1 Quelques rappels sur le multivarié

Soit A un anneau commutatif. Pour tout $i \in \{1; \dots; n\}$,

$$A[X_1, \dots, X_n] \simeq A[X_1, \dots, X_{i-1}, X_{i+1} \dots X_n][X_i]$$

ce qui permet de voir un polynôme multivarié comme un polynôme univarié à coefficient dans l'anneau $A[X_1, \dots, X_{i-1}, X_{i+1} \dots X_n]$ et de définir son degré partiel en X_i.

Théorèmes de transfert

- A intègre $\Rightarrow$ $A[X]$ intègre $\Rightarrow$ $A[X_1, \dots, X_n]$ intègre
- A factoriel $\Rightarrow$ $A[X]$ factoriel (Gauss) $\Rightarrow$ $A[X_1, \dots, X_n]$ factoriel ; en particulier on peut définir les pgcd, ppcm
- A noethérien $\Rightarrow$ $A[X]$ noethérien $\Rightarrow$ $A[X_1, \dots, X_n]$ noethérien

Attention : $A[X]$ principal $\iff$ A est un corps ; en particulier :

- $A[X_1, \dots, X_n]$ n'est jamais principal si $n \geqslant 2$; le théorème des restes chinois et le lemme de Bézout ne sont pas satisfaits
- si A n'est pas un corps, alors il n'y a pas de division euclidienne sauf si le coefficient dominant du diviseur est inversible

Remarque sur les racines de $P \in A[X_1, \dots, X_n]$

- Si $P(X_1, \dots, X_{n-1}, a) = 0$, alors $X_n - a | P$ (faire une division euclidienne)
- Par contre si $P(a_1, \dots, a_n) = 0$ alors $P \in (X_1 - a, \dots, X_n - a)$ et on ne peut rien dire de plus a priori.

2 Définitions, premières propriétés

Les résultants ont d'abord été introduits pour déterminer quand deux polynômes P et Q à coefficients dans un corps ont une racine commune dans une extension de K ou dit autrement un facteur commun non trival. Ce problème peut se reformuler sous la forme d'un problème d'algèbre linéaire en se ramenant au problème de déterminer s'il existe deux polynômes non nuls F et G à coefficients dans K tels que $FP = GQ$ avec $\deg F < \deg Q$ et $\deg G < \deg P$ (la condition sur le degré est importante sinon le problème aurait une solution triviale (Q, P)). En effet, si $R = P \wedge Q \neq 1$ alors le couple $(Q/R, P/R)$ convient, tandis que si $P \wedge Q = 1$ et que $FP = GQ$, alors par le lemme de Gauss $P \mid G$ donc $G = 0$ ou $\deg G \geqslant \deg P$.

On peut alors considérer le déterminant de l'application linéaire $(F, G) \in K[X]_{<\deg Q} \times K[X]_{<\deg P} \mapsto FP - GQ \in K[X]_{<\deg P + \deg Q}$ pour tester si le noyau est trivial ou pas.

Dans toute la suite, A désigne un anneau intègre commutatif, et $K = \mathrm{Fr}(A)$ son corps des fractions. Soient $P, Q \in A[X]$ deux polynômes de degré m et n respectivement.

Lemme 2.1. *Les polynômes P et Q sont premiers entre eux dans $K[X]$ si et seulement si*
$\begin{array}{ccc} \Psi : K[X]_{<n} \times K[X]_{<m} & \to & K[X]_{n+m} \\ (U,V) & \mapsto & UP+VQ \end{array}$ *est bijective.*

Proof. $\Leftarrow$ Si l'application est bijective, elle est surjective en particulier le polynôme constant égal à 1 est atteint et le lemme de Bézout donne le résultat.
$\Rightarrow$ Soient $(U,V) \in \ker \Psi$, alors $UP = -VQ$ donc $P|VQ$. L'hypothèse de co-primalité sur P et le lemme de Gauss donne alors $P|V$; mais comme $\deg V < \deg P$, nécessairement $V = 0$. On montre de même que $U = 0$, donc Ψ est injective et bijective par égalité des dimensions des espaces vectoriels de départ et d'arrivée. □

Matrice de Sylvester

On définit la matrice de Sylvester de P et Q comme (la transposée de) la matrice de l'application Ψ dans les bases $\mathcal{B}_1 = \{(X^{n-1},0),\dots,(X,0),(1,0),(0,X^{m-1}),\dots,(0,X),(0,1)\}$ et $\mathcal{B}_2 = (X^{n+m-1},\dots,X,1)$

En particulier, si $P = \sum_{k=1}^{m} a_k X^k$ et $Q = \sum_{k=1}^{n} b_k X^k$ (avec $a_m b_n \neq 0$), alors

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a_m & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & \dots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & \dots & a_0 \\ b_n & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & \dots & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & \dots & b_0 \end{pmatrix}$$

où l'on a répété $\deg Q$ (resp. $\deg P$) fois la ligne avec les coefficients de P (resp. Q).

