144 - Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Cadre : Tous les corps sont considérés comme commutatifs. K est un corps. A, B sont des anneaux unitaires. $n \in \mathbb{N}$.

I. Racines d'un polynôme. Multiplicité

1) Définition et caractérisation.

[Bu] ~421 **Th. ①** : On suppose A et B commutatifs. Soit $f : A \to B$ un morphisme d'anneaux, $b \in B$ et i l'inclusion naturelle de A dans $A[X]$. Alors il existe un unique morphisme d'anneaux $\varphi_{f,b} : A[X] \to B$ tel que $\varphi_{f,b}(X) = b$ et $f = \varphi_{f,b} \circ i$.

423 **Ex. ②** : Si A est un sous anneau et $b \in B$, $A[X] \longrightarrow B$, $P = \sum_{k=0}^{n} a_k X^k \longmapsto P(b) = \sum_{k=0}^{n} a_k b^k$ est un morphisme de groupes appelé évaluation en b. Si B est commutatif, c'est un morphisme d'anneaux.

Rq ③ : Si $P \in A[X]$ et $\tilde{P} : A \to A,\ a \mapsto P(a)$, alors $A[X] \longrightarrow \mathcal{F}(A,A),\ P \longmapsto \tilde{P}$ n'est pas nécessairement injective. Si $A = \mathbb{F}_2$ et $P = X^2 - X$, $\tilde{P} \equiv 0$.

♡ **Rq ④** : Si A est une K-algèbre (non nécessairement commutative), alors le Th ① appliqué à $f : K \longrightarrow A,\ \lambda \longmapsto \lambda.1_A$ et $a \in A$ reste vrai.

423 **Déf. ⑤** : Soit $P \in A[X]$ et $a \in A$. On dit que a est une racine de P si $P(a) = 0$.

424 **Prop. ⑥** : On suppose A commutatif. Soit $P \in A[X]$ et $a \in A$. Alors :
$$P(a) = 0 \iff \exists\, Q \in A[X] \ /\ P = (X-a)Q.$$

Prop. ⑦ : On suppose A commutatif. Alors tout $P \in A[X] \setminus \{0\}$ possède au plus $\deg(P)$ racines dans A SSI A est intègre.

424 **Rq ⑧** : 1) Faux si A n'est pas intègre : $\bar{2}X \in \mathbb{Z}/4\mathbb{Z}[X]$ admet deux racines

425 2) Faux si A n'est pas commutatif. Par exemple, $H = \left\{ M \in \mathcal{M}_2(\mathbb{C}) \ /\ M = \begin{pmatrix} z_1 & -\bar{z}_2 \\ z_2 & \bar{z}_1 \end{pmatrix} \right\}$ est un anneau à division intègre, et si $e = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, alors $\pm e$, $\pm j$ sont racines de $X^2 + I_2$.

On suppose dorénavant tous les anneaux commutatifs.

2) Multiplicité - Polynôme dérivé [Bu]

426 **Déf. ⑨** : Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. Le polynôme dérivé de P est $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

Prop. ⑩ : $P, Q \in A[X]$

1) P est constant $\Rightarrow P' = 0$. Si $\mathrm{car}(A) = 0$, alors P est constant $\iff P' = 0$
2) $(P+Q)' = P' + Q'$ et $(PQ)' = P'Q + PQ'$

Déf. ⑪ : Soit $P \in A[X]$ et $a \in A$. On dit que a est une racine de P d'ordre s si : $\exists\, Q \in A[X] \ /\ P = (X-a)^s Q$ et $Q(a) \neq 0$. Si $s = 1$, a est dit simple. s est alors appelée multiplicité de a.

Prop. ⑬ : On suppose $\mathrm{car}(A) = 0$. Si $a \in A$ est une racine de $P \in A[X]$ d'ordre $s \geq 1$, alors a est une racine de P' d'ordre $s-1$. 427

Prop. ⑭ : Si $\mathrm{car}(K) = 0$, alors $a \in K$ est une racine de $P \in K[X]$ d'ordre $s \geq 0$ SSI : 1) $\forall\, 1 \leq k \leq s-1$, $P^{(k)}(a) = 0$
2) $P^{(s)}(a) \neq 0$. ← mettre c.Ex. $\mathbb{F}_3[X]$

3) Polynôme scindé. Polynôme irréductible.

