Algèbre des polynômes à n indéterminées ($n \geq 2$).

117

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

I) Polynômes à n indéterminées [RO0]

Déf: . On appelle à n indéterminées sur A toute famille à support fini $P = (a_i)_{i \in \mathbb{N}^n}$ d'éléments de A.

. On note $A[X_1, \dots, X_n]$ l'ensemble des polynômes à n indéterminées à coefficients dans A.

I.1) L'algèbre $A[X_1, \dots, X_n]$

Déf: Soient $P = (a_i)_{i \in \mathbb{N}^n}$, $Q = (b_i)_{i \in \mathbb{N}^n} \in A[X_1, \dots, X_n]$, $\lambda \in A$.

On définit : . l'addition $P + Q = (a_i + b_i)_{i \in \mathbb{N}^n}$

. la multiplication $P \cdot Q = \left(\sum_{k+l=i} a_k b_l \right)_{i \in \mathbb{N}^n}$

. multiplication scalaire $\lambda P = (\lambda a_i)_{i \in \mathbb{N}^n}$

Théorème: $A[X_1, \dots, X_n]$ muni de ces trois opérations est une A-algèbre commutative d'élément neutre $(a_i)_{i \in \mathbb{N}^n} = (a_0, 0, \dots)$ pour la multiplication.

Prop: Tout polynôme de $A[X_1, \dots, X_n]$ s'écrit de façon unique comme combinaison linéaire des $(X_1^{i_1} \dots X_n^{i_n})_{i \in \mathbb{N}^n}$. De plus, les coefficients de la combinaison linéaire sont ceux du polynôme. Si $P = (a_i)_{i \in \mathbb{N}^n}$, $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}$.

Propriété universelle: Pour toute A-algèbre commutative $\varphi : A \to B$ et toute suite $(b_1, \dots, b_n)$ d'éléments de B, il existe un unique morphisme de A-algèbre $\Phi_{X_i \to b_i} : A[X_1, \dots, X_n] \to B$ qui envoie X_i sur b_i.

Théorème d'isomorphisme: $A[X_1, \dots, X_n] \simeq (A[X_1, \dots, X_{n-1}])[X_n]$

Déf (degré partiel): Soit $q \in [\![1; n]\!]$, $P \in A[X_1, \dots, X_n]$. Le degré partiel de P relativement à X_q, noté $\deg_{X_q}(P)$ est le degré de P vu comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$.

Déf (degré total): . Si $P = 0$, $\deg(P) = -\infty$

. Si $P \neq 0$, $\deg P = \max \{ |i| \mid a_i \neq 0 \}$ où on note pour $i \in \mathbb{N}^n$, $|i| = i_1 + \dots + i_n$.

Prop: $P, Q \in A[X_1, \dots, X_n]$. $\deg(P+Q) \leq \max(\deg P, \deg Q)$

. $\deg(PQ) = \deg P + \deg Q$ si A est intègre

Exemple: . $P = 2XY + 3Y^2Z + Z^3$.

. $\deg_Z(P) = 2$, et $\deg(P) = 3$

I.2) Propriétés arithmétiques

Prop: . A intègre $\Rightarrow A[X_1, \dots, X_n]$ intègre.

. A factoriel $\Rightarrow A[X_1, \dots, X_n]$ factoriel.

. $K[X_1, \dots, X_n]$ est factoriel

. $K[X_1, \dots, X_n]$ ($n \geq 2$) n'est pas principal.

Conséquence: $\rightarrow$ existence d'une décomposition unique en produit d'irréductibles

$\rightarrow$ existence de PGCD et PPCM d'une famille de polynômes

$\rightarrow$ le théorème de Gauss subsiste mais le théorème de Bézout est faux.

Divisibilité :

Thm : Soit $P \in K[X_1, \dots, X_n]$ et $a \in K[X_1, \dots, X_{n-1}]$. P est divisible par $(X_n - a)$ ssi le polynôme $P(X_1, \dots, X_{n-1}, a)$ est le polynôme nul.

Cor : $P \in K[X_1, \dots, X_n]$, P est divisible par $\prod (X_j - X_i)$ ssi : P est divisible par chacun des $X_j - X_i$. $^{i<j}$

I.3) Polynômes homogènes

Déf : Soit $p \in \mathbb{N}$. $P = (a_i)_{i \in \mathbb{N}^n}$. On dit que P est p-homogène si $|i| \neq p \Rightarrow a_i = 0$.

Exemple : On définit une forme quadratique comme un polynôme 2-homogène.

Théorème : - L'ensemble A_p de $A[X_1, \dots, X_n]$ constitué des polynômes p-homogènes est un sous-module de $A(X_1, \dots, X_n]$.

$$- A[X_1, \dots, X_n] = \bigoplus_{p=0}^{+\infty} A_p.$$

[P] Application : . théorème de Molien (admis) : Soit G un sous-groupe fini de $GL_n(\mathbb{C})$. On définit une action de G sur les K_p (char $K = 0$), on note $d_p(G) = \dim K_p^G$ alors :

$$\sum_{p \geq 0} d_p(G) t^p = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gt)}$$

[B] . irréductibilité du déterminant :

$\Delta = \det \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \cdots & X_{nn} \end{pmatrix} \in \mathbb{Z}[X_{11}, \dots, X_{nn}]$ est irréductible.

II) Fonction polynomiale et séries de polynômes

II).1) Fonctions polynômes [Gob] [ROO]

Déf : L'application $\tilde{P} : A^n \longrightarrow A$, $(a_1, \dots, a_n) \longmapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \cdots x_n^{i_n}$ est appelée fonction polynôme associée à P. Elle définit un morphisme de A-algèbres $A[X_1, \dots, X_n] \to \mathcal{F}(A^n, A)$.