Exercice : se forcer à écrire la matrice lorsque $m = 4$, $n = 3$

$$\begin{pmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{pmatrix} \in \mathcal{M}_7(A)$$

Définition 2.2. *Le résultant de P et Q (en la variable X) est défini par*

$$Res_X(P,Q) = \det(Syl(P,Q)).$$

Propriété 2.3. *On a équivalence entre les propriétés suivantes :*

1. $Res_X(P,Q) = 0$
2. *Ψ n'est pas bijective*

3. *P et Q ne sont pas premiers entre eux dans $K[X]$*
4. *P et Q ont une racine commune dans une extension de K*
5. *$P \wedge Q \notin A$ (si A est factoriel)*

Proof. Assez clairement, on a $1 \iff 2 \iff 3 \iff 4$ et $5 \Rightarrow 3$. On va montrer que $3 \Rightarrow 5$.
Soit $R \in K[X]$ de degré $\geqslant 1$ le pgcd (unitaire) de P, Q dans $K[X]$. On peut trouver $\lambda \in K^*$ tel que $S = \lambda R \in A[X]$ primitif, c'est encore un diviseur commun de P et Q dans $K[X]$. En particulier il existe $P_0, Q_0 \in K[X]$ tels que $P = SP_0$ et $Q = SQ_0$. Soit $\mu \in A$ tel que $\mu P_0 \in A[X]$, le lemme de Gauss sur les contenus donne alors $c(\mu P) = \mu c(P) = c(\mu P_0)$ donc $\mu | c(\mu P_0)$ dans A, et μ divise tous les coefficients de μP_0 donc $P_0 \in A[X]$. Le même argument permet de montrer que $Q_0 \in A[X]$. Donc R est un diviseur commun à P et Q dans $A[X]$. □

Autres propriétés du résultant

Propriété 2.4.
- *$Res_X(P, Q) = (-1)^{mn} Res_X(Q, P)$*
- *$Res_X(\lambda P, \mu Q) = \lambda^n \mu^m Res_X(P, Q)$*
- *$Res_X(P, Q)$ est un polynôme en chacun des coefficients de P (resp. Q) de degré total $\leqslant n$ (resp. $\leqslant m$).*

Proof. Les deux premières égalités découlent des propriétés classiques du déterminant (forme multilinéaire alternée). Le dernier point se déduit de la formule du déterminant

$$\det(m_{ij}) = \sum_{\sigma \in \mathfrak{S}_{n+m}} \epsilon(\sigma) \prod_{i=1}^{m+n} m_{i\sigma(i)}$$

où l'on voit que dans chaque terme un coefficient de la matrice n'apparait qu'une et une seule fois ; en particulier comme les coefficients de P n'apparaissent qu'une fois en au plus n lignes, le degré total en les coefficients de P est au plus n. □

Exemples :

- Si $\lambda \in A$, $\mathrm{Res}_X((X-\lambda), Q) = Q(\lambda)$, en développant le résultant par rapport à la dernière colonne

$$\begin{vmatrix} 1 & -\lambda & 0 & \dots & 0 \\ 0 & 1 & -\lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 & -\lambda \\ b_n & \dots & \dots & \dots & b_0 \end{vmatrix} = b_0 - (-\lambda) \begin{vmatrix} 1 & -\lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & -\lambda & \\ b_n & \dots & \dots & b_1 & \end{vmatrix} = b_0 + \lambda(b_1 + \lambda(b_2 + \dots)) = Q(\lambda)$$

- Soit $P = aX^2 + bX + c \in A[X]$ et $P' = 2aX + b$. Alors en développant par rapport à la première colonne le déterminant :

$$\mathrm{Res}_X(P, P') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(b^2 - 2(b^2 - 2ac)) = a(4ac - b^2) = -a\Delta(P).$$

Autrement dit : P a une racine double $\iff P \wedge P' \neq 1 \iff \mathrm{Res}_X(P,P') = 0 \iff \Delta(P) = 0$.

