

[Rom]
[Ber]
[Per] [Man]

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

K corps commutatif et A anneau intègre

I-Racines d'un polynôme [Rom] 362-363

- def racine
- a racine $\Leftrightarrow x-a \mid P$
- def racine d'ordre p
- $P(x) = (x-a_1)^{p_1} \cdots (x-a_r)^{p_r} Q(x)$ $Q(a_i) \neq 0$
- au + n racines si $\deg P = n$
- Δ Faux sur un anneau ex: $4X \in \mathbb{Z}_8[X]$ 3 racines
- K infini $P(x) = 0 \quad \forall x \in K \Rightarrow P = 0$
- Faux si K fini ex: $X^p - X \in \mathbb{F}_p[X]$
- def scindé
- def polynôme dérivé
- Formule de Taylor

II- Polynômes symétriques [Ber] 432-434-435

A commutatif

- def action de S_n sur $A[X_1, \dots, X_n]$ $n \geq 1$
- def polynôme symétrique + exemples
- j.e polynôme symétrique élémentaire
- def monôme et degré monôme
- def homogène
- Th structure des polynômes symétriques
- def support de P
- ex

DEV1

• Théorème de Kronecker

III- Extension de corps

1) Elements algébriques. [Ber] 66

- def et prop

2) Corps de rupture [Per] 70, 78

- def + exemple

- Th existence

- Pirméd de $K[x]$ ssi $\dots [L:K] \leq \frac{1}{2}$

3) Corps de décomposition [Per]

- def + ex

- Th existence

4) Cloture algébrique

- prop

- def alg des + ex

- Th d'Alembert Gauss

IV - Applications

1) Reduction des endomorphismes [Man] 51-54 80

- def polynôme min et caractéristique 105

- Cayley Hamilton

- def vp, vecteurs propres, ss espace propre

- Th diagonalisation et trigonalisation

2) Localisation de racines

DEV2

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

Soit K un corps commutatif. Soit $P \in K[X]$

I - Racines d'un polynôme

Définition 1: On dit que $\alpha \in K$ est racine de P , si $P(\alpha) = 0$

Proposition 2: $\alpha \in K$ est racine de P ssi $(X - \alpha)$ divise P

Définition 3: Soit $P \in K[X]$ non constant. Soit $\alpha \in K$ et $m \in \mathbb{N}^*$. On dit que α est racine d'ordre m de P si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P

Théorème 4: Soit P non constant. Soit $\alpha_1, \dots, \alpha_n \in K$ deux à deux distincts et $m_1, \dots, m_r \in \mathbb{N}^*$. On équivaut

- 1) $\forall k \in \{1, r\}$ α_k est racine de P de multiplicité m_k
- 2) $\exists Q \in K[X]$ tel que $P(X) = Q(X) \prod_{k=1}^r (X - \alpha_k)^{m_k}$ et $Q(\alpha_k) \neq 0$ $\forall k \in \{1, r\}$

Corollaire 5: Si $\deg P = n > 1$ alors P admet au plus n racines distinctes ou confondues dans K

Remarque 6: Ce résultat est faux dans un anneau commutatif unitaire: exemple $\mathbb{Z}[X]$ à 2 racines distinctes dans $\mathbb{Q}/2\mathbb{Z}[X]$.

Corollaire 7: Si K est infini et $P \in K[X]$ est tel que $P(\alpha) = 0 \forall \alpha \in K$ alors $P = 0$.

Remarque 8: Ce résultat est faux pour un corps fini

Définition 9: $P \in K[X]$ est scindé sur K s'il est constant ou de degré $n > 1$ et admet $r > 1$ racines distinctes dans K

[Rem] 362

363

de multiplicités respectives $m_1, \dots, m_r$ avec $\sum_{i=1}^r m_i = n$

Définition 10: le polynôme dérivé de $P \in K[X]$ est le polynôme P' défini par: $P'(X) = \begin{cases} 0 & \text{si } P = aX \\ \sum_{k=2}^n k a_k X^{k-1} & \text{si } P(X) = \sum_{k=0}^n a_k X^k \end{cases}$

