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

[RDO] Ramis-Deschamps-Odoux
[Gob] Gob, Algèbre commutative
[B] Briançon
[P] Peyré, Algèbre discrète de la transformée de Fourier
[Ser1] Serre, cours d'arithmétique
[Ser2] Denis Serre, les matrices
[SP] Szpirglas, Algèbre L3.

Cadre : A un anneau commutatif unitaire, K un corps commutatif, $n\geq 2$. $i\in\mathbb{N}^n$, $i=(i_1,\dots,i_n)$, $|i|=\sum_{k=1}^{n} i_k$

[RDO]

I. Polynômes à n indéterminées, généralités

Def : • On appelle polynôme à n indéterminées sur A toute famille à support fini $P=(a_i)_{i\in\mathbb{N}^n}$ d'éléments de A. Les a_i sont les coefficients de P.
• L'ensemble des polynômes à n indéterminées à coefficients dans A est noté $A[X_1,\dots,X_n]$

① Construction de l'algèbre $A[X_1,\dots,X_n]$ et 1ères définitions

Def : Soient $P=(a_i)$, $Q=(b_i)$ dans $A[X_1,\dots,X_n]$, $\lambda\in A$.
On définit • une addition $P+Q := (a_i+b_i)_{i\in\mathbb{N}^n}$
• une multiplication $P.Q := \left(\sum_{k+l=i} a_k b_l\right)_{i\in\mathbb{N}^n}$
• multiplication par un scalaire $\lambda P := (\lambda a_i)_{i\in\mathbb{N}^n}$

Thm : Muni de ces opérations $A[X_1,\dots,X_n]$ est une A-algèbre commutative d'élément neutre pour la multiplication le polynôme $e=(a_i)$ où $a_{(0,\dots,0)}=1$ et $a_i=0$ si $i\neq(0,\dots,0)$

Def : 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. Ainsi si $P=(a_i)_{i\in\mathbb{N}^n}$ alors $P=\sum_{i\in\mathbb{N}^n} a_i X_1^{i_1}\dots X_n^{i_n}$

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-algèbres : $\varphi_{X\to b} : A[X_1,\dots,X_n]\to B$ qui envoie X_i sur b_i

Thm d'isomorphisme canonique : l'application
$$\Phi : \begin{cases} A[X_1,\dots,X_n] \longrightarrow A[X_1,\dots,X_{n-1}][X_n] \\ \sum a_i X_1^{i_1}\dots X_n^{i_n} \longmapsto \sum_{k\in\mathbb{N}}\left(\sum a_{(i_1,\dots,i_{n-1},k)} X_1^{i_1}\dots X_{n-1}^{i_{n-1}}\right)X_n^k \end{cases}$$
est un isomorphisme d'algèbre

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

Def (Degré total) Soit $P=\sum a_i X_1^{i_1}\dots X_n^{i_n}\in A[X_1,\dots,X_n]$. Si $P=0$ on pose $\deg P=-\infty$. Si $P\neq 0$, $\deg P=\max\{|i|, a_i\neq 0\}$

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 } [Gob]

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

Exemple : $P=aX^2+2bXY+a'Y^2+2cX+2c'Y+d$
$P'_X=2(aX+bY+c)$ $P'_Y=2(bX+a'Y+c')$

② Polynômes homogènes

Def Soit $k\in\mathbb{N}$, $P=(a_i)\in A[X_1,\dots,X_n]$ est dit k-homogène si l'inégalité $|i|\neq k$ implique $a_i=0$

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

Thm : le sous-ensemble A_k de $A[X_1,\dots,X_n]$ constitué par les polynômes k-homogènes en est un sous-module. $A[X_1,\dots,X_n]$ est somme directe de la famille des sous-modules $(A_k)_{k\in\mathbb{N}}$

Application : • Théorème de Molien 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 [P]
$$\sum_{k\geq 0} a_k(G)X^k=\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-gX)}$$ DVP

• 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 [B]

+ Résultant si on veut
Discriminant
DVP : • Th. de structure
• Irréd. du det
• Poly. semi-symétriques