Remarque : : plus généralement, le discriminant d'un polynôme $P \in A[X]$ est égal à une constante près à $\mathrm{Res}_X(P,P')$ qui s'annule si et seulement si P n'est pas à racine simple dans une extension.

- Si $P = X^3 + pX + q$, alors $P' = 3X^2 + p$ et

$$\mathrm{Res}_X(P,P') = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 0 & 0 & -2p & -3 \\ 0 & 0 & 3 & 0 & -p \end{vmatrix} = -2p(-2p^2) + 3(9q^2) = 4p^3 + 27q^2.$$

3 Résultants multivariés, spécialisation

On considère deux polynômes multivariés $P, Q \in A[X,Y]$. On peut alors calculer $\mathrm{Res}_X(P,Q) \in A[Y]$ (ou $\mathrm{Res}_Y(P,Q) \in A[X]$). Si on note $a_m(Y)$ et $b_n(Y)$ les coefficients dominants de P et Q vus comme polynômes à coefficients dans $A[Y]$, alors pour tout $y \in A$, on a

$$(a_m(y)b_n(y) \neq 0) \Rightarrow (\mathrm{Res}_X(P,Q)(y) = \mathrm{Res}_X(P(X,y), Q(X,y)))\,.$$

Il est important de remarquer que si $a_m(y) = 0$ ou $b_m(y) = 0$, alors $\deg_X(P(X,y)) < \deg_X P$ et les résultants ne s'obtiennent plus avec les mêmes matrices de Sylvester. Plus précisément

Propriété 3.1. *Si $a_m(y) \neq 0$, on a $Res_X(P,Q)(y) = a_m(y)^{n-\deg Q(X,y)} Res_X(P(X,y), Q(X,y))$.*

Pour éviter cet écueil, on peut utiliser la notation $R_{m,n,X}(P,Q)$ afin de préciser la taille du déterminant.

Exemple : Le résultant de $P(X,Y) = XY^2 + 2XY - 1$ et $Q(X,Y) = X^2Y^2 - XY - 2X - 2$ est

$$R(Y) = -Y(Y+1)(Y^2 + \frac{7}{2}Y + 2)$$

On a $R(-1) = 0$; d'ailleurs $P(X,-1) = -X - 1$ et $Q(X,-1) = (X+1)(X+2)$ ont bien un facteur commun.
On a $R(0) = 0$; pourtant $P(X,0) = -1$ et $Q(X,0) = -2X - 2$ n'ont pas de facteur commun. En évaluant Y en 0, on observe une chute du degré en X de P et de Q.

Application au calcul de polynômes annulateurs
Soient α, β des nombres algébriques et $P, Q \in \mathbb{Z}[X]$ leurs polynômes minimaux. Comment calculer un polynôme annulateur de $\alpha + \beta$? le polynôme minimal ?

On considère $R(Y) = \mathrm{Res}_X(Q(Y-X), P(X)) \in \mathbb{Z}[Y]$; les polynômes $P(X)$ et $Q(Y-X)$ vus comme polynômes en X à coefficients dans $\mathbb{Z}[Y]$ sont bien de coefficients dominants constants en Y. On peut donc spécialiser en $y = \alpha + \beta \in \mathbb{C}$ où α est une racine commune de $Q(\alpha + \beta - X)$ et $P(X)$ et on a bien $R(\alpha + \beta) = 0$.

Si Q est un polynôme irréductible sur $\mathbb{Q}(\alpha)[X]$ et $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$, alors

$$[\mathbb{Q}(\alpha+\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg Q \deg P$$

et le degré du polynôme minimal de $\alpha+\beta$ sur $\mathbb{Q}$ est $\deg P \deg Q$. Or comme le résultant R est un polynôme de degré total $\leqslant \deg P$ en les coefficients de $Q(Y-X) \in \mathbb{Z}[Y][X]$ et que $\deg_Y Q(X,Y) = \deg Q$, son degré est inférieur ou égal à $\deg P \deg Q$ et c'est bien le polynôme minimal de $\alpha+\beta$ sur $\mathbb{Q}$.

