato di ordine $deg\ p + deg\ q$ con termine noto $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ e determinante della matrice dei coefficienti $Res(p, q, x) \neq 0$. Risolvendo il sistema con la regola di Cramer nel campo dei quozienti di R troviamo $\tilde{A}$ e $\tilde{B}$ soluzioni che hanno a denominatore $Res(p, q, x)$. Posto $A = \tilde{A}Res(p, q, x)$ e $B = \tilde{B}Res(p, q, x)$ si

Il risultante per polinomi in più variabili

Teorema

Siano $f, g \in K[x_1, \dots x_n]$ *di grado positivo in* x_1. *Allora*

- *i)* $Res(f, g, x_1) \in (f, g) \cap K[x_2, \dots, x_n]$ *(che si dice il primo ideale di eliminazione)*
- *ii)* $Res(f, g, x_1) \equiv 0 \iff f, g$ *hanno un fattore a comune di grado positivo in* x_1

Dimostrazione.

Consideriamo $f, g \in K[x_2, \dots x_n][x_1]$. Allora per il teorema 0.7 esistono due polinomi $A, B \in K[x_2, \dots x_n][x_1]$ tali che $Af + Bg = Res(f, g, x_1)$. Quindi $Res(f, g, x_1) \in (f, g) \cap K[x_2, \dots, x_n]$.
La seconda parte è esattamente il teorema 0.3 $\square$

Attenzione se il grado si abbassa

Osservazione critica Il risultante di due polinomi in piú variabili rispetto ad x_1 calcolato per un valore assegnato delle variabili rimanenti puó essere diverso dal risultante che si ottiene sostituendo subito i valori assegnati. Infatti nel secondo caso i gradi possono diminuire. Questa osservazione é cruciale per la comprensione della dimostrazione del teorema di estensione del prossimo capitolo. Ad esempio se $F(x_1, x_2) = (x_2 - 5)x_1 + 6$ e $G(x_1, x_2) = x_1^2 x_2^2 - (x_2 - 2)x_1 + 5x_2$ allora $Res(F(x_1, 0), G(x_1, 0), x_1) = -12$ e $Res(F, G, x_1)_{|\{x_2=0\}} = 60$
Dal teorema 0.8 i) sorge spontanea la domanda se, dati $f, g \in K[x, y]$, il polinomio in y $Res(f, g, x)$ è il generatore dell'ideale principale $(f, g) \cap K[y]$. L' esempio seguente dà una risposta negativa.

Esempio

Consideriamo $f = xy - 2$, $g = xy - 1$. In questo caso $Res(f, g, x) = y$ mentre $(f, g) \cap K[y] = (1)$. Notiamo che

Esercizi

Esercizio

Sia $p = x + y - 1$, $q = x^2 + y^2/4 - 1$, *poniamo* $I = (p, q) \subset K[x, y]$. *Provare che*

1. $V(I)$ *consiste dei due punti* $(-3, 5, 8/5), (1, 0)$.
2. $Res(p, q, x) = y(y - 8/5)$ *(a meno di scalari).*
3. *L'ideale di eliminazione* I_1 *è generato da* $y(y - 8/5)$. *Suggerimento. Sia* $\alpha(y)$ *il generatore dell'ideale di eliminazione. Per il Teorema 0.7 esistono* A, B *tali che* $\alpha(y) = A(x, y)p(x, y) + B(x, y)q(x, y)$. *Si sostituisca alle indeterminate rispettivamente i valori dei due punti di* $V(I)$.