142 Algèbre des polynômes à plusieurs indéterminées Applications

<u>Cadre</u> : A anneau commutatif unitaire, K corps, $n \in \mathbb{N}, n \geq 2$, $i \in \mathbb{N}^n$, $i = (i_1, \dots, i_n)$, $|i| = \sum_{j=1}^{n} i_j$

(I) Polynômes à plusieurs indéterminées

(1) L'algèbre $A[X_1, \dots, X_n]$. [RDO]

<u>Def 1</u> Un polynôme à plusieurs indéterminées sur A est une famille presque nulle $(a_i)_{i \in \mathbb{N}^n}$ d'éléments de A. On note $A[X_1, \dots, X_n]$ l'ensemble des polynômes à n indéterminées à coefficients dans A.

<u>Def 2</u> Soient $P = (a_i)_{i \in \mathbb{N}^n}$, $Q = (b_i)_{i \in \mathbb{N}^n} \in A[X_1, \dots, X_n]$ et $\lambda \in A$. On définit : - une addition : $P+Q = (a_i + b_i)_i$
- une multiplication : $PQ = \left(\sum_{k+l=i} a_k b_l\right)_i$
- une multiplication scalaire : $\lambda P = (\lambda a_i)_i$

<u>Théorème 3</u> $A[X_1, \dots, X_n]$ muni de ces opérations est une A-algèbre commutative d'élément neutre pour la multiplication $(a_i)_i$ avec $a_{(0,\dots,0)} = 1$ et $\forall i \neq (0, \dots, 0)$, $a_i = 0$.

<u>Prop 4</u> Tout élément de $A[X_1, \dots X_n]$ s'écrit de façon unique comme combinaison linéaire des $(X_1^{i_1} \cdots X_n^{i_n})_{i \in \mathbb{N}^n}$. Les coefficients de la combinaison linéaire sont ceux du polynôme.

<u>Propriété universelle 5</u> Soit B une A-algèbre commutative, $\varphi : A \to B$ un morphisme d'anneaux et $(b_1, \dots, b_n) \in B^n$. Alors il existe un unique morphisme de A-algèbres $\varphi_{X \mapsto b} : A[X_1, \dots, X_n] \to B$ qui envoie X_i sur b_i $\forall i \in [\![1, n]\!]$ et un élément a de A sur $\varphi(a)$ [GOB]

<u>Théorème d'isomorphisme 6</u> $A[X_1, \dots, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes via

$$\Phi : A[X_1, \dots, X_n] \to A[X_1, \dots, X_{n-1}][X_n]$$
$$\sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum_{k \in \mathbb{N}} \left(\sum a_i X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}\right) X_n^k$$

<u>Remarque</u> : on aurait pu particulariser n'importe quel X_k

<u>Def 7</u> Soit $q \in [\![1, n]\!]$, $P \in A[X_1, \dots, X_n]$. Le degré partiel de P relativement à X_q est le degré de P vu comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. On le note $\deg_{X_q}(P)$

<u>Def 8</u>. On définit le degré total de P comme étant $-\infty$ si $P = 0$ et $\deg P = \max_{i \in \mathbb{N}^n} \{ |i| \mid a_i \neq 0 \}$ sinon.

<u>Prop 9</u> $P, Q \in A[X_1, \dots, X_n]$. On a :
- $\deg(P+Q) \leq \max\{\deg P, \deg Q\}$
- $\deg(PQ) \leq \deg P + \deg Q$

<u>Exemple 10</u> $P = X^7 Y^2 Z^3 + 8 X Z^{10} \in \mathbb{Z}[X, Y, Z]$.
$\deg_Z(P) = 10$, $\deg(P) = 12$

<u>Def 11</u> $P \in A[X_1, \dots, X_n]$. On appelle polynôme dérivé partiel de P relativement à X_q ($q \in [\![1, n]\!]$) le polynôme dérivé de P vu comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. On le note $\frac{\partial P}{\partial X_q}$

<u>Def 12</u> $P, Q \in K[X_1, \dots, X_n]$. Le résultant en X_q ($q \in [\![1, n]\!]$) de P et Q est le déterminant de la matrice de Sylvester :

$$\begin{pmatrix} a_m & & & b_m & & \\ \vdots & \ddots & a_m & \vdots & \ddots & b_m \\ a_0 & & \vdots & b_0 & & \vdots \\ & \ddots & a_0 & & \ddots & b_0 \end{pmatrix} \in \mathcal{M}_{n+m}(K) \quad \text{où } P = \sum_{i=0}^{m} a_i X^i, \quad Q = \sum_{i=0}^{m} b_i X^i$$

et $a_i, b_i \in K[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n]$.