Exemple : calcul du polynôme minimal de $\sqrt[3]{2}+i$ sur $\mathbb{Q}[X]$
On pose $P(X) = X^3-2$ et $Q(X) = X^2+1$. On a alors

$$\begin{aligned}
\mathrm{Res}_X(((Y-X)^2+1, X^3-2) &= \mathrm{Res}_X(X^2-2XY+Y^2 1, X^3-2) \\
&= \begin{vmatrix} 1 & -2Y & Y^2+1 & 0 & 0 \\ 0 & 1 & -2Y & Y^2+1 & 0 \\ 0 & 0 & 1 & -2Y & Y^2+1 \\ 1 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 \end{vmatrix} = \begin{vmatrix} 1 & -2Y & Y^2+1 & 0 & 0 \\ 0 & 1 & -2Y & Y^2+1 & 0 \\ 0 & 0 & 1 & -2Y & Y^2+1 \\ 0 & 2Y & -Y^2-1 & -2 & 0 \\ 0 & 0 & 2Y & -Y^2-1 & -2 \end{vmatrix} \\
&= \begin{vmatrix} 1 & -2Y & Y^2+1 & 0 \\ 0 & 1 & -2Y & Y^2+1 \\ 0 & 3Y^2-1 & -2Y^3-2Y-2 & 0 \\ 0 & 0 & 3Y^2-1 & -2Y^2-2Y-2 \end{vmatrix} = \begin{vmatrix} 1 & -2Y & Y^2+1 \\ 0 & 4Y^3-4Y-2 & -3Y^4-2Y^2+1 \\ 0 & 3Y^2-1 & -2Y^3-2Y-2 \end{vmatrix} \\
&= (4Y^3-4Y-2)(-2Y^3-2Y-2) + (3Y^2-1)(3Y^4+2Y^2-1) = Y^6+3Y^4-4Y^3+3Y^2+12Y+5
\end{aligned}$$

Exercice : calculer le polynôme annulateur de $\alpha\beta$ avec des résultants.
On vérifie que $\mathrm{Res}_X(X^{\deg Q}Q(Y/X), P(X))$ admet pour racine $\alpha\beta$, en s'assurant que comme Q est irréductible son coefficient constant est non nul.

4 Résultants et élimination

Jusqu'à présent, on a vu deux propriétés élémentaires du résultant :

- le résultant de deux polynômes est un polynôme en les coefficients des deux polynômes dont on contrôle le degré
- le résultant de deux polynômes est nul si et seulement si les deux polynômes ont un facteur non trivial dans $K[X]$ où K est le corps de fractions de l'anneau des coefficients des polynômes

Une troisième propriété intéressante du résultant est d'appartenir à l'idéal engendré par P et Q, ce qui permet de faire de l'élimination de variables utile pour la recherche de racines de systèmes de polynômes multivariés.

Propriété 4.1. *Soient $P, Q \in A[X]$, alors il existe $U, V \in A[X]$ tels que $Res_X(P,Q) = UP + VQ \in ((P)+(Q)) \cap A$.*

Proof. On calcule le déterminant dans $A[X]$, sur-anneau de A en remplaçant la dernière colonne C_{m+n}

par $C_{m+n} + XC_{m+n-1} + \cdots + X^{n+m-1}C_1$:

$$\begin{vmatrix} a_m & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & \dots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & \dots & a_0 \\ b_n & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & \dots & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & \dots & b_0 \end{vmatrix} = \begin{vmatrix} a_m & \dots & \dots & \dots & \dots & a_0 & 0 & \dots & X^{n-1}P(X) \\ 0 & a_m & \dots & \dots & \dots & \dots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & XP(X) \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & \dots & P(X) \\ b_n & \dots & \dots & \dots & b_0 & 0 & \dots & \dots & X^{m-1}Q(X) \\ 0 & b_n & \dots & \dots & \dots & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & XQ(X) \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & \dots & Q(X) \end{vmatrix}$$

Un développement par rapport à la dernière colonne donne alors $\mathrm{Res}_X(P,Q) = UP+VQ$ avec $\deg U < \deg Q$ et $\deg V < \deg P$.

□

Plus généralement, si $f, g \in K[X_1, \dots, X_n]$, alors $\mathrm{Res}_{X_1}(f,g)$ appartient au premier idéal d'élimination $I_1 = ((f) + (g)) \cap K[X_2, \dots, X_n]$ qui est un idéal de $K[X_2, \dots, X_n]$.

