Polynômes à plusieurs variables. Résultant

Christophe Ritzenthaler

1 Relations coefficients-racines. Polynômes symétriques

Issu de [MS] et de [Goz]. Soit A un anneau intègre.

Définition 1.1. *Soit $a \in A \setminus \{0\}$. Le* degré *(resp.* poids*) du monôme $aX_1^{a_1} \cdots X_n^{a_n}$ est $\sum a_i$ (resp. $\sum i a_i$). Le* degré total *(resp.* poids total*) d'un polynôme non nul P est le maximum des degrés (resp. poids) des monômes non nuls dont il est la somme.*

Définition 1.2. *Un polynôme $F \in A[X_1, \ldots, X_n]$ est dit* symétrique *si pour toute permutation $\sigma \in \Sigma_n$ on a*

$$F(X_1, \ldots, X_n) = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Les polynômes

$$S_k(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}, \quad 1 \leq k \leq n$$

sont appelés fonctions symétriques élémentaires.
Le degré d'un polynôme symétrique par rapport à n'importe laquelle des variables est le même et est appelé degré partiel.

Théorème 1.1. *Pour tout polynôme symétrique $F \in A[X_1, \ldots, X_n]$ de degré d il existe un unique polynôme $G \in A[X_1, \ldots, X_n]$ tel que*

$$F = G(S_1, \ldots, S_n).$$

G est de poids d et de degré égal au degré partiel de F.

Expliquons comment cela est fait en pratique. On peut bien sûr procéder par identification (car le poids est donné) mais cela est coûteux. On préfère donc la méthode suivante :

1. On écrit F comme somme de polynômes (dits homogènes) dont les monômes ont tous même degré. Il suffit de raisonner sur un tel polynôme.
2. Soit F homogène. On considère le monôme $aX_1^{a_1} \cdots X_n^{a_n}$ le plus grand pour l'ordre lexicographique ($(b_i) < (c_i)$ si et seulement si il existe j tel que $b_j < c_j$ et $b_i \leq c_i$ pour $i < j$). Puisque F est symétrique on a
$$a_1 \geq \ldots \geq a_n.$$
3. On calcule alors $F(X_1, \ldots, X_n) - aS_1^{a_1 - a_2} S_2^{a_2 - a_3} \cdots S_{n-1}^{a_{n-1} - a_n} S_n^{a_n}$. C'est un polynôme symétrique, homogène mais tous ces monômes ont un ordre lexicographique strictement plus petit que celui de $aX_1^{a_1} \cdots X_n^{a_n}$.

Théorème 1.2 (Formules de Newton, [AF, p.428]). *Soit*

$$P_k(X_1,\dots,X_n)=\begin{cases}X_1^k+\ldots+X_n^k & 1\le k\le n\\ 0 & k>n\end{cases}.$$

On a

$$P_k-P_{k-1}S_1+P_{k-2}S_2+\ldots+(-1)^{k-1}P_1S_{k-1}+(-1)^k kS_k=0,\quad 1\le k\le n-1$$

et

$$P_k-P_{k-1}S_1+P_{k-2}S_2+\ldots+(-1)^{n-1}P_{k-n+1}S_{n-1}+(-1)^n S_nP_{k-n}=0,\quad k\ge n.$$

Application 1 ([Gou99, p.204]). *Si $tr(M^n)=tr(N^n)$ pour tout n alors M et N ont même polynôme caractéristique.*

Corollaire 1.1. *On a*

$$P_k=\begin{vmatrix} S_1 & 1 & 0 & \dots & 0\\ 2S_2 & S_1 & 1 & \dots & 0\\ 3S_3 & S_2 & S_1 & \dots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ kS_k & S_{k-1} & S_{k-2} & \dots & S_1\end{vmatrix}.$$

2 Le résultant de Sylvester

Une grande partie est tirée de `http://www.proba.jussieu.fr/pageperso/nourdin/LeSiteDeLAgregatif/sur_resultant.html`

