Décomposition uni-multivariée pour les polynômes et matrice Jacobienne

Guillaume CHÈZE
Institut de Mathématiques de Toulouse,
Equipe MIP

Salah NAJIB
ICTP
Trieste

Définition

Définition 1 *Soit* $f(X,Y) \in \mathbb{K}[X,Y]$, f *est décomposable lorsque* f *peut s'écrire :*

$$f = u(h) = u \circ h, \ \ avec\ u \in \mathbb{K}[T], \deg u \geq 2, \ \ et\ h \in \mathbb{K}[X,Y].$$

Exemple : $\mathbb{K} = \mathbb{Q}$,
$f(X,Y) = X^2 + Y^2 + 2XY + X + Y - 3 = (X+Y)^2 + (X+Y) - 3$,
$u(T) = T^2 + T - 3$,
$h(X,Y) = X + Y$.

Une remarque

Nous avons $u(T) = T^2 + T - 3 = \left(T - \frac{1+\sqrt{13}}{2}\right)\left(T - \frac{1-\sqrt{13}}{2}\right)$
donc :

$$\begin{aligned} f(X,Y) &= (X+Y)^2 + (X+Y) - 3, \\ &= \left((X+Y) - \frac{1+\sqrt{13}}{2}\right)\left((X+Y) - \frac{1-\sqrt{13}}{2}\right) \end{aligned}$$

La décomposition est un cas particulier de factorisation absolue.

Clôture algébrique et décomposition

Théorème 1 (Fried, Mac Rae 1969 ; Ayad 2002)

Soit p *la caractéristique de* $\mathbb{K}$.

Si $p = 0$ *ou* $\gcd(p, \deg f) = 1$ *alors :*

$$f \text{ décomposable sur } \mathbb{K} \iff f \text{ décomposable sur } \overline{\mathbb{K}}.$$

Motivations

- Arithmétique : f est indécomposable ssi $\mathbb{K}[f]$ est sa fermeture entière dans $\mathbb{K}[X,Y]$.
- Corps intermédaire : $f = u \circ h \Rightarrow \mathbb{K}(f) \subset \mathbb{K}(h) \subset \mathbb{K}(X,Y)$.
- Simplification d'écriture, évaluation rapide.
- Factorisation absolue particulière :

Théorème 2

f décomposable $\iff$ *$f(X,Y) - T$ réductible dans* $\overline{\mathbb{K}(T)}[X,Y]$.

But : Reprendre les théorèmes classiques de factorisation absolue dans le cadre de la décomposition.

Outil de base

Théorème 3 *Soit $f \in \mathbb{K}[X,Y]$ un polynôme de degré d.*
On note d_{min} le plus petit nombre premier divisant d.
On suppose $p = 0$, ou $p > d^2/d_{min}$.
On considère :

$$\begin{array}{rcl} Jac_f : \mathbb{K}[X,Y]_{d/d_{min}} & \longrightarrow & \mathbb{K}[X,Y] \\ H(X,Y) & \longmapsto & \partial_X f.\partial_Y H - \partial_Y f.\partial_X H \end{array}$$

On a :

$$Ker\, Jac_f = \{0\} \iff f \text{ est indécomposable.}$$

Remarque : Pour la factorisation absolue on considère :
$f(\partial_Y g - \partial_X h) + h\partial_X f - g\partial_Y f = 0$.
Ici nous avons rajouté : $g = \partial_X H$, et $h = \partial_Y H$.

Théorème d'Ostrowski

Théorème 4 (Ostrowski 1919 ; Ruppert 1986 ; Gao, Rodriguez 2003)

Soit $f \in \mathbb{Z}[X,Y]$ un polynôme absolument irréductible de bidegré (m,n). T désigne le nombre de points se trouvant dans le polytope de Newton de f.
Si $p > \left(\sqrt{m^2+n^2}.\|f\|_2\right)^{2T-3}$ alors $f \mod p$ est absolument irréductible.

Polygone de Newton

Définition 2 *Le polygone de Newton de* f **"modifié"** *est* $N(f+\lambda)$ *où* $\lambda \in \mathbb{K}$ *vérifie :* $f(0,0)+\lambda \neq 0$. *On note ce nouveau polygone* $\mathcal{N}(f)$.

