UN EXERCICE D'ÉLIMINATION (3e PARTIE)

JEAN-FRANÇOIS BURNOL

Nous considérons un anneau commutatif unitaire $\mathcal{A}$ et deux polynômes à coefficients dans $\mathcal{A}$:

$$P = a_p T^p + a_{p-1} T^{p-1} + \cdots + a_0$$
$$Q = b_q T^q + b_{q-1} T^{q-1} + \cdots + b_0$$

On considère la matrice de Sylvester $\mathcal{S}$ qui possède $p+q$ lignes et colonnes :

$$\mathcal{S} = (T^{q-1}P \mid T^{q-2}P \mid \cdots \mid P \mid T^{p-1}Q \mid \cdots \mid TQ \mid Q)$$

où chaque colonne donne les coefficients des polynômes en question dans l'ordre des puissances décroissantes (de T^{p+q-1} à T^0).

Théorème 1. *Supposons que a_p soit inversible. Alors le résultant $R(P,Q)$, déterminant de la matrice de* Sylvester *de taille $(p+q)\times(p+q)$, est également :*

$$\det \mathcal{S} = a_p^q \cdot \det_{p\times p} Q\left(\frac{1}{a_p}\begin{pmatrix} 0 & 0 & \dots & \dots & -a_0 \\ a_p & 0 & 0 & \dots & -a_1 \\ 0 & a_p & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2} \\ 0 & \dots & 0 & a_p & -a_{p-1} \end{pmatrix}\right) \tag{1}$$

Autrement dit, pour P unitaire, le résultant est le déterminant du « polynôme Q appliqué sur la matrice compagnon de P ».

Preuve. Il faut examiner attentivement la matrice de Sylvester (écrivez-là) et conclure au bout de longues minutes qu'elle a un bloc en haut à gauche de taille $q \times q$ qui est une matrice triangulaire inférieure avec a_p sur la diagonale. [1]

Donc, en utilisant l'inverse de a_p, on peut en soustrayant des combinaisons linéaires des q premières colonnes annuler complètement le bloc en haut à droite de taille $q \times p$. Par exemple on a donc retiré à $T^{p-1}Q$ une combinaison appropriée de $T^{q-1}P$, …, P, ce qui signifie exactement que l'on a fait la division euclidienne de $T^{p-1}Q$ par P pour le remplacer par le reste R_{p-1}. De même pour les autres colonnes, qui sont remplacées par les restes R_{p-2}, …, R_0 obtenus par divisions euclidiennes des T^jQ par P, $j = p-2, \dots, 0$.

Donc le déterminant est a_p^q fois $\det_{p\times p}(R_{p-1} \mid \cdots \mid R_0)$.

Maintenant tout élément de $\mathcal{A}[T]/(P)$ s'écrit de manière unique comme combinaison de T^{p-1}, …, T^0, et, quitte à passer à un anneau universel (quelque chose comme $\mathbb{Z}[A_0, \dots, A_p, B_0, \dots, B_q]$ avec des indéterminées) pour éviter les problèmes de diviseurs de zéros, on peut aussi supposer que $\mathcal{A}$ est intègre et considérer son corps des fractions $\mathcal{K}$. La matrice $(R_{p-1} \mid \cdots \mid R_0)$ est alors celle de l'endomorphisme ψ_Q de l'espace vectoriel $\mathcal{K}[T]/(P)$ qui fait $V \mapsto QV \pmod{P}$, exprimé dans la base $(T^{p-1}, \dots, T^0)$. Si l'on note ϕ l'endomorphisme $V \mapsto TV \pmod{P}$,

Date: 4 février 2019.

1. Le bloc $p \times p$ en bas à droite est triangulaire supérieur avec b_0 sur la diagonale, mais on ne va pas utiliser cela, ici. De même pour les blocs $q \times q$ en bas à gauche ou $p \times p$ en haut à droite.

on a $\psi_Q = Q(\phi)$. Par ailleurs la matrice de ϕ dans $(T^0, \dots, T^{p-1})$ est la matrice compagnon :

$$M = \begin{pmatrix} 0 & 0 & \dots & \dots & -a_0/a_p \\ 1 & 0 & 0 & \dots & -a_1/a_p \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{p-2}/a_p \\ 0 & \dots & 0 & 1 & -a_{p-1}/a_p \end{pmatrix} \tag{2}$$

Donc la matrice de ψ_Q dans cette nouvelle base est $Q(M)$ et le déterminant de $(R_{p-1} \mid \cdots \mid R_0)$ est aussi $\det Q(M)$. D'où le résultat. □

Théorème 2. *Supposons que b_q soit inversible. Alors le résultant $R(P,Q)$, déterminant de la matrice de* Sylvester *de taille $(p+q) \times (p+q)$, est également :*

$$\det \mathcal{S} = (-1)^{pq} \cdot b_q^p \cdot \det_{q\times q} P\Big(\frac{1}{b_q} \begin{pmatrix} 0 & 0 & \dots & \dots & -b_0 \\ b_q & 0 & 0 & \dots & -b_1 \\ 0 & b_q & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & -b_{q-2} \\ 0 & \dots & 0 & b_q & -b_{q-1} \end{pmatrix}\Big) \tag{3}$$

Autrement dit, pour Q unitaire, le résultant est $(-1)^{pq}$ fois le déterminant du « polynôme P appliqué sur la matrice compagnon de Q ».

Preuve. On considère le bloc de taille $p \times p$ en haut à droite de la matrice de Sylvester. Il est triangulaire inférieur avec b_q sur la diagonale. On peut donc, de manière unique, utiliser ces p colonnes pour annuler le bloc de taille $p \times q$ en haut à gauche de la matrice. En bas à gauche on a alors les (coefficients des) restes des $T^j P$ modulo Q. Le signe $(-1)^{pq}$ vient des pq transpositions de lignes que l'on peut faire pour amener ce bloc en haut à gauche. Le terme b_q^p vient alors du bloc en bas à droite (anciennement en haut à droite). Et l'on justifie l'apparition de la matrice compagnon de Q comme précédemment.

Ou alors on invoque $R(P,Q) = (-1)^{pq} R(Q,P)$. □