

L'algorithme de Waring

1. Le développement

On fixe un entier $n \in \mathbb{N}^*$ et un anneau unitaire et commutatif A . Pour tout entier $k \in \llbracket 1, n \rrbracket$, on note $S_k \in K[X_1, \dots, X_n]$ le k -ième polynôme symétrique élémentaire qui est défini par

$$S_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X^{i_1} \dots X^{i_k}$$

Théorème : Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique. Il existe un unique polynôme $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(S_1, \dots, S_n)$.

DÉMONSTRATION :

1) Pour l'existence de Q , on décrit l'algorithme de Waring. On munit l'ensemble des monômes de $A[X_1, \dots, X_n]$ de la relation d'ordre suivante

$$aX_1^{k_1} \dots X_n^{k_n} \succeq bX_1^{\ell_1} \dots X_n^{\ell_n}$$

avec $(a, b) \in (A^*)^2$ si et seulement si il existe $r \in \llbracket 1, n \rrbracket$ tel que

$$\forall i \in \llbracket 1, r-1 \rrbracket, \quad k_i = \ell_i \quad \text{et} \quad k_r \geq \ell_r.$$

De plus, si M_1, M_2, N_1 et N_2 sont des monômes unitaires, on a

$$M_1 \succeq N_1 \quad \text{et} \quad M_2 \succeq N_2 \quad \Rightarrow \quad M_1 N_1 \succeq M_1 N_2 \succeq M_2 N_2. \quad (*)$$

2) Si $P \in A[X_1, \dots, X_n]$ est un polynôme non nul, on note $m(P)$ le plus grand monôme de P pour l'ordre $\succeq$. Comme les polynômes symétriques élémentaires sont unitaires, on a avec la propriété (*) pour tout $(\ell_1, \dots, \ell_n) \in \mathbb{N}^n$ que

$$\begin{aligned} m(S_1^{\ell_1} \dots S_n^{\ell_n}) &= m(S_1^{\ell_1}) \dots m(S_n^{\ell_n}) \\ &= X_1^{\ell_1} (X_1 X_2)^{\ell_2} \dots (X_1 \dots X_{n-1})^{\ell_{n-1}} (X_1 \dots X_n)^{\ell_n} \\ &= X_1^{\ell_1 + \dots + \ell_n} X_2^{\ell_2 + \dots + \ell_n} \dots X_n^{\ell_n}. \end{aligned}$$

3) Si $P \in A[X_1, \dots, X_n]$ est un polynôme symétrique et non nul, alors en notant $m(P) = aX_1^{k_1} \dots X_n^{k_n}$, on a $k_1 \geq k_2 \geq \dots \geq k_n$. En effet, si on avait l'inégalité $k_i < k_j$ pour $(i, j) \in \llbracket 1, n \rrbracket$ avec $i > j$, alors on pourrait construire un monôme de P strictement plus grand avec la transposition (i, j) .

4) Avec les notations introduites, on peut donner l'algorithme de Waring. On se donne un polynôme symétrique $P \in A[X_1, \dots, X_n]$ non nul (sinon c'est trivial). En notant $m(P) = aX_1^{k_1} \dots X_n^{k_n}$, on peut définir d'après le point précédent

$$P_1 = P - aS_1^{k_1-k_2} S_2^{k_2-k_3} \dots S_n^{k_n} \in A[X_1, \dots, X_n]$$

D'après le second point, P_1 est la différence de deux polynômes admettant le même plus grand monôme pour l'ordre $\succeq$. On a deux cas.

- Si $P_1 = 0$, on a montré le résultat.
- Sinon on a $m(P_1) \prec m(P)$ et on réutilise l'algorithme avec P_1 .

On est certain que l'algorithme s'arrête car il n'y a qu'un nombre fini de monômes unitaires $M \in A[X_1, \dots, X_n]$ vérifiant $M \prec m(P)$.

