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

1. Notation. Dans cette leçon, on considère un corps K.

1. Racines d'un polynôme

1.1. Racines et multiplicités

2. Définition. Une *racine* d'un polynôme $P \in K[X]$ est un élément $\alpha \in K$ vérifiant la divisibilité $X - a \mid P$ dans $K[X]$.
3. Exemple. Le polynôme $X^2 - X$ admet 0 et 1 comme racines dans K.
4. Proposition. Un élément $a \in K$ est une racine d'un polynôme $P \in K[X]$ si et seulement si $P(a) = 0$.
5. Exemple. Le polynôme $X^2 + 1$ n'admet pas de racines dans $\mathbf{R}$.
6. Définition. L'*ordre* ou la *multiplicité algébrique* d'une racine $a \in K$ d'un polynôme $P \in K[X]$ est l'entier

$$\max\{k \in \mathbf{N} \mid (X - \alpha)^k \mid P\}.$$

7. Proposition. Un polynôme de degré $n \geqslant 1$ admet au plus n racines comptées avec multiplicité.
8. Corollaire. On suppose que le corps K est infini. Alors tout polynôme $P \in K[X]$ vérifiant $P(x) = 0$ pour tout $x \in K$ est nul.
9. Exemple. Le résultat est faux lorsque le corps est fini : il suffit de considérer le polynôme $X^q - X$ sur le corps $\mathbf{F}_q$.
10. Application *(interpolation de Lagrange)*. Soient $a_1, \dots, a_n \in K$ des éléments deux à deux distincts. Soient $b_1, \dots, b_n \in K$ des éléments. Alors il existe un unique polynôme $P \in K[X]_{<n}$ tel que

$$\forall i \in [\![1, n]\!], \qquad P(a_i) = b_i.$$

11. Théorème. On suppose que le corps K est de caractéristique nulle. Soit $P \in K[X]$ un polynôme non nul. Alors un élément $a \in K$ est une racine du polynôme P d'ordre $\alpha \geqslant 1$ si et seulement si

$$F(a) = F'(a) = \dots = F^{(\alpha-1)}(a) = 0 \qquad \text{et} \qquad F^{(\alpha)}(a) \neq 0.$$

12. Contre-exemple. Le résultat est faux est caractéristique non nulle : le polynôme $X^3 \in \mathbf{F}_3[X]$ admet zéro comme racine d'ordre 3 et pourtant on a $(X^3)^{(3)} = 0$.

1.2. Polynômes irréductibles et corps algébriquement clos

13. Proposition. Un polynôme irréductible sur K de degré $\geqslant 2$ n'admet aucune racine dans K.
14. Contre-exemple. La réciproque est fausse : le polynôme $(X^2+1)^2$ n'admet pas de racines dans $\mathbf{Q}$ et pourtant il est réductible.
15. Proposition. Un polynôme de degré 2 ou 3 n'admettant pas de racines dans K est irréductible dans K.
16. Exemple. Le polynôme $X^2 + X + 1$ est irréductible sur $\mathbf{F}_2$.
17. Exemple. Le corps K est algébriquement clos si tout polynôme de $K[X]$ admet une racine dans K.
18. Proposition. Si le corps K est algébriquement clos, alors tout polynôme de $K[X]$ est scindé sur K.
19. Théorème *(d'Alembert-Gauss)*. Le corps $\mathbf{C}$ est algébriquement clos.
20. Application. Toute matrice à coefficients complexes est trigonalisable.
21. Corollaire. Les polynômes irréductibles sur $\mathbf{C}$ sont les polynômes de degré 1. Les polynômes irréductibles sur $\mathbf{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatifs.

