Théorème d'extension

Références : Saux Picart, *Cours de calcul formel - Algorithmes fondamentaux*, p 148

On sait que si P et Q sont deux polynômes admettant une racine commune, alors leur résultant est nul en cette racine. Le calcul du résultant permet donc de trouver toutes les racines possibles.
Néanmoins les racines du résultant ne se remontent pas toutes en racines des polynômes. C'est ce que permet d'étudier le théorème d'extension.

Théorème.

Soit $\mathbb{K}$ un corps algébriquement clos et soient P, Q deux polynômes de $\mathbb{K}[Y_1, ..., Y_k][X]$, on note $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ avec m, $n \neq 0$ et a_i, $b_i \in \mathbb{K}[Y_1, ..., Y_k]$.
Si $(\alpha_1, ..., \alpha_k, \alpha)$ est tel que $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$, alors $\mathrm{Res}_X(P, Q)(\alpha_1, ..., \alpha_k) = 0$.
Réciproquement, si $\mathrm{Res}_X(P, Q)(\alpha_1, ..., \alpha_k) = 0$, alors une des propositions suivantes est vérifiée :

1. $\exists \alpha \in \mathbb{K}$, $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$,
2. $P(\alpha_1, ..., \alpha_k, X) = 0$,
3. $Q(\alpha_1, ..., \alpha_k, X) = 0$,
4. $a_m(\alpha_1, ..., \alpha_k) = b_n(\alpha_1, ..., \alpha_k) = 0$.

Pour prouver ce théorème, on va utiliser l'application suivante :

$$\Phi : \begin{array}{rcl} \mathbb{K}[Y_1, ..., Y_k][X] & \rightarrow & \mathbb{K}[X] \\ U & \mapsto & U(\alpha_1, ..., \alpha_k, X) \end{array}$$

Pour voir sa compatibilité avec le résultant, on a le résultat suivant.

Lemme.

Soient A, B deux anneaux, et φ un morphisme d'anneau de A dans B, alors si on note p et q les degrés respectifs de $\varphi(P)$ et $\varphi(Q)$, on a

$$\varphi(\mathrm{Res}_X(P, Q)) = \begin{cases} \varphi(a_m)^{n-q} \, \mathrm{Res}_X(\varphi(P), \varphi(Q)) & \text{si } \varphi(a_m) \neq 0, \\ \varphi(b_n)^{m-p} \, \mathrm{Res}_X(\varphi(P), \varphi(Q)) & \text{si } \varphi(b_n) \neq 0, \\ 0 & \text{si } \varphi(a_m) = \varphi(b_n) = 0. \end{cases}$$

Démonstration. Le résultant est défini comme le déterminant de la matrice de Sylvester. On a donc, comme le déterminant est un polynôme :

$$\varphi(\mathrm{Res}_X(P, Q)) = \varphi(\det(Sylv(P, Q))) = \det(\varphi(Sylv(P, Q))).$$

Si on note a'_i et b'_i les images des a_i et b_i par φ, alors

$$\varphi(Sylv(P, Q)) = \begin{pmatrix} a'_m & & & 0 & & \\ \vdots & \ddots & & b'_q & \ddots & \\ a'_0 & & \ddots & \vdots & \ddots & 0 \\ & \ddots & a'_m & b'_0 & & b'_q \\ & & \ddots \ \vdots & & \ddots & \vdots \\ & & a'_0 & & & b'_0 \end{pmatrix}.$$

Supposons $a'_m \neq 0$, alors en développant par rapport aux premières lignes, on a

$$\det(\varphi(Sylv(P,Q))) = (a'_m)^{n-q} \det(Sylv(\varphi(P), \varphi(Q))).$$

Il vient

$$\varphi(\mathrm{Res}_X(P,Q)) = (\varphi(a_m))^{n-q} \,\mathrm{Res}_X(\varphi(P), \varphi(Q)).$$

Si $a'_m = 0$ et $b'_n = 0$, la formule précédente marche encore car $\varphi(\mathrm{Res}_X(P,Q)) = 0$.
Enfin si $a'_m = 0$ et $b'_n \neq 0$, on a par le même raisonnement

$$\varphi(\mathrm{Res}_X(P,Q)) = (\varphi(b_n))^{m-p} \,\mathrm{Res}_X(\varphi(P), \varphi(Q)).$$

□

Passons à la preuve du théorème !

Démonstration. $\Leftarrow$: Si $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$, alors α est racine de $\Phi(P)$ et $\Phi(Q)$, donc $\mathrm{Res}_X(\Phi(P), \Phi(Q)) = 0$. Le lemme donne alors $\Phi(\mathrm{Res}_X(P,Q)) = 0$, donc $\mathrm{Res}_X(P,Q)(\alpha_1, ..., \alpha_k) = 0$.