5) Pour démontrer l'unicité, il suffit de montrer que si $Q \in A[X_1, \dots, X_n]$ est non nul, alors $Q(S_1, \dots, S_n) \neq 0$. Si $M = aX_1^{k_1} \dots X_n^{k_n} \in A[X_1, \dots, X_n]$ est un monôme, alors on a

$$m(M(S_1, \dots, S_n)) = aX_1^{k_1 + \dots + k_n} X_2^{k_2 + \dots + k_n} \dots X_n^{k_n}.$$

En particulier, si M et N sont deux monômes distincts de Q , alors les n -uplet des exposants de $m(M(S_1, \dots, S_n))$ et de $m(N(S_1, \dots, S_n))$ ne sont pas égaux. On en déduit qu'il existe un unique monôme M de Q donnant l'élément maximal pour l'ordre $\succeq$ dans $Q(S_1, \dots, S_n)$, donc $Q(S_1, \dots, S_n) \neq 0$ (car l'élément maximal de $Q(S_1, \dots, S_n)$ ne peut pas se simplifier en développant formellement le polynôme $Q(S_1, \dots, S_n)$). $\square$

Références : • Chapitre 3, Partie 3.1 de [Esc97].

2. Remarques sur le développement

On fixe un entier $n \in \mathbb{N}^*$ et un anneau unitaire et commutatif A . Rappelons simplement qu'un polynôme $P \in A[X_1, \dots, X_n]$ est symétrique si

$$\forall \sigma \in \mathfrak{S}_n, \quad P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$

3. Un exemple d'application de l'algorithme

On applique l'algorithme pour décomposer le polynôme symétrique

$$P = X^3 + Y^3 + Z^3 \in \mathbb{Z}[X, Y, Z].$$

Les polynômes symétriques élémentaires de $\mathbb{Z}[X, Y, Z]$ sont

$$S_1 = X + Y + Z, \quad S_2 = XY + XZ + YZ, \quad S_3 = XYZ.$$

Le plus haut terme de P pour $\succeq$ est X^3 . On applique l'algorithme

$$P_1 = P - S_1^3 = -3(X^2Y + X^2Z + XY^2 + XZ^2 + YZ^2 + YZ^2) - 6XYZ.$$

Le plus haut terme de P_1 pour $\succeq$ est X^2Y . On applique l'algorithme

$$P_2 = P_1 + 3S_1S_2 = 3XYZ.$$

Le plus haut terme de P_2 pour $\succeq$ est XYZ . On applique l'algorithme

$$P_3 = P_2 - 3S_3 = 0.$$

On conclut finalement que l'on a la décomposition

$$P = S_1^3 - 3S_1S_2 + 3S_3.$$

4. Les polynômes de Newton

On fixe un entier $n \in \mathbb{N}$ avec $n \geq 2$ et un anneau unitaire et commutatif A . On désigne par $S_1, \dots, S_n \in K[X_1, \dots, X_n]$ les polynômes symétriques élémentaires. On définit également $S_0 = 1$ et les polynômes de Newton par

$$\forall d \in \mathbb{N}, \quad N_d = \sum_{k=1}^n X_k^d.$$

Les polynômes de Newton sont symétriques, donc on peut les exprimer avec les polynômes symétriques élémentaires d'après le théorème du développement. Le théorème donne des relations explicites.

Théorème : On a les relations suivantes.

(i) Pour tout entier $d \in \llbracket 1, n-1 \rrbracket$, on a

$$\sum_{k=0}^{d-1} (-1)^k S_k N_{d-k} + (-1)^d d S_d = 0.$$

(ii) Pour tout $d \in \mathbb{N}$ avec $d \geq n$, on a

$$\sum_{k=0}^n (-1)^k S_k N_{d-k} = 0.$$

DÉMONSTRATION :

1) On introduit le polynôme

$$P = (T - X_1) \cdots (T - X_n) = \sum_{k=0}^n S_k T^{n-k} \in K[X_1, \dots, X_n, T].$$

Si $d \in \mathbb{N}$ avec $d \geq n$, alors en multipliant la relation ci-dessus par T^{d-n} , puis en substituant T par X_i pour $i \in \llbracket 1, n \rrbracket$, on obtient

$$\forall i \in \llbracket 1, n \rrbracket, \quad \sum_{k=0}^n S_k X_i^{d-k} = 0.$$

On obtient (ii) en sommant cette dernière relation pour $i \in \llbracket 1, n \rrbracket$.

