

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

I. Racines d'un polynôme

1. Racines et multiplicité [ROM]

Racine, multiplicité, décomposition d'un polynôme, polynôme dérivé, formule de Taylor, lien avec les dérivées

2. Polynôme scindé et irréductibilité [ROM]

Poly scindé, poly irréductible, poly de degré 2 et 3, corps algébriquement clos, théorème de d'Alembert-Gauss

3. Relations coefficients-racines [IP]

Polynômes symétriques élémentaires, relations coeff-racines

DEV 1 : Théorème de Kronecker, application

II. Extensions de corps

1. Elements algébriques [PER]

Elements algébriques et transcendants, polynôme minimal, extension algébrique

2. Corps de rupture et de décomposition [PER]

Corps de rupture, corps de décomposition, corps fini

III. Racines de l'unité et polynômes cyclotomiques [PER]

Racine n -ième de l'unité, racine primitive, poly cyclotomique et prop

DEV 2 : Irréductibilité de $\Phi_n(X)$ + polynôme minimal d'une racine primitive n -ième de l'unité

IV. Application à la réduction d'endomorphismes [MAN]

Valeurs propres, poly minimal, poly caractéristique, les vp sont les racines, déterminant et trace avec les racines, équivalences diagonalisabilité, équivalences trigonalisabilité

Présentation :

- On remarque qu'un polynôme n'admet pas forcément de racines dans un corps donné. Il est donc nécessaire d'aller dans des sur-corps du corps considéré pour trouver des racines d'un polynôme. C'est donc pour cela que l'on s'intéresse aux extensions de corps.
- Les corps de rupture permettent de passer d'un corps où le polynôme était irréductible, à un corps où celui-ci admet une racine. Cependant, il arrive que le polynôme ne soit toujours pas complètement scindé (il manque des racines dans le corps de rupture). On considère alors le corps de décomposition.
- Les polynômes cyclotomiques sont directement définis à partir de leurs racines. Ces polynômes ont de nombreuses propriétés.
- On observe l'utilité des polynômes scindés lorsque l'on cherche des CNS de réduction d'endomorphisme.

Développements :

- Théorème de Kronecker

- L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte, p277
- Carnet de voyage en Algèbre, Caldero-Peronnier, p30
- Algèbre linéaire-réduction des endomorphismes, Mansuy-Mneimné, p111
- Irréductibilité des polynômes cyclotomiques + degré d'une extension cyclotomique
 - Théorie de Galois, Gozard, p69
 - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p384
 - Cours d'algèbre, Perrin, p80

Références :

- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [IP] L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte
- [PER] Cours d'algèbre, Perrin
- [MAN] Algèbre linéaire réduction des endomorphismes, Mansuy-Mneimné

Leçon 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

1) Racines et multiplicité [ROM]

Déf 1: On dit que $d \in K$ est racine de P si $P(d) = 0$.

Prop 2: $d \in K$ est racine de P si $(x-d)$ divise P .

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

Théorème 4: Soit P non constant. Soit $d_1, \dots, d_n \in K$ deux à deux distincts et $m_1, \dots, m_n \in \mathbb{N}^*$. On a équivalence entre:

- d_k est racine de P de multiplicité $m_k \quad \forall k \in \{1, \dots, n\}$
- il existe $Q \in K[X]$ tel que $P(x) = Q(x) \cdot \prod_{k=1}^n (x-d_k)^{m_k}$ et $Q(d_k) \neq 0 \quad \forall k \in \{1, \dots, n\}$.

Corollaire 5: Si P non constant admet $n \geq 1$ racines distinctes de multiplicités $m_1, \dots, m_n$, alors $\deg(P) \geq \sum_{k=1}^n m_k$.

Corollaire 6: Si P est de degré $n \geq 1$, il admet au plus n racines distinctes au corps K .

Remarque 7: Le n -ième plus valable pour des polynômes à coefficients dans un anneau commutatif unitaire: dans $\mathbb{Z}/6\mathbb{Z}[X]$, $3X$ est de degré 1 et a deux racines distinctes 0 et 2.

Déf 8: Le polynôme dérivé de P est le polynôme P' défini par:

$$P'(x) = \begin{cases} 0 & \text{si } P = 0, \text{ est constant} \\ \sum_{k=1}^n k a_k x^{k-1} & \text{si } P(x) = \sum_{k=0}^n a_k x^k \text{ est de degré } n \geq 1 \end{cases}$$

Théorème 9 (Formule de Taylor): Soit K de caractéristique 0.