2.1 Définition

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

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

possède les solutions $u=g_1$ et $v=-f_1$. Réciproquement, puisque $g|uf$ mais ne divise pas u, l'existence d'une solution non nulle implique l'existence d'un facteur commun non trivial. En projetant l'équation (1) sur la base canonique de $K_{m-1}[X]\times K_{n-1}[X]$, l'existence d'une solution non nulle est équivalente à la nullité du déterminant :

$$\begin{vmatrix} a_m & & & & b_n & & & \\ a_{m-1} & a_m & & & b_{n-1} & b_n & & \\ & a_{m-1} & \ddots & & & b_{n-1} & \ddots & \\ \vdots & & \ddots & a_m & \vdots & & \ddots & b_n\\ a_0 & \vdots & & a_{m-1} & b_0 & \vdots & & b_{n-1}\\ & a_0 & & & & b_0 & & \\ & & \ddots & \vdots & & & \ddots & \vdots\\ & & & a_0 & & & & b_0\end{vmatrix} \tag{2}$$

(les a_i sont répétés n fois et les b_i m fois).

Définition 2.1. *Le déterminant (2) est appelé le* résultant *de f et g et se note $Res_X(f,g)$. C'est un élément de K.*

2.2 Propriétés

Théorème 2.1. *Le résultant possède les propriétés suivantes :*

1. $Res_X(f,0) = 0$
2. $Res_X(f,g) = (-1)^{mn} Res_X(g,f)$
3. *Si* $\deg(f) = m \leq n = \deg(g)$ *et si* h *est le reste de la division de* g *par* f *on a* $Res_X(f,g) = a_m^{n-m} Res_X(f,h)$. *Cette propriété peut servir à calculer le résultant. Reste le problème du facteur dominant qui est résolu par la théorie des sous-résultants.*
4. $Res_X(f,g) = 0$ *si et seulement si* f *et* g *ont un facteur non trivial.*
5. *On se place dans une cloture algébrique* $\overline{K}$ *de* K. *Si* (α_i) *sont les racines de* f *et* (β_j) *les racines de* g *alors on a*

$$Res_X(f,g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n} (\alpha_i - \beta_j). \quad (3)$$

Remarque 1. *Le résultant est un polynôme entier en les coefficients de* f *et* g, *i.e.* $Res_X(f,g) \in \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_m]$. *Ceci permet de le calculer dans un anneau (commutatif)* A *quelconque. Si on suppose que* 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 *ont 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* $Frac(A)$. *Cette démarche permet de traiter le cas des polynômes en plusieurs variables, i.e. si* $f \in K[X_1, \ldots, X_n]$, *on utilise* $f \in A[X_n]$ *avec* $A = K[X_1, \ldots, X_{n-1}]$ *qui est intègre et factoriel.*

2.3 Résultant et PGCD

Proposition 2.1. *Soient* $f, g \in K[X]$. *Alors il existe* $A, B \in K[X]$ *tels que*

$$Af + Bg = Res_X(f,g).$$

De plus A, B *sont des polynômes entiers en les coefficients de* f *et* g.

Corollaire 2.1. f, g *sont premiers entre eux si et seulement si* $Res_x(f,g) \neq 0$.

Exemple 1. *En utilisant Cor. 2.1 on peut démontrer le résultat suivant [Gou99, p.207] :*
Si on note D *l'ensemble des matrices diagonalisables de* $M_n(\mathbb{C})$ *alors* $\overset{\circ}{D}$ *est l'ensemble des matrices diagonalisables à valeurs propres distinctes.*

2.4 Discriminant

Pour $f = \sum_{i=0}^{m} a_i X^i$ polynôme sur un anneau intègre A, on définit le *discriminant* de f par $\mathrm{Res}_X(f, f') = (-1)^{m(m-1)/2} a_m \mathrm{Discr}(f)$. C'est un élément de A.

3 Théorie de l'élimination

3.1 Elimination

On se donne deux polynômes $f, g \in A[X_1, \ldots, X_r]$, notés de la manière suivante

$$f(X) = \sum_{i=0}^{m} f_i X_r^i, \quad g(X) = \sum_{i=0}^{n} g_i X_r^i$$

avec $f_m g_n \neq 0$.