SAVOIR décomposer un polySym en polySymElem. ⚠

3) Propriétés arithmétiques

→ liens avec A, permanence des propriétés

Prop : • A intègre $\Rightarrow A[X_1, \dots, X_n]$ intègre
• A noethérien $\Rightarrow A[X_1, \dots, X_n]$ noethérien
• A factoriel $\Rightarrow A[X_1, \dots, X_n]$ factoriel

Prop : $K[X_1, \dots, X_n]$ est factoriel

Prop : $n \geq 2$, $K[X_1, \dots, X_n]$ n'est pas principal

Conséquences → existence d'une décomposition unique en produits d'irréductibles non associés
→ existence de PGCD et PPCM d'une famille de polynômes
→ le thm de Gauss subsiste mais le thm de Bézout est faux !

→ Divisibilité

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

Cor : $P \in K[X_1, \dots, X_n]$ est divisible par $\prod_{i<j} (X_j - X_i)$
ssi P est divisible par $X_j - X_i$ $\forall j > i$

[God] II - Fonctions polynômes, zéros de polynômes

1) Fonctions polynômes

[RDO] **Def** : $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$. L'application $\tilde{P} : A^n \to A$, $(x_1, \dots, x_n) \mapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \dots x_n^{i_n}$ est appelée fonction polynôme associée au polynôme P. On a ainsi défini un morphisme de A-algèbres $A[X_1, \dots, X_n] \longrightarrow \mathcal{F}(A^n, A)$

Prop Soient K un corps infini, $S_1, \dots, S_n$ des parties infinies de K, $P \in K[X_1, \dots, X_n] \setminus \{0\}$
et S_P l'ensemble des $x \in S_1 \times \dots \times S_n$ vérifiant $P(x) \neq 0$. Alors S_P est un ensemble infini

Application : 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

2) Prolongements d'identités

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

Ces importants : $A = \mathbb{Z}$, tout anneau peut être regardé de manière unique comme une $\mathbb{Z}$-algèbre les identités dans $\mathbb{Z}[X_1, \dots, X_n]$ sont donc universelles
exemple : l'identité de Newton dans $\mathbb{Z}[X, Y]$
$(X+Y)^p = \sum_{k=0}^{p} \binom{p}{k} X^k Y^{p-k}$ donne dans $\mathbb{F}_p[X, Y]$
$(X+Y)^p = X^p + Y^p$

Prop (Prolongement des identités) Soit K un corps infini, $P_1, \dots, P_m \in K[X_1, \dots, X_n] \setminus \{0\}$. Soit $V(P_j)$ l'ensemble des $x \in K^n$ tels que $P_j(x_1, \dots, x_n) = 0$.
Si F et $F' \in K[X_1, \dots, X_n]$ tels que $\forall x \in K^n \setminus \bigcup V(P_j)$
$F(x) = F'(x)$ alors $F = F'$.

Application : Soient $A, B \in \mathcal{M}_n(K)$ alors $\chi_{AB} = \chi_{BA}$

3) Théorème de Chevalley-Warning

Thm Soit K un corps de caractéristique p et de cardinal q, $P_1, \dots, P_r \in K[X_1, \dots, X_n]$ et $V = \{x \in K^n, \forall i, P_i(x) = 0\}$
Si $\sum_{i=1}^{r} \deg P_i < n$ alors $\# V \equiv 0 [p]$ [SER1] DVP

3

[Sp3] [RDO]

Cor : $(P_1,\dots,P_r) \in K[X_1,\dots,X_n]$ si $\sum \deg P_i < n$ et P_i sans termes constants alors ils ont un zéro non trivial commun.

Cor : Toute forme quadratique d'au moins 3 variables sur $\mathbb{F}_q$ a un zéro non trivial.

