Résultant

Rappel.

Soient k un corps, $\mathrm{P} \in k[\mathrm{X}]$ un polynôme non constant. On a vu l'équivalence des propriétés suivantes :

(i) P, P' ont une racine commune (dans une extension de k)
(ii) P a une racine multiple (dans une extension de k)
(iii) $\deg \operatorname{pgcd}(\mathrm{P}, \mathrm{P}') \geqslant 1$

Le point (iii) offre ainsi un moyen par des calculs restant dans k (l'algorithme d'Euclide), d'obtenir des informations sur les racines de P dans les extensions de k.

L'énoncé précédent s'étend à deux polynômes : soit $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$ des polynômes non constants, on a alors équivalence entre

(i) P, Q ont une racine commune (dans une extension de k)
(ii) $\deg \operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) \geqslant 1$

En effet, si P, Q ont une racine commune a dans une extension K de k, alors $(\mathrm{X} - a)$ divise le pgcd de P et Q vu comme polynôme à coefficient dans K mais ce pgcd est le même que celui vu comme polynôme à coefficient dans k. Il est donc de degré plus grand que 1. Inversement, si $\operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) \geqslant 1$ alors ce pgcd admet une racine dans une extension de k (par exemple un corps de décomposition de $\operatorname{pgcd}(\mathrm{P}, \mathrm{Q})$) qui est une racine commune de P et Q.

L'objectif est d'étudier un autre moyen de caractériser la situation dans laquelle $\deg \operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) \geqslant 1$: c'est le résultant. Le résultant présente l'avantage de d'avoir une dépendance en P et Q plus facile à comprendre que le pgcd.

Application de Sylvester.

Pour définir le résultant, on définit d'abord une application linéaire $\mathcal{R}$ puis sa matrice dans des bases bien choisies (la matrice de Sylvester) et enfin on prend le déterminant.

On introduit la notation suivante : pour $p \in \mathbb{N}$, on pose $k_p[\mathrm{X}] = \operatorname{vect}(1, \mathrm{X}, \ldots, \mathrm{X}^{p-1})$. On a en particulier, $\dim k_p[\mathrm{X}] = p$. On fixe $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$ avec $\deg \mathrm{P} = m$ et $\deg \mathrm{Q} = n$ et on considère l'application

$$\mathcal{R} \colon \begin{cases} k_n[\mathrm{X}] \times k_m[\mathrm{X}] & \longrightarrow k_{n+m}[\mathrm{X}] \\ \quad (\mathrm{U}, \mathrm{V}) & \longmapsto \mathrm{UP} + \mathrm{VQ} \end{cases}$$

L'application $\mathcal{R}$ est bien définie : si $\deg \mathrm{U} < n$ et $\deg \mathrm{V} < m$ alors $\deg(\mathrm{UP} + \mathrm{VQ}) < m + n$. C'est une application linéaire. On l'appelle *application de Sylvester associée à* P *et* Q. De plus, on a la propriété suivante

Proposition 1 On a équivalence entre

(i) $\mathcal{R}$ n'est pas injective
(ii) $\mathcal{R}$ n'est pas surjective
(iii) $\mathcal{R}$ n'est pas bijective
(iv) $\deg \operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) \geqslant 1$
(v) P, Q ont une racine commune (dans une extension de k).

Preuve. L'équivalence de (i), (ii) et (iii) résulte du fait que $\mathcal{R}$ est linéaire et que

$$\dim k_n[\mathrm{X}] \times k_m[\mathrm{X}] = m + n = k_{n+m}[\mathrm{X}]$$

L'équivalence de (iv) et (v) a été vue au-dessus.