Théorème 3.1. *On a l'alternative suivante :*
- *Si $Res_{X_r}(f,g) = 0$ alors f et g ont un facteur commun.*
- *Sinon, l'équation $Res_{X_r}(f,g) = 0$ donne une équation en $r-1$ variables.*

Dans la pratique, on dispose par exemple de r équations à r variables. Par des calculs de résultants successifs, on met notre système sous forme échelonnée, et on peut résoudre la dernière équation de façon approchée puisqu'elle ne comporte qu'une variable. Cependant, contrairement à la résolution par pivotage des équations linéaires, ici, le premier cas du théorème nous dit seulement qu'une solution $(x_0, \ldots, x_r)$ du système va donner naissance à un facteur non trivial, et donc que x_0 va être racine de la dernière équation. De nouvelles racines peuvent apparaître. C'est ce qui est précisé dans la suite.

Soient $f, g \in K[X_1, \ldots, X_r]$ et $h = \mathrm{Res}_{X_r}(f,g)$.

Proposition 3.1. *Si $(\alpha_1, \ldots, \alpha_r)$ est un zéro commun de f et de g alors $h(\alpha_1, \ldots, \alpha_{r-1}) = 0$.*

Théorème 3.2. *On suppose connu $(\alpha_1, \ldots, \alpha_{r-1})$ tel que $h(\alpha_1, \ldots, \alpha_{r-1}) = 0$. Alors si $f_m(\alpha_1, \ldots, \alpha_{r-1}) g_n(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$ then il existe α_r tel que $(\alpha_1, \ldots, \alpha_r)$ soit un zéro commun à f et à g.*

Exemple 2. *$Res_Y(XY-1, XY) = X$ mais la racine 0 ne se relève pas en une solution $(0, y)$ du système $XY - 1 = XY = 0$.*

4 Applications

4.1 Intersection de deux courbes dans $\mathbb{R}^2$

Si on considère les deux polynômes de $\mathbb{R}[X,Y]$:

$$f(X,Y) = X^4 + Y^4 - 1 \quad (4)$$
$$g(X,Y) = X^5Y^2 - 4X^3Y^3 + X^2Y^5 - 1 \quad (5)$$

ils définissent deux courbes de $\mathbb{R}^2$. Les points (x,y) se trouvant sur leur intersection doivent vérifier

$$\begin{aligned}\mathrm{Res}_X(f,g) = 0 \quad = \quad & 2Y^{28} - 16Y^{27} + 32Y^{26} + 249Y^{24} + 48Y^{23} - 128Y^{22} + 4Y^{21} \\ & -757Y^{20} - 112Y^{19} + 192Y^{18} - 12Y^{17} + 758Y^{16} + 144Y^{15} - 126Y^{14} \\ & +28Y^{13} - 25Y^{12} - 64Y^{11} + 30Y^{10} - 36Y^9 - Y^8 + 16Y^5 + 1\end{aligned}$$

Numériquement les solutions réelles de cette équation sont :

$$\{-0.09242096683, -0.5974289870, 0.7211133862, 0.9665062969\}$$

L'intersection possède donc 4 points. En remplaçant dans (4) on obtient 16 candidats parmi lesquels il est facile de trouver les solutions.

4.2 Equation implicite d'une courbe rationnelle

On suppose donnée une courbe plane paramétrée de façon rationelle :

$$\mathcal{C} = \left\{ \left(\frac{a(t)}{b(t)}, \frac{c(t)}{d(t)} \right) \in \mathbb{R}^2, t \in \mathbb{R} \right\}.$$

Les points (x, y) sont sur la courbe $\mathcal{C}$ si et seulement si $b(t)x - a(t) = d(t)y - c(t) = 0$, ce qui fournit une équation implicite de $\mathcal{C}$:

$$f(x, y) = \mathrm{Res}_t(b(t)x - a(t), d(t)y - c(t)) = 0.$$

4.3 Formule de Héron

On se propose de déterminer la formule donnant l'aire d'un triangle en fonction des longueurs de ses trois côtés a, b, c. Pour se faire, on se place dans un repère orthonormé comme indiqué sur la figure 2.

