Resultant, applications à l'intersection de courbes et surfaces algébriques.

I) Le résultant, propriétés algébriques

1) définition dans un anneau commutatif A

cadre : A anneau commutatif unitaire
$A_d[X]$ désigne le sous-module de $A[X]$ des poly. de deg $\le d$

déf : $P, Q \in A[X]$ $\deg P = p$ $\deg Q = q$ $p \le q$
on considère $\Phi_{P,Q} : A_{q-1}[X] \times A_{p-1}[X] \longrightarrow A_{p+q-1}[X]$
$(U, V) \longmapsto UP + VQ$

Dans les bases canoniques la matrice de $\Phi_{P,Q}$ est
$(0,\dots,0,X^{q-1},0)$ dire plutôt base de monômes.

$$\begin{pmatrix} a_p & 0 & \cdots & 0 & b_q & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & \vdots & \ddots & & b_q \\ a_0 & & \ddots & a_p & b_0 & & \ddots & \vdots \\ 0 & \ddots & & \vdots & & \ddots & & b_q \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{pmatrix}$$
$\underbrace{\qquad}_{q}$ $\underbrace{\qquad}_{p}$

$(1, \dots 0)$
$(0\ 0, \dots X^{p-1})$ où B

$$\begin{cases} P = a_0 + \cdots + a_p X^p \\ Q = b_0 + \cdots + b_q X^q \end{cases}$$

On définit $\mathrm{Res}(P, Q) = \det(\Phi_{P,Q})$

ex : $\mathrm{Res}(aX^2 + bX + c, \alpha X + \beta) = \begin{vmatrix} a & \alpha & 0 \\ b & \beta & \alpha \\ c & 0 & \beta \end{vmatrix} = \alpha^2 c + a\beta^2 - \alpha b \beta$

2) Résultant universel pour $A_{p,q} = \mathbb{Z}[U_0, \dots, U_p, V_0, \dots, V_q]$

déf : Le résultant universel de taille (p,q) est le résultant $R(U,V)$ des deux polynômes $P_U = U_0 + U_1 X + \cdots + U_p X^p$ $Q_V = V_0 + \cdots + V_q X^q$ dans l'anneau $A_{p,q} = \mathbb{Z}[U_0, \dots U_p, V_0, \dots, V_q]$ aussi noté $\mathbb{Z}[U,V]$

Rq : on obtient le résultant de deux polynômes dans un anneau quelconque par spécialisation.

propriétés : i) $R(ZU, V) = Z^q \cdot R(U,V)$ $R(U, ZV) = Z^p R(U,V)$
(R est homogène de degré q en $(U_0, \dots, U_p)$ et de degré p en $(V_0, \dots, V_q)$)

ii) il existe $\Phi_{U,V}(X), \Psi_{U,V}(X) \in \mathbb{Z}[U,V][X]$ tels que $\Phi_{UV}(X) P_U(X) + \Psi_{UV}(X) Q_V(X) = R(U,V)$

coroll : si K sous corps d'un corps L, si $P, Q \in K[X]$ ont une racine commune dans L alors $\mathrm{Res}(P,Q) = 0$

3) expressions en fonction des racines $A = \mathbb{Z}[U_p, \alpha_1, \dots, \alpha_p, V_q, \beta_1, \dots, \beta_q]$

Th : on considère $P = U_p \prod_{i=1}^{p} (X - \alpha_i) = U_p X^p + U_{p-1} X^{p-1} + \cdots + U_0$
$Q = V_q \prod_{j=1}^{q} (X - \beta_j) = V_q X^q + V_{q-1} X^{q-1} + \cdots + V_0$

$\left[\text{où } U_i = (-1)^{p-i}\, U_p \times \sum_{1 \le i_1 < \cdots < i_{p-i} \le p} \alpha_{i_1} \cdots \alpha_{i_{p-i}}\right]$

Alors $\boxed{\mathrm{Res}(P, Q) = U_p^q V_q^p \prod_{i,j} (\beta_j - \alpha_i)}$
$= V_q^p \prod_{j=1}^{q} P(\beta_j) = (-1)^{pq} U_p^q \prod_{i=1}^{p} Q(\alpha_i)$