(iv) $\Rightarrow$ (ii). Soit $\mathrm{R} = \operatorname{pgcd}(\mathrm{P}, \mathrm{Q})$. On écrit $\mathrm{RP}_1 = \mathrm{P}$ et $\mathrm{RQ}_1 = \mathrm{Q}$, on a alors $\mathrm{UP} + \mathrm{VQ} = \mathrm{R}(\mathrm{UP}_1 + \mathrm{VQ}_1)$. En particulier, si $(\mathrm{UP}_1 + \mathrm{VQ}_1) \neq 0$ alors $\deg \mathrm{UP} + \mathrm{VQ} \geqslant 1$ et donc hormis le polynôme nul, aucun polynôme constant n'est dans l'image de P. Ainsi $\mathcal{R}$ n'est pas surjective.

(i) $\Rightarrow$ (iv). On va montrer que (non (iv)) implique (non (i)). On suppose donc que $\operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) = 1$ et que $(\mathrm{U}, \mathrm{V}) \in \operatorname{Ker} \mathcal{R}$, on a alors $\mathrm{UP} + \mathrm{VQ} = 0$ et comme $\operatorname{pgcd}(\mathrm{P}, \mathrm{Q}) = 1$, on obtient $\mathrm{P} \mid \mathrm{V}$. Or $\deg \mathrm{V} < m = \deg \mathrm{P}$. On en déduit que $\mathrm{V} = 0$. De même $\mathrm{U} = 0$ et donc $\mathcal{R}$ est injective.

Corollaire 2 – Identité de Bézout forte. Soit $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$. Il existe $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}]$ avec $\deg \mathrm{U} < \deg \mathrm{Q}$ et $\deg \mathrm{V} < \deg \mathrm{P}$ tel que $\mathrm{UP} + \mathrm{VQ} = \operatorname{pgcd}(\mathrm{P}, \mathrm{Q})$.

Preuve. Commençons par le cas $\mathrm{pgcd}(\mathrm{P},\mathrm{Q})=1$. On a alors $\mathcal{R}$ qui est surjective et donc $1\in\mathrm{Im}\,\mathcal{R}$. Si $\deg\mathrm{pgcd}(\mathrm{P},\mathrm{Q})\geqslant 1$, on écrit $\mathrm{P}=\mathrm{pgcd}(\mathrm{P},\mathrm{Q})\mathrm{P}_1$ et $\mathrm{Q}=\mathrm{pgcd}(\mathrm{P},\mathrm{Q})\mathrm{Q}_1$ et on applique le résultat à P_1 et Q_1 qui ont 1 comme pgcd. On trouve U,V tel que $\mathrm{UP}_1+\mathrm{VQ}_1=1$ et en multipliant par $\mathrm{pgcd}(\mathrm{P},\mathrm{Q})$, on obtient le résultat voulu, on a même $\deg\mathrm{U}<\deg\mathrm{Q}-\deg\mathrm{pgcd}(\mathrm{P},\mathrm{Q})$ et $\deg\mathrm{V}<\deg\mathrm{P}-\deg\mathrm{pgcd}(\mathrm{P},\mathrm{Q})$.

Matrice de Sylvester.

On écrit $\mathrm{P}=a_m\mathrm{X}^m+a_{m-1}\mathrm{X}^{m-1}+\cdots+a_0$ et $\mathrm{Q}=b_n\mathrm{X}^n+b_{n-1}\mathrm{X}^{n-1}+\cdots+b_0$. On appelle matrice de Sylvester associée à P et Q, la matrice de $\mathscr{R}$ dans les bases $((1,0),\dots,(\mathrm{X}^{n-1},0),(0,1),\dots,(0,\mathrm{X}^{m-1}))$ et $(1,\dots,\mathrm{X}^{n+m-1}$. Elle est donnée par

$$\mathrm{Syl}(\mathrm{P},\mathrm{Q})=\begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & a_1 & \ddots & & \vdots & a_1 & \ddots & \\ a_{m-1} & & \ddots & a_0 & b_{n-1} & & \ddots & b_0 \\ a_m & a_{m-1} & & a_1 & b_n & b_{n-1} & & b_1 \\ & a_m & \ddots & \vdots & & b_n & \ddots & \vdots \\ & & \ddots & a_{m-1} & & & \ddots & b_{n-1} \\ & & & a_m & & & & b_n \end{bmatrix}\in\mathrm{M}_{n+m}(k)$$

où il y a n colonnes avec les coefficients de P (ce sont les images de $(1,0),\dots,(\mathrm{X}^{n-1},0)$) et m colonnes avec les coefficients de Q (ce sont les images de $(0,1),\dots,(0,\mathrm{X}^{m-1})$).

