

14. Racines d'un polynôme. Fonctions symétriques élémentaires. Ex. et appli.

Soit K un corps et L/K (K commutatif). A un anneau intègre commutatif.

I. Racines d'un polynôme $P \in K[X]$

a) Définitions et premières propriétés

Def. 1: Soit $a \in L$. Si $P(a) = 0$ alors on dit que a est une racine de P .

Prop. 2: Soit $a \in K$. a est une racine de P si $X - a$ divise P .

Def. 3: Soient $a \in K$ et $n \in \mathbb{N}^*$. On dit que a est racine d'ordre n si $(X - a)^n | P$ et $(X - a)^{n+1} \nmid P$.

Prop. 4: Soient $a_1, \dots, a_n$ des racines de P d'ordres $n_1, \dots, n_m$ (a_i 2 à 2 distincts). Alors il existe $Q \in K[X]$ tq
 $P(X) = (X - a_1)^{n_1} \dots (X - a_m)^{n_m} Q(X)$ et $\forall i, Q(a_i) \neq 0$.

Prop. 5: Si $\deg(P) = n$ alors P a au plus n racines.

Rmq. 6: la prop. précédente fausse si K est un anneau. Par ex, dans $\mathbb{Z}_8$, $P = 4X \in \mathbb{Z}_8[X]$ a 3 racines dans $\mathbb{Z}_8$, mais $\deg(P) = 1$.

Prop. 7: Si K est infini et pour tout $a \in K, P(a) = 0$ alors $P = 0$.

Rmq. 8: Si K est fini le résultat est fausse. Si $K = \{a_1, \dots, a_n\}$, $D(X) = (X - a_1) \dots (X - a_n)$, $D(a) = 0 \forall a \in K$ mais $D \neq 0$.

Def. 9: On dit que P est scindé sur K si on peut écrire $P = \lambda (X - a_1)^{n_1} \dots (X - a_r)^{n_r}$ où $\lambda \in K, n_i \in \mathbb{N}^*, a_i \in K$.

b) Dérivation et racines

Def. 10: Si $P = a_n X^n + \dots + a_1 X + a_0$, on appelle polynôme dérivé et on note $P' = na_n X^{n-1} + \dots + a_1$.

Rmq. 11: Si P est constant, alors $P' = 0$. La réciproque est vraie si $\text{car}(K) = 0$.

Ex. 12: $X^2 + 1 \in \mathbb{Z}_2[X]$, $(X^2 + 1)' = 2X = 0$ dans $\mathbb{Z}_2$.

Thm. 13: (Formule de Taylor) Si $\text{car}(K) = 0$ et si $\deg P \leq n$ alors
 $\forall a \in K, P(X) = P(a) + \frac{(X-a)}{1!} P'(a) + \dots + \frac{(X-a)^n}{n!} P^{(n)}(a)$

Thm. 14: Si $\text{car}(K) = 0, P \neq 0$, a est racine d'ordre $n \in \mathbb{N}^*$ si $\forall i \in \{1, \dots, n-1\}, P^{(i)}(a) = 0$ et $P^{(n)}(a) \neq 0$.

Rmq. 15: Le résultat est fausse si $\text{car}(K) \neq 0$. $P = X^3$ a 3 racines d'ordre 3, or $P'(0) = 0$.

Prop. 16: $P \neq 0, a \in K$ est racine simple de P si $P(a) = 0$ et $P'(a) \neq 0$.

c) Polynômes Interpolateurs de Lagrange

Thm. 17: (Interpolation de Lagrange) Soient $a_1, \dots, a_n \in K$ 2 à 2 distincts et $b_1, \dots, b_n \in K$. Il existe un unique $P \in K[X]$ tq $\deg(P) \leq n-1$ et $\forall i, P(a_i) = b_i$.