Prop : A intègre. Le morphisme défini ci-dessus est injectif ssi : $\mathrm{card}(A) = +\infty$.

II.2) Prolongement des identités

Déf : Une identité entre m polynômes $P_1, \dots, P_m$ de $A[X_1, \dots, X_n]$ est une égalité de la forme $G(P_1, \dots, P_m) = 0$ où G est dans $A[Y_1, \dots, Y_m]$.

Cas important : $A = \mathbb{Z}$, tout anneau peut être regardé comme $\mathbb{Z}$-algèbre de manière unique, les identités dans $\mathbb{Z}[X_1, \dots, X_n]$ sont donc universelles.

Exemple : $(X+Y)^p = \sum_{k=0}^{p} \binom{p}{k} X^k Y^{p-k}$ donne $\mathbb{F}_p[X, Y]$

$(X+Y)^p = X^p + Y^p$

Théorème (prolongement des identités) : A intègre, $\mathrm{card}(A) = +\infty$. Soient $P_1, \dots, P_m \in A[X_1, \dots, X_n]$. Soit $V(P_j)$ l'ensemble des $x \in A^n$, $P_j(x_1, \dots, x_n) = 0$. Si F et G sont deux polynômes de $A[X_1, \dots, X_n]$ tels que $F(x) = G(x)$ pour tout $x \in A^n \setminus \bigcup_{j=1}^{m} V(P_j)$, alors $F = G$.

DVPT 1

II.3) Théorème de Chevalley-Warning

Thm : Soit K un corps de caractéristique p, de cardinal q et $P_1, \dots P_m \in K[X_1, \dots, X_n]$ et $V = \{x \in K^n / \forall i,\ P_i(x) = 0\}$

Si $\sum_{i=1}^{m} \deg P_i < n$ alors $\#V \equiv 0 \ [p]$. (admis)

[SER]

Corollaire: $(P_1, \dots, P_m) \in K[X_1, \dots, X_m]$. Si $\sum \deg P_i < n$ et P_i sans terme constant, alors ils ont un zéro non trivial commun.

III) Polynômes symétriques

III.1) Relations coefficients racines

Déf: On définit pour $k \in [1;n]$ le k-ième polynôme symétrique élémentaire $\Sigma_k = \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$

Prop: Soit $P \in K[X]$, $P = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$. Si on peut écrire $P = a_n \prod_{i=1}^{n} (X - \alpha_i)$ on a alors les relations :

$$[S_p]_{a_n}^{a_{n-1}} = \Sigma_1(\alpha_1, \dots, \alpha_n), \dots, \frac{a_{n-k}}{a_n} = (-1)^k \Sigma_k(\alpha_1, \dots, \alpha_n).$$

III.2) Polynômes symétriques

→ action de $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$

[RDO]

Déf: $\sigma \in \mathfrak{S}_n$, $P \in A[X_1, \dots, X_n]$, $\sigma(P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

$\Leftrightarrow$. P est dit symétrique si $\forall \sigma \in \mathfrak{S}_n$, $\sigma(P) = P$

Exemple:
- Les polynômes symétriques élémentaires Σ_k.
- Le discriminant $\Delta(X_1, \dots, X_n) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (X_j - X_i)$
- Les sommes de Newton $S_k = \sum_{p=1}^{n} X_p^k$.

Déf:
- Le poids du monôme $X_1^{i_1} \dots X_n^{i_n}$ est l'entier $\sum_{k=1}^{n} k i_k$ et le poids d'un polynôme est le maximum du poids de ses monômes, on le note $\pi(P)$.

Déf: Soit $P \in A[X_1, \dots, X_n]$ symétrique. P a même degré partiel par rapport à chaque indéterminée, que l'on appelle ordre de P et que l'on note $\omega(P)$.

Théorème de structure:

Soit $P \in A[X_1, \dots, X_n]$ symétrique, $\deg(P) = p$ et $\omega(P) = w$. Alors il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$.
De plus, Q est de poids p et de degré w.
→ Sommes de Newton

Thm (Relations de Newton): Les polynômes symétriques et homogènes S_k vérifient : [RDO]

(i) Pour $k \ge n$

$$S_k - \Sigma_1 S_{k-1} + \dots + (-1)^p \Sigma_p S_{k-p} + \dots + (-1)^n \Sigma_n S_{k-n} = 0$$

(ii) Pour $1 \le k \le n$

$$S_k - \Sigma_1 S_{k-1} + \dots + (-1)^p \Sigma_p S_{k-p} + \dots + (-1)^k k \Sigma_k = 0$$

III.3) Algorithme

[RDO]

. P non nul, symétrique homogène : $P = \sum_{i_1 + \dots + i_n = p} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$

$\mathbb{N}^n$ est totalement ordonné par l'ordre lexicographique sous $k = (k_1, \dots, k_n)$ le plus grand n-uplet pour cet ordre tel que $a_k \neq 0$. On a $k_1 \ge k_2 \ge \dots \ge k_n$.

$$P - a_k (\Sigma_1)^{k_1 - k_2} (\Sigma_2)^{k_2 - k_3} \dots (\Sigma_n)^{k_n}$$

Le polynôme est symétrique, homogène de degré pour l'ordre lexicographique strictement inférieur à k.

. Dans le cas général, on décompose le polynôme symétrique P en polynômes symétriques homogènes.

Références : [RDO] Ramis - Deschamps - Odoux : Algèbre

[Gob] Lot Algèbre commutative

[B] Briançon

[P] Peyré, Algèbre discrète de la transformée de Fourier.

[Ser] Serre, cours d'arithmétique

[Spi] Spring, Algèbre 63.

Autres développements possible :

- Chevalley - Warning
- Théorème de Molien
- Irréductibilité du déterminant
- Théorème des zéros de Hilbert