

Il Risultante di due polinomi

Dato A un anello commutativo, con 1, dominio di integrità (ID), dominio a fattorizzazione unica (UFD), sia $A[x]$ l'anello dei polinomi in una indeterminata a coefficienti in A e siano $f = a_n x^n + \cdots + a_0$ e $g = b_m x^m + \cdots + b_0$ elementi di $A[x]$. Si pensi tranquillamente che $A = \mathbb{R}$ o $\mathbb{C}$.

Definizione 1 *Il risultante $R(f, g)$ di f e g è l'elemento di A definito come il determinante della matrice quadrata di dimensione $n + m$*

$$R(f, g) = \begin{vmatrix} a_n & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_n & \cdots & \cdots & a_0 \\ \hline b_m & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_m & \cdots & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_m & \cdots & b_0 \end{vmatrix}$$

Chiameremo *matrice risultante* la matrice il cui determinante è il risultante.

Osservazione. Il primo 'rettangolo' della matrice ha lunghezza $(n + 1) + (m - 1)$ ed altezza m , il secondo ha stessa lunghezza $(m + 1) + (n - 1)$ ed altezza n .

Proposizione 2 *Dati due polinomi f, g , il risultante $R(f, g)$ è nullo se e solo se esistono due polinomi φ, ψ in $A[x]$ con $\deg \varphi < \deg g$ e $\deg \psi < \deg f$ tali che $f\varphi + g\psi = 0$*

Dimostrazione: Il risultante è zero se e solo se ci sono elementi $u_0, \dots, u_{m-1}, v_0, \dots, v_{n-1}$ in A tali che la matrice risultante calcolata sul vettore $(u_0, \dots, u_{m-1}, v_0, \dots, v_{n-1})$ dà il vettore nullo. Questa condizione può essere riscritta nel seguente modo:

$$u_0 f + u_1 x f + \cdots + u_{m-1} x^{m-1} f + v_0 g + v_1 x g + \cdots + v_{n-1} x^{n-1} g = 0.$$

Quest'ultima è precisamente l'equazione $f\varphi + g\psi = 0$ con $\varphi = u_0 + u_1 x + \cdots + u_{m-1} x^{m-1}$ e $\psi = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$. Il fatto che i coefficienti potrebbero essere nel campo delle frazioni di A non è un problema, dal momento che si può moltiplicare φ e ψ per il denominatore comune dei loro coefficienti. Il viceversa è triviale. $\square$

Ricordiamo che se A è UFD allora anche $A[x]$ è UFD ([Herstein82] pag. 179).

Proposizione 3 *Il risultante $R(f, g)$ è nullo se e solo se f e g hanno fattori comuni in $A[x]$.*

Dimostrazione: Siano $f = f_1 \cdots f_h$ e $g = g_1 \cdots g_k$ fattorizzazioni di f e g . Se il risultante è nullo, allora esistono φ e ψ tali che $f\varphi + g\psi = 0$. Ma allora $f|\psi g$ e, siccome $\deg f > \deg \psi$, necessariamente f e g hanno fattori in comune. Il viceversa è immediato. $\square$

Esempio. Sia $f = ax^2 + bx + c$ e $g = \alpha x + \beta$. Il risultante è $R(f, g) = \alpha^2 (a(\beta/\alpha)^2 + c - b(\beta/\alpha))$; ovvero $R(f, g) = 0$ se e solo se $-\beta/\alpha$ è radice di f , ovvero se e solo se $f = (\alpha x + \beta)(\gamma x + \delta)$.

Esempio. Sia $f = ax^2 + bx + c$ e $g = f' = 2ax + b$. Il risultante è nullo se e solo se $4a(b^2 - ac) = 0$, ovvero se e solo se il solito discriminante è nullo.

Definizione 4 *Il discriminante $D(f)$ di un polinomio f è il risultante di f e della sua derivata prima f' . In formule: $D(f) = R(f, f')$.*

Osservazione. Nel caso speciale in cui $A = \mathbb{C}$, allora $D(f) = 0$ se e solo se f ha radici multiple.

Esempio. Computare il discriminante del generico polinomio cubico monico $f = x^3 + ax^2 + bx + c$ e per la famiglia di polinomi cubici in forma normale $f = x^3 + px + q$. Il risultante $R(f, f')$ è

$$\begin{vmatrix} c & b & a & 1 & 0 \\ 0 & c & b & a & 1 \\ \hline b & 2a & 3 & 0 & 0 \\ 0 & b & 2a & 3 & 0 \\ 0 & 0 & b & 2a & 3 \end{vmatrix} = -(a^2 b^2) + 4b^3 + 4a^3 c - 18abc + 27c^2$$

Nel caso particolare in cui $a = 0$ (ovvero quando il polinomio di terzo grado è scritto nella forma canonica $x^3 + px + q$, forma che si può ottenere con la traslazione $x \mapsto x + a/3$) allora il discriminante è $4p^3 + 27q^2$.