Résultant.

Définition 3 – Résultant. On définit le résultant de P et Q par $\mathrm{Res}(\mathrm{P},\mathrm{Q}):=\det(\mathrm{Syl}(\mathrm{P},\mathrm{Q}))$.

Attention, le résultant n'est pas $\det\mathcal{R}$. En effet, $\det\mathcal{R}$ n'a pas de sens puisque $\mathcal{R}$ n'est pas un endomorphisme.

Proposition 4 Si P et Q sont de degré respectif m et n, on a équivalence entre

(*i*) $\mathcal{R}$ n'est pas injective
(*ii*) $\mathcal{R}$ n'est pas surjective
(*iii*) $\mathcal{R}$ n'est pas bijective
(*iv*) $\deg\mathrm{pgcd}(\mathrm{P},\mathrm{Q})\geqslant 1$
(*v*) P,Q ont une racine commune (dans une extension de k).
(*vi*) $\mathrm{Res}(\mathrm{P},\mathrm{Q})=0$

Remarque 5 Pour $\mathrm{P}=a_m\mathrm{X}^m+a_{m-1}\mathrm{X}^{m-1}+\cdots+a_0$ et $\mathrm{Q}=b_n\mathrm{X}^n+b_{n-1}\mathrm{X}^{n-1}+\cdots+b_0$, on écrit parfois $\mathrm{Syl}_{m,n}(\mathrm{P},\mathrm{Q})$ et $\mathrm{Res}_{m,n}(\mathrm{P},\mathrm{Q})$ pour indiquer la taille de la matrice. Cela est pratique lorsqu'on ne contrôle pas le degré de P ou Q mais qu'on sait simplement qu'il est majoré par m (resp. n). Attention dans ce cadre là, $\mathrm{Res}(\mathrm{P},\mathrm{Q})=0$ n'implique plus nécessairement P,Q ont une racine commune dans une extension de k, on peut aussi avec $a_m=b_n=0$.

Proposition 6 – Propriétés du résultant. Soit $\mathrm{P}=a_m\mathrm{X}^m+a_{m-1}\mathrm{X}^{m-1}+\cdots+a_0\in k[\mathrm{X}]$ et $\mathrm{Q}=b_n\mathrm{X}^n+b_{n-1}\mathrm{X}^{n-1}+\cdots+b_0\in k[\mathrm{X}]$. On a

(*i*) $\mathrm{Res}_{m,n}(\mathrm{P},\mathrm{Q})=\mathrm{Res}_{n,m}(\mathrm{Q},\mathrm{P})$.
(*ii*) Si $m=0$, on a $\mathrm{Res}(\mathrm{P},\mathrm{Q})={a_0}^n$.
(*iii*) Si $m=1$, on a $\mathrm{Res}(\mathrm{P},\mathrm{Q})=(-1)^n(b_0a_1^n-b_1{a_1}^{n-1}a_0+\cdots+(-1)^nb_n{a_0}^n)$ et si $a_1\neq 0$, $\mathrm{Res}(\mathrm{P},\mathrm{Q})=(-1)^n{a_1}^n\mathrm{Q}(-a_0/a_1)$. En particulier, si $\mathrm{P}=\mathrm{X}-a$, on a $\mathrm{Res}(\mathrm{P},\mathrm{Q})=(-1)^n\mathrm{Q}(a)$.
(*iv*) Si $m>0$ alors $\mathrm{Res}(\mathrm{P},\mathrm{P})=0$.
(*v*) Pour $a\in k$, $\mathrm{Res}(\mathrm{P}(\mathrm{X}-a),\mathrm{Q}(\mathrm{X}-a))=\mathrm{Res}(\mathrm{P},\mathrm{Q})$.
(*vi*) Si $a_m=0$, $\mathrm{Res}_{m,n}(\mathrm{P},\mathrm{Q})=b_n\mathrm{Res}_{m-1,n}(\mathrm{P},\mathrm{Q})={b_n}^{m-\deg\mathrm{P}}\mathrm{Res}_{\deg\mathrm{P},n}(\mathrm{P},\mathrm{Q})$.
(*vii*) Si $\mathrm{P}=\mathrm{QU}+\mathrm{R}$ avec $\deg\mathrm{R}\leqslant\deg\mathrm{P}$. On a