<u>Prop 13</u> (lien résultant - racines) Avec les mêmes notations, si $P = a_n(X-\alpha_1)\cdots(X-\alpha_n)$ et $Q = b_m(X-\beta_1)\cdots(X-\beta_m)$ alors on a :

$$\mathrm{Res}_X(P, Q) = a_m^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$
$$= a_m^m \prod_{i=1}^{n} Q(\alpha_i)$$
$$= (-1)^{mn} \mathrm{Res}_X(Q, P)$$

[SZP]

② Propriétés arithmétiques [RDO]

<u>Prop 14</u> – A intègre $\Rightarrow A[X_1,\dots,X_n]$ intègre
– A factoriel $\Rightarrow A[X_1,\dots,X_n]$ factoriel
– $K[X_1,\dots,X_n]$ n'est pas principal.

Conséquences : on a l'existence d'une décomposition unique en produit d'irréductibles, du pgcd et ppcm d'une famille de polynômes.

<u>Théorème 15</u> $P \in K[X_1,\dots,X_n]$, $Q \in K[X_1,\dots,X_{n-1}]$
P est divisible par $X_n - Q$ ssi $P(X_1,\dots,X_{n-1},Q)=0$

<u>Cor 16</u> $P \in K[X_1,\dots,X_n]$. $\prod_{i<j}(X_j - X_i) \mid P$ ssi $\forall i<j$, $(X_j - X_i) \mid P$

③ Polynômes homogènes [RDO]

<u>Def 17</u> Soit $p \in \mathbb{N}$, $P = (a_i)_i \in A[X_1,\dots,X_n]$
On dit que P est p-homogène si on a : $|i| \neq p \Rightarrow a_i = 0$.

<u>Exemple 18</u> On définit une forme quadratique comme un polynôme 2-homogène.

<u>Def 19</u> On note A_p l'ensemble des polynômes p-homogènes de $A[X_1,\dots,X_n]$

<u>Théorème 20</u> $\forall p \in \mathbb{N}$, A_p est un sous-module de $A[X_1,\dots,X_n]$ et on a :
$$A[X_1,\dots,X_n] = \bigoplus_{p \geq 0} A_p$$

<u>Application 21</u> (Théorème de Molien)
Soit G un groupe fini de $GL_n(\mathbb{C})$. On définit une action de G sur les A_p ($p \in \mathbb{N}$), $a_p = \dim A_p^G$. Alors on a :
$$\sum_{p \geq 0} a_p X^p = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gX)}$$
[PEY]

II Fonctions polynômes et zéros de polynôme

① Fonctions polynômes [RDO]

<u>Def 22</u> $P \in A[X_1,\dots,X_n]$. On définit
$\tilde{P} : A^n \to A$, $(x_1,\dots,x_n) \mapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \cdots x_n^{i_n}$
la fonction polynôme associée à P.
$\varphi : P \mapsto \tilde{P}$ est un morphisme de A-algèbres de $A[X_1,\dots,X_n]$ vers $\mathcal{F}(A^n, A)$.

<u>Prop 23</u> Supposons A intègre infini, soient $(A_i)_{i \in [\![1,n]\!]}$ des parties infinies de A. Si $\tilde{P}$ s'annule en tout point de $\prod A_i$, alors $P = 0$.

<u>Application 24</u> $K = \mathbb{R}$ ou $\mathbb{C}$, $P \in K[X_1,\dots,X_n]$
Si $\tilde{P}$ s'annule sur un ouvert non vide, alors $P = 0$.

② Prolongement des identités. [GOB]

<u>Def 25</u> Une identité entre m polynômes $F_1,\dots,F_m$ de $A[X_1,\dots,X_n]$ est une égalité de la forme $G(F_1(X_1,\dots,X_n),\dots,F_m(X_1,\dots,X_n)) = 0$ où $G \in A[Y_1,\dots,Y_m]$.

<u>Prop 26</u> (prolongement des identités) $P_i \neq 0$
Supposons A intègre infini. Soient $P_1,\dots,P_m \in A[X_1,\dots,X_n]$ et $V_j = \{x \in A^n, \tilde{P}_j(x) = 0\}$ pour $j \in [\![1,m]\!]$.
Si $P, Q \in A[X_1,\dots,X_n]$ sont tels que $\forall x \in A^n \setminus (\bigcup_j V_j)$, $\tilde{P}(x) = \tilde{Q}(x)$ alors $P = Q$

<u>Application 27</u> Soit $A \in \mathcal{M}_n(K)$. Alors :
$\forall M \in \mathcal{M}_n(K)$, $\chi(AM) = \chi(MA)$.

③ Théorème de Chevalley-Warning.