Corollaire 4.2. *Soient $f, g \in K[X_1, \dots, X_n]$. Pour tout $(x_1, \dots, x_n) \in K^n$*

$$(f(x_1, \dots, x_n) = g(x_1, \dots, x_n) = 0) \Rightarrow Res_{X_1}(f,g)(x_2, \dots, x_n) = 0.$$

On note souvent $V(f,g)$ l'ensemble des points de K^n annulant f et g : c'est la variété algébrique associée à l'idéal $(f) + (g)$ qui correspond à l'intersection de deux hypersurfaces.

La réciproque de l'implication du corollaire est partiellement vraie :

Théorème 4.3 (Théorème d'extension)**.** *Soient $f = a_p(X_2, \dots, X_n)X_1^p + \cdots + a_0(X_2, \dots, X_n) \in K[X_2, \dots, X_n][X_1]$ et $g = b_q(X_2, \dots, X_n)X_1^q + \cdots + b_0(X_2, \dots, X_n) \in K[X_2, \dots, X_n][X_1]$ avec $p = \deg_{X_1} f$ et $q = \deg_{X_1} g$.*
Soit $(x_2, \dots, x_n) \in K^{n-1}$ tel que $Res_{X_1}(f,g)(x_2, \dots, x_n) = 0$.
Si $a_p(x_2, \dots, x_n) \neq 0$ ou $b_p(x_2, \dots, x_n) \neq 0$, alors il existe $x_1 \in \bar{K}$ tel que $f(x_1, \dots, x_n) = g(x_1, \dots, x_n) = 0$.

Autrement dit, si on note $\pi : (x_1, \dots, x_n) \in K^n \mapsto (x_2, \dots, x_n) \in K^{n-1}$ la projection sur les $n-1$ dernières coordonnées, et si K est algébriquement clos

$$\pi(V(f,g)) \subset V(Res_{X_1}(f,g)) \subset \pi(V(f,g)) \cup V(a_p, b_q).$$

Proof. Sans perte de généralité on peut supposer $a_p(x_2, \dots, x_n) \neq 0$. Alors

$$\mathrm{Res}_{X_1}(f,g)(x_2, \dots x_n) = 0 = a_p(x_2, \dots, x_n)^{q - \deg_{X_1}(g(X_1, x_2, \dots, x_n))} \mathrm{Res}_{X_1}(f(X_1, x_2, \dots, x_n), g(X_1, x_2, \dots, x_n)).$$

Donc $\mathrm{Res}_{X_1}(f(X_1, x_2, \dots, x_n), g(X_1, x_2, \dots, x_n)) = 0$ et il existe $x_1 \in \bar{K}$ racine commune de $f(X_1, x_2, \dots, x_n)$ et $g(X_1, x_2, \dots, x_n)$. □

Exercice 1 de la feuille de TP :

1. Intersection de courbes planes.
   Le résultant $\mathrm{Res}_X(f,g) = 4Y^3 - 4Y^2 - 3Y = Y(2Y-3)(2Y+1)$ admet trois racines :
   - la racine $y = 0$ ne se complète pas en une solution puisque les coefficients dominants s'annulent.
   - la racine $y = 3/2$ donne le système $\{3X + 2 = 0; 6X + 9 - 6 + 1 = 0\}$ qui se remonte en une solution $(-2/3, 3/2)$.
   - la racine $y = -1/2$ se remonte en $(2, -1/2)$.

   Il y a donc deux points d'intersection.

2. Intersection d'un cercle avec une ellipse.
   Le résultant $\mathrm{Res}_X(f,g) = (Y^2-4)^2$ a deux racines $y = \pm 2$ qui n'annulent pas les termes de tête des polynômes. Le théorème d'extension s'applique mais quand on réinjecte, on obtient $x^3 + 2 = 0$ soit $x = \pm i\sqrt{3} \notin \mathbb{R}$.

Autre application : implicitation de courbes paramétrées

On souhaite trouver une équation cartésienne d'une courbe paramétrée

$$\mathcal{C} : \begin{cases} x(t) = \frac{p_1(t)}{q_1(t)} \\ y(t) = \frac{p_2(t)}{q_2(t)} \end{cases}$$

donnée par deux fractions rationnelles de $K(t)$.

