A anneau commutatif unitaire. $\mathbb{K}$ est un corps. $n \geq 2$

I - Généralités [1]

1 - L'algèbre $A[X_1, ..., X_n]$

Déf 1. Un élément de $\mathbb{N}^n$ sera noté $i = (i_1, ..., i_n)$ et on désignera par $|i|$ l'entier naturel $i_1 + ... + i_n$ qui est appelé **longueur** du n-uplet i.

Déf 2. On appelle **polynôme à n indéterminées sur A** toute famille $(a_i)_{i\in\mathbb{N}^n}$ presque nulle d'éléments de A où on appelle **indéterminées** les polynômes $X_q = (b_{q,j})_{j\in\mathbb{N}^n}$, $1 \leq q \leq n$ définis par :

$$\begin{cases} b_{q,j} = 1 \text{ si } j = (j_1, ..., j_n) \text{ vérifie } j_q = 1 \text{ et } j_k = 0 \text{ si } k \neq q \\ b_{q,j} = 0 \text{ sinon.} \end{cases}$$

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

Déf 3. Soit $P = (a_i)_{i\in\mathbb{N}^n}, Q = (b_i)_{i\in\mathbb{N}^n} \in A[X_1, ..., X_n]$. Soit $\lambda \in A$. Alors, on définit :

$$P + Q = (a_i + b_i)_{i\in\mathbb{N}^n} \quad P \times Q = (\sum_{k+l=i} a_k b_l)_{i\in\mathbb{N}^n} \quad \lambda.P = (\lambda a_i)_{i\in\mathbb{N}^n}.$$

Muni de ces lois, $A[X_1, ..., X_n]$ est une A-algèbre commutative.

NB 4. L'élément neutre pour la multiplication est $(a_i)_{i\in\mathbb{N}^n}$ avec $a_{(0,...0)} = 1$ et pour tout $i \neq (0, ...0), a_i = 0$.

Théo 5. *Tout polynôme de $A[X_1, ..., X_n]$ s'écrit de façon unique comme combinaison linéaire de la famille $(X_1^{i_1} \times ... \times X_n^{i_n})_{(i_1,...,i_n)\in\mathbb{N}^n}$. Les coefficients de cette combinaison linéaire sont les coefficients du polynôme.*

Prop 6. *Soit B une A-algèbre et $(b_1, ..., b_n) \in B^n$. Alors il existe un unique morphisme de A-algèbre*

$$\begin{array}{rcl} A[X_1, ..., X_n] & \longrightarrow & B \\ X_i & \longmapsto & b_i \end{array}$$

Prop 7. *$A[X_1, ..., X_n]$ est isomorphe à $A[X_1, ..., X_{n-1}][X_n]$.*

2 - Degrés d'un polynôme à n indéterminées et polynôme homogène

Déf 8. Soit $1 \leq q \leq n$, on appelle **degré partiel du polynôme P de $A[X_1, ..., X_n]$, relativement à l'indéterminée** X_q le degré de ce polynôme considéré comme un élément de $A[X_1, ..., X_{q-1}, X_{q+1}, ..., X_n][X_q]$. On le note $\deg_{X_q}(P)$.

Ex 9. Soit $P(X, Y) = 3X^2Y^3 + 4XY^2 + 2XY + 4$.
On a $\deg_X(P) = 2$ et $\deg_Y(P) = 3$.

Déf 10. Soit $P = (a_i)_{i\in\mathbb{N}^n} \in A[X_1, ..., X_n]$.
Si P n'est pas nul l'ensemble

$$\{k \in \mathbb{N} : \exists i \in \mathbb{N}^n (a_i \neq 0) \text{ et } (|i| = k)\}$$

des longueurs des éléments du support de P, admet un plus grand élément, qui est dit **degré total de** P et noté $\deg(P)$.
Si P est nul, on a la convention $\deg(P) = -\infty$.

Ex 11. Soit P le polynôme de l'exemple 9.
Alors, on a $\deg(P) = 5$.