Pour $i \in \{1, \dots, n\}$ posons:

$$L_i = \frac{(X - a_1) \dots (X - a_{i-1})(X - a_{i+1}) \dots (X - a_n)}{(a_i - a_1) \dots (a_i - a_{i-1})(a_i - a_{i+1}) \dots (a_i - a_n)}$$

$P = \sum_{i=1}^n b_i L_i$ est l'unique polynôme vérifiant l'interpolation.

II. Polynômes symétriques élémentaires

a) Généralités sur les polynômes à plusieurs variables

Def. 17: Soit $P \in A[X_1, \dots, X_n]$, $P = \sum_{j=0}^h P_j(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$, pour tout 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 un pol. en X_i , on note $\deg_{X_i}(P)$.

Def. 18: Le degré total d'un monôme $\alpha X_1^{i_1} \dots X_n^{i_n}$ $\alpha \in A \setminus \{0\}$ est $i_1 + \dots + i_n$.

Le degré total de P , noté $\deg(P)$ est le plus grand degré total des monômes qui forment P .

Prop. 20: Si K est infini. $P \in K[X_1, \dots, X_n]$. Si $P(x_1, \dots, x_n) = 0$ pour tout $x_1, \dots, x_n \in K$ on a $P = 0$.

Rmq. 21: Le résultat est fausse si K est fini.

Rmq. 23: On peut avoir $P(x_1, \dots, x_n) = 0$ pour une infinité de x_i sous que $P = 0$.

Ex. 24: $P = X - Y \in \mathbb{R}[X, Y]$ a une infinité de racine et $P \neq 0$.

b) Polynômes symétriques et théorème de structure

Def. 25: $P \in A[X_1, \dots, X_n]$ est dit symétrique si $\forall \sigma \in S_n$
 $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

Ex. 26: Dans $\mathbb{R}[X, Y, Z]$ $P = XY + YZ + ZX$ est symétrique

Def. 27: Soit $M = X_1^{d_1} \dots X_n^{d_n} \in A[X_1, \dots, X_n]$. Soit $S \in S_n$, on pose $M_S = X_{\sigma(1)}^{d_1} \dots X_{\sigma(n)}^{d_n} = \sum M_S$ est symétrique dans $A[X_1, \dots, X_n]$ M_S distincts.

On l'appelle symétrisé de M et on note ΣM .

[600]
p. 63

[600]
p. 65

[600]
p. 83

[600]
p. 64

(600)
p.83
-84

Ex.28: Dans $K[X_1, X_2]$ $\sum X_1^i X_2^j = X_1^2 X_2 + X_1 X_2^2$

Def.29: On appelle pol. symétrique élémentaire de $A[X_1, \dots, X_n]$ les pol. :

$$\sum_p = \sum X_1 \dots X_p = \sum_{i_1 < \dots < i_p} X_{i_1} \dots X_{i_p} \quad p \in \{1, \dots, n\}$$

Ex.30: $\sum_1 = \sum X_i = X_1 + \dots + X_n$, $\sum_2 = \sum X_i X_j = \sum_{i < j} X_i X_j$
 $\sum_n = X_1 \dots X_n$.

Thm.31: (Relation coefficient racines) $P = X^n + \dots + a_0 \in K[X]$ où a_i et $\alpha_1, \dots, \alpha_n$ ses racines alors pour $i \in \{1, \dots, n\}$

$$(-1)^i a_i = \sum_j (\alpha_1, \dots, \alpha_n)$$

Thm.32: (Structure) Soit $P \in A[X_1, \dots, X_n]$ symétrique.

Il existe un unique $\phi \in A[\sum_1, \dots, \sum_n]$ tq $P = \phi(\sum_1, \dots, \sum_n)$

III - Théorie des corps et polynômes

a) Éléments algébriques

Def.33: On dit que α est algébrique sur K si il existe $P \in K[X]$ tq $P(\alpha) = 0$. Sinon on dit α est transcendant sur K .

Def.34: Si α est algébrique $\{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal, donc admet un unique générateur unitaire.