Proposition 4.4. *Soit $C(X,Y) = Res_T(Xq_1(T) - p_1(T), Yq_2(T) - p_2(T))$. Alors $\mathcal{C} \subset \{(x,y) : C(x,y) = 0\}$.*

Proof. Soit $(x,y) \in \mathcal{C}$, alors il existe $t \in K$ tel que $\begin{cases} x = \frac{p_1(t)}{q_1(t)} \\ y = \frac{p_2(t)}{q_2(t)} \end{cases}$. En particulier, $Xq_1(T) - p_1(T)$ et $Yq_2(T) - p_2(T)$ s'annulent en (x,y,t) donc $C(X,Y)$ s'annule en (x,y) puisque le résultant en T est une combinaison linéaire de ces deux polynômes. □

Remarque : lorsque $C(x,y) = 0$, il y a trois cas possibles :

1. Les deux coefficients dominants en T de $Xq_1(T) - p_1(T)$ et $Yq_2(T) - p_2(T)$ s'annulent quand on évalue en (x,y) et ce point d'annulation est forcément $\lim_{t\to\infty} \left(\frac{p_1(t)}{q_1(t)}, \frac{p_2(t)}{q_2(t)}\right)$ si les limites existent.
   En effet :
   on note $n = \deg_T p_1$, $d = \deg_T q_1$ et a_n, b_d les coefficients dominants de p_1 et q_1 respectivement.
   Alors $Xq_1(T) - p_1(T) = b_d T^d X - a_n T^n + \dots$ et son coefficient dominant est :
   - $-a_n$ si $n > d$, qui ne s'annule jamais, mais alors $\lim_{t\to\infty} \frac{p_1(t)}{q_1(t)} = \pm\infty$
   - $b_d X - a_d$ si $n = d$, qui s'annule en $x = \lim_{t\to\infty} \frac{p_1(t)}{q_1(t)} = \frac{a_d}{b_d}$
   - $b_d X$ si $n < d$, qui s'annule en $x = \lim_{t\to\infty} \frac{p_1(t)}{q_1(t)} = 0$.

   On fait de même pour le polynôme en Y.

2. Dans les deux autres cas, on peut appliquer le théorème d'extension dans $\bar{K}$:

(a) Si $t \in K$, on retrouve un point de la courbe. En effet, il serait possible que l'on ait $q_1(t) = 0$ par exemple mais alors on a forcément $p_1(t) = 0$, ce qui contredit $p_1 \wedge q_1 = 0$.

(b) Si $t \in \bar{K}$, on ne retrouve pas un point de la courbe.

Exemple : retrouver l'équation d'un cercle à partir de son équation paramétrique

$$(\mathcal{C}) : \begin{cases} x(t) = \frac{1-t^2}{1+t^2} \\ y(t) = \frac{2t}{1+t^2} \end{cases}$$

(que l'on peut retrouver en utilisant les formules trigonométriques permettant d'exprimer $\cos\theta$ et $\sin\theta$ en fonction de $\tan(\theta/2)$). Alors $\mathrm{Res}_T((1+T^2)X - (1-T^2), (1+T^2)Y - 2T) = 4(X^2+Y^2-1)$ et l'annulation simultanée des deux coefficients dominants en T se fait en $(-1, 0) \in V(X^2+Y^2-1)\backslash\mathcal{C}$.

Exemple : retrouver l'équation d'un demi-cercle à partir de son équation paramétrique

$$(\mathcal{C}) : \begin{cases} x(t) = \frac{1-t^4}{1+t^4} \\ y(t) = \frac{2t^2}{1+t^4} \end{cases}$$

On obtient alors $\mathrm{Res}_T((1+T^4)X - (1-T^4), (1+T^4)Y - 2T^2) = 16(X^2+Y^2-1)^2$ qui est toujours l'équation du cercle. Dans cet exemple il manque donc la moitié des points, les valeurs manquantes correspondent aux valeurs complexes de t.

