142 Algèbre des polynômes à plusieurs indéterminées. Applications

Cadre : A anneau commutatif unitaire. K un 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 n INDÉTERMINÉES. [RDO]

1. Algèbre $A[X_1, \dots, X_n]$

p185

Def 1 On appelle polynôme à n indéterminées sur A toute famille presque nulle d'éléments de A indexée par $\mathbb{N}^n$. Il est alors de la forme $P = (a_i)_{i \in \mathbb{N}^n}$.
L'ensemble des polynômes à n indéterminées à coefficients dans A est noté $A[X_1, \dots, X_n]$.

Def 2. 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 une addition : $(P+Q) = (a_i + b_i)_i$
une multiplication $(P.Q) = (\sum_{k+l=i} a_k b_l)_i$
une multiplication par un scalaire $(\lambda P) = (\lambda a_i)_i$

Thm 3 Muni de ces opérations, l'ensemble $A[X_1, \dots, X_n]$ est une A algèbre commutative.

Thm 4. Dans $A[X_1, \dots, X_n]$, tout polynôme s'écrit de façon unique comme combinaison linéaire de $(X_1^{i_1} \dots X_n^{i_n})_{(i_1, \dots, i_n) \in \mathbb{N}^n}$; les coefficients de la combinaison linéaire sont ceux du polynôme.

Prop 5 Propriété universelle [GOB]
Soient $\varphi : A \to R$ une A-algèbre et $(x_1, \dots, x_n) \in R^n$.
Alors il existe un unique morphisme de A-algèbres $\Phi : A[X_1, \dots, X_n] \to R$ tel que $\Phi(X_i) = x_i$ $\forall i \in [1, n]$.

p171

Thm 6 Isomorphisme canonique. [RDO]
$A[X_1, \dots, X_{n-1}, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes via $\Phi : P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \longrightarrow \sum_{k \in \mathbb{N}} \left(\sum_{(i_1, \dots, i_{n-1}, k) \in \mathbb{N}^n} a_{i_1 \dots i_{n-1} k} X_1^{i_1} \dots X_{n-1}^{i_{n-1}} \right) X_n^k$

p188

sans référence

Ex 7. Le déterminant est un polynôme à plusieurs indéterminées; les coefficients du polynôme caractéristique sont des polynômes à plusieurs indéterminées.

2. Degré et polynômes homogènes. [RDO]

p189

Def 8 Soient $n, q \in \mathbb{N}$ tels que $1 \leq q \leq n$. On appelle degré partiel du polynôme P de $A[X_1, \dots, X_n]$ relativement à l'indéterminée X_q, le degré de P comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. Ce degré est noté $\deg_{X_q}(P)$.

Def 9 Soit $P = (a_i)_i \in A[X_1, \dots, X_n]$. Si $P = 0$, $\deg(P) = -\infty$.
Si $P \neq 0$ $\deg P = \max \{ |i| \mid i \in \mathbb{N}^n, a_i \neq 0 \}$
$\deg(P)$ est appelé le degré total de P.

Prop 10 Quels que soient les polynômes $P, Q \in A[X_1, \dots, X_n]$.
$\deg(P+Q) \leq \sup(\deg P, \deg Q)$.
$\deg(P.Q) \leq \deg(P) + \deg Q$ (égalité si A intègre).

Ex 11 $P = Y - X^2 + XYZ$ est de degré total 3.

Appli 12 A intègre $\Rightarrow$ $A[X_1, \dots, X_n]$ intègre [TAU] p212

p190

Def 13 $p \in \mathbb{N}$, $P = (a_i)_i \in A[X_1, \dots, X_n]$ est dit p-homogène ssi l'inégalité $|i| \neq p \Rightarrow a_i = 0$

Ex 14 $P = X^2 + XY$ est homogène.

Rq Si deux polynômes de $A[X_1, \dots, X_n]$ sont respectivement p-homogène et q-homogène, leur produit est $(p+q)$-homogène.

Classification des polynômes homogènes (de degré ≤ 2)
degré 0 : les constantes $\lambda \in A$ ...
degré 1 : les formes linéaires
degré 2 : les formes quadratiques

Appli 15. Théorème de Molien. [LEi] et [PEY] DVPT
$\forall k \in \mathbb{N}$, on note A_k l'espace des polynômes homogènes de degré k de $A[X_1, \dots, X_n]$. Soit G groupe fini de $GL_n(\mathbb{C})$. On définit une action de G sur les A_k. On note $a_k(G) = \dim A_k^G$.
Alors $\sum_{k \geq 0} a_k(G) X^k = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gX)}$

p95 et p221

Def 16 On appelle polynôme dérivé partiel de $P \in A[X_1, \dots, X_n]$ par rapport à l'indéterminée X_q $(1 \leq q \leq n)$ le polynôme dérivé de P considéré comme un élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. On le note $\partial P / \partial X_q$. [RDO]

p193

p196

Thm 17 D'EULER [RDO]

Soit K un corps commutatif de caractéristique nulle, $P \in K[X_1, \dots, X_n]$. Sont équivalents :

1) P est p-homogène. 2) $\sum_{q=1}^{n} X_q \frac{\partial P}{\partial X_q} = pP$.