Thm.35: Les ASSE:

(i) α est algébrique sur K (iii) $\dim_K K[\alpha] < \infty$

(ii) $K[\alpha] = K(\alpha)$

Si $\mu_{\alpha, K}$ est le pol. min de α , $\dim_K K[\alpha] = \deg \mu_{\alpha, K}$ et entier est appelé degré de α .

Def.36: L est dite finie si $[L:K] < \infty$. L est dite algébrique si $\forall \alpha \in L$ α est algébrique sur K .

Remq.36: Si L est fini alors L est algébrique. La réciproque est fautive.

Thm.37: $\{x \in L \mid x \text{ alg. sur } K\}$ est un corps.

Def.38: K est dit algébriquement clos si K vérifie un des ASSE:

(i) Tout $P \in K[X]$ de $\deg(P) \geq 1$ admet une racine dans K

(ii) Tout $P \in K[X]$ est produit de pol. de $\deg. 1$.

(iii) Les irréductibles de $K[X]$ sont les $X - \alpha$ $\alpha \in K$

(iv) Si L/K est algébrique alors $L=K$.

Thm.33: (D'Alembert-Goursat) $\mathbb{C}$ est algébriquement clos.

b) Corps de ruptures et de décompositions $P \in K[X]$, $p \in P$, $n \in \mathbb{N}^*$, $q = p^n$

Def.40: Soit $P \in K[X]$ irréductible. L est dite corps de rupture de P sur K si $L = K(\alpha)$ et $P(\alpha) = 0$. ($\alpha \in L$).

Thm.41: Si P irréductible, il existe un unique (à iso. près) corps de rupture de P sur K . Le corps est $K[X]/(P)$.

Def.42: On appelle corps de décomposition de P ($\deg(P) = n$) sur K une L/K tq:

- 1) P a toutes ses racines dans L .
- 2) L est minimal pour cette ppt.

Thm.43: Il existe un unique (à iso. près) corps de décomp. de P sur K . On le note $D_K(P)$

Ex.44: $K = \mathbb{Q}$ $P = X^3 - 2$ $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, j)$

Thm.45: Il existe un unique corps $\bar{\alpha}$ q éléments, $D_{\mathbb{F}_p}(X^q - x)$.

Prop.46: Soit $P \in \mathbb{F}_q[X]$, unitaire, irréductible. Le corps de rupture de P et de décomposition de P coïncident.

c) Quelques critères d'irréductibilité

Thm.47: (Eisenstein) - Soit A un anneau factoriel, $K = Fr(A)$.

Soit $P = a_n X^n + \dots + a_0$. Si il existe $p \in A$ irréductible tq:

- (i) $p \mid a_m$
- (ii) $p \nmid a_i$ pour $i \in \{0, \dots, m-1\}$
- (iii) $p^2 \nmid a_0$

Alors P est irréductible dans $K[X]$ (et dans $A[X]$ si $\text{pgcd}(a_i) = 1$)

Ex.48: $X^2 + 3X + 12$ est irr. dans $\mathbb{Q}[X]$

Thm.49: Soit A factoriel, $K = Fr(A)$ et I un idéal premier de A .

Posons $B = \frac{A}{I}$ et $L = Fr(B)$. Soit $P = a_n X^n + \dots + a_0 \in K[X]$, modulo I . Si $\bar{a}_n \neq 0$ et $\bar{P}$ irréductible sur L ou B alors P est irr. sur K .

Remq.50: Un cas fréquent d'utilisation est $A = \mathbb{Z}$, $I = (p)$, $B = \frac{\mathbb{Z}}{p\mathbb{Z}}$

Ex.51: $X^3 + 6X^2 + 2933X - 67691$ est irr. sur $\mathbb{Z}$. (regarder mod. 7)

Thm.52: $P \in K[X]$ de $\deg. m$. P est irr. sur P n -ième pps de racines dans $\mathbb{Z}$ autres L/K tq $[K:\mathbb{Q}] \leq \frac{m}{2}$.