Soit $a \in K$ et $P(x) = \sum_{k=0}^n a_k x^k$. Alors $P(x) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (x-a)^k$.

Théorème 10: Soit K de caractéristique 0. Soit P non nul, $d \in K$ et $m \in \mathbb{N}^*$. On a équivalence entre:

- d est racine d'ordre m de P
- il existe $Q \in K[X]$ tel que $P(x) = Q(x) \cdot (x-d)^m$ avec $Q(d) \neq 0$
- $P^{(k)}(d) = 0$ pour $k \in \{0, \dots, m-1\}$ et $P^{(m)}(d) \neq 0$.

2) Polynôme scinde et irréductibilité [ROM]

Déf 11: On dit que P est scinde sur K si il est de la forme $P(x) = \lambda \prod_{k=1}^n (x-d_k)^{m_k}$ où $\lambda \in K$, les d_k sont des scalaires distincts et $m_k \in \mathbb{N}^*$.

Si tous les m_k sont égaux à 1, on dit que P est scinde à racines simples.

Déf 12: On dit que $P \neq 0$ est irréductible si il est non constant et n'est divisible que par des constantes non nulles ou les polynômes λP avec $\lambda \in K^*$.

Exemple 13: $X^2 - 2$ est irréductible dans $\mathbb{R}[X]$, mais irréductible dans $\mathbb{Q}[X]$.

Prop 14: Un polynôme de degré 1, 2 ou 3 est irréductible dans $K[X]$ si il admet au moins une racine dans K .

Exemple 15: $(X^2+1)^n$ est irréductible dans $\mathbb{R}[X]$ mais n'admet pas de racines dans $\mathbb{R}[X]$.

Déf 16: On dit que K est algébriquement clos si tout polynôme $P \in K[X]$ est scinde sur K .

Théorème 17 (de d'Alembert-Goursat): Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

Exemple 18: $P(x) = x^2 + 1$ est irréductible sur $\mathbb{R}[X]$ mais scinde dans $\mathbb{C}[X]$: $P(x) = (x-i)(x+i)$.

3) Relations coefficients-racines [IP]

Soit A un anneau commutatif unitaire intègre.

Déf 19: Soit $m \in \mathbb{N}$ et $k \in \{0, \dots, m\}$. On définit le k -ième

polynôme symétrique élémentaire e_k de $A[x_1, \dots, x_n]$ par :

$$e_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}$$

où $\mathcal{P}_h(\mathbb{Q}, \mathbb{D})$ désigne l'ensemble des parties à h éléments de $\mathbb{Q} \cup \mathbb{D}$

Exemple 20 : On a $e_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n$ et $e_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n$

Théorème 21 : Soit $P \in A[x]$ un polynôme scindé unitaire, i.e. $P(x) = \sum_{i=0}^n a_i x^i$ avec $a_n = 1$, dont on note $z_1, \dots, z_n$ ses racines.

Alors : $\forall k \in \mathbb{Q} \cup \mathbb{D}$, $e_k(z_1, \dots, z_n) = (-1)^k a_{n-k}$.

Théorème 22 (de Kronecker) : Soit $P \in \mathbb{C}[x]$ un polynôme unitaire dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$ (on s'est pas racine). Alors toutes les racines de P sont des racines de l'unité.

Corollaire 23 : Soit $P \in \mathbb{Z}[x]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = x^n$ ou P est un polynôme cyclotomique.

DEV 1

II Extensions de corps

1) Éléments algébriques [PER]

Déf 24 : Soit $K \subset L$ une extension de corps et $d \in L$. Soit $\varphi : K[x] \rightarrow L$ le morphisme qui à $P(x)$ associe $P(d)$.

1) Si φ est injectif, on dit que d est transcendant sur K .
 2) Sinon, on dit que d est algébrique sur K . Ainsi il existe $P \in K[x]$ non nul tel que $P(d) = 0$. Si $\text{Ker}(\varphi) = (p_d)$ avec $p_d \in K[x]$, $p_d \neq 0$ et p_d unitaire, on dit que p_d est le polynôme minimal de d sur K .

Exemple 25 : 1) e et π sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.
 2) $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$.

Théorème 26 : Soit L/K une extension et $d \in L$. On a équivalence entre :

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

On a que p_d est irréductible et $\dim_K K(d) = \deg(p_d)$.

Déf 27 : Une extension L/K est dite algébrique si pour tout $d \in L$, d est algébrique sur K .

