7 €

117 Polynômes irréductibles à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications

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

I - Généralités

1) Définitions [G] p 77

Déf: $A[X_1]$ est un anneau commutatif unitaire: on peut donc définir l'anneau à une indéterminée à coefficients dans $A[X_1]$: c'est $A[X_1][X_2]$. On définit ainsi par récurrence $A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$ appelé anneau des polynômes à n indéterminées

Déf: Soit $P \in A[X_1, \dots, X_n]$ P s'écrit $\sum_j P_j X_i^j$ avec $i \in [\![1, n]\!]$ et $\forall j$, $P_j \in A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$, on appelle degré partiel de P selon X_i le degré de P considéré comme polynôme en X_i et on le note $\deg_{X_i}(P)$

Déf: Le degré total d'un monôme $a X_1^{i_1} \dots X_n^{i_n}$, $a \neq 0$ est $i_1 + \dots + i_n$. Si $P \in A[X_1, \dots, X_n]$ le degré total de P, noté deg(P), est le plus grand degré total des monômes qui forment P

Rmq: $A[X_1 \dots X_n]$ est un anneau commutatif unitaire. Muni de la multiplication par un scalaire $A[X_1 \dots X_n]$ est une algèbre.

2) Propriété

Soit K un corps commutatif infini et $P \in K[X_1 \dots X_n]$
Si $P(x_1, \dots, x_n) = 0$ $\forall (x_1, \dots, x_n) \in K^n$ alors $P \equiv 0$

Rmq: faux si K est un corps fini
CE: Dans $\mathbb{Z}/p\mathbb{Z}[X_1 \dots X_n]$, p premier, le polynôme $X_1(X_1 - \bar{1}) \dots (X_1 - (\bar{p-1}))X_2 \dots X_n$ est non nul et pourtant, $\forall (x_1 \dots x_n) \in \mathbb{Z}/p\mathbb{Z}$ $P(x_1 \dots x_n) = 0$

Prop: • $\deg_{X_i}(P+Q) \leq \sup[\deg_{X_i}(P), \deg_{X_i}(Q)]$ [R.D.O] p(K)
• $\deg_{X_i}(P \cdot Q) \leq \deg_{X_i}(P) + \deg_{X_i}(Q)$ avec égalité si A est intègre.

Prop: • $\deg(P+Q) \leq \sup[\deg(P), \deg(Q)]$
• $\deg(P \cdot Q) \leq \deg(P) + \deg(Q)$ avec égalité si A est intègre.

Application: Théorème de Chevalley-Warning: K un corps fini de cardinal q avec q puissance de p premier. Soit $P_\alpha \in K[X_1 \dots X_n]$ tels que $\sum \deg(P_\alpha) < n$ et soit $V = \{x \in K^n / P_\alpha(x) = 0 \ \forall \alpha\}$
alors, $\text{card}(V) \equiv 0 \pmod p$.

Propriété universelle : A, B deux anneaux. La donnée d'un morphisme $f : A[X_1 \dots X_n] \longrightarrow B$ équivaut à la donnée de sa restriction à A et des images de X_i. [P.-C.]

Application: $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ est principal [Ortiz]

3) Polynôme dérivé partiel [RDO]

Déf: $P \in A[X_1, \dots X_n]$, on appelle polynôme dérivé partiel de P par rapport à l'indéterminée X_i, $i \in [\![1,n]\!]$ et on note P'_{X_i} ou $\frac{\partial P}{\partial X_i}$ le polynôme dérivé de P considéré comme un élément de $A[X_1 \dots X_{i-1}, X_{i+1} \dots X_n][X_i]$

ex: $P = aX^2 + 2bXY + a'Y^2 + 2cX + 2c'Y + d$

$P'_X = 2(aX + bY + c)$ $\quad P'_Y = 2(bX + a'Y + c')$

Notons D_i l'application qui a tout polynôme de $A[X_1 \dots X_n]$ associe son polynôme dérivé partiel par rapport à X_i.

Th: $D_i(P.Q) = D_i(P)Q + P.D_i(Q)$

Th: $\forall p, q \in \mathbb{N}$, $D_p \circ D_q = D_q \circ D_p$

Prop: $D_1^{i_1} \circ \dots \circ D_n^{i_n}$ une dérivation partielle d'ordre $k = i_1 + \dots + i_n$ du polynôme $P \in A[X_1 \dots X_n]$ alors,

si $\deg(P) < k$, $D_1^{i_1} \circ \dots \circ D_n^{i_n}(P) = 0$

si $\deg(P) \geq k$, $\deg(D_1^{i_1} \circ \dots \circ D_n^{i_n}(P)) \leq \deg(P) - k$

4) Polynômes homogènes [R-Do]

Déf: $p \in \mathbb{N}$ $P \in A[X_1 \dots X_n]$ est p-homogène si tous ses monômes ont un degré égal à p.

Prop: si P est p-homogène et Q q-homogène, PQ est $(p+q)$ homogène.

Prop: soit P p-homogène alors, $\forall i \in [\![1,n]\!]$, si $p = 0$, $\frac{\partial(P)}{\partial X_i} = 0$ et si $p \geq 1$ $\frac{\partial(P)}{\partial X_i}$ est $(p-1)$ homogène

Th d'Euler: K un corps commutatif de caractéristique nulle $P \in K[X_1 \dots X_n]$ alors,

P p-homogène $\Leftrightarrow \sum_{i=1}^{n} X_i P'_{X_i} = pP$

II - Propriétés arithmétiques

1) Liens avec A et $A[X]$ [Pe-] [RDO]

Prop: A intègre $\Rightarrow A[X_1 \dots X_n]$ intègre

Prop: A noethérien $\Rightarrow A[X_1 \dots X_n]$ noethérien

Prop: A factoriel $\Rightarrow A[X_1 \dots X_n]$ factoriel

Th: si K est un corps commutatif, $K[X_1 \dots X_n]$ factoriel

Prop: $K[X_1 \dots X_n]$ n'est pas principal.