Thm.53: $P \in K[X]$ tq $\deg P = m$, si L/K de degré m tq $\text{pgcd}(m, n) = 1$ Alors P est irréductible sur L .

CPERS
p.63
-68

[PER]
p.90
-73

[PER]
p.76
-79

1) Polynômes cyclotomiques: $n \in \mathbb{N}^*$

On note $\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$. On note μ_n^* ses générateurs.

Def. 54: On appelle n -ème polynôme cyclotomique

$$\Phi_n = \prod_{\zeta \in \mu_n^*} (x - \zeta)$$

Prop. 55: $x^n - 1 = \prod_{d \mid n} \Phi_d$

Prop. 56: Les Φ_n sont unitaires de deg. $\varphi(n)$

Prop. 57: $\Phi_n \in \mathbb{Z}[x]$

Prop. 58: Φ_n est irr. sur $\mathbb{Z}[x]$

Cor. 59: $\zeta \in \mu_n^*$, $\mu_{\zeta, \mathbb{Q}} = \Phi_n$ et $\mathbb{C}(\zeta) : \mathbb{Q} = \mathbb{P}(n)$

II - Quelques applications

a) Réduction des endomorphismes E K -ev. de dim. $n \in \mathbb{N}^*$, $u \in \mathcal{L}(E)$

$A = \text{Mat}_K(u)$ ou B est une base de E .

Def. 60: On appelle polynôme caractéristique de u , $\chi_u = \det(XI_n - A)$

Prop. 61: Les racines de χ_u sont exactement les vp. de u .

Prop. 62: Si χ_u est scindé alors $\text{tr}(A)$ est la somme des vp de u et $\det(A)$ est le produit des vp de u .

Def. 63: Soit $P = X^n + \dots + a_0$, on appelle matrice compagnon de P

$$C_P = \begin{pmatrix} 0 & \dots & 0 & -a_0 \\ 1 & \dots & 0 & -a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

Prop. 64: $\chi_{C_P} = P$

Thm. 65: (Cayley - Hamilton) $\chi_u(u) = 0$.

Thm. 66: (Lemme des noyaux) $P = P_1 \dots P_k \in K[X]$, P_i 1^{er} entre eux

Alors $\text{Ker}(P(f)) = \text{Ker}(P_1(f)) \oplus \dots \oplus \text{Ker}(P_k(f))$

Cor. 67: u est diagonalisable si il existe $P \in K[X]$ scindé à racines simples sur K tq $P(u) = 0$.

Thm. 68: u est diagonalisable si χ_u est scindé et la dimension de chaque sous-espace propre est égal à la multiplicité de la vp. dans χ_u .

Thm. 70: u est trigonalisable si χ_u est scindé
si il existe un polynôme annulateur de u scindé

b) Localisation de racines

Thm. 71: (Gauss - Lucas) $P \in \mathbb{C}[X]$ non constant. Les racines de P' sont toutes dans l'enveloppe convexe des racines de P .

Appli. 72: Le plus grand $n \in \mathbb{N}^*$ tq $(x+1)^n - x^n - 1$ a toutes ses racines non nulles de module 1 est 7.

Références:

[GOU]: Gordan, Alg. et probab.

[PERS]: Perrin, Cours d'alg.

[MAN]: Monod, red-endo.

[FRA]: Fraconer, Cours 1^{er} alg. L.

Commentaires:

- on peut enlever IIa)

- on peut épaissir IV b) ou mettre DEV2 à la fin de I b)

[MAN] p. 106

[FRA] p. 229 ou 230

[FRA] p. 225

DEV2

[PERS] p. 80 - 81

DEV1

[MAN] p. 54 - 56

[MAN] p. 71 - 73

[MAN] p. 81

[GOU] p. 125

[MAN] p. 93