Déf. ⑮ : $P \in A[X]$ est dit scindé sur A si l'on peut écrire $P = \lambda (X-a_1)^{s_1} \cdots (X-a_n)^{s_n}$, $\lambda, a_1 \dots a_n \in A$ et $s_1 \dots s_n \in \mathbb{N}^*$

Déf. ⑯ : Si A est intègre, $P \in A[X]$ est dit irréductible sur A si : $P \notin A^\times$ et $P = QR \Rightarrow Q \in A^\times$ ou $R \in A^\times$

Rq ⑰ : $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$

II. Fonctions symétriques élémentaires. Polynômes symétriques.

1) Relations coefficients-racines

[Gou] **Déf. (18).** Soit $n \in \mathbb{N}^*$ et $k \in \{1 \dots n\}$. On définit

$$\sigma_{n,k} : K^n \longrightarrow K$$
$$(x_1 \dots x_n) \longmapsto \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$$

Th. (19). Soit $P = a_0 X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in K[X]$ un polynôme scindé de racines $\alpha_1 \dots \alpha_n$ (comptées avec multiplicité).

60 Alors : $\forall 1 \leq k \leq n$, $\sigma_{n,k}(\alpha_1 \dots \alpha_n) = (-1)^k \dfrac{a_k}{a_0}$.

En particulier : $\sigma_{n,1}(\alpha_1 \dots \alpha_n) = \sum_{i=1}^n x_i = -\dfrac{a_1}{a_0}$ $\quad \sigma_{n,2}(\alpha_1 \dots \alpha_n) = \sum_{1 \leq i < j \leq n} x_i x_j = \dfrac{a_2}{a_0}$

$\sigma_{n,n}(\alpha_1 \dots \alpha_n) = \prod_{i=1}^n x_i = (-1)^n \dfrac{a_n}{a_0}$.

2) Polynômes symétriques $\quad n \in \mathbb{N}^*$

[Ber] **Déf. (20) :** $P \in A[X_1 \dots X_n]$ est dit symétrique si pour tout $\sigma \in S_n$

433 $P(X_{\sigma(1)} \dots X_{\sigma(n)}) = P(X_1 \dots X_n)$

Ex. (21) : 1) $X_1 + X_2 + X_3 \in A[X_1, X_2, X_3]$ est symétrique

2) $X_1 + X_2 + X_3 \in A[X_1, X_2, X_3, X_4]$ n'est pas symétrique.

Lemme (22) : Pour tout $1 \leq k \leq n$, $\Sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k} \in A[X_1 \dots X_n]$ est un polynôme symétrique.

434 **Déf. (23) :** Pour $1 \leq k \leq n$, Σ_k défini au Lemme (22) est appelé k-ième polynôme symétrique élémentaire de $A[X_1 \dots X_n]$

[Gou] **Ex. (24) :** $\Sigma_1 = X_1 + \dots + X_n$, $\Sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j$, $\Sigma_n = X_1 \dots X_n$

78 **Prop. (25) :** Les polynômes symétriques élémentaires vérifient

$(T - X_1) \dots (T - X_n) = T^n - \Sigma_1 T^{n-1} + \Sigma_2 T^{n-2} + \dots + (-1)^{n-1} \Sigma_{n-1} T + (-1)^n \Sigma_n$

Coro. (26) : Si $P = X^n + a_1 X^{n-1} + \dots + a_n = (X - \alpha_1) \dots (X - \alpha_n) \in K[X]$, alors pour tout $1 \leq i \leq n$, $(-1)^i a_i = \Sigma_i(\alpha_1 \dots \alpha_n)$.

Rq (27) : Si $\Phi \in A[X_1 \dots X_n]$, alors $\Phi(\Sigma_1, \dots \Sigma_n)$ est symétrique.

Th (28) *(théorème de structure des polynômes symétriques)*

Soit $P \in A[X_1 \dots X_n]$ un polynôme symétrique. Alors, il existe un unique polynôme $\Phi \in A[X_1 \dots X_n]$ tel que $P = \Phi(\Sigma_1 \dots \Sigma_n)$.

Ex. (29) : $X_1^2 + \dots + X_n^2 = \Sigma_1^2 - 2\Sigma_2$

Coro (29) : Si $P \in \mathbb{Z}[X]$ est unitaire de racines $\alpha_1 \dots \alpha_n \in \mathbb{C}$, alors si $F \in \mathbb{Z}[X_1 \dots X_n]$ est symétrique, $F(\alpha_1 \dots \alpha_n) \in \mathbb{Z}$.

Appli. (30) : *(théorème de Kronecker)*

Soit $P \in \mathbb{Z}[X]$ unitaire, $\deg P = n \geq 1$ et irréductible dans $\mathbb{Q}[X]$. 89

On suppose que toutes les racines de P sont de module ≤ 1.

Alors $P = X$ ou il existe $k \in \mathbb{N}^*$ tel que $P \mid X^k - 1$

Appli. (31) : Si $M \in O_n(\mathbb{Z})$, alors son polynôme caractéristique est produit de polynômes cyclotomiques. ♡

III. Corps finis

Cadre : $p \in \mathbb{N}$ est un nombre premier.

