

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

Dans cette leçon, sauf mention contraire, on considère $\mathbb{K}$ un corps et $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ un polynôme.

1 Racines d'un polynôme

1.1 Généralités

Définition 1. On dit que $\alpha \in \mathbb{K}$ est une racine de P lorsque $P(\alpha) = 0$.

Proposition 2. Soit $a \in \mathbb{K}$, alors a est une racine de P si et seulement si $X - a$ divise P dans $\mathbb{K}[X]$.

Définition 3. Soit $\alpha \in \mathbb{K}$ une racine de P , on dit que α est racine de multiplicité $m \in \mathbb{N}^*$ de P lorsque $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P .

Théorème 4. Soit P non constant, $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ et $m_1, \dots, m_r \in \mathbb{N}^*$ alors on a équivalence :

1. Pour tout $k \in \llbracket 1, r \rrbracket$, α_k est racine de P de multiplicité m_k ,
2. Il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X) \prod_{k=1}^r (X - \alpha_k)^{m_k}$ et $Q(\alpha_k) \neq 0$ pour tout $k \in \llbracket 1, r \rrbracket$.

Corollaire 5. Un polynôme de degré $n \geq 1$ admet au plus n racines dans $\mathbb{K}$.

Corollaire 6. Si P de degré n admet au moins $n + 1$ racines comptées avec multiplicité alors $P = 0$.

Définition 7. Soit $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$ famille d'éléments distincts, on définit alors la famille de polynômes définis par $L_i(X) = \prod_{\substack{j=0 \\ j \neq i}}^n \frac{X - x_j}{x_j - x_i}$ pour $0 \leq i \leq n$ observons que $L_i(x_j) = \delta_{i,j}$.

Théorème 8. La famille $(L_i(X))_{0 \leq i \leq n}$ est une base de $\mathbb{K}_n[X]$.

Théorème 9. Avec les notations précédentes, pour tous scalaires $y_0, \dots, y_n$ et $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$ famille d'éléments distincts, il existe un unique polynôme de degré n tel que $P(x_j) = y_j$ pour tout $j \in \llbracket 0, n \rrbracket$. Ce polynôme dit interpolateur de Lagrange s'écrit $P = \sum_{k=0}^n y_k L_k(X)$.

Définition 10. Un polynôme est dit scindé sur $\mathbb{K}$ lorsqu'il est constant ou admet $r \geq 1$ racines distinctes dans $\mathbb{K}$ de multiplicités respectives $m_1, \dots, m_r$ avec $\sum_{k=1}^r m_k = n$. Dans le cas où tous les m_i valent 1 on dit qu'il est scindé à racines simples.

Définition 11. On dit que $\mathbb{K}$ est algébriquement clos lorsque tout polynôme de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Théorème 12. (D'Alembert-Gauss) Le corps $\mathbb{C}$ est algébriquement clos.

Définition 13. On appelle polynôme dérivé de P noté P' le polynôme $P' = \sum_{k=1}^n k a_k X^{k-1}$.

Théorème 14. Si $\mathbb{K}$ est de caractéristique nulle, alors tout polynôme P de degré inférieur ou égal à $n \in \mathbb{N}$ vérifie pour tout $a \in \mathbb{K}$, $P(X) = P(a) + \frac{(X-a)}{1!} P'(a) + \dots + \frac{(X-a)^n}{n!} P^{(n)}(a)$.

Proposition 15. Si $\mathbb{K}$ est de caractéristique nulle et si $P \neq 0$ alors $a \in \mathbb{K}$ est racine d'ordre k si et seulement si pour tout $i \in \llbracket 1, k-1 \rrbracket$ on a $P^{(i)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

1.2 Polynômes symétriques élémentaires

Définition 16. Un polynôme $P = \sum a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \in \mathbb{K}[X_1, \dots, X_n]$ est dit de degré total égal à d si $a_{i_1, \dots, i_n} = 0$ pour

toute liste $(i_1, \dots, i_n) \in \llbracket 1, n \rrbracket^n$ telle que $\sum_{k=1}^n i_k > d$ et si il existe $(i_1, \dots, i_n)$ telle que $\sum_{k=1}^n i_k = d$ et $a_{i_1, \dots, i_n} \neq 0$.

Définition 17. On dit qu'un polynôme $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique lorsque pour tout $\sigma \in \mathcal{S}_n$ il vérifie $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Définition 18. Les polynômes $\sigma_{k,n} = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$ pour $k \in \llbracket 1, n \rrbracket$ sont appelés polynômes symétriques élémentaires.

