142

Algèbre de polynômes à plusieurs indéterminées, exemples et applications.

Cadre : Tous les anneaux considérés sont commutatifs et unitaires.

I) Algèbre des polynômes à n indéterminées

I.1) Construction de $A[X_1,\dots,X_n]$

<u>Def 1</u> : Soit A un anneau. Soit $n\geq 1$. On définit <u>$A[X_1,\dots,X_n]$</u> l'ensemble des suites indexées par $\mathbb{N}^n$, à support fini, et à coefficients dans A.

<u>Prop 2</u> : $A[X_1,\dots,X_n]$ muni de $a\cdot(a_{i_1\dots i_n})_{(i_1,\dots,i_n)} := (a\,a_{i_1\dots i_n})_{(i_1,\dots,i_n)}$;
$(a_{i_1\dots i_n})_{(i_1\dots i_n)} + (b_{i_1\dots i_n})_{i_1\dots i_n} := (a_{i_1\dots i_n}+b_{i_1\dots i_n})_{(i_1\dots i_n)}$; $(a_{i_1\dots i_n})_{(i_1\dots i_n)} \times (b_{i_1\dots i_n})_{(i_1\dots i_n)} := (c_{j_1\dots j_n})_{(j_1\dots j_n)}$
avec $c_{j_1\dots j_n} := \sum\limits_{(i_1,\dots,i_n)+(k_1,\dots,k_n)=(j_1,\dots,j_n)} a_{i_1\dots i_n}\, b_{k_1\dots k_n}$ est une A-algèbre commutative unitaire.
Un élément $P\in A[X_1,\dots,X_n]$ est appelé <u>polynôme à n indéterminées</u>.

<u>Notation 3</u> : $\forall 1\leq j\leq n$, on note $\underline{X_j} := \big(\delta_{(i_1,\dots,i_n)}^{(0,\dots,0,1,0,\dots,0)}\big)_{(i_1,\dots,i_n)}$ (1 en j ème coordonnée) la j-ème indéterminée de $A[X_1,\dots,X_n]$.
Pour $P\in A[X_1,\dots,X_n]$, $P = \sum\limits_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1\dots i_n} X_1^{i_1}\dots X_n^{i_n}$.

<u>Théorème 4</u> : $A[X_1,\dots,X_{n-1}][X_n] \underset{A\text{-algèbres}}{\overset{\text{isom}}{\simeq}} A[X_1,\dots,X_n]$

I.2) Théorèmes de transfert

<u>Prop 5</u> : Si A est intègre, alors $A[X]$ est intègre.

<u>Prop 6</u> : Si A est intègre, alors $A[X]^\times = A^\times$.

<u>Ex 7</u> : $\mathbb{Z}[X_1,\dots,X_n]$ est intègre, et $\mathbb{Z}[X_1,\dots,X_n]^\times = \{\pm 1\}$.

<u>Prop 8</u> : A est un corps $\iff$ $A[X]$ est principal.

<u>Cor 9</u> : $A[X_1,\dots,X_n]$ n'est jamais principal $\forall n\geq 2$.

<u>Contre-ex 10</u> : $(2;X)$ n'est pas principal dans $\mathbb{Z}[X]$.

<u>Théorème 11</u> : Si A est factoriel, alors $A[X]$ est factoriel.

<u>Conséquences 12</u> : On a l'existence du PGCD, PPCM de deux polynômes. Pour P,Q, P unitaire, on a une division euclidienne de Q par P. Les théorèmes de Gauss sur les facteurs irréductibles sont vrais, mais pas le théorème de Bézout.

<u>Ex 13</u> : $\mathbb{R}[X_1,\dots,X_n]$ est factoriel, $\mathbb{Q}[\sqrt{5}][X,Y]$ est factoriel, mais pas $\mathbb{Z}[\sqrt{5}][X,Y]$.

<u>Théorème 14</u> : Si A est noethérien, alors $A[X]$ est noethérien.

I.2) Degrés, polynômes homogènes

<u>Def 15</u> : Le degré total de P est $\deg_{tot}(P) := \{i_1+\dots+i_n,$ avec $a_{i_1\dots i_n}\neq 0\}$.
$\forall 1\leq j\leq n$, le <u>j-ème degré partiel</u> de P, $\deg_j(P)$, est le degré de P vu dans $A[X_1,\dots,X_{j-1},X_{j+1},\dots,X_n][X_j]$.