Théorème 11 (Taylor) Soit K de caractéristique nulle. Soit $a \in K$ et $P(X) = \sum_{k=0}^n a_k X^k \in K[X]$. Alors $P(X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k$

II - Polynômes symétriques

Soit A un anneau commutatif et $P \in A[X_1, \dots, X_n]$

Notation: si $\alpha = (\alpha_1, \dots, \alpha_n) \in N^n$, on pose $X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ et $P = \sum_{\alpha} a_{\alpha} X^{\alpha}$ avec $a_{\alpha} \in A$

Si $\tau \in S_n$ on pose $\tau \cdot P = P(X_{\tau(1)}, \dots, X_{\tau(n)})$ l'action de S_n sur $A[X_1, \dots, X_n]$.

Définition 12: On dit que P est symétrique s'il est fixe sous l'action de S_n : si $P(X_{\tau(1)}, \dots, X_{\tau(n)}) = P(X_1, \dots, X_n) \forall \tau \in S_n$.

Exemples 13: si $n=3$ $X_1 + X_2 + X_3$ est symétrique si $n=4$ $X_1 + X_2 + X_3$ n'est pas symétrique.

Définition 14: Soit $j \in \{1, n\}$. le polynôme

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} X_{i_1} X_{i_2} \dots X_{i_j} \in A[X_1, \dots, X_n]$$

est appelé

le j ème polynôme symétrique élémentaire de $A[X_1, \dots, X_n]$

Définition 15: Un élément de $A[X_1, \dots, X_n]$ de la forme αX^{α} avec $\alpha \in A, \alpha = (\alpha_1, \dots, \alpha_n) \in N^n$ est appelé un monôme.

[Bar] 432

434

le degré d'un monôme $a_1 x_1^{m_1} \dots x_n^{m_n}$, $a_i \in \mathbb{A}[x_1, \dots, x_n]$ est $m_1 + m_2 + \dots + m_n$.

le degré de $P \in \mathbb{A}[x_1, \dots, x_n]$ non nul est le maximum des degrés des monômes non nuls de P .
On dit que $P \in \mathbb{A}[x_1, \dots, x_n]$ non nul est homogène de degré $d \geq 0$ s'il est somme de monômes de même degré d .

Théorème 16: $\forall P \in \mathbb{A}[x_1, \dots, x_n]$ symétrique, il existe un unique polynôme $Q \in \mathbb{A}[T_1, \dots, T_n]$ tel que $P = Q(\sigma_1, \dots, \sigma_n)$.

Définition 17: Soit $P = \sum_{\alpha} a_{\alpha} x^{\alpha} \in \mathbb{A}[x_1, \dots, x_n]$ le support de P noté $\text{Supp}(P)$ est l'ensemble $\text{Supp}(P) = \{\alpha \in \mathbb{N}^n \mid a_{\alpha} \neq 0\}$

Théorème 18: (Kronecker) DEV1
Soit $P \in \mathbb{C}[X]$ unitaire. Si les racines complexes de P sont non nulles et de module inférieur ou égal à 1, alors ce sont les racines de l'unité

III - Extensions de corps

1) Elements algébriques

Définition 19: Soit $K \subset L$ une extension de corps et $\alpha \in L$. Soit $\varphi: K[X] \rightarrow L$ morphisme d'évaluation de α .

1) Si φ est injectif on dit que α est transcendant sur K

2) Sinon on dit que α est algébrique sur K . Il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Si $\text{ker}(\varphi) = (m_X)$ alors m_X est le polynôme minimal de α sur K avec m_X unitaire.

Exemples 20: e et π sont transcendants sur $\mathbb{Q}$.
 $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$.

Théorème 21: Soit L/K une extension et $\alpha \in L$. On a équivalence

- 1) α est algébrique sur K
- 2) $K[\alpha] = K(\alpha)$
- 3) $\dim_K K(\alpha) < +\infty$

On dit que L est irréductible et $\dim_K L(\alpha) = \deg(m_{\alpha})$

2) Corps de rupture

Définition 22: Soit $P \in K[X]$ irréductible. L'extension K_K est appelé un corps de P sur K si $L = K(\alpha)$ et α racine de P .

Théorème 23: Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K unique à isomorphisme près.