Proposition 1 *Soient* $f = u \circ h$, $\deg u = r$. *Si* (i_1, i_2) *est un sommet de* $\mathcal{N}(f)$ *alors il existe un sommet* (j_1, j_2) *de* $\mathcal{N}(h)$ *tel que :*

$$(i_1, i_2) = (r.j_1, r.j_2).$$

Autrement dit : $\mathcal{N}(f) = r.\mathcal{N}(h)$.

Corollaire 1 *Si* $\gcd(\{\textit{coordonnées des sommets de } \mathcal{N}(f)\}) = 1$ *alors* f *est indécomposable.*

Test d'indécomposabilité

Proposition 2 *Soit* $f \in \mathbb{Z}[X, Y]$.
Si $f \mod p$ *est indécomposable et* $\deg(f) = \deg(f \mod p)$ *alors* f *est indécomposable.*

Donc : Polygone de Newton "modifié" + mod p =test indécomposabilité.

d	$Succes$	T_{moy}	T_{max}	T_{min}
10	1000	0.002	0.011	0
30	1000	0.002	0.011	0
50	1000	0.013	0.06	0
100	1000	0.171	0.63	0.139
200	1000	2.581	9.451	2.16

Indécomposabilité modulo p

Théorème 5 *Soit $f \in \mathbb{Z}[X,Y]$ un polynôme indécomposable de degré d.*
Soit D_{min} le plus petit premier divisant
$gcd(\text{“ } coordonnées\ des\ sommets\ de\ \mathcal{N}(f)'')$.
Soit T' le nombre de points entiers de $\mathcal{N}(f)_{D_{min}}$.
Si $p > \max\left[\frac{d^2}{d_{min}}, \left(\frac{d^2}{D_{min}}\|f\|_2\right)^{T'}\right]$ *alors* $f \mod p$ *est indécomposable.*

Preuve

1. f indécomposable $\Rightarrow$ il existe un mineur maximal $\mathcal{M}$ de Jac_f non nul.

2. La matrice Jac_f est remplie avec les coefficients de f.

3. On peut borner $\mathcal{M}$ à l'aide du théorème de Hadamard : $|\mathcal{M}| < \mathcal{B}$.

4. Remarquer :
– Si $p > B$ alors $\mathcal{M} \mod p \neq 0$.
– $\mathcal{M} \mod p$ est un mineur maximal de $Jac_f \mod p$.

5. Conclure : $Jac_f \mod p$ est de rang maximal, donc $f \mod p$ est indécomposable.

Théorème de Noether

Théorème 6 (Noether 1922 ; Ruppert 1986)
Soient $d \geq 2$, $n \geq 2$ et

$$f(X_1, \ldots, X_n) = \sum_{0 \leq e_1 + \cdots + e_n \leq d} c_{e_1,\ldots,e_n} X_1^{e_1} \ldots X_n^{e_n} \in \mathbb{K}[X_1, \ldots, X_n].$$

Il existe un nombre fini de polynômes :

$$\Phi_t(\ldots, C_{e_1,\ldots,e_n}, \ldots) \in \mathbb{Z}[\ldots, C_{e_1,\ldots,e_n}, \ldots]$$

tels que

$$\forall t, \Phi_t(\ldots, c_{e_1,\ldots,e_n}, \ldots) = 0 \iff f \text{ est réductible dans } \overline{\mathbb{K}}[X_1, \ldots, X_n] \text{ ou } \deg(f) < d.$$

Si $\mathbb{K}$ est de caractéristique $p > d(d-1)$, les coefficients de Φ_t doivent être pris modulo p dans le membre de gauche de l'égalité.
De plus, $\deg \Phi_t \leq d^2 - 1$.

