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

Introduction : La notion de racine d'un polynôme se situe au carrefour de l'algèbre (divisibilité), algèbre linéaire (valeurs propres), analyse (zéros d'une fonction). D'où la multiplicité des méthodes et applications relatives à ce concept.

Soit K un corps.

1 Racines d'un polynôme

1.1 Premières définitions et propriétés

Définition 1. Soient $P \in K[X], a \in K$. On dit que a est une racine de P si $P(a) = 0$.

Proposition 2. a est racine de P ssi $(X - a)$ divise P.

Proposition 3. Soient a racine de $P, k \in \mathbb{N}^*$. Il y a équivalence entre :

(i). $P(X) = (X - a)^k Q(X)$ avec $Q(a) \neq 0$.

(ii). $(X - a)^k$ divise P et $(X - a)^{k+1}$ ne divise pas P.

Définition 4. On dit alors que a est racine de P d'ordre (ou de multiplicité) k.

Théorème 5. a est racine d'ordre k si et seulement si $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Théorème 6. Si $\deg(P) = n$ alors P possède au plus n racines (comptées avec multiplicité).

***Contre-exemple* 7.** *C'est faux sur un anneau commutatif : $X^2 - 3X + 2$ admet 4 racines dans $\mathbb{Z}/6\mathbb{Z}$.*

***Application* 8** (Vandermonde)**.**

Soient $x_1, \cdots, x_n \in K$. Alors $\begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_i - x_j)$

Définition 9. P est dit scindé s'il possède exactement n racines (comptées avec multiplicité).

Proposition 10. Si $P \in \mathbb{R}[X]$ est scindé, alors P' aussi.

Théorème 11 (D'Alembert, Gauss)**.** Si $P \in \mathbb{C}[X]$, alors P est scindé.

***Application* 12.** *Toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable.*

Corollaire 13. Les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1, et les irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 à discriminant négatif.

***Contre-exemple* 14.** *$(X^2+1)^2$ n'a pas de racines dans $\mathbb{Q}, \mathbb{R}$ mais non irréductible.*

1.2 Propriétés topologiques

Théorème 15. Soit $P = \prod_{i=1}^{n}(X - \lambda_i) \in \mathbb{C}_n[X]$, soit $(P_k)_{k\in\mathbb{N}} \in \mathbb{C}_n[X]^{\mathbb{N}}$ suite de polynômes unitaires de degré n qui converge vers P pour la topologie de la norme. Alors on peut écrire $P_k = \prod_{i=1}^{n}(X - \lambda_i^{(k)})$, avec pour tout $i \in [\![1, n]\!], \lambda_i^{(k)} \underset{k\to+\infty}{\longrightarrow} \lambda_i$.

Proposition 16. Soit $P_0 \in \mathbb{R}_n[X]$, soit a racine simple de P. Alors il existe U voisinage de P dans $\mathbb{R}_n[X], V$ voisinage de a dans $\mathbb{R}$ et $\varphi \in \mathcal{C}^\infty(U, V)$ tels que pour tous $P \in U, x \in V, P(x) = 0 \Leftrightarrow x = \varphi(P)$.

2 Racines et extensions de corps

2.1 Algébricité et transcendance

Définition 17. Soit L/K une extension, soit $a \in L$. On dit qu'il est algébrique sur K s'il existe $P \in K[X]$ tel que $P(a) = 0$. Il est dit transcendant s'il n'est pas algébrique. On dit que l'extension L/K est algébrique si tous les éléments de L sont algébriques sur K.

***Exemple* 18.** *i est algébrique sur $\mathbb{R}$, $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, π est transcendant sur $\mathbb{Q}$.*

Proposition 19. a algébrique sur K ssi $K(a) = K[a]$ ssi $[K(\alpha) : K] < \infty$.

Proposition 20. Si $[L : K] < \infty$ alors l'extension L/K est algébrique.

Corollaire 21. Si a, b sont algébriques sur K, alors $a + b$ et ab algébriques sur K.

Définition 22. Soit $a \in L$ algébrique sur K. L'ensemble $\{P \in K[X], P(a) = 0\}$ est un idéal de $K[X]$, il est donc engendré par un unique polynôme unitaire : celui-ci est appelé polynôme minimal de a sur K, et noté π_a.

***Exemple* 23.** *Le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$ sur $\mathbb{Q}$ et $X - \sqrt{2}$ sur $\mathbb{R}$.*

2.2 Adjonction de racines

Définition 24. Soit K/L une extension de corps, soit $a \in L$. a est dit algébrique sur K s'il existe $P \in K[X], P(a) = 0$.

Proposition 25. Soit $P \in K[X]$. Alors P est irréductible, si et seulement si, $K[X]/(P)$ est un corps.

Définition 26. Soit $P \in K[X]$ irréductible. On appelle corps de rupture de P une extension de corps L/K telle qu'il existe $\alpha \in L$ avec $P(\alpha) = 0$ et $L = K(\alpha)$.

Théorème 27. $K[X]/(P)$ est un corps de rupture de P engendré par K et $\overline{X}$, et si $L = K(\alpha), L' = K(\beta)$ sont deux corps de rupture de P, alors il existe un unique K-isomorphisme $\varphi : L \to L'$ tel que $\varphi(\alpha) = \beta$.

***Exemple* 28.** $\mathbb{C}$ *est le corps de rupture de* $P = X^2 + 1 \in \mathbb{R}[X]$.

***Exemple* 29.** $\mathbb{F}_4 \simeq \mathbb{F}_2/(X^2+X+1)$ *est le corps de rupture de* $X^2+X+1 \in \mathbb{F}_2[X]$.