3. Propriétés arithmétiques

p199

Propr 18 A factoriel $\Rightarrow A[X_1, \dots, X_n]$ factoriel.

Propr 19 On se place ici dans un corps commutatif K.

Pour $n \geq 2$, l'anneau $K[X_1, \dots, X_n]$ n'est pas principal.

Propr 18 : $K[X_1, \dots, X_n]$ factoriel.

↳ existence d'une décomposition unique en produit de polynômes irréductibles non associés

↳ existence du PGCD et du PPCM

↳ le théorème de Gauss subsiste (mais pas le théorème de Bézout).

p198 **Prop 20**. Dans $K[X_1, \dots, X_n]$, le polynôme A est divisible par le polynôme $X_n - B$ (B polynôme de $K[X_1, \dots, X_{n-1}]$) ssi le polynôme obtenu en substituant, dans A, le polynôme B à l'indéterminée X_n soit le polynôme nul.

Ex 21. Dans $\mathbb{Q}[X, Y, Z]$, $X^3 + Y^3 + Z^3 + mXYZ$ est divisible par $X + Y + Z$ ssi $m = -3$

Coro 22. $A \in K[X_1, \dots, X_n]$ est divisible par $\prod_{1 \leq i < j \leq n} (X_j - X_i)$ ssi A est divisible séparément par chacun des $X_j - X_i$ $(1 \leq i < j \leq n)$.

II. FONCTIONS POLYNÔMES

1. Fonctions polynômes et prolongement des identités

[RDO] p191 **Def 23** $P = \sum a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$. L'application

$$\tilde{P} : A^n \to A, \quad (x_1, \dots, x_n) \mapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \dots x_n^{i_n}$$

est appelée fonction polynôme de n variables (abus d'écriture : $P = \tilde{P}$)

Prop 24. Soient A intègre et $(A_i)_{1 \leq i \leq n}$ une famille de sous-ensembles infinis de A. Alors pour tout polynôme $P \neq 0$ de $A[X_1, \dots, X_n]$, il existe une infinité de points de $\prod_{i=1}^{n} A_i$ en lesquels la fonction polynôme $\tilde{P}$ prend une valeur non nulle. p192

Thm 25 Si A intègre infini, alors $\Psi : P \in A[X_1, \dots, X_n] \to \tilde{P}$ est un isomorphisme de $A[X_1, \dots, X_n]$ sur l'algèbre des fonctions polynômes de n variables sur A.

Appli 26 Si $K = \mathbb{R}$ ou $\mathbb{C}$, $P \in K[X_1, \dots, X_n]$. Si $\tilde{P}$ s'annule sur un ouvert non vide, le polynôme P est nul.

Def 27 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 $G(Y_1, \dots, Y_m) \in A[Y_1, \dots, Y_m]$ [GOB] p172 Ⓐ

Prop 28. PROLONGEMENT DES IDENTITÉS. [GOB] p173.

A intègre de cardinal infini. $P_1, \dots, P_m \in A[X_1, \dots, X_n] \setminus \{0\}$.

Soit $V(P_j) = \{x \in A^n \mid P_j(x) = 0\}$. Si $F_1, F_2 \in A[X_1, \dots, X_n]$ sont tels que $\forall x \in A^n \setminus (\bigcup_j V(P_j))$, $F_1(x) = F_2(x)$, alors $F_1 = F_2$.

Appli 29 K un corps ; $M, N \in \mathcal{M}_n(K)$ Alors $\chi(MN) = \chi(NM)$

2. Corps finis [SER] p13-14

Soit q une puissance d'un nombre premier p et soit K un corps à q éléments.

Thm 30 CHEVALLEY - WARNING. DVPT

Soient $P_1, \dots, P_r \in K[X_1, \dots, X_n]$ tels que $\sum_{i=1}^{r} \deg(P_i) < n$, et V l'ensemble de leurs zéros communs dans K^n.

On a $\operatorname{card} V \equiv 0 \, [p]$.

Coro 31 Avec les mêmes conditions et si les P_i sont sans terme constant, alors ils ont un zéro commun non trivial.

Appli 32. Toute forme quadratique d'au moins 3 variables sur K a un zéro non trivial.

3. Corps $\mathbb{R}$ ou $\mathbb{C}$. [GOB] p173

Prop 33 Si $F_1, F_2 \in K[X_1, \dots, X_n]$ ($K = \mathbb{R}$ ou $\mathbb{C}$) tels que les fonctions polynômes coïncident sur un ouvert non vide de K^n. Alors $F_1 = F_2$.

Appli 34 on obtient le théorème de Cayley-Hamilton.

III APPLICATION : POLYNÔMES SYMÉTRIQUES ET SEMI-SYM.

1. Polynômes symétriques

[RDO] p200 **Def 35**. $P \in A[X_1, \dots, X_n]$ est dit symétrique si $\forall \sigma \in \mathfrak{S}_n$ $\sigma(P) = P$ où $\sigma(P)$ est le polynôme obtenu en substituant aux n indéterminées $X_1, \dots, X_n$ les n polynômes $X_{\sigma(1)}, \dots, X_{\sigma(n)}$.