<u>Théorème 28</u> (Chevalley-Warning). Soit K corps de caractéristique p, soient $P_1,\dots,P_r \in K[X_1,\dots,X_n]$ / $\sum_{i=1}^{r} \deg(P_i) < n$, $V = \bigcap_{i=1}^{r} V_i$. Alors $\mathrm{Card}(V) \equiv 0\ [p]$.

DVP 1
[SER]

[SZP]

DVP 2

[FGN]

Cor 29 $P_1, \dots, P_r \in K[X_1, \dots, X_n]$ / $\sum_{i=1}^{r} \deg P_i < n$ et les P_i sont sans terme constant. Alors ils ont un zéro commun non trivial.

Application 30 Toute forme quadratique d'au moins trois variables sur K a un zéro non trivial.

III Polynômes symétriques

1 Relations coefficients - racines.

Def 31 Pour $k \in [\![1,n]\!]$, $\sigma_k = \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$ est le k-ième polynôme symétrique élémentaire.

Prop 32 $P = \sum_{i=1}^{n} a_i X^i$ / $a_n \neq 0$. Si P s'écrit $P = a_n \prod_{i=1}^{n} (X - \alpha_i)$ avec $a_i, \alpha_i \in K$ ($\forall i \in [\![1,n]\!]$) alors on a $\frac{a_{n-k}}{a_n} = (-1)^k \sigma_k(\alpha_1, \dots, \alpha_n)$ ($k \in [\![1,n]\!]$)

Théorème 33 (Kronecker) Soit P polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module plus petit que 1 et tel que $P(0) \neq 0$. Alors les racines de P sont des racines de l'unité.

2 Polynômes symétriques. [RDO]

Def 34 $P \in A[X_1, \dots, X_n]$ est dit symétrique si $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

Remarque Les polynômes symétriques élémentaires sont symétriques.

Def 35 - Le poids du monôme $X_1^{i_1} \dots X_n^{i_n}$ est $\sum_{k=1}^{n} k i_k$ - Le poids de $P \in A[X_1, \dots, X_n]$ est $-\infty$ si $P = 0$ et est le maximum des poids de ses monômes sinon.

Def 36 (Prop) Soit $P \in A[X_1, \dots, X_n]$ symétrique. Alors P a même degré partiel relativement à chaque indéterminée. On appelle ce degré partiel ordre de P, on le note $\omega(P)$.

Théorème 37 (de structure) Soit $P \in A[X_1, \dots, X_n]$ symétrique de degré p et d'ordre ω. Alors il existe un unique $Q \in A[Y_1, \dots, Y_n]$ tel que $P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n)$. De plus Q est de poids p et de degré ω.

3 Algorithme (pour déterminer Q)

Soit $P \in A[X_1, \dots, X_n]$ symétrique non nul. On peut supposer P homogène car tout polynôme se décompose en une somme de polynômes symétriques homogènes. On écrit $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}$ et on munit $\mathbb{N}^n$ de l'ordre lexicographique.

- Soit $k = (k_1, \dots, k_n) \in \mathbb{N}^n$ le plus grand n-uplet tel que $a_k \neq 0$. On peut montrer que $k_1 \geq \dots \geq k_n$. On calcule $P - a_k \sigma_1^{k_1 - k_2} \dots \sigma_{n-1}^{k_{n-1} - k_n} \sigma_n^{k_n}$. Ce polynôme est alors symétrique et homogène et son k associé est strictement inférieur à celui de P. Si ce polynôme est nul, on a terminé, sinon on recommence.

Cet algorithme se termine bien par décroissance stricte du k à chaque étape.

[RDO]

Références : → Ramis - Deschamps - Odoux — Algèbre 1. [RDO]
→ Goblot — Algèbre commutative [GOB]
Szpirglas — Algèbre [SZP]
Peyré (pour Molien) — Algèbre discrète de la transformée de Fourier (p219) [PEY]
Serre (pour Chevalley-Warning) — Cours d'arithmétique (p13) [SER]
Francinou - Gianella - Nicolas (pour Kronecker) — Oraux X-ENS Algèbre 1. (p213) [FGN]

Autres idées :
- application de la factorialité : déterminant de Vandermonde, de Cauchy
- poly. invariants sous $\mathfrak{S}_n$: $K[\sigma_1, \dots, \sigma_n, V_n]$ (car $k \neq 2$), V_n le Vandermonde [GOB] [SZP]
- identité d'Euler : P homogène de deg d $\Rightarrow$ $\sum_{i=1}^{n} X_i \frac{\partial P}{\partial X_i} = d \cdot P$ [RDO]
- fonction polynôme associée sur un corps fini [Francinou-Gianella]
- $\mathbb{C}$ alg. clos par Lagrange (Samuel, T.A.N, p.53)
- sommes de Newton $\sum_{i=1}^{n} X_i^k$ (lem thm de Burnside)