Application : si K est un corps algébriquement clos, $P, Q \in K[X]$
Alors P et Q sont scindés et on peut spécialiser les relations ci dessus pour le calcul du résultant.

corollaire 1 : soit K un corps $P, Q \in K[X]$ scindés dans une extension L de K sont équivalents : (i) $\mathrm{Res}(P,Q) = 0$ (avec $p = \deg P$, $q = \deg Q$)
(ii) P, Q ont un zéro commun dans L ou $a_p = 0$ et $b_q = 0$
(iii) P, Q ont un facteur irréductible commun ou $a_p = 0$ et $b_q = 0$

application : construction d'un polynôme annulateur pour $\alpha + \beta$, $\alpha\beta$ si α, β sont algébriques sur un corps K.

corollaire 2 : le résultant universel est irréductible dans $\mathbb{Z}[U,V]$

4) utilisation dans un anneau de polynômes. $A = K[X_1, \dots, X_{n-1}]$

définition : K corps Alors On considère $A = K[X_1, \dots, X_{n-1}]$
si $P, Q \in K[X_1, \dots, X_n]$, on définit
$\mathrm{Res}_{X_n}(P,Q) \in K[X_1, \dots, X_{n-1}]$ en voyant $P, Q \in A[X_n]$

ex : $P = X^2 + 2X - XY + 2Y - 6$ $Q = 3X^2 - 5X + 5 + XY - 2Y$
$\mathrm{Res}_X(P, Q) = 36Y^2 - 211Y + 309$

prop : $P, Q \in K[X_1, \dots, X_n]$ homogènes de degré p, q respect.

Alors $\mathrm{Res}_{X_n}(P, Q) \in K[X_1, \dots, X_{n-1}]$ homogène de degré pq

ex : $\mathrm{Res}_Y (X^2+Y^2, X^2Y + X^3) = 2X^6$

→ que se passe-t-il qd les pol ne st pas homogènes
↳ on peut ptet les homogénéiser
on trouve deg $\leq pq$ qd on fait le résultant et qu'on vire la variable ajoutée

corollaire à 12

Soit $P, Q \in K[X_1, \dots, X_n]$ $\quad x_1, \dots, x_n \in K$

$$\left.\begin{array}{l} P(x_1, \dots, x_n) = 0 \\ Q(x_1, \dots, x_n) = 0 \end{array}\right\} \Rightarrow \left[\mathrm{Res}_{X_n}(P, Q)\right](x_1, \dots, x_{n-1}) = 0$$

II Élimination.

On se donne un système d'équations polynômiales

$$(1)\begin{cases} x^2+y+z = 1 \\ x+y^2+z = 1 \\ x+y+z^2 = 1 \end{cases}$$

On cherche à le résoudre. Pour cela on élimine successivement des variables à l'aide du résultant. Ici on obtient $z^6 - 4z^4 + 4z^3 - z^2 = 0$ (2) (si (x,y,z) vérifie (1) alors z vérifie (2)).

On résout (2) et on détermine les valeurs de z trouvées qui se relèvent en des solutions de (1) (c'est l'extension).

1) Définitions.

Idéal d'élimination. $\quad f, g \in K[X_1, \dots, X_{n-1}][X_n] \qquad f = \sum f_i X_n^i$

$$I_n = \langle f, g \rangle \cap K[X_1, \dots, X_{n-1}]$$

Prop. $h = \mathrm{Res}_{X_n}(f, g)$. Si $(\alpha_1, \dots, \alpha_n) \in \overline{K}^n$ est un zéro commun à f et g alors $h(\alpha_1, \dots, \alpha_{n-1}) = 0$

Extension. $h = \mathrm{Res}_{X_n}(f, g)$. On suppose que $(\alpha_1, \dots, \alpha_{n-1}) \in \overline{K}^{n-1}$ vérifie $h(\alpha_1, \dots, \alpha_{n-1}) = 0$. Alors $\exists\, \alpha_n \in \overline{K}$ tel que $(\alpha_1, \dots, \alpha_n)$ soit un zéro commun à f et g si on a pas

$f_i(\alpha_1, \dots, \alpha_{n-1}) = 0 \quad \forall i$

ou $g_i(\alpha_1, \dots, \alpha_{n-1}) = 0 \quad \forall i$

ou $f_m(\alpha_1, \dots, \alpha_{n-1}) = g_n(\alpha_1, \dots, \alpha_{n-1}) = 0 \quad \begin{pmatrix} m = \deg_{X_n} f \\ n = \deg_{X_n} g \end{pmatrix}$

2) Interprétation géométrique.