Conséquences: on peut décomposer un polynôme de $K[X_1 \dots X_n]$ en produit de polynômes irréductibles non associés, il y a existence du ppcm et du pgcd. Le th. de Gauss et ses conséquences restent vraies ce qui est faux pour le th. de Bezout

2) Divisibilité dans $K[X_1 \dots X_n]$ [R-Dv]

Prop: Pour que le polynôme A soit divisible par $X_n - B$ avec $B \in K[X_1 \dots X_{n-1}]$ il faut et il suffit que le polynôme obtenu en substituant, dans A, le polynôme B à l'indéterminée X_n soit le polynôme nul

ex: A quelle condition $X+Y+Z$ divise $X^3 + Y^3 + Z^3 + mXYZ$?

Prop: A divisible par $\prod_{i<j\leq n}(X_j - X_i)$ $\Leftrightarrow$ A divisible par chacun des $X_j - X_i$; $1 \leq i < j \leq n$

III - Polynômes symétriques

1) Définition

Déf: $P \in A[X_1, \dots, X_n]$ est dit **symétrique** si $\forall \sigma \in \mathfrak{S}_n$ on a $\varphi_\sigma(P) = P$ avec $\varphi_\sigma(X_i) = X_{\sigma(i)}$ $\forall i \in [\![1, n]\!]$

ex: $P(X_1, X_2, X_3) = X_1 X_2 X_3$ est symétrique

Prop: Les polynômes symétriques forment une sous-algèbre de $A[X_1, \dots, X_n]$

2) Polynômes symétriques élémentaires

Déf: $n \geq 0$ $\forall k \leq n$ le **polynôme symétrique élémentaire** de degré k de $A[X_1, \dots, X_n]$ noté Σ_k est :

$$\Sigma_k = \sum_{H \subset [\![1,n]\!] \atop |H| = k} \left(\prod_{i \in H} X_i \right)$$

Rmq: les Σ_k sont des polynômes homogènes

ex: si $n = 2$, on a $\Sigma_0 = 1$ $\Sigma_1 = X_1 + X_2$ $\Sigma_2 = X_1 X_2$

Th: soit P un polynôme symétrique de $A[X_1, \dots, X_n]$ il existe un unique polynôme T de $A[X_1, \dots, X_n]$ tel que $T(\Sigma_1, \dots, \Sigma_n) = P$.

ex: $X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = T(\Sigma_1, \Sigma_2)$ avec $T(S_1, S_2) = S_1^2 - 2S_2$.

Application: Th. de D'Alembert : $\mathbb{C}$ est algébriquement clos [Ex-p.53]

Prop: Dans $A[X_1 \dots X_n, X]$, le polynôme $P = \prod_{i=1}^{n} (X - X_i)$ a aussi pour expression $P = Y^n + \sum_{p=1}^{n} (-1)^p \Sigma_p Y^{n-p}$

3) Formules de Newton

Prop: $\forall d \geq 1$, posons $S_d = \sum_{i=1}^{n} (X_i)^d$ dans $A[X_1, \dots, X_n]$

pour $d \geq 1$, on a $S_d = \sum_{k=1}^{d-1} (-1)^{k-1} \Sigma_k S_{d-k} + (-1)^{d-1} d\Sigma_d$.

Les S_d sont appelés **sommes de Newton**

ex: si $d = 2$, $S_2 = S_1 S_1 - 2S_2$ ie $X_1^2 + X_2^2 = (X_1 + X_2)(X_1 + X_2) - 2X_1X_2$

Application: comptage de racines

IV - Résultant

Soit K un corps $\subset \mathbb{C}$ corps alg. clos.

Déf: $F, G \in K[X]$ de degrés n et m respectivement. On suppose $F(X) = a_n X^n + \dots + a_0$ et $G(X) = b_m X^m + \dots + b_0$ on appelle **résultant de F et G** le déterminant

$$Rés(F,G) = \begin{vmatrix} a_0 & & & b_0 & & \\ a_1 & a_0 & & b_1 & b_0 & \\ \vdots & \ddots & a_0 & \vdots & \ddots & b_0 \\ a_{n-1} & & a_1 & b_m & & b_1 \\ a_n & & \ddots & & b_m & \vdots \\ & a_n & & & & b_m \end{vmatrix}$$

Prop:
- $Res(F,G) = 0 \Leftrightarrow F$ et G ont une racine commune dans $\mathbb{C}$.
- $Res(F,G) = 0 \Leftrightarrow F$ et G ont un pgcd non constant au nul dans $K[X]$

Prop: $Res(F,G) \in A[a_0, \dots, a_m, b_0, \dots, b_n]$

ex: Trouver $\{(\alpha, \beta) \in \mathbb{C}^2 / P(\alpha, \beta) = Q(\alpha, \beta) = 0\}$

avec $\begin{cases} P = X^2 + 2X - XY + 2Y - 6 \\ Q = 3X^2 - 5X + 5 + XY - 2Y \end{cases}$

3) Propriétés. [A r n]

Σ_i est homogène

Si A_k est l'ensemble des poly homogènes de degré k

A_k est de dim $\binom{k+n-1}{k}$

Application : Th de Mollien

$A[X_1, \dots, X_n] \longrightarrow$ poly symé.

$P \longmapsto P(\Sigma_1, \dots, \Sigma_n)$ est bijec.

Application : $Q \in \mathbb{Z}[X]$ $t_1, \dots, t_n$ les racines de Q

$\prod_{i \neq j} (t_i - t_j) \in \mathbb{Z}[|e_1|]$