1.3. Extensions de corps

22. Définition. Soit $P \in K[X]$ un polynôme irréductible. Un *corps de rupture* sur K du polynôme P est une extension L/K si le polynôme P admet une racine sur L.
23. Théorème. Un polynôme irréductible $P \in K[X]$ sur K admet un corps de rupture qui est unique à isomorphisme près : il s'agit du quotient $K[X]/(P)$.
24. Définition. Soit $P \in K[X]$ un polynôme. Un *corps de décomposition* sur K du polynôme P est une extension L/K telle que
    - le polynôme P soit scindé sur L ;
    - ce soit la plus petite extension variant ce dernier point.
25. Exemple. Le corps $\mathbf{C}$ est un corps de décomposition du polynôme $X^2 + 1$ sur $\mathbf{R}$.
26. Théorème. Un polynôme irréductible $P \in K[X]$ sur K admet un corps de décomposition qui est unique à isomorphisme près.
27. Définition-théorème. Soient p un nombre premier et $n \in \mathbf{N}^*$ un entier non nul. Alors il existe un corps à $q \coloneqq p^n$ éléments. De plus, il s'agit d'un corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$. En particulier, il est unique à isomorphisme près, noté $\mathbf{F}_q$.
28. Définition. On considère un corps K de caractéristique $p \geqslant 0$ et un entier $n > 0$ avec $p \nmid n$. Une *racine n-ième de l'unité* est un élément $\xi \in K$ tel que $\xi^n = 1$. Elle est *primitive* si $\xi^d \neq 1$ pour $d < n$. On note $\mu_n(K)$ (resp. $\mu_n^\times(K)$) les ensembles de racines n-ième (resp. primitives). Soit K_n un corps de décomposition du polynôme $X^n - 1$ sur K. Le *n-ième polynôme cyclotomique* est le polynôme

$$\Phi_{n,K} \coloneqq \prod_{\xi \in \mu_n^\times(K_n)} (X - \xi) \in K_n[X].$$

29. Proposition. On a $\Phi_n \coloneqq \Phi_{n,\mathbf{Q}} \in \mathbf{Z}[X]$. Soit $\sigma \colon \mathbf{Z} \longrightarrow K$ l'unique morphisme d'anneaux que l'on étend en un morphisme d'anneaux $\sigma \colon \mathbf{Z}[X] \longrightarrow K[X]$ en envoyant l'indéterminée X sur elle-même. Alors $\Phi_{n,K} = \sigma(\Phi_{n,\mathbf{Q}})$.
30. Théorème. Le polynôme Φ_n est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$. — D1 —
31. Corollaire. Soit $\xi \in \mu_n^\times(\mathbf{C})$. Alors son polynôme minimal sur $\mathbf{Q}$ est le polynôme Φ_n. En particulier, on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

2. Polynômes symétriques

32. Notation. Dans la suite, on considère un anneau commutatif unitaire intègre A.

2.1. Définitions et relations coefficients-racines

33. Définition. Un polynôme $P \in A[X_1, \dots, X_n]$ est *symétriques* si
$$\forall \sigma \in \mathfrak{S}_n, \qquad \sigma \cdot P(X_1, \dots, X_n) \coloneqq P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$
Le groupe $\mathfrak{S}_n$ agit donc sur l'ensemble $A[X_1, \dots, X_n]$. L'ensemble des polynômes symétriques est noté $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$.

34. Exemple. Le polynôme $X^2 + XY + 1$ est symétrique. Les polynômes
$$S_k \coloneqq X_1^k + \dots + X_n^k \quad \text{avec} \quad k \in \mathbf{N}$$
sont symétriques.

35. Définition. Les *polynômes symétriques élémentaires* sont les polynômes
$$\Sigma_p \coloneqq \sum_{1 \leqslant i_1 < \dots < i_p \leqslant n} X_{i_1} \cdots X_{i_p}$$
pour un entier $p \in [\![1, n]\!]$.

