

117: Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications

Pierre Lissy

April 27, 2010

1 Algèbre des polynômes à n indéterminées

Dans toute la suite A est un anneau supposé tout de même intègre.

1.1 Définition

Définition 1. Un polynôme à n indéterminées est une famille presque nulle d'éléments de A , famille indexée par $\mathbb{N}^n$.

Proposition 1. l'ensemble des polynômes à n indéterminées est déjà muni d'une structure d'anneau?

Proposition 2. On a la définition équivalente par récurrence sur n ; $A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}[X_n]$.

Proposition 3. On munit cet ensemble d'une structure d'algèbre avec une opération interne:
$$ij \times b_{ij} = \sum_{k=0}^i a_{kj} b_{i-k,j}$$

Théorème 1 (Propriété universelle des anneaux de polynômes). On considère deux anneaux intègres A et B , f un morphisme entre les deux et i l'inclusion de A dans $A[X_1, \dots, X_n]$. Pour tout $b \in B^n$ il existe un unique morphisme F vérifiant $F(i) = f$ et $F(X_j) = b_j$.

Définition 2. Dérivée formelle d'un polynôme par rapport à la k -ème variable.

1.2 Degré partiel, total

Définition 3. Le degré partiel de P en X_k est le degré de P en tant que polynôme de $F[X_k]$ avec $F = A[X_1, \dots, X_n]$.

Proposition 4. $\deg_k(P + Q) \leq \max(\deg_k(P), \deg_k(Q))$ avec égalité si P et Q sont de degré différents. $\deg_k(PQ) = \deg_k(P) + \deg_k(Q)$. Le degré de P est la plus grande puissance de P qui intervient dans un monôme $a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$.

Définition 4. Le degré total de P est $-\infty$ si P est nul, $\sup|\alpha|$ avec les notations précédentes sinon.

Proposition 5. $\deg(P + Q) \leq \max(\deg_k(P), \deg_k(Q))$ avec égalité si P et Q sont de degré différents. $\deg(PQ) = \deg(P) + \deg(Q)$.

Définition 5. Un polynôme est dit homogène de degré k ssi $a_\alpha \neq 0 \Rightarrow a_\alpha = k$, autrement dit le degré total de chaque monôme apparaissant dans A est k .

Remarque 1. Autre définition équivalente: dans l'algèbre $A[X_1, \dots, X_n, Y]$, on a la relation $P(YX_1, \dots, YX_n) = Y^k P(X_1, \dots, X_n)$.

Proposition 6. le produit de deux polynômes homogènes de degré k, l est homogène de degré $k+l$. La somme de deux polynômes homogènes en est un. C'est donc un sous-module.

Proposition 7. Identité d'Euler: Si P est homogène de degré k , on a $X_1 P'_{X_1} + \dots + X_n P'_{X_n} = kP$. La réciproque est vraie dans un corps de caractéristique nulle.

Définition 6. Combinaison avec répétition de m éléments p à $p =$ on choisit p éléments pas forcément distincts (on peut choisir le même p fois). Notation: Γ_m^p .

Proposition 8. $p\Gamma_m^p = m\Gamma_m^{p-1} + (p-1)\Gamma_m^{p-1}$

On en déduit

Théorème 2. $\Gamma_m^p = C_{m+p-1}^m$.

Application 1. Le nombre de termes du polynôme homogène de degré p à m indéterminées est Γ_m^p

Proposition 9. Dans le cas d'un corps, la dimension de l'espace des polynômes homogènes de degré k est C_{n+1-d}^d .

1.3 Théorèmes de transfert

Remarque 2. Dès que $n \geq 2$, A n'est JAMAIS un anneau principal.

Définition 7. Contenu d'un polynôme sur un anneau factoriel: pgcd des coefficients. Un polynôme de contenu 1 est dit primitif.

Lemme 1. Les polynômes irréductibles dans $A[X]$ sont les constantes irréductibles et les polynômes primitifs irréductibles dans $\text{Frac}(A)[X]$

Théorème 3 (Gauss). A factoriel implique $A[X]$ factoriel. du coup par récurrence $A[X_1, \dots, X_n]$ factoriel et c'est même encore vrai avec un infinité d'inconnues

Théorème 4 (Hilbert). Si A est un anneau noetherien, il en est de même de $A[X]$ et du coup il en est de même de $A[X_1, \dots, X_n]$.