1) Construction de corps finis

Prop. (32) : Soit $P \in K[X]$. Alors $K[X]/(P)$ est un corps ssi P est irréductible sur K.

Th. (33) : Soit $P \in \mathbb{F}_p[X]$ un polynôme unitaire irréductible de degré $n \geq 1$. Alors $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal p^n.

Rq (34) : En posant $q = p^n$, $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est alors le corps de rupture de P sur $\mathbb{F}_p$, unique à isomorphisme près.

Ex. 35 : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$

2) Existence de polynômes irréductibles sur $\mathbb{F}_p$

[Dem] 220 DVP1

Th. 36 : Soit $n \in \mathbb{N}^*$ et $S = X^{p^n} - X \in \mathbb{F}_p[X]$. Alors S est exactement le produit des polynômes unitaires irréductibles sur $\mathbb{F}_p$ dont le degré divise n. De plus, si on note m_n le nombre de polynômes unitaires irréductibles de degré n, alors
$$\frac{p^n - p^{\lfloor \frac{n}{2} \rfloor}}{n} \leq m_n \leq p^n \text{, et on a donc } m_n \underset{+\infty}{\sim} \frac{p^n}{n}$$

Rq 37 : Si $P \in \mathbb{F}_p[X]$ est sans facteur carré, alors l'algorithme de Berlekamp nous permet de déterminer ses facteurs irréductibles.

IV. Application en algèbre linéaire. Résultant

1) Réduction des endomorphismes

Cadre 38 : E est un K-ev de dimension finie $n \geq 1$

Déf. 39 : Soit $u \in \mathcal{L}(E)$. Alors $\det(X\,id - u) \in K[X]$ est un polynôme unitaire de degré n appelé polynôme caractéristique de u. On le note χ_u.

Le polynôme minimal de u est l'unique polynôme unitaire $\mu_u \in K[X]$ tel que $(\mu_u) = \{P \in K[X] \,/\, P(u) = 0\}$.

Prop. 40 : λ est une valeur propre de u SSI λ est racine de μ_u
SSI λ est racine de χ_u

Th. 41 : 1) u est trigonalisable SSI χ_u est scindé.
2) u est diagonalisable SSI μ_u est scindé à racines simples
3) si $K = \mathbb{F}_q$, u est diagonalisable SSI u annule $X^q - X$

2) Résultant

A, B intègres commutatifs

Déf. 42 : Soit $f = a_m X^m + \dots + a_0$, $g = b_n X^n + \dots + b_0 \in A[X]$ $m, n \geq 1$. Alors le résultant de f et g est $\mathrm{Res}_X(f,g) = \det(\mathrm{Syl}_X(f,g)) \in A$ où $\mathrm{Syl}_X(f,g)$ est la matrice donnée en ANNEXE.

Prop. 43 : (lemme de spécialisation)
Soit $\phi : A \to B$ un morphisme d'anneaux. Avec les notations de Déf. 42, si $\phi(a_m) \neq 0$ et $\phi(b_n) \neq 0$, alors
$$\mathrm{Res}(\phi(f), \phi(g)) = \phi(\mathrm{Res}(f,g)) \in B.$$

Th. 44 : On suppose A factoriel. $f, g \in A[X]$ de degré ≥ 1. Alors, $\mathrm{Res}(f,g) = 0$ SSI f et g ont un facteur commun de degré ≥ 1.

Lemme 45 : $\overline{\mathbb{Z}} = \{z \in \mathbb{C} \,/\, \exists\, P \in \mathbb{Z}[X]$ unitaire irréductible, $P(z) = 0\}$ est un sous-anneau de $\mathbb{C}$. [Rom]

Th. 46 : Soit G un groupe fini de cardinal n et $\rho : G \to GL(V)$ une représentation irréductible de degré d. Alors, $d \mid n$ DVP2

ANNEXE

Déf. (42) :

$$\mathrm{Syl}_X(f,g) = \begin{array}{c} n \\ \\ \\ m \\ \\ \end{array} \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & 0 \\ & \ddots & & & \ddots & \\ 0 & & a_m & \cdots & & a_0 \\ b_n & \cdots & b_0 & & & 0 \\ & \ddots & & & \ddots & \\ 0 & & b_n & \cdots & & b_0 \end{pmatrix} \in \mathcal{M}_{m+n}(A)$$

Références :

- [Ber] Berhuy, Algèbre, le grand combat
- [Gou] Gourdon, Algèbre (2e éd.)
- [Dem] Demazure, Cours d'algèbre
- [Rom] Rombaldi, Algèbre et géométrie