En appliquant la formule de Pythagore deux fois, et on calculant l'aire $\mathcal{S}$ du triangle, on obtient le système d'équations suivant :

$$\begin{aligned} p &= (a-x)^2 + y^2 - b^2 = 0 && (6)\\ q &= x^2 + y^2 - c^2 = 0 && (7)\\ r &= ay - 2\mathcal{S} = 0 && (8) \end{aligned}$$

On cherche donc à éliminer les variables x, y en calculant les résultants suivants :

$$\begin{aligned} r_1 = \mathrm{Res}_x(p, q) &= 4a^2y^2 - 2a^2c^2 + a^4 - 2a^2b^2 + b^4 - 2b^2c^2 + c^4 && (9)\\ r_2 = \mathrm{Res}_y(r, r_1) &= -2a^4c^2 + a^6 - 2a^4b^2 + a^2b^4 - 2a^2b^2c^2 + a^2c^4 + 16\mathcal{S}^2a^2 && (10) \end{aligned}$$

On a donc la formule de Héron

$$\mathcal{S}^2 = \frac{1}{16}(a+b-c)(b+a+c)(a-b+c)(-c+a-b).$$

4.4 Le problème de la cinématique inverse

voir texte.

4.5 Nombres algébriques

Soient $a, b \in \mathbb{C}$ deux nombres algébriques sur $\mathbb{Q}$ de polynômes minimaux f, g. Si on note p (resp. q) le polynôme minimal de $a + b$ (resp. ab) alors on a

$$p(z) = Res_x(f(x), g(z-x)) \quad q(z) = \mathrm{Res}_x(f(x), g(z/x)x^{\deg(g)}).$$

Exemple 3. *Si on prend* $a = \sqrt[5]{2}$ *et* $b = \sqrt[3]{-7/2 - 1/18\sqrt{3981}} - \sqrt[3]{-7/2 + 1/18\sqrt{3981}}$, *on vérifie que l'on a* $f(x) = x^5 - 2$ *et* $g(x) = x^3 + x + 7$. *On a par exemple*

$$q(x) = x^{15} - 70x^{10} + 984x^5 + 134456.$$

Références

[AF] J.M. Arnaudiès, H. Fraysse : cours de mathématiques-1 Algèbre, Dunod Université.

[Gou99] X. Gourdon, mathématiques pour M', algèbre, ellipses, Paris 1999.

[Goz] I. Gozard, Théorie de Galois.

[Har77] R. Hartshorne, Algebraic geometry, Graduate Texts **52**, Springer-Verlag, 1977.

[MS] M. Mignotte, D. Stefanescu, *Polynomials, an algorithmic approach*, Springer.

[Per95] D. Perrin, Géométrie algébrique, une introduction, CNRS édition 1995.

[Ser70] J.-P. Serre, cours d'arithmétique, Presse universitaire de France, 1970.

Autres références en français : Lenong-Ferrand, Arnaudiès (cours de Mathématiques, Tome 1), Malliavin (Algèbre commutative), Tauvel (mathématiques générales pour l'agrégation).

FIGURE 1 – Intersection de deux courbes planes

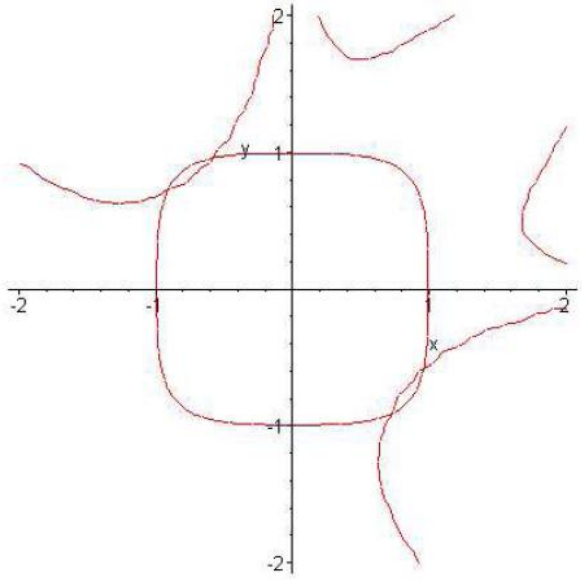

FIGURE 2 – Formule de Héron