142

Algèbre des polynômes à plusieurs indéterminées - Applications

Soit A un anneau commutatif unitaire
Soit K un corps, soit $n \geq 2$

I Généralités

1) Définitions

Déf : Soit $A^{(\mathbb{N}^n)}$ l'ensemble des suites $(a_i)_{i \in \mathbb{N}^n} = f$ où les a_i sont presque tous nuls et les indices i étant en n-uplets $(i_1, \dots, i_n) = (i)$.

Déf : Soient f et g dans $A^{(\mathbb{N}^n)}$, $f = (a_i)$, $g = (b_i)$. On définit dans $A^{(\mathbb{N}^n)}$ l'addition et la multiplication :

- $f+g = (c_i)_{i \in \mathbb{N}^n}$ où $c_i = a_i + b_i \quad \forall i \in \mathbb{N}^n$
- $fg = (d_i)_{i \in \mathbb{N}^n}$ où $d_{(i_1, \dots, i_n)} = \sum_{\substack{j_k + l_k = i_k \\ 1 \leq k \leq n}} a_{(j_1, \dots, j_n)} b_{(l_1, \dots, l_n)}$

De plus, $A^{(\mathbb{N}^n)}$ est muni de la loi externe définie, pour $\lambda \in A$, $(a_i)_{i \in \mathbb{N}^n} \in A^{(\mathbb{N}^n)}$, par $\lambda \cdot (a_i) = (\lambda a_i)_{i \in \mathbb{N}^n}$.

On obtient une A-algèbre unitaire et commutative.

Déf : Soit $p \in [\![1, n]\!]$, on note X_p l'élément de $A^{(\mathbb{N}^n)}$ $(a_i)_{i \in \mathbb{N}^n}$ où $a_{(0, \dots, 0, 1, 0, \dots, 0)} = 1$ et $a_i = 0$ sinon.

Les éléments $X_1, \dots, X_p$ sont appelés indéterminées.

Déf : L'algèbre $A^{(\mathbb{N}^n)}$ sera notée $A[X_1, \dots, X_n]$ et un élément de cette algèbre est appelé polynôme à n indéterminées sur A.

Déf : Un polynôme du type $\lambda X_1^{i_1} \dots X_n^{i_n}$, $\lambda \in A$, $(i_1, \dots, i_n) \in \mathbb{N}^n$ est appelé monôme.

Prop : Les monômes forment une base de $K[X_1, \dots, X_n]$ (comme K-espace vectoriel)

2) Propriétés arithmétiques

Pté : On peut injecter A comme sous-algèbre de $A[X_1, \dots, X_n]$

Pté : Si A est factoriel, alors $A[X]$ est factoriel.

Pté : Soit $(X_i)_{i \leq n}$ n indéterminées : alors $(A[X_1])[X_2] = A[X_1, X_2]$ et $\forall j \in [\![1, n]\!]$, $(A[X_1, \dots, \hat{X_j}, \dots, X_n])[X_j] = A[X_1, \dots, X_n]$

Cor : Si A est factoriel, $A[X_1, \dots, X_n]$ est factoriel.

Pté : Si A est intègre, alors $A[X_1, \dots, X_n]$ est intègre.

Propriété universelle : Soit B une K-algèbre commutative unitaire, soit $(x_1, \dots, x_n) \in E^n$. Alors il existe un unique $\phi \left(\begin{array}{l} K[X_1, \dots, X_n] \to E \\ P(X_1, \dots, X_n) \mapsto P(x_1, \dots, x_n) \end{array} \right)$ morphisme de K-algèbre appelé morphisme de substitution.

Déf : Soit $P \in K[X_1, \dots, X_n]$, $P(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$.
La fonction polynôme associée à P est la fonction de K^n dans K $\hat{P} \left((x_1, \dots, x_n) \overset{K^n}{\longmapsto} \overset{K}{P}(x_1, \dots, x_n) \right)$

Prolongement des identités algébriques : Soit K infini.
Soit $P \in K[X_1, \dots, X_n]$ tel que $\hat{P} = 0$.
Alors P est le polynôme nul.

3) Degré et polynômes homogènes

Déf : Soit $X_1^{i_1} \dots X_n^{i_n}$ un monôme de $A[X_1, \dots, X_n]$.
Le degré total de $X_1^{i_1} \dots X_n^{i_n}$ est l'entier $i_1 + \dots + i_n$.

Déf : Soit $P \in A[X_1, \dots, X_n]$, $P \neq 0$. On appelle :
- degré partiel de P en X_j $(1 \leq j \leq n)$, le degré de P vu comme polynôme de $(A[X_1, \dots, \hat{X_j}, \dots, X_n])[X_j]$ i.e. en l'indéterminée X_j et à coeff dans $A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$
- degré total de P le maximum des degrés totaux des monômes dont il est la somme.