Exemple 24: $\mathbb{C} = \mathbb{R}[X]_{(X^2+1)}$ est un corps de rupture de X^2+1

Théorème 25: Soit $P \in K[X]$ de degré $n > 0$. Alors P est irréductible sur K ssi P n'a pas de racines dans les extensions K de K vérifiant $[K:K] \leq \frac{n}{2}$

3) Corps de décomposition

Définition 26: Soit $P \in K[X]$. On appelle corps de décomposition de P sur K une extension L de K telle que

- 1) P est scindé sur L
- 2) L est engendré par les racines de P

Théorème 27: Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K unique à isomorphisme près

Exemple 28: Pour $K = \mathbb{Q}$, $P(X) = X^3 - 2$ a pour corps de décomposition $\mathbb{Q}(\sqrt[3]{2}, i)$

IV- Applications

1) Réduction des endomorphismes

Soit E un K - espace vectoriel de dimension finie non nulle
Soit u un endomorphisme de E .

Définition 29: Une valeur propre λ de u est un scalaire tel que il existe $x \in E \setminus \{0\}$ avec $u(x) = \lambda x$.
 λ est appelé vecteur propre de u associé à λ .

Proposition 30: Soit P un polynôme annulateur de u . Alors les valeurs propres de u sont des racines de P .

Définition 31: Le polynôme minimal de u est l'unique polynôme unitaire, noté μ_u , qui engendre l'idéal des polynômes annulateurs de u .

Définition 32: Le polynôme caractéristique de $u \in \text{End}(K)$ est $\chi_u(X) = \det(XI_n - A)$.

Le polynôme caractéristique de u , χ_u , est celui de sa matrice associée dans n'importe quelle base.

Proposition 33: On a l'équivalence entre:

- 1) λ est valeur propre de u
- 2) λ est racine de χ_u
- 3) λ est racine de μ_u

Théorème 34: On a l'équivalence:

- 1) u diagonalisable
- 2) u admet un polynôme annulateur scindé à racines simples
- 3) μ_u est scindé à racines simples

Théorème 35 On a l'équivalence entre :

- 1) u est trigonalisable
- 2) χ_u est scindé sur K
- 3) μ_u est scindé sur K

2) Localisation des racines

Soit $n \in \mathbb{N}^*$. Soit $A = (a_{ij})_{i,j \in [1,n]} \in M_n(\mathbb{C})$

On pose pour $i \in [1,n]$ $R_i = \sum_{j=1}^n |a_{ij}|$

Théorème 36: Si $A \in M_n(\mathbb{C})$ est à diagonale strictement dominante (i.e. $\forall i \in [1,n] \quad |a_{ii}| > R_i$)

Alors $\det(A) \neq 0$ et $\lambda_i(A) = a_{ii} - R_i$

DEV2

$$P = \sum_{k=0}^n a_k X^k \in K[X]$$

Forme standard $\rightarrow$ Polynômes symétriques

Qu'est-ce qu'une racine d'un polynôme?

$\rightarrow$ Un polynôme n'a pas forcément de racines dans un corps

$$P(x) = 0$$

bonné? Au + n racines

si K corps et $\deg P = n$

ordre? $(x-\alpha)^m \mid P$
 $(x-\alpha)^{m+1} \nmid P$

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

algèbre
 $\rightarrow$ Th des corps

Formules de Taylor

corps
 $\rightarrow$ racines de l'unité

Polynômes symétriques

$\rightarrow$ relation coefficients/racines

$\rightarrow P$ fixe sous l'action de S_n

$\rightarrow$ lien avec les racines de l'unité

Th de Kronecker **DEV 1**

Applications

vp
 $\rightarrow$ réduction d'endo

Réduction des endomorphismes

Racine et polynômes annulateurs

$\rightarrow$ s'écrit? $\rightarrow$ diag
 Krone

localisation des vp

DEV 2

Corps de rupture

P a d'au moins une racine mais pas toujours s'écrit

$$Q(\sqrt[3]{2}) \quad Q(\sqrt[3]{2}) \quad x^3 - 2$$

Existence et unicité

Corps de décomposition

$$P \text{ s'écrit } K(\alpha, \lambda) = \mathbb{L}$$

$$Q(\sqrt[3]{2}, j)$$