$\pi_n : (x_1, \dots, x_n) \longmapsto (x_1, \dots, x_{n-1}) \qquad \overline{K}^n \to \overline{K}^{n-1}$

Prop. $V(I_n) = \pi_n(V) \cup \left(V(f_m, g_n) \cap V(I_n)\right)$

avec les notations précédentes.

(où $V(I) = \{x \in \overline{K}^k \mid \forall h \in I \quad h(x) = 0\}$ où I idéal de $K[X_1, \dots, X_k]$ « variété algébrique »)

Intuitivement $V(I_n)$ contient l'ens. des solutions partielles, $\pi_n(V)$ ne contient que les solutions partielles relevables en des solutions de tout le système.

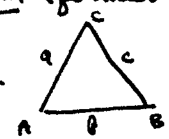
Ex. $\begin{cases} xz = 1 \\ xy = 1 \end{cases}$ (*) $\quad f = zx - 1,\ g = yx - 1 \in K[y,z][x]$

$$I_n = \langle f, g \rangle \cap K[y,z] = \langle y - z \rangle$$

(car $\quad \mathrm{Res}_x \langle f, g \rangle = \begin{vmatrix} -1 & -1 \\ z & y \end{vmatrix} = z - y$)

Si (x,y,z) vérifie (*) alors $y = z$. Mais pour $y = z = 0$ ne se relève pas en une solution de (*) (dans ce cas f et g ne sont plus de degré 1 en x).

Ex. (formule de Héron, méthode brutale) (élimination)



S l'aire du triangle alors

$$S^2 = p(p-a)(p-b)(p-c) \quad \text{avec } p = \tfrac{1}{2}(a+b+c)$$

3) Intersections de deux courbes dans $\mathbb{R}^2$.

Pour des courbes implicitement on élimine une des variables x ou y et on résout l'équation obtenue.

$$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases} \qquad \mathbb{R}[y][x]$$

Ex. $\begin{cases} x^4 + y^4 - 1 = 0 \\ x^5y^2 - 4x^3y^3 + x^2y^5 - 1 = 0 \end{cases}$

$$\begin{aligned} \mathrm{Res}_x(f,g) = {} & 2y^{28} - 16y^{27} + 32y^{26} + 249y^{24} + 48y^{23} - 128y^{22} \\ & + 4y^{21} - 757y^{20} - 112y^{19} + 192y^{18} - 12y^{17} + 758y^{16} \\ & + 144y^{15} - 126y^{14} + 28y^{13} - 251y^{12} - 64y^{11} + 30y^{10} \\ & - 36y^9 - y^8 + 16y^5 + 1 \end{aligned}$$

(sympa)

On trouve numériquement les y solutions (il y en a 4) (et comme le coeff. de x^4 ne s'annule pas les solutions se relèvent).

4) Implicitation d'une courbe rationnelle.

Prop. si $\mathcal{C} = \{ (\frac{a(t)}{b(t)}, \frac{c(t)}{d(t)}) \in \mathbb{R}^2, \ t \in \mathbb{R} \}$ a, b, c, d polynômes.
Alors $\mathrm{Res}_t (b(t)x - a(t), d(t)y - c(t)) = 0$ est une équation implicite de $\mathcal{C}$.

Ex. On considère le trèfle à quatre feuilles paramétrés en coordonnées polaires par $r(\theta) = \sin(2\theta)$ 
Alors $(x^2+y^2)^3 = 4x^2y^2$ est une équation implicite du trèfle.

Enveloppes. Soit $F \in K[x,y,t]$.
On note $V(t) = \{(x,y) \mid F(x,y,t) = 0\}$.
F défini une famille de courbes.