III Polynômes symétriques, relations coefficients-racines

1) Relations coefficients-racines

Def : On définit pour $k \in [\![1,n]\!]$ le kième polynôme symétrique élémentaire $\sigma_k \in K[X_1,\dots,X_n]$

$$\sigma_k(X_1,\dots,X_n) = \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$$

Prop : Soit $P \in K[X]$, $P(X) = a_0 + \dots + a_n X^n$, $a_n \neq 0$. Si P est scindé dans $K[X]$, c'est-à-dire s'il existe $\alpha_1,\dots,\alpha_n \in K$ tels que $P(X) = a_n \prod (X - \alpha_j)$ on a alors les relations

$$\frac{a_{n-1}}{a_n} = -\sigma_1(\alpha_1,\dots,\alpha_n), \quad \frac{a_{n-k}}{a_n} = (-1)^k \sigma_k(\alpha_1,\dots,\alpha_n), \quad \frac{a_0}{a_n} = (-1)^n \sigma_n(\alpha_1,\dots,\alpha_n)$$

2) Polynômes symétriques

→ action S_n sur $A[X_1,\dots,X_n]$

Def : $\sigma \in S_n$, $P \in A[X_1,\dots,X_n]$, on définit $\sigma(P)$ par $\sigma(P)(X_1,\dots,X_n) = P(X_{\sigma(1)},\dots,X_{\sigma(n)})$

Prop : σ, $P \mapsto \sigma(P)$ est un automorphisme d'algèbre de $A[X_1,\dots,X_n]$ dans lui-même

Def : $P \in A[X_1,\dots,X_n]$ est symétrique si $\forall \sigma \in S_n$, $\sigma(P) = P$

Exemples : · 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 : $S_k = \sum_{p=1}^{n} X_p^k$

→ théorème de structure

Def : Soit $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1,\dots,X_n]$. On définit le poids de P $\pi(P) = \begin{cases} -\infty & \text{si } P = 0 \\ \max\{\sum_{k=1}^{n} k \cdot i_k / a_i \neq 0\} & \text{si } P \neq 0 \end{cases}$

en particulier $P \in A[X_1,\dots,X_n]^{S_n}$. Alors $\deg_{X_r}(P) = \deg_{X_s}(P)$ $\forall r,s$

Def : $P \in A[X_1,\dots,X_n]^{S_n}$ l'ordre de P est $w(P) := \deg_{X_q}(P)$ $\forall q$

Thm : $P \in A[X_1,\dots,X_n]^{S_n}$ tel que $\deg(P) = p$ et $w(P) = w$. Alors $\exists!\, Q \in A[X_1,\dots,X_n]$ 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.

[GOU]

Application : π est transcendant.

→ Sommes de Newton

Thm (Relations de Newton) les polynômes symétriques élémentaires S_k vérifient

(i) Pour $k \geq n$
$$S_k - \sigma_1 S_{k-1} + \dots + (-1)^p \sigma_p S_{k-p} + \dots + (-1)^n \sigma_n S_{k-n} = 0$$

(ii) Pour $1 \leq k \leq n$
$$S_k - \sigma_1 S_{k-1} + \dots + (-1)^p \sigma_p S_{k-p} + \dots + (-1)^{k-1} \sigma_{k-1} S_1 + (-1)^k k S_k = 0$$

En général, les $S_1,\dots,S_k$ ne sont pas algébriquement indépendants

Corollaire : Si car $K = 0$, $(S_i)_{1 \le i \le n}$ est algébriquement libre sur K et engendre $K[X_1,\dots,X_n]^{S_n}$

[Ser]

Application : Méthode de Leverrier par le calcul du polynôme caractéristique d'une matrice M.

Pour calculer le polynôme caractéristique on doit calculer les σ_k qui s'expriment en fonction des S_k et les S_k sont connus puisque ce sont les traces des matrices M^k

3) Action de A_n, polynômes semi-symétriques

[Gob]

Def : $P \in A[X_1,\dots,X_n]$ est semi-symétrique si $\forall \sigma \in A_n$ $\sigma . P = P$

Def/Prop : On définit $D(X_1,\dots,X_n) = \prod_{i<j} (X_j - X_i)$

D est un polynôme semi-symétrique

Prop : Soit K un corps de caractéristique distincte de 2. Pour qu'un polynôme $P \in K[X_1,\dots,X_n]$ soit semi-symétrique il faut et il suffit qu'il existe Q_1, Q_2 symétriques nécessairement uniques tels que

$$P(X_1,\dots,X_n) = Q_1(X_1,\dots,X_n) + D(X_1,\dots,X_n)\, Q_2(X_1,\dots,X_n)$$