5 Expression du résultant avec les racines et méthodes de calcul

Théorème 5.1. *Soient $P, Q \in A[X]$ et $\lambda_1, \ldots, \lambda_m$ les racines de P avec multiplicité dans une extension de $K = Fr(A)$. Alors*

$$Res_X(P, Q) = a_m^n \prod_{i=1}^{m} Q(\lambda_i)$$

Corollaire 5.2. *En notant $\mu_1, \ldots, \mu_n$ les racines de Q, on a*

$$Res_X(P, Q) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\lambda_i - \mu_j) = (-1)^{mn} b_n^m \prod_{j=1}^{n} P(\mu_j).$$

Corollaire 5.3 (Multiplicativité du résultant)**.**

$$Res_X(P_1P_2, Q) = Res_X(P_1P_2, Q)$$

Corollaire 5.4. *Pour tout $c \in A$,*

$$Res_X(P(cX), Q(cX) = c^{mn} Res_X(P(X), Q(X))$$

$$Res_X(P(X+c), Q(X+c) = Res_X(P(X), Q(X))$$

Proof. On se place dans l'anneau universel $A = \mathbb{Z}[U, X_1, \ldots, X_m, V, Y_1, \ldots, Y_n]$ et on calcule le résultant de $P = U\prod_{i=1}^{m}(X - X_i) \in A[X]$ et $Q = V\prod_{i=1}^{n}(X - Y_j) \in A[X]$. Comme on peut écrire $P = U(X^m - \sigma_1(X_1, \ldots, X_m) + \cdots + (-1)^m\sigma_m(X_1, \ldots, X_m))$, tous les coefficients de P sont de

degré 1 en chacun des X_i donc $\mathrm{Res}_X(P,Q)$ est de degré $\leqslant n$ en chacun X_i (puisque de degré total $\leqslant n$ en chacun des coefficients de P). Avec la même analyse sur Q, on obtient

$$\deg_{X_i} \mathrm{Res}_X(P,Q) \leqslant n \qquad \deg_{Y_i} \mathrm{Res}_X(P,Q) \leqslant m.$$

Par ailleurs, on sait qu'il existe deux polynômes R, S de $A[X]$ tels que

$$\mathrm{Res}_X(P,Q) = R(X)P(X) + S(X)Q(X).$$

Donc en évaluant en $X = X_i$, on obtient

$$\mathrm{Res}_X(P,Q) = S(X_i)Q(X_i) = S(X_i)V\prod_{j=1}^{n}(X_i - Y_j).$$

En particulier pour tout i,j, on a $(X_i - Y_j)|\mathrm{Res}_X(P,Q)$. Comme les $X_i - Y_j$ sont tous premiers entre eux dans A anneau factoriel, on a bien $\prod_{i,j}(X_i - Y_j)|\mathrm{Res}_X(P,Q)$, autrement dit

$$\mathrm{Res}_X(P,Q) = B\prod_{i,j}(X_i - Y_j), \text{ avec } B \in A \tag{1}$$

Il reste à voir que B est bien la constante attendue. Comme le degré en X_{i_0} (resp. Y_{j_0}) de $\prod_{i,j}(X_i - Y_j)$ vaut m (resp. n), le degré de B en X_{i_0} et Y_{j_0} est forcément nul. On a donc $B \in \mathbb{Z}[U,V]$. Par ailleurs, si on note $Q = \sum_{k=0}^{n} b_k X^k$, en évaluant en $(X_1,\dots,X_n) = (0,\dots,0)$, on obtient

$$\begin{aligned}
\mathrm{Res}_X(P,Q)(0,\dots,0,Y_1,\dots,Y_n) &= \mathrm{Res}_X(P(0,\dots,0), Q(Y_1,\dots,Y_n)) \\
&= \begin{vmatrix}
U & 0 & \dots & \dots & \dots & 0 \\
 & \ddots & \ddots & & & \vdots \\
 & & U & \ddots & & \vdots \\
b_n & \dots & & b_0 & \ddots & \vdots \\
 & \ddots & & & \ddots & 0 \\
 & & b_n & \dots & & b_0
\end{vmatrix} \\
&= U^n b_0^m \\
&= U^n (V(-1)^n Y_1 \dots Y_n)^m \\
&= (-1)^{mn} U^n V^m (Y_1 \dots Y_n)^m
\end{aligned}$$

Or d'après l'équation (1), ceci est également égal à $B(U,V)(-1)^{mn}\prod_{j=1}^{m}(y_j)^m$, donc $B(U,V) = U^n V^m$. En spécialisant U et V, on obtient le résultat du théorème. □