36. Exemple. On a $\Sigma_1 = X_1 + \dots + X_n$ et $\Sigma_n = X_1 \cdots X_n$.

37. Proposition. Dans l'anneau $A[X_1, \dots, X_n, T]$, on a
$$(T - X_1) \cdots (T - X_n) = T^n + \sum_{p=1}^{n} (-1)^p \Sigma_p T^{n-p}.$$
En particulier, soit $X^n + a_1 X^{n-1} + \dots + a_n \in K[X]$ un polynôme scindé sur K de racines $\alpha_1, \dots, \alpha_n \in K$. Alors pour tout $i \in [\![1, n]\!]$, on a
$$(-1)^i a_i = \Sigma_i(\alpha_1, \dots, \alpha_n).$$

2.2. Structure des polynômes symétriques

38. Théorème. Soit $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ un polynôme symétrique. Alors il existe un unique polynôme $\Phi \in A[X_1, \dots, X_n]$ tel que $P = \Phi(\Sigma_1, \dots, \Sigma_n)$.

39. Corollaire. Soit $P \in \mathbf{Z}[X]$ un polynôme unitaire. Notons $\alpha_1, \dots, \alpha_n \in \mathbf{C}$ ses racines. Soit $F \in \mathbf{Z}[X_1, \dots, X_n]^{\mathfrak{S}_n}$ un polynôme symétrique. Alors $F(\alpha_1, \dots, \alpha_n) \in \mathbf{Z}$.

40. Proposition *(formule de Newton)*. Pour tout entier $k \in [\![1, n-1]\!]$, on a
$$S_k - \Sigma_1 S_{k-1} + \dots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k \Sigma_k k = 0$$
et, pour tout entier $p \in \mathbf{N}$, on a
$$S_{p+n} - \Sigma_1 S_{p+n-1} + \dots + (-1)^{n-1} \Sigma_{n-1} S_{p+1} + (-1)^n \Sigma_n S_p = 0.$$

41. Exemple. On peut calculer les polynômes
$$S_1 = \Sigma_1,$$
$$S_2 = \Sigma_1^2 - 2\Sigma_2,$$
$$S_3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$$
et réciproquement les polynômes
$$\Sigma_1 = S_1,$$
$$\Sigma_2 = \tfrac{1}{2} S_1^2 - \tfrac{1}{2} S_2,$$
$$\Sigma_3 = \tfrac{1}{6} S_1^3 - \tfrac{1}{2} S_1 S_2 + \tfrac{1}{3} S_3$$

3. Recherche, comptage et localisation des racines

3.1. Liens avec la réduction

42. Théorème. Soient E un K-espace vectoriel de dimension finie. Alors les valeurs propres dans K d'un endomorphisme $u \in \mathscr{L}(E)$ sont exactement les racines de son polynôme caractéristique (respectivement minimal) dans K.

43. Exemple. Pour un polynôme $P \in \mathbf{K}[X]$ avec $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$, les valeurs propres de sa matrice compagnon C_P sont ses racines.

44. Théorème *(décomposition QR)*. Soit $A \in \mathrm{GL}_n(\mathbf{C})$ une matrice inversible. Alors il existe un unique couple $(Q, R) \in \mathscr{M}_n(\mathbf{C})$ tel que
- $A = QR$;
- la matrice Q soit unitaire ;
- la matrice R soit triangulaire supérieure où les coefficients de sa diagonale sont positifs.

45. Théorème *(méthode QR)*. Soit $A \in \mathrm{GL}_n(\mathbf{C})$ une matrice dont les valeurs propres sont de modules deux à deux distincts. On peut alors trouver une matrice $P \in \mathrm{GL}_n(\mathbf{C})$ et des complexes $\lambda_1, \dots, \lambda_n \in \mathbf{C}$ triés par modules décroissants tels que
$$A = P \Lambda P^{-1} \quad \text{avec} \quad \Lambda \coloneqq \operatorname{diag}(\lambda_1, \dots, \lambda_n).$$
De plus, on suppose que la matrice P admet une décomposition LU. Définissons la suite $(A_k)_{k \in \mathbf{N}}$ de matrice de la manière suivante : D2
- on pose $A_0 = A$;
- pour tout entier $k \in \mathbf{N}$, on pose $A_{k+1} \coloneqq R_k Q_k$ où le couple (Q_k, R_k) est la décomposition QR de la matrice A_k.