Prop 28 : Soit L/K une extension et $M = \{x \in L; x \text{ algébrique sur } K\}$. Alors M est un sous-corps de L .

2) Corps de rupture et de décomposition [PER]

Déf 29 : Soit $P \in K[x]$ un polynôme irréductible. L'extension L/K est appelée un corps de rupture de P sur K si $L = K(d)$ et d est une racine de P .

Théorème 30 : Soit $P \in K[x]$ irréductible. Il existe un corps de rupture de P sur K , unique à K -isomorphisme près.

Exemple 31 : $\mathbb{Q} = \mathbb{R}[x]/(x^2+1)$ est un corps de rupture de x^2+1

Déf 32 : Soit $P \in K[x]$. On appelle corps de décomposition de P sur K une extension L de K tel que :

- 1) P se scinde sur L
- 2) L est engendré par les racines de P .

Théorème 33 : Pour tout $P \in K[x]$, il existe un corps de décomposition de P sur K , unique à K -isomorphisme près.

Exemple 34 : Pour $K = \mathbb{Q}$, $P(x) = x^3 - 2$ a pour corps de décomposition $\mathbb{Q}(\sqrt[3]{2}, i)$.

Théorème 35 : Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit $q = p^n$. Alors il existe un corps à q éléments, c'est le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.

III Racines de l'unité et polynômes cyclotomiques [PER]

Déf 36 : On note $\mu_n = \{z \in \mathbb{C}; z^n = 1\}$ l'ensemble des racines n -ièmes de l'unité. C'est un groupe cyclique.

Déf 37 : On appelle racine n -ième primitive de l'unité

tout générateur de U_n . Leur ensemble est noté U_n^* .

Prop 38: On a $U_n^* = \{z \in \mathbb{C}; z^n = 1 \text{ et } z^d \neq 1 \forall d < n\}$.
Ainsi $1, U_n^* + 1 = \mathbb{C}(n)$ et $\mathbb{C}$ est l'inductrice d'Enden.

Def 39: On appelle n -ième polynôme cyclotomique le polynôme: $\Phi_n(x) = \prod_{z \in U_n^*} (x - z) \quad \forall n \in \mathbb{N}^*$

Prop 40: Φ_n est unitaire, de degré $\varphi(n)$.

Prop 41: On a la formule: $x^{n-1} = \prod_{d|n} \Phi_d(x)$

Exemple 42: $\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$,

$\Phi_4(x) = x^2+1$

Corollaire 43: Si p est premier:

$$\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

Prop 44: $\forall n \in \mathbb{N}^*$, $\Phi_n(x) \in \mathbb{Z}[x]$

Théorème 45: Le polynôme cyclotomique $\Phi_n(x)$ est irréductible sur $\mathbb{Q}$.

Corollaire 46: Si $\xi \in U_n^*$, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_n(x)$, et donc $[\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$. DEV 2

IV Application à la réduction d'endomorphismes [MAN]

Soit E un K -espace vectoriel de dimension finie $n \in \mathbb{N}^*$. Soit m un endomorphisme de E .

Def 47: Une valeur propre λ de m est un scalaire tel que $m - \lambda \text{id}_n$ est pas injective, c-à-d qu'il existe $x \in E \setminus \{0\}$ tel que $m(x) = \lambda x$.

Prop 48: Soit P un polynôme annulateur de m . Alors les valeurs propres de m appartiennent à l'ensemble des racines de P .

Def 49: Le polynôme minimal de m est l'unique polynôme unitaire, noté μ_m , qui engendre l'idéal des polynômes

annulateurs de m .

Def 50: Le polynôme caractéristique de $A \in M_n(K)$ est: $\chi_A(x) = \det(xI_n - A)$.

Le polynôme caractéristique de m , noté χ_m , est le polynôme caractéristique de n -importe laquelle de ses matrices.

Prop 51: On a équivalence entre:

- 1) λ est valeur propre de m
- 2) λ est racine de χ_m
- 3) λ est racine de μ_m .

Prop 52: On suppose que χ_m est scindé sur K . Alors la somme des valeurs propres (comptées avec leurs multiplicités) est la trace de m , et leur produit est le déterminant de m .

Théorème 53: Il y a équivalence entre:

- 1) m est diagonalisable
- 2) m admet un polynôme annulateur scindé à racines simples.
- 3) μ_m est scindé à racines simples.

Théorème 54: Il y a équivalence entre:

- 1) m est trigonalisable
- 2) χ_m est scindé sur K
- 3) μ_m est scindé sur K .