2) En posant la division euclidienne de P par $T - X_i$ pour $i \in \llbracket 1, n \rrbracket$, on a

$$P = (T - X_i) \left[\sum_{d=0}^{n-1} \left(\sum_{k=0}^d (-1)^{d-k} S_k X_i^{d-k} \right) T^{n-1-d} \right].$$

Finalement, en injectant cette dernière expression dans la relation

$$\frac{\partial P}{\partial T} = \sum_{i=1}^n \frac{P}{T - X_i},$$

on obtient

$$\sum_{d=0}^{n-1} (n-d) S_d T^{n-1-d} = \sum_{d=0}^{n-1} \left(\sum_{k=0}^d (-1)^{d-k} S_k N_{d-k} \right) T^{n-1-d},$$

ce qui permet de conclure en identifiant les coefficients en T . $\square$

Corollaire : Si K un corps de caractéristique nulle, alors on a

$$K[S_1, \dots, S_n] = K[N_1, \dots, N_n].$$

DÉMONSTRATION :

Comme $1, 2, \dots, n$ ne sont pas nuls dans K , on remarque avec le théorème précédent que chaque S_k pour $k \in \llbracket 1, n \rrbracket$ est un polynôme en $N_1, \dots, N_n$. On conclut avec le théorème du développement. $\square$

Ce dernier résultat peut être utile dans divers problèmes. On a par exemple le résultat suivant.

Proposition : Soit $(A, B) \in \mathcal{M}_n(K)^2$ où K un corps de caractéristique nulle. Les matrices A et B ont le même polynôme caractéristique si et seulement si

$$\forall k \in \llbracket 1, n \rrbracket, \quad \text{Tr}(A^k) = \text{Tr}(B^k).$$

DÉMONSTRATION :

1) Quitte à remplacer K par un corps de décomposition de $\chi_A \cdot \chi_B$, on peut supposer que χ_A et χ_B sont scindés sur K .

2) Si $\chi_A = \chi_B$, alors A et B ont les mêmes valeurs propres $\lambda_1, \dots, \lambda_n \in K$ comptées avec multiplicité. En trigonalisant, on a

$$\forall k \in \llbracket 1, n \rrbracket, \quad \text{Tr}(A^k) = \sum_{i=1}^n \lambda_i^k = \text{Tr}(B^k).$$

3) On note $\lambda_1, \dots, \lambda_n \in K$ les valeurs propres de A comptées avec multiplicité. Par le résultat précédent, il existe $P_1, \dots, P_n \in \mathbb{Q}[X_1, \dots, X_n]$ tels que

$$\forall k \in \llbracket 1, n \rrbracket, \quad S_k = P_k(N_1, \dots, N_n).$$

Comme pour le sens direct, on a

$$\forall k \in \llbracket 1, n \rrbracket, \quad N_k(\lambda_1, \dots, \lambda_n) = \sum_{i=1}^n \lambda_i^k = \text{Tr}(A^k).$$

En posant $S_0 = 1$, on a finalement

$$\chi_A(X) = \sum_{k=0}^n S_k(\lambda_1, \dots, \lambda_n) X^{n-k} = \sum_{k=0}^n P_k(\text{Tr}(A), \dots, \text{Tr}(A^n)) X^{n-k}.$$

On peut donc exprimer χ_A avec $\text{Tr}(A^k)$ pour $k \in \llbracket 1, n \rrbracket$, d'où le résultat. $\square$

Attention : Le résultat précédent est faux en caractéristique fini. Par exemple, si K est un corps de caractéristique $p \in \mathbb{N}$, alors $\text{Tr}(\text{I}_p^k) = 0 = \text{Tr}(\text{O}_p^k)$ pour tout entier $k \in \mathbb{N}$, mais I_p et O_p n'ont pas le même polynôme caractéristique.

Bibliographie

[Esc97] J.-P. ESCOFIER – *Théorie de galois*, Dunod, 1997.