$$\mathrm{Res}_{m,n}(\mathrm{P},\mathrm{Q})=(-1)^{mn}{b_n}^{m-\deg\mathrm{R}}\mathrm{Res}_{n,\deg\mathrm{R}}(\mathrm{Q},\mathrm{R})\,.$$

(*viii*) Pour $\mathrm{Q}_1,\mathrm{Q}_2\in k[\mathrm{X}]$, on a $\mathrm{Res}_{m,\deg\mathrm{Q}_1+\deg\mathrm{Q}_2}(\mathrm{P},\mathrm{Q}_1\mathrm{Q}_2)=\mathrm{Res}_{m,\deg\mathrm{Q}_1}(\mathrm{P},\mathrm{Q}_1)\mathrm{Res}_{m,\deg\mathrm{Q}_2}(\mathrm{P},\mathrm{Q}_2)$.

(ix) Si $\mathrm{P(X)} = a_m \prod_{i=1}^{m} (\mathrm{X} - \alpha_i)$ et $\mathrm{Q} = b_n \prod_{j=1}^{n} (\mathrm{X} - \beta_j)$ est scindé, on a

$$\mathrm{Res(P,Q)} = (-1)^{mn} {a_m}^n \prod_{i=1}^{m} \mathrm{Q}(\alpha_i) = {b_n}^m \prod_{j=1}^{n} \mathrm{P}(\beta_j) = (-1)^{mn} {a_m}^n {b_n}^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

Changement d'anneaux.

Le cas d'un anneau intègre. Soient A un anneau intègre et k son corps de fraction. On suppose que P, Q sont à coefficients dans A. On a alors $\mathrm{Res(P,Q)} \in \mathrm{A}$ puisque c'est le déterminant d'une matrice à coefficient dans A.

On a alors le résultat suivant :

Proposition 7 Soit $\mathrm{P}, \mathrm{Q} \in \mathrm{A[X]}$ avec $\deg \mathrm{P} = m$ et $\deg \mathrm{Q} = n$ et $m+n > 0$. Alors il existe $\mathrm{U}, \mathrm{V} \in \mathrm{A[X]}$ tels que $\deg \mathrm{U} < \deg \mathrm{Q}$ et $\deg \mathrm{V} < \deg \mathrm{P}$ tel que $\mathrm{UP} + \mathrm{VQ} = \mathrm{Res(P,Q)}$.

De plus, on a $\mathrm{Res(P,Q)} = 0$ si et seulement si il existe $\mathrm{U}, \mathrm{V} \in \mathrm{A[X]}$ non nuls tels que $\deg \mathrm{U} < \deg \mathrm{Q}$ et $\deg \mathrm{V} < \deg \mathrm{P}$ tel que $\mathrm{UP} + \mathrm{VQ} = \mathrm{Res(P,Q)}$.

Le cas d'une extension de corps.