<u>Prop 16</u> : $\deg_j(P)\leq \deg_{tot}(P)$, $\forall 1\leq j\leq n$.
Si A est intègre, $\deg_{tot}(PQ) = \deg_{tot}(P)+\deg_{tot}(Q)$; $\deg_j(PQ) = \deg_j(P)+\deg_j(Q)$
$\deg_{tot}(P+Q)\leq \max\{\deg_{tot}(P);\deg_{tot}(Q)\}$; $\deg_j(P+Q)\leq\max\{\deg_j(P);\deg_j(Q)\}$.

<u>Ex 17</u> : $\deg_{tot}(X^2Y)=3$.

<u>Def 18</u> : Soit $k\geq 0$. Un polynôme P est dit <u>k-homogène</u> ssi chaque monôme de P est de degré total k.
On note H_k l'ensemble des polynômes k-homogènes de $A[X_1,\dots,X_n]$.

<u>Rem 19</u> : $0\in H_k$, $\forall k\geq 0$, et pour $P,Q\in H_k$, $P+Q\in H_k$. Donc H_k est un groupe additif.
Pour $P\in H_k$, $Q\in H_l$, $PQ\in H_{k+l}$.

<u>Def 20</u> : Soit $1\leq j\leq n$. Le j-ème polynôme dérivé partiel de P, $\frac{\partial P}{\partial X_j}$ vaut :
$\frac{\partial P}{\partial X_j} := \sum\limits_{\substack{(i_1,\dots,i_n)\in\mathbb{N}^n\\ i_j\geq 1}} i_j\, a_{i_1\dots i_n} X_1^{i_1}\dots X_j^{i_j-1}\dots X_n^{i_n}$.

<u>Théorème 21</u> : (d'Euler) Soit A de caractéristique nulle.
Alors $P\in H_k \iff \sum\limits_{i=1}^{n} X_i\frac{\partial P}{\partial X_i} = kP$.

II) Fonctions polynôme

II.1) Morphismes d'évaluation

<u>Def 22</u> : Soit B une A-algèbre. On définit $ev : \begin{array}{l} A[X_1,\dots,X_n]\to \mathrm{Fonct}(B^n;B) \\ P\mapsto \left(\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\mapsto P(x_1,\dots,x_n)\right)\end{array}$ <u>le morphisme d'évaluation</u>.

<u>Prop 23</u> : ev est un morphisme de A-algèbres.

<u>Prop 24</u> : Si A est intègre infini, ev est injectif.

<u>Contre-ex 25</u> : Si $A=B=\mathbb{F}_q$, $ev(X_1^q-X_1)$ est la fonction nulle.

<u>Prop 26</u> : Si A est intègre infini, $\{x\in A^n \text{ tq } P(x)\neq 0\}$ est infini.

<u>Théorème 27</u> : (Prolongement des identités) Soit A intègre infini. Soit $P\in A[X_1,\dots,X_n]$ et $V=\{x\in A^n \text{ tq } P(x)=0\}$. Soient F_1,F_2 tq $ev(F_1)=ev(F_2)$ sur $A^n\setminus V$. Alors $F_1=F_2$.

<u>Corollaire 28</u> : Soit A intègre. $\forall M,N\in M_n(A)$, $\chi_{MN}=\chi_{NM}$.

<u>Prop 29</u> : Soit A intègre, $P\in A[X]$, $a\in A$.
Alors $P(a)=0 \iff (X-a)\mid P(X)$.

Application 30 : Soit A intègre.

$X_n - Q(X_1;\dots;X_{n-1}) \mid P(X_1;\dots;X_n) \iff P(X_1;\dots;X_{n-1};Q(X_1;\dots;X_{n-1})) = 0$ dans $A[X_1;\dots;X_{n-1}]$.

Application 31 :

Soit $V_n := \begin{vmatrix} 1 & \dots & 1 \\ X_1 & \dots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \dots & X_n^{n-1} \end{vmatrix} \in \mathbb{Z}[X_1;\dots;X_n]$. Alors $V_n = \prod_{i<j}(X_i - X_j)$.

Application 32 : Soit A intègre.

$P = \begin{vmatrix} X_{11} & \dots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \dots & X_{nn} \end{vmatrix}$ est irréductible dans $A[X_{11};\dots;X_{nn}]$.

Théorème 33 : Soit A intègre. Soit $M \in M_n(A)$. Alors $\chi_M(M) = 0$.

I. 2) Fonction polynômes sur des corps finis

Soit $q = p^\alpha$, $\alpha \in \mathbb{N}^*$, p premier. Soit $\mathbb{F}_q$ le corps à q éléments.

Théorème 34 : $\dfrac{\mathbb{F}_q[X_1;\dots;X_n]}{\langle X_1^q - X_1;\dots;X_n^q - X_n\rangle} \underset{\mathbb{F}_q\text{-algèbres}}{\overset{\text{isom}}{\simeq}} \mathrm{Fonct}(\mathbb{F}_q^n;\mathbb{F}_q)$

$\boxed{\text{Développement 1}}$ Théorème de Chevalley-Warning.