Def 36. Dans $A[X_1, \dots, X_n]$, on définit pour $k \in [\![1, n]\!]$
$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}.$$
On pose $\sigma_0 = 1$.

[RDO] p201 ou [GOB] p177 **Prop 37** Soit $P \in A[X_1, \dots, X_n, Y]$, $P = \prod_{i=1}^{n} (Y - X_i)$ alors $P = \sum_{k=1}^{n} (-1)^k \sigma_k(X_1, \dots, X_n) Y^{n-k}$.

Rq On retrouve les relations coefficients-racines connues dans $A[X]$.

[RDO] p201 **Thm 38** Les polynômes σ_k sont symétriques et appelés polynômes symétriques élémentaires. Ils sont k-homogènes.

[FGN AL 1] **Thm 39** 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.

[RDO] p202 **Def 40** • On appelle poids du monôme $X_1^{i_1} \dots X_n^{i_n}$ l'entier $\sum_{k=1}^{n} k i_k$
• le poids d'un polynôme P est le maximum des poids de ses monômes. Il vaut $-\infty$ si $P = 0$. On le note $\Pi(P)$.

(B)

Thm / Def 41. Soit P un polynôme symétrique de $A[X_1, \dots, X_n]$. P a même degré partiel par rapport à indéterminée. Ce degré s'appelle ordre de P et est noté $\omega(P)$.

Thm 42 THÉORÈME DE STRUCTURE [RDO] p204

Soit P un polynôme symétrique de $A[X_1, \dots, X_n]$ de degré p et d'ordre ω. Alors il existe un unique polynôme Φ de $A[Y_1, \dots, Y_n]$ tel que $P(X_1, \dots, X_n) = \Phi(\sigma_1, \dots, \sigma_n)$.
Ce polynôme Φ est de poids p et de degré ω.

(C) (D)

Algorithme pour déterminer Φ [RDO] p205
Soit $P \in A[X_1, \dots, X_n]$ symétrique non nul.
On suppose P homogène. $P = \sum_{|i|=p} a_i X_1^{i_1} \dots X_n^{i_n}$.
On ordonne $\mathbb{N}^n$ avec l'ordre lexicographique.
Soit $k = (k_1, \dots, k_n)$ le plus grand n-uplet tel que $a_i \neq 0$.
↳ On peut montrer que $k_1 \geq \dots \geq k_n$.
On calcule alors $\Phi = P - a_k (\sigma_1)^{k_1 - k_2} (\sigma_2)^{k_2 - k_3} \dots (\sigma_{n-1})^{k_{n-1} - k_n} (\sigma_n)^{k_n}$
On a Φ • symétrique homogène.
• nul ou de degré inférieur à k strictement pour l'ordre lexicographique.
Si Φ nul, l'algorithme est terminé.
Sinon on recommence l'opération avec Φ.
↳ En un nombre fini d'opération, on aboutit à un polynôme nul. (Car décroissance stricte de la suite des degrés)

2. Polynômes semi-symétriques [GOB] p180

Def 43. Un polynôme $P \in A[X_1, \dots, X_n]$ est dit semi-symétrique si $\forall \tau \in \mathfrak{A}_n$ $\tau(P) = P$

Rq on aurait pu définir les polynômes alternés :
Si F est alterné, $\forall \sigma \in \mathfrak{S}_n$, $\sigma(F) = \varepsilon(\sigma) F$.
→ les polynômes alternés sont des polynômes semi-symétriques particuliers.

Def 44. On définit $V(X_1, \dots, X_n) = \prod_{i<j} (X_i - X_j)$.

Ex 45 V est semi-symétrique (et symétrique en caractéristique 2)

Prop 46 Soit K un corps avec car $K \neq 2$. Pour que $F \in K[X_1, \dots, X_n]$ soit semi-symétrique, il faut il suffit qu'il existe P, Φ symétriques (nécessairement uniques) tels que $F = P + V\Phi$.

Références

- [RDO] Ramis, Deschamps, Odoux, Algèbre 1, 2ème édition
- [GOB] Goblot, Algèbre commutative 2ème édition.
- [SER] Serre, Cours d'arithmétique.
- [TAU] Tauvel, Algèbre
- FGN Algèbre 1 pour dvpt Kronecker.

Autres dvpts possibles.

- Thm de structure
- Irréductibilité de det
- Polynômes semi-symétriques
- étude des fonctions polynomiales associées.

(A) On aurait pu rajouter le cas important de $A = \mathbb{Z}$.

(B) " " " " le degré du polynôme obtenu en remplaçant les indéterminées par les σ_k. [RDO] p202.

(C) " " " " le fait que l'algèbre des polynômes symétriques de $A[X_1, \dots, X_n]$ est engendrée par les polynômes symétriques élémentaires [TAU] p219

(D) " " " " les relations de Newton [RDO] p207

On peut faire une partie "Résultant"