Exemple 19. On a $\sigma_{1,n} = \sum_{i=1}^n X_i$, $\sigma_{2,n} = \sum_{1 \leq i < j \leq n} X_i X_j$ et $\sigma_{n,n} = X_1 \dots X_n$.

Théorème 20. Si $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique, alors il existe un unique polynôme $Q \in \mathbb{K}[\sigma_{1,n}, \dots, \sigma_{n,n}]$ tel que $P(X_1, \dots, X_n) = Q(\sigma_{1,n}, \dots, \sigma_{n,n})$.

Proposition 21. Si $P(X) = \prod_{k=1}^n (X - \alpha_k)$ est un polynôme scindé de degré supérieur à 1 de $\mathbb{K}[X]$, on a alors $P(X) = \sum_{k=0}^n a_k X^{n-k}$ où $a_k = (-1)^k \sigma_{n,k}(\alpha_1, \dots, \alpha_n)$.

Théorème 22. (Formule de Poincaré) Si $(A_k)_{1 \leq k \leq n}$ suite finie d'éléments d'un espace probabilisé, on a alors $\mathbb{P}(\bigcup_{k=1}^n A_k) = \sum_{k=1}^n (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k})$.

1.3 Corps de rupture et décomposition

Définition 23. Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible. Une extension $\mathbb{L} \supset \mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ lorsque $\mathbb{L}$ est une extension monogène $\mathbb{L} = \mathbb{K}[\alpha]$ avec $P(\alpha) = 0$.

Théorème 24. Soit $P \in \mathbb{K}$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$ unique à isomorphisme près.

Définition 25. Soit $P \in \mathbb{K}[X]$ de degré n (irréductible ou non). On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :

1. Dans $\mathbb{L}[X]$, P est produit de polynôme de degré 1 (ou alors P a toutes ses racines dans $\mathbb{L}$).
2. Le corps $\mathbb{L}$ est minimal pour cette propriété (ou alors les racines de P engendrent $\mathbb{L}$).

Théorème 26. Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près que l'on note $D_{\mathbb{K}}(P)$.

2 Applications

2.1 Irréductibilité

Définition 27. Un polynôme $P \in A[X]$ est dit irréductible si il n'est pas inversible et si $P = AB$ avec $A, B \in A[X]$ alors A inversible ou B inversible.

Exemple 28. Si A est un corps alors les polynômes de degré 1 sont les seuls polynômes irréductibles.

Théorème 29. Soit $P \in \mathbb{K}[X]$ non nul, alors il se décompose de manière unique à l'ordre près sous la forme $P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$ où $\lambda \in \mathbb{K}^*$, $\alpha_i \in \mathbb{N}^*$ et les P_i polynômes distincts unitaires et irréductibles.

Définition 30. Une racine n -ième primitive de l'unité de $\mathbb{K}$ est un élément $\zeta \in \mathbb{K}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mu_n(\mathbb{K})$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mu_n^*(\mathbb{K})$.

Définition 31. Le n -ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Exemple 32. Sur $\mathbb{Q}$ on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Remarque 33. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $\text{pgcd}(d, n) = 1$. Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 34. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 35. Dans $\mathbb{Q}$ on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 36. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Théorème 37. Soit $\zeta \in \mu_n^*(\mathbb{K})$, alors Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$.

Corollaire 38. Soit $\zeta \in \mu_n^*(\mathbb{K})$, alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Définition 39. On définit la fonction de Möbius comme $\mu(1) = 1$, $\mu(n) = (-1)^r$ si $n = \prod_{i=1}^r p_i$ dans sa décomposition en facteurs carrés et $\mu(n) = 0$ sinon.

Théorème 40. (Möbius) Soient $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$ des suites réelles alors $\forall n \in \mathbb{N}^*, u_n = \sum_{d|n} v_d \iff \forall n \in \mathbb{N}^*, v_n =$

$$\sum_{d|n} \mu(d) u_{\frac{n}{d}}.$$

On pose $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ et $\mathcal{U}_d(p) = \{P \in \mathbb{F}_p[X] \mid \deg(P) = d, \text{ irréductible et unitaire} \}$ pour tout $n \in \mathbb{N}^*$ et p premier fixé.

Lemme 41. Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n . Réciproquement pour tout diviseur d de n tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n .

Théorème 42. Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a $X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P(X)$.

Théorème 43. Pour tout entier $n \in \mathbb{N}^*$ on a $|\mathcal{U}_n(p)| = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$.