Exercice :
Soit $P = \prod_{i=1}^{n}(X - a_i)$, montrer que

$$\mathrm{Res}_X(P,P') = (-1)^{\frac{n(n-1)}{2}} \prod_{1\leqslant i<j\leqslant n}(a_i - a_j)^2.$$

Proof. Comme $P' = \sum_j \prod_{i\neq j}(X - a_i)$, on a

$$\begin{aligned}
\mathrm{Res}_X(P,P') = \prod_{k=1}^{n} P'(a_k) = \prod_{k=1}^{n}\sum_j\prod_{i\neq j}(a_k - a_i) = \prod_{k=1}^{n}\prod_{i\neq k}(a_k - a_i) &= \prod_{i<k}(a_k - a_i)(a_i - a_k) \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{1\leqslant i<j\leqslant n}(a_i - a_j)^2
\end{aligned}$$

□

Méthodes de calcul

1. Idée 1 : calcul du déterminant par pivot de Gauss
   La difficulté de cette approche est que l'on doit travailler dans $\mathrm{Frac}(A)$, la taille des coefficients a alors tendance à exploser pour faire une fausse complexité cubique. On peut sauver l'approche dans certains cas en effectuant les calculs modulo plusieurs facteurs premiers pour les "remonter" avec le théorème des restes chinois (ce qui nécessite que l'anneau A soit principal pour avoir a minima Bézout).

2. Idée 2 : utiliser un algorithme de type Euclide

   Propriété 5.5. *Soient $P, Q \in K[X]$ de degré m et n respectivement et $R \in K[X]$ le reste dans la division euclidienne de Q par P. Alors*

   $$Res_X(P,Q) = a_m^{n-\deg R} Res_X(P,R).$$

   Proof. On effectue la division euclidienne dans $\mathrm{Frac}(A)[X]$: $Q = SP + R$, $\deg R < \deg P$. En notant $P = a_m \prod (X - \lambda_i)$

   $$\mathrm{Res}_X(P,Q) = a_m^n \prod_{i=1}^{m} Q(\lambda_i) = a_m^n \prod_{i=1}^{m} R(\lambda_i) = a_m^{n-\deg R} \mathrm{Res}_X(P,R).$$

   □

   Cette approche permet d'avoir un algorithme de calcul en $O(\deg P)^2$ dans $\mathrm{Frac}(A)$ avec des dénominateurs potentiellement gros dans les calculs.

   Pour éviter ceci, on peut remplacer la division euclidienne par une pseudo division euclidienne.

   Propriété 5.6. *Soient $P, Q \in A[X]$ et a_m le coefficient dominant de P. Alors il existe un unique couple $(S,R) \in A[X]^2$ tel que $a_m^{n-m+1} Q = SP + R$.*
   En particulier

   $$(a_m^{n-m+1})^m Res(P,Q) = Res(P, a_m^{n-m+1} Q) = Res(P, SP+R) = a_m^{n-\deg R} Res(P,R)$$

   Proof. Il suffit de chasser les dénominateurs. □

Exemple :

$$\begin{aligned}
\mathrm{Res}(2X^2-5X+1, 3X^2-7) &= \frac{1}{9}\mathrm{Res}_{2,2}(6X^2-15X+3, 3X^2-7)\\
&= \frac{1}{9}\mathrm{Res}_{2,2}(0X^2-15X+17, 3X^2-7)\\
&= \frac{1}{9}\begin{vmatrix} 0 & -15 & 17 & 0\\ 0 & 0 & -15 & 17\\ 3 & 0 & -7 & 0\\ 0 & 3 & 0 & -7 \end{vmatrix}\\
&= \frac{1}{3}\mathrm{Res}_{1,2}(-15X+17, 3X^2-7)\\
&= \frac{1}{3\times 15^2}\mathrm{Res}_{1,2}(-15X+17, 15^2(3X^2-7))\\
&= \frac{1}{3\times 15^2}\mathrm{Res}_{1,2}(-15X+17, 675X^2-1575))\\
&= \frac{1}{3\times 15^2}\mathrm{Res}_{1,2}(-15X+17, 765X-1575)\\
&= \frac{1}{3\times 15^2}\mathrm{Res}_{1,2}(-15X+17, -708)\\
&= \frac{(-15)^2}{3\times 15^2}\mathrm{Res}_{1,0}(-15X+17, -708)\\
&= \frac{-708}{3}\\
&= -236
\end{aligned}$$