Si K est une extension de k et $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$. On peut évidemment voir P, Q comme des polynômes à coefficients dans K mais $\mathrm{Res(P,Q)}$ ne dépend pas du corps dans lequel on le calcule. En particulier, si P et Q ne sont pas scindé dans K, on peut toujours considérer une extension de k dans laquelle ils vont être scindés (par exemple le corps de décomposition de PQ).

Applications.

Polynôme annulateur d'une somme d'éléments algébriques.

Proposition 8 Soit $\mathrm{P} \in k[\mathrm{X}]$ de degré m dont les racines (dans une extension de k) sont $\alpha_1, \ldots, \alpha_m$ (on note a_m le coefficient dominant de P) et $\mathrm{Q} \in k[\mathrm{X}]$ de degré n dont les racines (dans une extension de k) sont $\beta_1, \ldots, \beta_n$ (on note b_n le coefficient dominant de Q).

Le polynôme $\mathrm{R} = \mathrm{Res_U}(\mathrm{Q(U)}, \mathrm{Res_T}(\mathrm{P(T)}, \mathrm{X}-(\mathrm{T}+\mathrm{U}))) \in k[\mathrm{X}]$ a pour racine $\alpha_i + \beta_j$ pour $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$.

Preuve. On a

$$\mathrm{Res_T}(\mathrm{P(T)}, \mathrm{X} - (\mathrm{T} + \mathrm{U}))) = (-1)^{\deg \mathrm{P}} \mathrm{P(X - U)} = (-1)^{\deg \mathrm{P}} a_m \prod_{i=1}^{m} (\mathrm{X} - \alpha_i - \mathrm{U})$$

Ainsi R est égal à

$${a_m}^n (-1)^{nm} \prod_{i=1}^{m} \mathrm{Res_U}(\mathrm{Q(U)}, \mathrm{X} - \alpha_i - \mathrm{U}) = {a_m}^n \prod_{i=1}^{m} \mathrm{Q(X} - \alpha_i) = {a_m}^n {b_n}^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\mathrm{X} - \alpha_i - \beta_j)$$

Implicitation de courbe paramétrée.

Soit $t \mapsto (x(t), y(t))$ une courbe paramétrée où x et y sont des fractions rationnelles en t. On peut trouver grâce au résultant une équation implicite (sous la forme $\mathrm{P}(x, y) = 0$) de la courbe paramétrée.

Écrivons $x(t) = \mathrm{P}(t)/\mathrm{Q}(t)$ et $y(t) = \mathrm{R}(t)/\mathrm{S}(t)$ avec $\mathrm{P}, \mathrm{Q}, \mathrm{R}, \mathrm{S} \in k[\mathrm{T}]$. Si le point de coordonnées (x, y) est sur la courbe, il existe t tel que les polynômes $\mathrm{Q(T)}x - \mathrm{P(T)}$ et $\mathrm{S(T)}y - \mathrm{R(T)}$ aient t comme racine commune. Ainsi $\mathrm{Res}(\mathrm{Q}x - \mathrm{P}, \mathrm{S}y - \mathrm{T}) = 0$ donne l'équation cherchée.

Application 9 On cherche l'équation implicite de la courbe d'équation

$$x(t) = \frac{1 - t^2}{1 + t^2} \qquad y(t) = \frac{2t}{1 + t^2}\,.$$

On cherche à calculer le résultant de $(1 + \mathrm{T}^2)x - (1 - \mathrm{T}^2) = \mathrm{T}^2(1 + x) + (x - 1)$ et $(1 + \mathrm{T}^2)y - 2\mathrm{T} = \mathrm{T}^2 y - 2\mathrm{T} + y$ c'est-à-dire le déterminant de

$$\begin{bmatrix} x-1 & & y & \\ 0 & x-1 & -2 & y \\ x+1 & 0 & y & -2 \\ & x+1 & & y \end{bmatrix}$$

On trouve $4(x^2 + y^2 - 1)$. Ainsi la courbe paramétrée décrit une partie du cercle.