$\Rightarrow$: Supposons que $\mathrm{Res}_X(P,Q)(\alpha_1, ..., \alpha_k) = 0$.

- Si $\Phi(a_m) \neq 0$, alors le lemme donne $\Phi(a_m)^{n-q} \,\mathrm{Res}_X(\Phi(P), \Phi(Q)) = 0$, donc $\mathrm{Res}_X(\Phi(P), \Phi(Q)) = 0$. On en déduit que soit $\Phi(Q) = 0$ (cas 3), soit $\Phi(Q) \neq 0$ et $\Phi(P)$ et $\Phi(Q)$ ont une racine commune α. Alors $(\alpha_1, ..., \alpha_k, \alpha)$ est racine commune de P et Q.

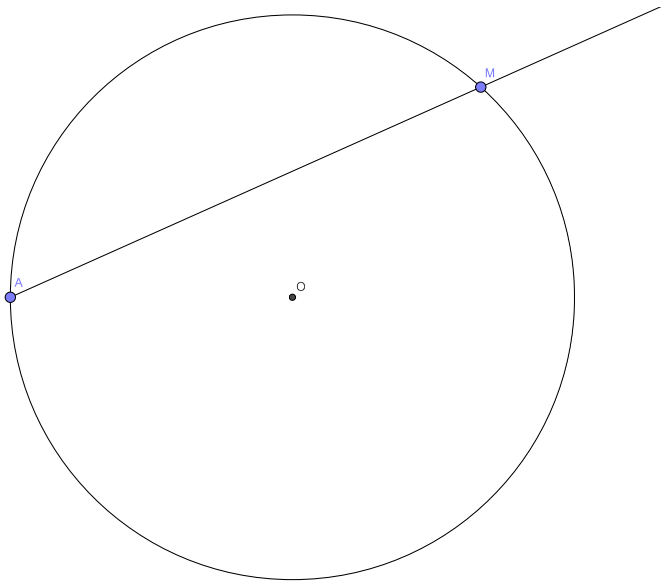
- Si $\Phi(b_n) \neq 0$, on peut refaire le raisonnement pour tomber sur les cas 1 ou 3.

- Si $\Phi(a_m) = \Phi(b_n) = 0$, on est dans le cas 4. □

Application : Paramétrisation du cercle
On tente de trouver une paramétrisation du cercle centré en 0 et de rayon 1. Pour cela, on choisit un point A sur le cercle (ici $(-1, 0)$). L'intersection d'une droite de pente $t \in \mathbb{R}$ passant par A - et non-tangente au cercle - avec le cercle est appelée $M(t)$. $M(t)$ est donc racine de $P = X^2 + Y^2 - 1$ et $Q = Y - t(X+1)$.
Pour trouver une expression en t des coordonnées de $M(t)$, on fait un résultant :

$$\mathrm{Res}_Y(P,Q) = \begin{vmatrix} 1 & 1 & 0 \\ 0 & -t(X+1) & 1 \\ X^2-1 & 0 & -t(X+1) \end{vmatrix} = P(t(X+1))) = (1+t^2)X^2 + 2t^2X + t^2 - 1$$

Pour calculer ce résultant rapidement, on a utilisé la formule magique avec les racines : on a juste à faire le produit des $P(\alpha_i)$ avec α_i les racines de Q.
On trouve deux racines au polynôme obtenu : $X = -1$ (qui correspond au point A), et $X = \dfrac{1-t^2}{1+t^2}$. Finalement, la paramétrisation du cercle est donnée ici par $M(t) = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.



Refaisons maintenant le raisonnement à l'envers ! Supposons que j'ai la paramétrisation précédente, et que je veuille trouver une équation de la courbe décrite par cette paramétrisation. Puis-je remonter les racines du résultant en racines des deux polynômes ?
On pose $P = (1+t^2)X + t^2 - 1$ et $Q = (1+t^2)Y - 2t$, alors

$$\mathrm{Res}_t(P,Q) = \begin{vmatrix} X+1 & 0 & Y & 0 \\ 0 & X+1 & -2 & Y \\ X-1 & 0 & Y & -2 \\ 0 & X-1 & 0 & Y \end{vmatrix} = 4(X^2+Y^2-1).$$

Les zéros du résultant décrivent le cercle $\mathcal{C}(0,1)$, or $M(t)$ paramétrise le cercle privé du point A. Le point A représente le cas 4 du théorème, c'est à dire que comme $\Phi(P) = -2$ et $\Phi(Q) = -2t$, le terme dominant a disparu dans les deux polynômes.

Remarques : • Pour illustrer les cas 2 et 3 du théorème, on peut juste prendre $P = (Y_1 - \alpha_1)P'$ car alors $a'_i = 0$ pour tout i et la matrice de Sylvester est de déterminant nul (pareil pour Q pour le cas 3).