Alors la suite $(A_k)_{k \in \mathbf{N}}$ converge coefficient par coefficient vers la matrice Λ.

46. Remarque. Pour un polynôme $P \in \mathbf{C}[X]$, on applique la méthode QR à la matrice C_P lorsque les hypothèses sont vérifiées pour trouver les racines du polynôme P.

3.2. Localisation et comptages des racines dans le cas réel ou complexe

47. Théorème. Soit $X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbf{C}[X]$ un polynôme dont on note les racines $\alpha_1, \dots, \alpha_d \in \mathbf{C}$. Alors le réel $r_0 \coloneqq \max(|\alpha_1|, \dots, |\alpha_n|)$ vérifie
$$r_0 \leqslant \max(1, |a_1| + \dots + |a_n|),$$
$$r_0 \leqslant 1 + \max(|a_1|, \dots, |a_n|)$$

48. Définition. La *mesure de Mahler* d'un polynôme
$$P \coloneqq a_d X^d + \dots + a_0 = a_d (X - \alpha_1) \cdots (X - \alpha_n) \in \mathbf{C}[X] \quad \text{avec} \quad a_d \neq 0$$
est le réel
$$M(P) \coloneqq a \max(1, |\alpha_1|) \cdots \max(1, |\alpha_n|)$$
et sa norme 2 est le réel
$$\|P\| \coloneqq (|a_0|^2 + \dots + |a_n|^2)^{1/2}.$$

49. Théorème. Soit $P \coloneqq a_d X^d + \dots + a_0 \in \mathbf{C}[X]$ un polynôme non constant. Alors
$$M(P)^2 + |a_0 a_d|^* 2 M(P)^{-2} \leqslant \|P\|^2.$$

50. Proposition. Soit $P \coloneqq a_n X^n + \dots + a_0 \in \mathbf{C}[X]$ un polynôme non constant

vérifiant

$$|c_j| > \sum_{i \neq j} |c_i|$$

pour une certain indice $j \in [\![0, n]\!]$. Alors ce polynôme P possède exactement j racines de module < 1 et aucune de module 1.

51. Proposition. Soient $m \geqslant 1$ un entier et $P \coloneqq X^n + a_1 X^{n-1} + \cdots + a_0 \in \mathbf{R}[X]$ un polynôme avec $n \geqslant m$ et $a_i \geqslant 0$ pour tout $i \in [\![1, m-1]\!]$. Alors toute racine $x \in \mathbf{R}$ du polynôme P vérifie

$$x < 1 + A^{1/m} \quad \text{avec} \quad A \coloneqq \max(-a_m, \dots, -a_n, 0).$$

52. Définition. La *suite de Sturm* d'un polynôme $P \in \mathbf{R}[X]$ à coefficients réels est la suite finie $(P_0, \dots, P_k)$ de polynômes vérifiant

- $P_0 = P$ et $P_1 = P'$;
- pour tout $i \in [\![1, k-1]\!]$, le polynôme f_{i+1} est l'opposé du reste de la division euclidienne de P_{i-1} par P_i ;
- $P_k = 0$.

Pour un réel $x \in \mathbf{R}$ tel que $P(x) \neq 0$, on définit le nombre $s_P(x) \in \mathbf{N}$ de changements de signes dans la suite $(P_0(x), \dots, P_k(x))$.

53. Théorème *(Sturm).* Soient $P \in \mathbf{R}[X]$ un polynôme à coefficients réels et $a, b \in \mathbf{R}$ deux réels avec $a < b$ tels que $P(a) \neq 0$ et $P(b) \neq 0$. Alors le nombre de racines du polynôme f sur le segment $[a, b]$ vaut $s_P(a) - s_P(b)$.

[1] Philippe Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation.* 3e tirage. Masson, 1982.

[2] Xavier Gourdon. *Algèbre.* 2e édition. Ellipses, 2009.

[3] Maurice Mignotte. *Mathématiques pour le calcul formel.* Presses Universitaires de France, 1989.

[4] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.