Prop 12. *Pour tout $P, Q \in A[X_1, ..., X_n]$, on a*

$$\deg(P + Q) \leq \sup(\deg(P), \deg(Q))$$
$$\deg(P \times Q) \leq \deg(P) + \deg(Q)$$

Déf 13. Soit $p \in \mathbb{N}$. Un polynôme $P = (a_i)_{i\in\mathbb{N}^n} \in A[X_1, ..., X_n]$ est dit **p-homogène** si et seulement si l'inégalité $|i| \neq p$ implique $a_i = 0$.

Ex 14. Le polynôme $Q(X, Y) = X^5 + Y^4X + 3Y^2X^3 + 2X^4Y$ est un polynôme 5-homogène.

NB 15. (i) Pour un polynôme p-homogène non nul, p n'est autre que le degré total.

(ii) Pour tout $p \in \mathbb{N}$, le polynôme nul, dont le degré total est $-\infty$, est p-homogène.

Prop 16. *Si deux polynômes de $A[X_1, ..., X_n]$ sont respectivement p-homogène et q-homogène, leur produit est $p+q$-homogène.*

Prop 17. *Soit $P \in A[X_1, ..., X_n]$ un polynôme q-homogène, alors on a*

$$\sum_{i=1}^{n} X_i \frac{\partial P}{\partial X_i} = qP.$$

3 - Propriétés arithmétiques de $A[X_1, ..., X_n]$

NB 18. On a

$$A[X_1, ..., X_n]^* = A^*.$$

Prop 19. *Si A est intègre alors $A[X_1, ..., X_n]$ est intègre.*

Théo 20. *Soit $A, B \in A[X_1, ..., X_n]$ tels que B soit non nul et tel que son coefficient dominant relativement à l'indéterminée X_n soit un élément inversible de $A[X_1, ..., X_{n-1}]$ alors il existe un couple unique (Q, R) de polynômes de $A[X_1, ..., X_n]$ tels que*

$$A = BQ + R \text{ et } \deg_{X_n}(R) < \deg_{X_n}(B).$$

Prop 21. *Soit $P \in A[X_1, ..., X_n]$ et $Q \in A[X_1, ..., X_{n-1}]$. Alors, on a*

$$X_n - Q | P \text{ si et seulement si } P(X_1, ..., X_{n-1}, Q) = 0.$$

Prop 22. *L'anneau $\mathbb{K}[X_1, ..., X_n]$ n'est pas principal alors que $\mathbb{K}[X]$ l'est.*

Théo 23. *Si A est un anneau factoriel, l'anneau $A[X_1, ..., X_n]$ est factoriel.*

Théo 24 (Hilbert Nullstellensatz)**.** *Si $\mathcal{I}$ est un idéal maximal de $\mathbb{K}[X_1, ..., X_n]$, le quotient $\mathbb{K}[X_1, ..., X_n]/\mathcal{I}$ est une extension finie de $\mathbb{K}$.*

II - Fonction polynôme

1 - Définition et prolongement des identités [1]

Déf 25. Soit $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} ... X_n^{i_n} \in A[X_1, ..., X_n]$, $(i = (i_1, ..., i_n))$. L'application $\tilde{P} : A^n \longrightarrow A$ définie par :

$$x_1, ..., x_n \longmapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} ... x_n^{i_n}$$

est appelée **fonction polynôme de n variables associées au polynôme P**.

Théo 26. *Si A est un anneau intègre infini, l'application qui à $P \in A[X_1, ..., X_n]$ associe la fonction polynôme $\tilde{P}$ est un isomorphisme de $A[X_1, ..., X_n]$ sur l'algèbre des fonctions polynômes de n variables sur A.*

NB 27. On pourra donc identifier P à $\tilde{P}$.

Déf 28. Une **identité** entre m polynômes $F_1, ..., F_m$ de $A[X_1, ..., X_n]$ est une égalité de la forme $G(F_1(X_1, ..., X_n), ..., F_m(X_1, ..., X_n)) = 0$ où $G(Y_1, ..., Y_m)$ est dans $A[Y_1, ..., Y_m]$.

