Résultant et application à l'élimination

Gabriel Peyré

Soient $f(X)=\sum_{i=0}^{m} a_iX^i$et $g(X)=\sum_{i=0}^{n} a_iX^i$deux polynômes sur un corps $\mathbb{K}$. Lorsque $f$et $g$possèdent un facteur non trivial, ie. $f=f_1h$et $g=g_1h$, l'équation :

$$uf+vg=0 \quad \text{avec } \deg(u)\leq\deg(g)-1 \text{ et } \deg(v)\leq\deg(f)-1 \tag{1}$$

possède les solutions $u=g_1$et $v=-f_1$. Réciproquement, l'existence de solution nulle implique l'existence d'un facteur commun non trivial. En projetant l'équation (1) sur la base canonique de $\mathbb{K}_m[X]\times\mathbb{K}_n[X]$, l'existence de solution non nulle est équivalente à la nullité du déterminant :

$$\begin{vmatrix}
a_m & & & & b_n & & & \\
a_{m-1} & a_m & & & b_{n-1} & b_n & & \\
 & a_{m-1} & \ddots & & & b_{n-1} & \ddots & \\
\vdots & & \ddots & a_m & \vdots & & \ddots & b_n \\
a_0 & \vdots & & a_{m-1} & b_0 & \vdots & & b_{n-1} \\
 & a_0 & & & & b_0 & & \\
 & & \ddots & \vdots & & & \ddots & \vdots \\
 & & & a_0 & & & & b_0
\end{vmatrix}$$

Définition 0.1. Le déterminant (**??**) se nomme le résultant de $f$et $g$et se note $Res_X(f,g)$.

Théorème 0.1. PROPRIÉTÉS DU RÉSULTANT

(i) $Res_X(f,g)=(-1)^{mn}Res_X(g,f)$

(ii) $Res_X(f,b_0)=b_0^m$*, pour* $b_0\in\mathbb{K}$.

(iii) Si $\deg(f)=m\leq n=\deg(g)$*, et si* h *est le reste de la division de* g *par* f*, on a*

$$Res_X(f,g)=a_m^{n-m}Res_X(f,h).$$

(iv) $Res_X(f,g)=0$ *si et seulement si* f *et* g *ont un facteur non trivial.*

(v) Si f *et* g *s'écrivent :*

$$f=a_0(X-\alpha_1)(\ldots)(X-\alpha_m) \tag{2}$$
$$g=b_0(X-\beta_1)(\ldots)(X-\beta_n) \tag{3}$$

alors on a :

$$Res_X(f,g)=a_m^n\prod_{i=1}^{m}g(\alpha_i)=(-1)^{mn}b_n^m\prod_{j=1}^{n}f(\beta_j)=a_m^nb_n^m\prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i-\beta_j)$$

Remarque. Si on se place dans la clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$, alors l'écriture (2) est toujours réalisée et on peut appliquer (v).

Proposition 0.2. Généralisation *Le résultant est un polynôme entier en les coefficient de f et g, i.e. $Res_X(f,g) \in \mathbb{Z}[a_0,\dots,a_m,b_0,\dots,b_m]$. Ceci permet de le calculer dans un anneau A quelconque.*
Si l'anneau A est intègre et factoriel, en utilisant le théorème précédent dans le corps de fraction $Frac(A)$, on garde la propriété que f et g on un facteur commun non trivial si et seulement si $Res_X(f,g)=0$, ce qui est équivalent à une racine commune dans une extension algébriquement close de A.

Remarque. La proposition 0.2 nous permet de traiter le cas des polynômes en plusieurs variables, i.e. si $f \in \mathbb{K}[X_1,\dots,X_n]$, on utilise $f \in A[X_n]$ avec $A = \mathbb{K}[X_1,\dots,X_{n-1}]$ qui est intègre et factoriel.

On souhaite éliminer la variable X_r entre deux polynômes $f, g \in \mathbb{K}[X_1,\dots,X_r]$, notés de la façon suivante :

$$\begin{array}{lll} f = \sum_{i=0}^m f_i X_r^i & f_i \in \mathbb{K}[X_1,\dots,X_{r-1}] & f_m \neq 0 \\ g = \sum_{i=0}^n g_i X_r^i & g_i \in \mathbb{K}[X_1,\dots,X_{r-1}] & g_n \neq 0 \end{array}$$

Définition 0.2. Idéal d'élimination Pour $f \in \mathbb{K}[X_1,\dots,X_r]$, on note $f(\alpha_1,\dots,\alpha_r)$ le polynôme évalué en $(\alpha_1,\dots,\alpha_r) \in \overline{\mathbb{K}}^r$. On pose $h = Res_{X_r}(f,g) \in \mathbb{K}[X_1,\dots,X_{r-1}]$. Soit $I = \langle f, g\rangle$. On note $I_r = I \cap \mathbb{K}[X_1,\dots,X_{r-1}]$. C'est l'idéal d'élimination. En quelque sorte, l'idéal I_r contient toutes les façons d'éliminer la variable X_r des équations $\{f=0,\ g=0\}$.

Proposition 0.3. Elimination *On a $h \in I_r$. Donc si $(\alpha_1,\dots,\alpha_r) \in \overline{\mathbb{K}}^r$ est un zéro commun de f et g, alors $h(\alpha_1,\dots,\alpha_{r-1}) = 0$. Au final, le calcul de h conduit à une équation en $r-1$ variables.*

Théorème 0.4. Extension *On suppose connu $(\alpha_1,\dots,\alpha_{r-1}) \in \overline{\mathbb{K}}^{r-1}$ tels que $h(\alpha_1,\dots,\alpha_{r-1}) = 0$. Alors, si on n'est pas dans l'un des cas suivants :*
- $\forall i \in \{0,\dots,m\},\ f_i(\alpha_1,\dots,\alpha_{r-1}) = 0$
- $\forall i \in \{0,\dots,n\},\ g_i(\alpha_1,\dots,\alpha_{r-1}) = 0$
- $f_m(\alpha_1,\dots,\alpha_{r-1}) = g_n(\alpha_1,\dots,\alpha_{r-1}) = 0$

il existe $\alpha_r \in \overline{\mathbb{K}}$ tel que $(\alpha_1,\dots,\alpha_r)$ soit un zéro commun à f et g.

Référence : [?, p.147][?, p.25][?, p.162]
Utilisation : (***,0) (**,3) (*,0)
Mots clefs : déterminant, polynômes, équations polynomiales, élimination.

115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	**
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**
121	Déterminant. Applications.	**