Soient $P_1;\dots;P_r \in \mathbb{F}_q[X_1;\dots;X_n]$ tq $\sum_{i=1}^{r} \deg_{tot}(P_i) < n$.

Alors $\#(\{x \in \mathbb{F}_q^n \text{ tq } P_1(x) = \dots = P_r(x) = 0\}) \equiv 0 \mod (p)$.

Corollaire 35 :

Si $P_1;\dots;P_r$ sont annulés par $(0;\dots;0)$, ils ont au moins une racine commune non-triviale dans $\mathbb{F}_q^n$.

Corollaire 36 :

Toute forme quadratique à au moins 3 variables sur $\mathbb{F}_q$ admet un zéro non-trivial.

I. 3) Classification des quadriques sur $\mathbb{R}$

Def 37 : Soit $P \in \mathbb{R}[X_1;X_2;X_3]$, $P(X_1;X_2;X_3) = aX_1^2 + a'X_2^2 + a''X_3^2 + 2bX_1X_2 + 2b'X_1X_3 + 2b''X_2X_3 + cX_1 + c'X_2 + c''X_3 + d$, avec $\deg_{tot}(P) = 2$.

La <u>quadrique Q</u> associée à P est : $Q := \{(x,y,z) \in \mathbb{R}^3 \text{ tq } P(x,y,z) = 0\}$.

On définit $M_Q := \begin{pmatrix} a & b & b' \\ b & a' & b'' \\ b' & b'' & a'' \end{pmatrix}$ la partie quadratique de P, $L := \begin{pmatrix} c \\ c' \\ c'' \end{pmatrix}$ la partie linéaire de P,

$C := (d)$ la partie constante de P. On a $M_Q \neq 0$.

M_Q est symétrique réelle, donc diagonalisable dans $M_3(\mathbb{R})$. Soient $\lambda_1;\lambda_2;\lambda_3$ ses valeurs propres.

Théorème 38 : (classification des quadriques réelles)

Soit p le nombre de vp > 0 de M_Q. Soit q le nb de vp < 0 de M_Q.

Le couple $(p;q)$, appelé signature de M_Q, permet de classifier les différentes quadriques.

$(p;q)$	Quadrique non dégénérée	Quadrique dégénérée
$(3;0)$ ou $(0;3)$	ellipsoïde	$\emptyset$ ou point
$(2;1)$ ou $(1;2)$	hyperboloïde à 1 ou 2 nappes	cône
$(2;0)$ ou $(0;2)$	paraboloïde elliptique ou cylindre elliptique	$\emptyset$ ou droite
$(1;1)$	paraboloïde hyperbolique ou cylindre hyperbolique	réunion de deux plans
$(1;0)$ ou $(0;1)$	cylindre parabolique	$\emptyset$ ou plan ou réunion de 2 plans

Ex 39 : Ellipsoïde : $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 1$; Hyperboloïde à 2 nappes : $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = -1$.

Cylindre parabolique : $x^2 = 2py$.

II) Polynômes symétriques, relations coefficients-racines

II. 1) Polynômes symétriques

Def 40 : $\mathfrak{S}_n$ agit sur $A[X_1;\dots;X_n]$ par : $\sigma \cdot P(X_1;\dots;X_n) := P(X_{\sigma(1)};\dots;X_{\sigma(n)})$.

On définit alors <u>$A[X_1;\dots;X_n]^{\mathfrak{S}_n}$</u> $:= \{P \text{ tq } \sigma \cdot P = P, \forall \sigma \in \mathfrak{S}_n\}$, l'ensemble des polynômes symétriques de $A[X_1;\dots;X_n]$.

Prop 41 : $A[X_1;\dots;X_n]^{\mathfrak{S}_n}$ est une sous-A-algèbre de $A[X_1;\dots;X_n]$.

Def 42 : $\forall 1 \leq j \leq n$, on définit $\Sigma_j := \sum_{1 \leq i_1 < \dots < i_j \leq n} X_{i_1} \dots X_{i_j}$ le j-ème polynôme symétrique élémentaire.

Prop 43 : $\forall 1 \leq j \leq n$, $\Sigma_j \in A[X_1;\dots;X_n]^{\mathfrak{S}_n}$.