1.4 Zeros d'un polynôme

Définition 8. Fonction polynôme : la fonction associée à ce polynôme.

Définition 9. Zero d'un polynôme: un élément qui annule le polynôme associé.

Théorème 5. On suppose k infini. Alors $P = 0$ ssi pour tout $x \in K$, $P(x) = 0$. REst vrai avec n'importe quel sous-corps infini de k .

Théorème 6. l'ensemble des zéros d'un polynôme non nul de $R[X_1, \dots, X_n]$ ou $C[X_1, \dots, X_n]$ est d'intérieur vide dans $\mathbb{R}^n$.

Théorème 7 (Chevalley-Waring). Un polynôme sur $\mathbb{F}_q$ de degré d à n variables tel que $f(0, \dots, 0) = 0$ a au moins un autre zéro si $n > d$. Plus précisément, le nombre de zéros est congru à 0 modulo q . Enfin, si l'on se donne $f_1, \dots, f_r$ des polynômes de degré $d_1, \dots, d_r$ à n indéterminées, s'ils n'ont pas de terme constant et si $n > \sum d_i$ alors ils ont un autre zéro en commun.

Corollaire 1. Une fonction arbitraire $f : k^n \mapsto k$ peut être représentée par un polynôme.

Théorème 8 (Nullstellensatz). Soit k un corps de clôture algébrique Ω et I un idéal de $k[X_1, \dots, X_n]$. Soit f un polynôme tel que $f(c) = 0$ pour tout $c \in \Omega$ tel que $\forall g \in I, g(c) = 0$. Alors il existe un m tel que $f^m \in I$.

1.5 Polynômes symétriques

1.6 Définition

Définition 10. Un polynôme est dit symétrique ssi pour tout $\sigma \in S_n$ on a $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Exemple 1. Somme de Newton $S_p = \sum X_i^p$. Polynôme symétrique élémentaire $\Sigma_p = \sum X_{i_1} X_{i_2} \dots X_{i_p}$

Définition 11. Un polynôme symétrique homogène de degré total p est dit de poids p . Son degré partiel par rapport à l'une quelconque de ses indéterminées est appelé ordre, noté $w(P)$.

Définition 12. Symétrisé d'un polynôme: $\sum_{M_\sigma} M_{\sigma} o$ où M_σ est le polynôme M sur lequel o na fait agir la permutation σ . Notation $\sum \sigma$.

1.7 Théorème de structure

Théorème 9. Soit G un polynôme de $K[X_1, \dots, X_n]$ homogène symétrique de poids supérieur ou égal à 1. Il existe un unique polynôme Φ tel que $G(X_1, \dots, X_n) = \Phi(\Sigma_1(X), \dots, \Sigma_n(X))$. le degré total de Φ est égal à l'ordre de G et tout monôme de Φ est tel que $\sum n\alpha_n = p$.

Corollaire 2. Si l'on considère un polynôme quelconque, en appliquant ce qui précède au monôme il existe un unique polynôme F tq comme au dessus.

Corollaire 3. De la démonstration résulte que si G a tous ses coefficients dans un sous-anneau de K , il en est de même pour F .

Exemple 2. $X_1^3 + X_2^3 + X_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

1.8 Méthodes de détermination de F

Exemple 3. Par abaissement de l'ordre. Si $S = \sum X_i^3$. On remarque que $\Sigma_1(\sum X_i^2) = S + T$ avec $T = \sum X_i^2 X_j$. De plus, $\sum X_i^2 = \sigma_1^2 - 2\sigma_2$. On recalcule T par abaissement de l'ordre et on trouve $T = \sigma_1\sigma_2 - 3\sigma_3$. Ainsi, $S = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Exemple 4. Par identification. $S = \sum X_i^2 X_j^2$. S est homogène d'ordre 2 et de poids 4, donc d'après le théorème précédent il ne peut contenir que des termes en $\sigma_1\sigma_3, \sigma_2^2, \sigma_4$ (ce sont les seuls de poids 4). $S = A\sigma_1\sigma_3 + B\sigma_2^2 + C\sigma_4$. Or $X^4 + X^2 = 0$ correspond par exemple à $\sigma_1 = \sigma_3 = \sigma_4 = 0, \sigma_2 = 1, S = 1$. D'où $B = 1$.