Rq : Le degré total du polynôme nul est $-\infty$.

Ex : Le polynôme $X_1^2 X_3^2 + X_2^3 X_1^2$ est de degré total 5 et de degré partiel 3 en X_2, 2 en X_1 ou en X_3.

Déf : Un polynôme $P \in A[X_1,\dots,X_n]$ est dit homogène de degré d s'il est somme de monômes de degré total d.

Déf : On note $K_d[X_1,\dots,X_n]$ le sev engendré par 0 et par $\{X_1^{i_1}\cdots X_n^{i_n}\}_{i_1+\dots+i_n=d}$

C'est un K-ev de dimension $\binom{n+d-1}{n-1}$

Coro : Soit $K_{\le d}[X_1,\dots,X_n]$ le sev engendré par 0 et par $\{X_1^{i_1}\cdots X_n^{i_n}\}_{i_1+\dots+i_n\le d}$; c'est de dimension $\binom{n+d}{n}$

Prop : $K_d[X_1,\dots,X_n]$ est l'ensemble des polynômes homogènes de degré d. Si $\mathrm{car}(K)=0$, alors P est homogène de degré d ssi $\forall \lambda\in K$, $P(\lambda X_1,\dots,\lambda X_n)=\lambda^d P(X_1,\dots,X_n)$

II Applications

1) Action sur $K[X_1,\dots,X_n]$

1/ $K=\mathbb{C}$ dans cet exemple ; notons $V=\mathbb{C}[X_1,\dots,X_n]$ et pour $s\in\mathbb{N}$, $\mathbb{C}_s[X_1,\dots,X_n]=V_s$

On définit une action de $GL_n(\mathbb{C})$ sur V par :

si $A\in GL_n(\mathbb{C})$, $A^{-1}=(a_{ij})$ $\quad A\cdot P(Y)=P(A^{-1}\cdot Y)$

si $P\in V$ $\quad$ ie $A\cdot P(X_1,\dots,X_n)=P\left(\sum_{j=1}^n a_{1j}X_j,\dots,\sum_{j=1}^n a_{nj}X_j\right)$

si $Y=(X_1,\dots,X_n)$

Lemme de Reynolds : Soit G un groupe fini et (V,ρ) une représentation sur G. On définit $R_G\in\mathcal{L}(V)$ par

$$R_G=\frac{1}{|G|}\sum_{g\in G}\rho(g)$$

Alors $V^G=\{x\in V \mid \forall g,\ \rho(g)(x)=x\}=\mathrm{Im}(R_G)=\mathrm{Ker}(R_G-\mathrm{Id})$

et $\dim_{\mathbb{C}}(V^G)=\mathrm{Tr}(R_G)$

REV 1 — Théorème de Molien

Soit G un groupe fini de $GL_n(\mathbb{C})$. Alors :

- $\forall s\in\mathbb{N}$, l'action précédente induit une représentation de G sur V_s
- soit $a_s=\dim_{\mathbb{C}}(V_s^G)$ et soit $\Phi(X)=\sum_{s\ge0}a_sX^s$ la série de Molien

Alors $\Phi(\lambda)=\sum_{A\in G}\frac{1}{\det(\mathrm{Id}-\lambda A)}$

2/ Soit l'action de S_n sur $A[X_1,\dots,X_n]$ définie par :

pour $\sigma\in S_n$, $P\in\dots$, $\sigma\cdot P(X_1,\dots,X_n)=P(X_{\sigma(1)},\dots,X_{\sigma(n)})$

Rq : On peut restreindre l'action aux sous-ensembles $K_d[X_1,\dots,X_n]$ pour $d\in\mathbb{N}^*$.

Déf : Soit $P\in K[X_1,\dots,X_n]^{S_n}$ ie P vérifiant, $\forall\sigma\in S_n$, $\sigma\cdot P=P$.

Un tel polynôme est appelé polynôme symétrique et ces polynômes forment une sous-algèbre qu'on note $K[X_1,\dots,X_n]^{S_n}$.

Sz
RDO

2) Polynômes symétriques

Sz
RDO

Déf : Soit $p\in[\![1,n]\!]$, on pose

$$\sigma_p(X_1,\dots,X_n)=\sum_{1\le i_1<\dots<i_p\le n}X_{i_1}\cdots X_{i_p}$$

σ_p est un polynôme symétrique et les $(\sigma_p)_{1\le p\le n}$ sont appelés polynômes symétriques élémentaires.