2.2 Algèbre linéaire

Définition 44. On appelle idéal annulateur de u l'idéal $I_u = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ et polynôme minimal de u le générateur unitaire de cet idéal noté μ_u .

Définition 45. Le polynôme caractéristique $\chi_u \in \mathbb{K}[X]$ de u est défini par $\det(u - XId)$.

Théorème 46. L'endomorphisme u est trigonalisable sur $\mathbb{K}$, si et seulement si son polynôme caractéristique est scindé sur $\mathbb{K}$.

Théorème 47. (CNS de diagonalisabilité) Les assertions suivantes sont équivalentes :

1. L'endomorphisme u est diagonalisable,
2. Le polynôme caractéristique de u est scindé sur $\mathbb{K}$ de racines $\lambda_1, \dots, \lambda_p$ dans $\mathbb{K}$, étant de multiplicité $\alpha_k = \dim(\ker(u - \lambda_k Id))$,
3. Il existe un polynôme annulateur de u scindé à racines simples,
4. Le polynôme minimal μ_u de u est scindé à racines simples.

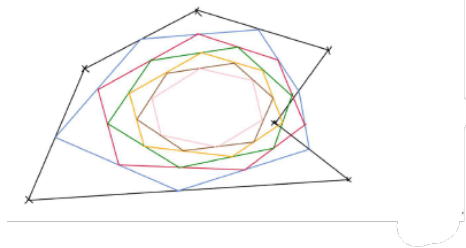
Proposition 48. (Déterminant Circulant) Soient $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, $\omega = e^{2i\pi/n}$ et $P = \alpha_n X^{n-1} + \dots + \alpha_2 X + \alpha_1$ on a alors

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_n & \alpha_1 & \dots & \alpha_{n-1} \\ \vdots & \dots & \dots & \vdots \\ \alpha_2 & \alpha_3 & \dots & \alpha_1 \end{pmatrix} = \prod_{i=0}^{n-1} P(\omega^i)$$

Applications 49. Soient $\mathcal{P} = (z_1, \dots, z_n)$ un polynôme à n sommets et $a, b \in]0, 1[$ tels que $a + b = 1$. La suite vectorielle définie par $\mathcal{P}_0 = \mathcal{P}$ et $\mathcal{P}_{k+1} = (ap_{k,1} + bp_{k,2}, \dots, ap_{k,n} + bp_{k,1})$ où $\mathcal{P}_k = (p_{k,1}, \dots, p_{k,n})$ converge vers l'isobarycentre de $\mathcal{P}$.

3 Annexe

FIGURE 2: Suite de polygones



Suite de polygones

Dev 1 : Dénombrement polynômes irréductibles de Fq 40,41,42 et 43

Dev 2 : Suites de polygones 48

Dev 3 : Polynômes cyclotomiques irréductibles 35 et 36

Références

- [GOU21] Xavier GOURDON : Les maths en tête. Algèbre et probabilités. Ellipses, 2021.
- [PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.
- [ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.
- [TAU07] Patrice TAUVEL : Corps commutatifs et théorie de Galois : cours et exercices. Calvage et Mounet, 2007.

RAPPORT DU JURY :

Dans cette leçon, il est indispensable de bien définir l'ordre de multiplicité d'une racine (définition algébrique et analytique, quand c'est possible). Les fonctions symétriques élémentaires et les relations entre coefficients et racines doivent être maîtrisées et pouvoir être mises en œuvre. Des méthodes, même élémentaires, de localisation des racines ont toute leur place et peuvent déboucher sur des résultats de topologie à propos de la continuité des racines. Il est pertinent d'introduire la notion de polynôme scindé et de citer le théorème de d'Alembert-Gauss. On peut faire apparaître le lien entre la recherche des racines d'un polynôme et la réduction des matrices. Les candidates et candidats peuvent également s'intéresser aux racines des polynômes orthogonaux, ou aux règles des signes de Descartes et de Sturm. L'étude des propriétés des nombres algébriques ont leur place dans cette leçon. La théorie des corps et le cas particulier des corps finis peuvent aussi être évoqués de façon pertinente.

Les candidates et candidats peuvent aller plus loin en s'intéressant à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin ou au calcul effectif d'expressions polynomiales symétriques des racines d'un polynôme. Il ne s'agit par contre en aucun cas d'adapter le plan de la leçon 141 : l'irréductibilité des polynômes peut être évoquée mais ne doit pas être l'élément central de la leçon.