Application 2. cf gourdon algèbre linéaire. On considère le polynôme caractéristique dont le coefficient de X^i est noté $f_i(A)$. On montre que pour tout A et B on a $f_i(AB) = f_i(BA)$. Inversement, toute fonction polynômiale en les coefficients de A , notée Q , vérifiant $Q(AB) = Q(BA)$ est telle qu'il existe un polynôme F vérifiant $Q(A) = F(f_1(A), \dots, f_n(A))$.

1.9 Formules de Newton

Théorème 10. les polynômes de Newton vérifient (avec $S_0 = n$) que $S_k - \Sigma_1 S_{k-1} + \dots + (-1)^n \sigma_n S_{k-n} = 0$ pour $k \geq n$ et $S_k - \Sigma_1 S_{k-1} + \dots + (-1)^k \sigma_k k = 0$ pour $k \leq n$.

On les calcule ainsi de proche en proche.

Exemple 5. $S_1 = \Sigma_1$. $S_2 = \sigma_1^2 - 2\sigma_2$. $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. $S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_3\sigma_1 + 2\sigma_2^2 - 4\sigma_4$.

2 Relations coefficients-racines et applications

2.1 Relations coefficients-racines et premières applications

Théorème 11. On considère dans $\mathbb{C}$ un polynôme $P = \sum a_i X^i$, dont les racines sont les x_i . Alors $\Sigma_p = (-1)^p a_p / a_0$.

Application 3. Dans $\mathbb{M}_n(\mathbb{C})$, les coefficients du polynôme caractéristique sont des polynômes en $\text{Tr}(M^k)$. On en déduit que A nilpotente ssi pour tout k , $\text{tr}(M^k) = 0$. On en déduit le théorème de Burnside: tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini. On en déduit aussi la réduction des endomorphismes de rang 2.

Application 4. Kronecker: un polynôme à coefficients entiers ne s'annulant pas en 0 et a à racines complexes de module plus petit que 1 est tel que les racines sont des racines de l'unité.

Application 5. On considère E l'ensemble des polynômes réels scindés à coef dans $1, 0, -1$. Alors tout polynôme de P est forcément de degré inférieur ou égal à 3 et on obtient neuf éléments.

Application 6. Théorème fondamental de l'algèbre gourdon page 84-85

2.2 Résultant

Définition 13. *Résultant de deux polynômes.* Deux polynômes ont un pgcd différent de 1 ssi $Au = BV$. On construit à partir de là un morphisme comme dans le Gourdon. Le lelong-ferrand-arnaudiès fournit alors l'expression développée du résultant. page 191-192

Application 7. On appelle discriminant le résultant de f et de f' . Le vandermonde permet de donner la valeur de ce discriminant: $\delta(f) = (-1)^{m(m-1)/2} D$ avec D un déterminant qui s'exprime en utilisant les somems de Newton des racines de f .

2.3 Résolution par radicaux

Application 8. *Résolution par radicaux des équations de degré 3.* On veut résoudre une équation de degré 3 qu'on ramène à l'aide d'une translation $z^3 + pz + q$. Le polynôme suivant: $(X^2 + jY + j^2Z)^3$ ne prend que trois valeurs différentes quand on permute les racines, notée A et B . De plus, grâce aux relations coefficients racines on voit que A et B sont racines du polynôme $z^2 + 27qz - 27p^3 = 0$. On déduit à partir de là A et B ; Notons u et v des racines cubiques de A et B . Alors les racines sont $1/3(u+v)$, $1/3(j^2u+jv)$, $1/3(ju+j^2v)$. Enfin on voit facilement si les racines sont réelles ou non, grâce au discriminant $27(4p^3 + 27q^2)$: si il est négatif, trois racines réelles, si il est positif une racine réelle et deux racines complexes conjuguées.

Application 9. *Résolution par radicaux des équations de degré 4.* Le polynôme $XY + ZT$ ne prend que 3 valeurs lorsqu'on permute les racines de $F = z^4 + az^2 + bz + c$. On déroule le même raisonnement

Remarque 3. Cette technique échoue aux degrés supérieurs (non résolubilité par radicaux des équations de degré supérieur ou égal à 5 dans le cas général)

References

[1]