Ex 44 : $\Sigma_1 = X_1 + \dots + X_n$; $\Sigma_n = X_1 \dots X_n$; $\Sigma_2 = X_1X_2 + \dots + X_1X_n + X_2X_3 + \dots + X_2X_n + \dots + X_{n-1}X_n$

Théorème 45 : (Théorème de structure)

$\phi : \begin{array}{l} A[X_1;\dots;X_n] \to A[X_1;\dots;X_n]^{\mathfrak{S}_n} \\ P(X_1;\dots;X_n) \mapsto P(\Sigma_1;\dots;\Sigma_n) \end{array}$ est un isomorphisme de A-algèbres. $\forall P$ symétrique, $\exists! Q \in A[X_1;\dots;X_n]$ tq $P(X_1;\dots;X_n) = Q(\Sigma_1;\dots;\Sigma_n)$.

Ex 46 : $\forall k \geq 0$, $S_k := X_1^k + \dots + X_n^k \in A[X_1;\dots;X_n]^{\mathfrak{S}_n}$.

Prop 47 : Soit $P(T) := \prod_{i=1}^{n} (T - X_i) \in A[X_1, \dots, X_n][T]$.

Alors $P(T) = \sum_{i=1}^{n} T^i \times (-1)^{n-i} \Sigma_{n-i} \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}[T]$, et $\operatorname{disc}(P) := \prod_{i<j} (X_i - X_j) \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$

Prop 48 (Formules de Newton) :

$\forall k \geq n, \quad S_k - \Sigma_1 S_{k-1} + \dots + (-1)^n \Sigma_n S_{k-n} = 0.$

$\forall 1 \leq k \leq n, \quad S_k - \Sigma_1 S_{k-1} + \dots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k \Sigma_k \times k = 0.$

Appli 49.

Si $\operatorname{car}(A) = 0$, $\{S_1, \dots, S_n\}$ est une base algébrique de l'algèbre $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$

Appli 50 :

Soit A intègre. Soit $M \in M_n(A)$ tq $\operatorname{Tr}(M^k) = 0 \ \forall 1 \leq k \leq n$. Alors M est nilpotente.

Appli 51 :

Soit A intègre. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$. Soit K le corps des fraction de A.
Soit $\overline{K}$ une clôture algébrique de K. On a $P(X) = a_n \prod_{i=1}^{n} (X - \lambda_i)$ dans $\overline{K}[X]$.
Alors, $\forall k \geq 0$, $\lambda_1^k + \dots + \lambda_n^k \in A$ et sont calculables à partir des a_i sans avoir à déterminer les λ_i.

Ex 52 : $P(X) = X^5 - 5X - 5$. On a $a_0 = a_1 = -5$, $a_2 = a_3 = a_4 = 0$, $a_5 = 1$.
P est irréductible sur $\mathbb{Q}$. Ses racines ne sont pas radicales sur $\mathbb{Q}$ (admis)
Pourtant, $S_0 = 5$, $S_1 = S_2 = S_3 = 0$, $S_4 = 20$, $S_5 = 25$, $S_6 = 0$, $S_7 = 0$, $S_8 = 100, \dots$

$\forall k \geq 5, \ S_k = -5 S_{k-4} - 5 S_{k-5} \in \mathbb{Z}.$

$\boxed{\text{Développement 2}}$: Caractérisation des polynômes alternés

Soit A intègre. On définit $A[X_1, \dots, X_n]^{\mathfrak{A}_n} := \{P \text{ tq } \sigma P = P, \forall \sigma \in \mathfrak{A}_n\}$, l'ensemble des polynômes alternés. Soit $V_n := \prod_{i<j} (X_i - X_j)$, $\Theta_n := \prod_{i<j} (X_i + X_j)$, $W_n := \frac{1}{2}(V_n + \Theta_n)$.
Alors $W_n \in A[X_1, \dots, X_n]$, et $A[X_1, \dots, X_n]^{\mathfrak{A}_n} = A[X_1, \dots, X_n]^{\mathfrak{S}_n} \oplus W_n . A[X_1, \dots, X_n]^{\mathfrak{S}_n}$.

On a : $\dfrac{A[X_1, \dots, X_n]^{\mathfrak{S}_n}[T]}{\langle T^2 - \Theta_n T + W_n^2 \rangle} \underset{A[X_1, \dots, X_n]^{\mathfrak{S}_n}\text{-algèbres}}{\overset{\text{isom}}{\simeq}} A[X_1, \dots, X_n]^{\mathfrak{A}_n}$

Auteurs : AGNIEL Vidal
BERAUD Vivien

Références :

Ramis, Deschamps, Odoux ; Cours de mathématiques spéciales I, p185-209.

Goblot, Algèbre commutative, p174-213

Szpirglas, Algèbre commutative, p604-605 [Dvpt 2]

Mérindol, Nombres et algèbre.

Serre, Cours d'Arithmétique [Dvpt 1].

Rennes, 2016