Équations pour la decomposabilité

Théorème 7 *Soient* $d \geq 2$, $n \geq 2$ *et*

$$f(X_1, \ldots, X_n) = \sum_{0 \leq e_1 + \cdots + e_n \leq d} c_{e_1,\ldots,e_n} X_1^{e_1} \ldots X_n^{e_n} \in \mathbb{K}[X_1, \ldots, X_n].$$

Il existe un nombre fini de polynômes :

$$\Phi_t(\ldots, C_{e_1,\ldots,e_n}, \ldots) \in \mathbb{Z}[\ldots, C_{e_1,\ldots,e_n}, \ldots]$$

tels que

$$\forall t, \Phi_t(\ldots, c_{e_1,\ldots,e_n}, \ldots) = 0 \iff f \text{ est décomposable dans } \mathbb{K}[X_1, \ldots, X_n] \text{ ou } \deg(f) < d.$$

Si $\mathbb{K}$ *est de caractéristique* $p > d^2/d_{min}$, *les coefficients de* Φ_t *doivent être pris modulo* p *dans le membre de gauche de l'égalité.*

De plus, $\deg \Phi_t \leq \frac{1}{2}(\frac{d}{d_{min}} + 1)(\frac{d}{d_{min}} + 2) := \mathcal{B}$.

Preuve

1. Si $n = 2$ alors prendre les mineurs maximaux de Jac_f.

2. Si $n > 2$ alors se ramener au cas précédent à l'aide de :

Théorème 8 *Soit* $f(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$. *Soit* $\mathbb{L} := \mathbb{K}(U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n)$, *où* $U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n$ *sont des variables.*
Le polynôme bivarié

$$\tilde{f}(X, Y) = f(U_1X + V_1Y + W_1, \ldots, U_nX + V_nY + W_n) \in \mathbb{L}[X, Y]$$

est indécomposable sur $\mathbb{L} \iff f$ *est indécomposable sur* $\mathbb{K}$.

Remarque :
Si $d = 10$ alors $\mathcal{B} = 21$, et $d^2 - 1 = 99$.

Théorème de Bertini

Théorème 9 *Soient $\mathbb{K}$ un corps et S un sous-ensemble fini de $\mathbb{K}$.*
Soit $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme absolument irréductible de degré d.
On suppose que la caractéristique $p = 0$ ou $p > d(d-1)$.
On note

$$\overline{f}(X, Y) = f(u_1 X + v_1 Y + w_1, \ldots, u_n X + v_n Y + w_n) \in \mathbb{K}[X, Y].$$

La probabilité d'obtenir $\overline{f}$ absolument irréductible lorsque l'on fait un tirage aléatoire uniforme des u_i, v_i et w_i dans S est supérieure à

$$1 - 2d^3/|S| \text{ (Gao 2003)},$$

$$1 - 3d^2/|S| \text{ (Lecerf 2005)}.$$

Réduction à deux variables pour la décomposition

Théorème 10 *Soient $\mathbb{K}$ un corps et S un sous-ensemble fini de $\mathbb{K}$.*
Soit $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme indécomposable de degré d.
On suppose que la caractéristique $p = 0$ ou $p > d^2/d_{min}$.
On note

$$\overline{f}(X, Y) = f(u_1X + v_1Y + w_1, \ldots, u_nX + v_nY + w_n) \in \mathbb{K}[X, Y].$$

La probabilité d'obtenir $\overline{f}$ indécomposable lorsque l'on fait un tirage aléatoire uniforme des u_i, v_i et w_i dans S est supérieure à $1 - d.\mathcal{B}/|S|$.

Remarque : $d.\mathcal{B} = O(d^3)$.

Preuve

1. f indécomposable sur $\mathbb{K} \iff \tilde{f}(X,Y)$ indécomposable sur $\mathbb{L}$ où $\tilde{f}(X,Y) = f(U_1X + V_1Y + W_1, \ldots, U_nX + V_nY + W_n)$ et $\mathbb{L} = \mathbb{K}(U_1, \ldots, W_n)$.

2. $\tilde{f}$ indécomposable $\iff \Phi_{t_0}(\tilde{f}) = \Psi_{t_0}(U_1, \ldots, W_n) \neq 0$.

3. $\deg \Psi_{t_0} = \deg\left(\Phi_{t_0}(\tilde{f})\right) = d.\mathcal{B}$.

4. $\overline{f}$ indécomposable $\iff \Psi_{t_0}(u_1, \ldots, w_n) \neq 0$.

5. Conclure avec le lemme de Zippel-Schwartz.