Théo 29. *Si, pour tout $i \in [1, n], E_i$ est une partie infinie de l'anneau intègre A et si $P(x_1, ..., x_n) = 0$, pour tout $(x_1, ..., x_n) \in E_1 \times ... \times E_n$, alors $P = 0$.*

Prop 30 (Prolongement des identités)**.** *Soit A un anneau intègre, de cardinal infini. Soit $P_1, ..., P_m$ de $A[X_1, ..., X_n]$. On note*

$$V(P_j) = \{(x_1, ..., x_n) \in A^n : P_j(x_1, ..., x_n) = 0\}.$$

Soit $Q, R \in A[X_1, ..., X_n]$ avec $Q(x) = R(x)$ pour tout $x \in A^n \backslash (\bigcup_{j=1}^{m} V(P_j))$ alors $Q = R$.

2 - Corps fini [2]

Soit q une puissance d'un nombre premier p.

Théo 31 (Chevalley-Warning)**.** *[Développement 1] Soit $(f_i)_{i\in[\![1,r]\!]}$ une famille de polynômes non nuls de $\mathbb{F}_q[X_1,...,X_n]$. On suppose que les degrés de ces polynômes vérifient l'inégalité $\sum_{i=1}^r \deg(f_i) < n$. On pose*

$$V = \{x \in \mathbb{F}_q^n : \forall i \in [\![1,r]\!], f_i(x) = 0\} \subset \mathbb{F}_q^n.$$

Alors, on a $Card(V) \equiv 0[p]$.

Théo 32 (Erdös-Ginzburg-Ziv)**.** *Soit $n \in \mathbb{N}^*$ et $a_1,...,a_{2n-1}$ des entiers. Alors, il existe $i_1,...,i_n \in \{1,...,2n-1\}$ tels que*

$$a_{i_1} + ... + a_{i_n} \equiv 0[n].$$

III - Polynômes symétriques [1]

1 - Définitions

Déf 33. On dit que P est un **polynôme symétrique** si pour tout $\sigma \in \mathfrak{S}_n$, on a $P(X_{\sigma(1)},...,X_{\sigma(n)}) = P(X_1,...,X_n)$.

Déf 34. Dans $A[X_1,...,X_n]$, les n polynômes Σ_p, $(1 \leq p \leq n)$ définis par :

$$\Sigma_p = \sum_{1\leq i_1<...<i_p\leq n} X_{i_1}...X_{i_p}$$

sont symétriques et portent le nom de **polynômes symétriques élémentaires**.

NB 35.
- On a $\Sigma_1 = X_1 + ... + X_n,\ \Sigma_n = X_1...X_n$ et que Σ_p est la somme de $\binom{n}{p}$ monômes.
- Σ_p est p-homogène et le degré partiel de Σ_p par rapport à chaque indéterminée est 1.

2 - Théorème de structure

Théo 36 (Développement 2)**.** *Soit $P \in A[X_1,...,X_n]$ symétrique. Alors il existe un unique polynôme $Q \in A[Y_1,...,Y_n]$ tel que $P(X_1,...,X_n) = Q(\Sigma_1,...,\Sigma_n)$.*

Ex 37. Soit $P = X^3 + Y^3 + Z^3 \in \mathbb{R}[X,Y,Z]$.
Alors $P(X,Y,Z) = Q(\Sigma_1,\Sigma_2,\Sigma_3)$ avec $Q(X,Y,Z) = X^3 - 3XY + 3Z$.

3 - Formules de Newton

Déf 38. On appelle **sommes de Newton** les polynômes

$$S_p = \sum_{i=1}^n X_i^p \in A[X_1,...,X_n].$$

NB 39. Les sommes de Newton sont des polynômes symétriques. On peut leur appliquer le théorème de structure. Les formules de Newton ci-dessous nous donne une expression du Q du théorème.

Prop 40 (Formules de Newton)**.**

(i) Pour $1 \leq k \leq n$,

$$S_k - \Sigma_1 S_{k-1} + ... + (-1)^p \Sigma_p S_{k-p} + ... + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k = 0$$

(ii) Pour $k \geq n$

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

App 41. Soit $\mathbb{K}$ un corps de caractéristique nulle.
Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que pour tout $k \in [\![1,n]\!], Tr(A^k) = 0$ alors A est nilpotente.

Références

[1] Edmond Ramis, Claude Deschamps, and Jacques Odoux. *Cours de mathématiques spéciales Algèbre 1.* Masson, 1990.

[2] Maxime Zavidovique. *Un max de math.* Calvage & Mounet, 2013.