Prop : Soit $P\in K[X]$, $P(X)=a_0+\dots+a_{n-1}X^{n-1}+X^n$ et supposons P scindé de racines $\alpha_1,\dots,\alpha_n$ dans L ie $P(X)=\prod_{j=1}^n(X-\alpha_j)$

Alors pour tout $i\in[\![1,n]\!]$, $a_{n-i}=(-1)^i\sigma_i(\alpha_1,\dots,\alpha_n)$

Rq : Ces relations sont appelées relations coefficients-racines d'un polynôme.

Th de structure : Soit A un anneau commutatif.

Soit P un polynôme symétrique à n indéterminées de degré total d. Alors il existe un polynôme Q à n indéterminées tel que :

$$P(X_1,\dots,X_n)=Q(\sigma_1(X_1,\dots,X_n),\dots,\sigma_n(X_1,\dots,X_n))$$

Rq : Il y a en fait unicité de Q.

Mieux, on a en fait $A[X_1,\dots,X_n]^{S_n}=A[\sigma_1,\dots,\sigma_n]$

Ex : Sommes de Newton.

Pour $k \in \mathbb{N}^*$, on appelle k-ième somme de Newton à n variables le polynôme $S_k = X_1^k + \dots + X_n^k$ et $S_0 = 0$

Pplé : $\forall k \in \mathbb{N}^*$, la k-ième somme de Newton S_k est symétrique et homogène de degré k.

Prop : On a les relations suivantes :

$$0 = S_k - \sigma_1 S_{k-1} + \dots + (-1)^l \sigma_l S_{k-l} + \dots + (-1)^n \sigma_n S_{n-k} \quad \text{si } k \geq n$$

$$0 = S_k - \sigma_1 S_{k-1} + \dots + (-1)^l \sigma_l S_{k-l} + \dots + (-1)^{k-1} \sigma_{k-1} S_1 + (-1)^k k \sigma_k$$

3) Résultant

Déf : Soient P, Q deux polynômes de degré p et q dans $A[X]$ avec $P(X) = a_0 X^p + \dots + a_p$ où $a_0 b_0 \neq 0$
$Q(X) = b_0 X^q + \dots + b_q$

On appelle résultant de P et Q (par rapport à la variable X) noté $R(A,B)$ l'élément de A donné par :

$$R(A,B) = \begin{vmatrix} a_0 & & 0 & b_0 & & 0 \\ \vdots & \ddots & & \vdots & \ddots & \\ & & a_0 & & & b_0 \\ a_p & & \vdots & b_q & & \vdots \\ & \ddots & & & \ddots & \\ 0 & & a_p & 0 & & b_q \end{vmatrix}$$

aussi appelé déterminant de la matrice Sylvester dans $M_{p+q}(A)$

Rq : La matrice de Sylvester est la matrice représentant dans les bases canoniques de $K_{\leq p-1}[X]$, $K_{\leq q-1}[X]$ et de $K_{\leq p+q-1}[X]$ l'application $\Phi_{P,Q}$ $\left(\begin{array}{ccc} K_{\leq p-1}[X] \times K_{\leq q-1}[X] & \longrightarrow & K_{\leq p+q-1}[X] \\ (A, B) & \longmapsto & PB + QA \end{array} \right)$

Pplé : Le résultant $R(P,Q)$ est non nul si et ssi P et Q n'ont aucune racine commune dans toute extension de K ie $P \wedge Q = 1$

Prop : Soient $\alpha_1, \dots, \alpha_p$ les racines de P et $\beta_1, \dots, \beta_q$ celles de Q dans K. Alors

$$\mathrm{Res}(P,Q) = B(\alpha_1) \dots B(\alpha_p) = A(\beta_1) \dots A(\beta_q) = \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

Appli : Théorème de Kronecker

Soit $P \in \mathbb{Z}[X]$ tel que P est unitaire, $X \nmid P$, de degré ≥ 1 et de racines complexes de modules ≤ 1.

Alors les racines complexes de P sont des racines de l'unité

Rev2 : Théorème de Bezout

) Cela revient au problème de placer d boules dans n boîtes.

Le nombre de parties à $n-1$ éléments dans $[\![1, n+d-1]\!]$

$\lfloor 00 \rfloor \; \lfloor\;\rfloor \; \lfloor 0 \rfloor \; \ldots \; \lfloor 0 \rfloor$

$0\,0\,|\,|\,0\,|\,\ldots\,0\,(1)$ en plus

Références

[Cal] J. CALAIS Éléments de théorie des anneaux

[Szp] SZPIRGLAS L3 Algèbre

[RDO] RAMIS-DESCHAMPS-ODOUX Cours de mathématiques 1. Algèbre

[Gob] GOBLOT Algèbre commutative