Déf. L'enveloppe de F est
$$\{(x,y) \mid \exists t \quad F(x,y,t) = \frac{\partial F}{\partial t}(x,y,t) = 0\}$$

Ex. $F(x,y,t) = (x-t)^2 + (y-t^2)^2 - 4$ (cercle de rayon 2 se baladant sur la parabole (t, t^2))
L'enveloppe est contenue dans
$$\{(x,y) \in \mathbb{R}^2 \mid 16y^4 - 32x^2y^3 - 136y^3 + 16x^4y^2 - 96x^2y^2 + 225y^2 - 40x^2y + 30x^2y + 544y + 16x^6 - 131x^4 + 1688x^2 - 1156 = 0\}$$

Ex. (tout aussi sympathique) La caustique d'un cercle de rayon 1 est une épicycloïde d'équation $(4(x^2+y^2)-1)^3 = 27y^2$
(c'est la courbe que vous observez tous les matins dans votre tasse à café ou votre bol de lait !)
$F(x,y,\alpha) = \sin(2\alpha)x - \cos(2\alpha)y - R\sin\alpha$

5) Théorème de Bézout.

discriminant.

Soit $P \in K[X]$ $P = X^p + a_{p-1}X^{p-1} + \dots + a_0$ K corps
$\alpha_1, \dots, \alpha_p$ les racines de P dans $\overline{K}$ un corps algébriquement clos contenant K

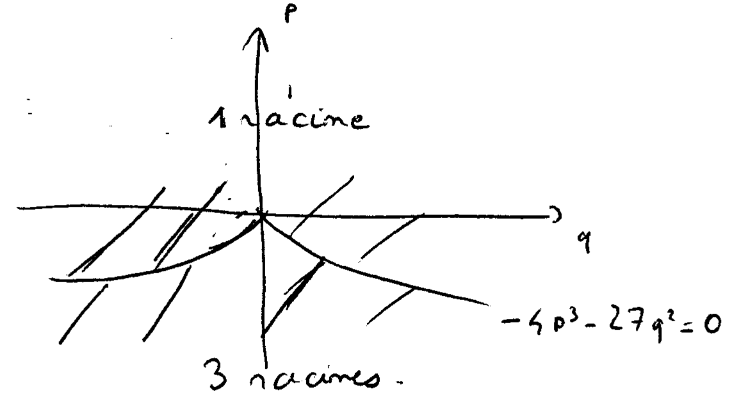
on définit $\mathrm{disc}(P) = \prod_{1 \le i < j \le p} (\alpha_i - \alpha_j)^2$

prop : $\mathrm{disc}(P) = (-1)^{\frac{p(p-1)}{2}} \mathrm{res}(P, P')$

ex : $\mathrm{Disc}(X^3 + pX + q) = -4p^3 - 27q^2$

Thm : (P et P' ont un facteur commun non constant) $\Leftrightarrow \mathrm{disc}(P) = 0$

Appli. ici $K = \mathbb{R}$ soit $p, q \in \mathbb{R}$
on note $f_{p,q}(X) = X^3 + pX + q$
alors $(p,q) \longmapsto \#\{x \in \mathbb{R} \ f_{p,q}(x) = 0\}$ est constant sur les composante connexe de $\{\Delta(f_{p,q}) = 0\}$



Références. Deux articles de M. Coste sur le site de la prépa :

- Élimination, résultant. Discriminant.
- Systèmes d'éq. linéaires et courbes passant par des points fixés.

Lang, Lelong-Ferrand Arnaudiès

Voir Gozlot aussi pr les bases de Gröbner

Articles :

- Le th. de Bézout et le résultant de deux polynômes, Michel Waldschmidt (publié dans la RMS n° 114-1)

  Gourdon ds le cas d'un corps

- Intro. to Resultants, Bernd Sturmfels (publié dans Applications of Computational Algebraic Geometry par l'AMS)

- chapitre 3 (Elimination Theory) de David Cox, John Little, Donald O'Shea, Ideals, varieties and algorithms
- Algebraic Geometry, Brendan Hassett.

Dynamaths est réssucité !