Définition 30. Soit $P \in K[X]$.
On dit qu'une extension L/K est un corps de décomposition de P s'il existe $\lambda, \alpha_1, \cdots, \alpha_r \in L$ tel que sur L, $P = \lambda(X - \alpha_1)\cdots(X - \alpha_r)$ et $L = K(\alpha_1, \cdots, \alpha_r)$.

***Exemple* 31.** $\mathbb{C}$ *est un corps de décomposition de* $X^2 + 1 \in \mathbb{R}[X]$ *et* $\mathbb{Q}(j, \sqrt[3]{2})$ *est un corps de décomposition de* $X^3 - 2 \in \mathbb{Q}[X]$.

Proposition 32. Si L, L' sont deux corps de décomposition de P, alors ils sont K-isomorphes.

***Application* 33.** *Si* p *premier,* $n \in \mathbb{N}^*, q = p^n$, *le corps fini* $\mathbb{F}_q$ *est défini comme le corps de décomposition de* $X^q - X \in \mathbb{F}_p[X]$.

Théorème 34. P possède un corps de décomposition L, unique à K-isomorphisme près, et $[L : K] \leq n!$.

***Application* 35** (Théorème de l'élément primitif)**.** *Soit* K *un corps de caractéristique nulle, soit* L *extension de* K *de degré fini. Alors il existe* $x \in L$ *tel que* $L = K(x)$. *De plus,* L *extension de* K, *on a* $[L : K] \leq n \Leftrightarrow \forall x \in L, [K(x) : K] \leq n$.

3 Fonctions symétriques élémentaires

$\mathcal{S}_n$ agit sur $K[X_1, \cdots, X_n]$ par $\sigma \cdot P(X_1, \cdots, X_n) = P(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$.

Définition 36. $P \in K[X_1, \cdots, X_n]$ est dit symétrique si pour tout $\sigma \in \mathcal{S}_n$, on a $\sigma \cdot P = P$.

***Exemple* 37.** *Dans* $K[X_1, X_2]$, *les polynômes* $P = X_1 + X_2, Q = X_1X_2, R = X_1^2X_2 + X_1X_2^2$ *sont symétriques.*

Définition 38. Soit $k \leq n$. On définit Σ_k, le polynôme symétrique élémentaire de degré k de $K[X_1, \cdots, X_n]$, par $\Sigma_k = \sum_{\substack{H \subseteq [\![1,n]\!] \\ |H|=k}} \left(\prod_{i \in H} X_i \right)$.

***Exemple* 39.** *Dans* $K[X_1, X_2, X_3]$, *on a* $\Sigma_1 = X_1 + X_2 + X_3, \Sigma_2 = X_1X_2 + X_2X_3 + X_1X_3$, $\Sigma_3 = X_1X_2X_3$.

Théorème 40 (Relations coefficients-racines)**.** Si $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ de racines $x_1, \cdots, x_n$, alors pour tout $k \in [\![1, n]\!], a_{n-k} = (-1)\Sigma_k(x_1, \cdots, x_n)$.

Théorème 41 (Structure des polynômes symétriques)**.** Soit $P \in K[X_1, \cdots, X_n]$ polynôme symétrique. Alors il existe $T \in K[X_1, \cdots, X_n]$ tel que $P = T(\Sigma_1, \cdots, \Sigma_n)$.

4 Localisation des racines

Théorème 42 (Newton)**.** Soit $P(x) = (x-a_1)^{m_1} \cdots (x-a_r)^{m_r}$ fonction polynomiale réelle, avec $a_1 < \cdots < a_r$ et $\forall i, m_i \geq 1$.

Soit $x_0 > a_r$, et on pose, pour tout $n \in \mathbb{N}, x_{n+1} = x_n - \dfrac{P(x_n)}{P'(x_n)}$.

Alors $(x_n)_{n \in \mathbb{N}}$ converge en décroissant vers a_r, et on peut estimer la rapidité de convergence :

- Si $m_r = 1$, alors $\forall \varepsilon > 0, |x_n - a_r| = o(\varepsilon^n)$.
- Si $m_r \geq 2$, alors $\exists c > 0, |x_n - a_r| \sim c \left(1 - \dfrac{1}{m_r}\right)^n$.

Définition 43. Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in K[X]$.

On définit sa matrice compagnon par $C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$.

Proposition 44. Les racines de P sont exactement les valeurs propres de $C(P)$.

Définition 45. Soit $A = (a_{i,j})_{i,j} \in \mathcal{M}_n(\mathbb{C})$. Pour $i \in [\![1, n]\!]$, on définit le i-ème disque de Gershgorin de A comme le disque de centre $a_{i,i}$ et de rayon $\sum_{j \neq i} |a_{i,j}|$.

On définit le domaine de Gershgorin de A comme $\mathcal{G} = \bigcup_{i=1}^{n} D_i$.

Proposition 46. Le spectre de A est inclus dans $\mathcal{G}$.

Théorème 47. Soit $\mathcal{E}$ une composante connexe de $\mathcal{G}$, contenant p disques de Gershgorin. Alors il y a p valeurs propres de A dans $\mathcal{E}$, comptées avec multiplicité.

Développements

— Théorème de l'élément primitif.
— Méthode de Newton pour les polynômes.

Références

[1] V. Beck, J. Malick, G. Peyré, Objectif Agrégation, H&K.

[2] J.-P. Escofier, Théorie de Galois, Dunod.

[3] I. Gozard, Théorie de Galois, Ellipses.

[4] X. Gourdon, Les maths en tête - Algèbre, Ellipses.

[5] I. Nourdin, Agrégation de mathématiques - Épreuve orale, Dunod.

[6] E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques spéciales - Algèbre 1, Masson.

[7] D. Serre, Les matrices, Dunod.