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

Pandou

2 mai 2022

1 Racines de polynômes

1.1 Définitions

Définition 1. *On dit que $x \in K$ est une racine de P si $P(x) = 0$.*

Théorème 2. *Soit $a \in K$ et $P \in K[X]$. Alors, a est racine de P si, et seulement si, $X - a$ divise P.*

Définition 3. *On dit que a est racine de multiplicité k de P si $(X-a)^k$ divise P mais pas $(X-a)^{k+1}$.*

Proposition 4. *Soit $P \in K[X]$ et $a_1, ..., a_r$ des racines de multiplicité $k_1, ..., k_r$, alors il existe $Q \in K[X]$ tel que*

$$P = (X-a_1)^{k_1}...(X-a_r)^{k_r}Q(X) \qquad et \qquad Q(a_i) \neq 0$$

Corollaire 5. *Si K est de caractéristique nulle, alors une racine de P est de multiplicité k si, et seulement si, $\forall i \leqslant k-1, P^{(i)}(a) = 0$ et $P^{(k)}(a) \neq 0$.*

Corollaire 6. *Si $P \in K[X]$ de degré n, alors P a au plus n racines comptées avec multiplicité.*

Corollaire 7. *L'application $P \in K[X] \longmapsto P \in \mathcal{F}(K, K)$ est injective si, et seulement si, K est infini.*

Application 8 : Il y a $\dfrac{q-1}{2}$ carrés non nuls dans $\mathbb{F}_q$. Ce sont exactement les éléments qui vérifient $x^{\frac{q-1}{2}} = 1$.

Application 9 : Soit $x_1, ..., x_n \in K$ deux à deux distincts et $y_1, ..., y_n \in K$, alors il existe un unique polynôme de degré au plus n tel que $\forall i, P(x_i) = y_i$.

Application 10 : Soit K un corps, alors tout sous-groupe fini de K^* est cyclique.

Application 11 : Si $\overline{\mathbb{F}_p}$ est une clôture algébrique de $\mathbb{F}_p$, alors

$$\mathbb{F}_q \simeq \left\{x \in \overline{\mathbb{F}_p}, x^q = x\right\}$$

1.2 Corps de rupture, corps de décomposition

Définition 12. *Soit $P \in K[X]$ irréductible, on dit que L/K est un corps de rupture de P si L est engendré par une racine de P.*

Théorème 13. *Soit $P \in K[X]$ irréductible, alors il existe un corps de rupture de P sur K, unique à isomorphisme près : il est isomorphe à $K[X]/(P)$.*

Exemples 14 :

- $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1.
- $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2. On remarque qu'il ne contient pas toutes les racines de X^3-2.

Théorème 15. *Soit $P \in K[X]$ de degré $\geqslant 1$. Alors, P est irréductible sur K si, et seulement si, P n'admet aucune racine dans les extensions L/K de degré $\leqslant \dfrac{n}{2}$.*

Exemple 16 : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Théorème 17. *Soit $P \in K[X]$ irréductible de degré n et L/K une extension de degré m avec $m \wedge n = 1$, alors P est irréductible sur L.*

Exemple 18 : $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$.

Définition 19. *Soit $P \in K[X]$ de degré n. Un corps de décomposition de P est une extension L/K dans laquelle P est scindé et qui est engendrée par les racines de P.*

Théorème 20. *Il existe, à isomorphisme près, un unique corps de décomposition de P sur K.*

Application 21 : $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

1.3 Clôture algébrique

Théorème 22. *Les conditions suivantes sont équivalentes :*

1. *Tout polynôme de degré $\geqslant 1$ de $K[X]$ est scindé sur K.*
2. *Tout polynôme de degré $\geqslant 1$ de $K[X]$ a une racine dans K.*

3. *Les irréductibles de $K[X]$ sont les polynômes de degré 1.*
4. *Toute extension algébrique de K est égale à K lui-même.*

On dit que K est algébriquement clos.

Proposition 23. *Tout corps algébriquement clos est infini.*

Théorème 24 (D'Alembert-Gauss). *$\mathbb{C}$ est algébriquement clos.*

Définition 25. *Soit K un corps, une clôture algébrique de K est une extension algébrique $\overline{K}/K$ telle que $\overline{K}$ est algébriquement clos.*

Théorème 26 (Admis). *Tout corps admet une unique clôture algébrique, à isomorphisme près.*

2 Polynômes symétriques

2.1 Relations coefficients-racines

Définition 27. *Soit $\alpha_1, ..., \alpha_n \in K$, on pose*

$$\sigma_k(\alpha_1, ..., \alpha_n) = \sum_{1 \leqslant i_1 < ... < i_k \leqslant n} \alpha_{i_1} ... \alpha_{i_k}$$

Exemple 28 : $\sigma_1 = \sum_{i=1}^{n} \alpha_i$ et $\sigma_n = \prod_{i=1}^{n} \alpha_i$.

Théorème 29. *Soit $P = a_n X^n + ... + a_1 X + a_0 \in K[X]$ de degré $n \geqslant 1$, scindé sur K. Soit $\alpha_1, ..., \alpha_n$ ses racines, comptées avec multiplicitées, alors*

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Application 30 : Les racines de $P(X) = \sum_{k=0}^{p} (-1)^k \binom{2p+1}{2k+1} X^{p-k}$ sont les $\cotan^2\left(\frac{k\pi}{2p+1}\right)$, on en déduit le calcul

$$\sum_{n \geqslant 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Théorème 31 (Relations de Newton). *Soit $\alpha_1, ..., \alpha_n \in K$, on note $S_p = \sum_{i=1}^{n} \alpha_i^p$. Alors, on a*

1. *Si $p > n$, alors*
$$S_p - \sigma_1 S_{p-1} + ... + (-1)^k \sigma_k S_{p-k} + ... + (-1)^n \sigma_n S_{p-n} = 0$$
2. *Si $p \leqslant n$, alors*
$$S_p - \sigma_1 S_{p-1} + ... + (-1)^k \sigma_k S_{p-k} + ... + (-1)^{p-1} \sigma_{p-1} S_1 + (-1)^p p \sigma_p = 0$$

Application 32 : Soit $A \in M_n(\mathbb{C})$, on pose $A_0 = A$ et $A_{k+1} = A\left(A_k - \frac{1}{k+1}\mathrm{Tr}(A_k) I_n\right)$, alors

$$\chi_A(X) = X^n + \sum_{k=1}^{n} \left(-\frac{1}{k}\mathrm{Tr}(A_{k-1})\right) X^{n-k}$$

Application 33 : Grâce au résultat de l'application 30, on peut en déduire aussi que $\sum_{n \geqslant 1} \frac{1}{n^4} = \frac{\pi^4}{90}$.

2.2 Théorème de structure

Définition 34. *Soit A un anneau intègre, on a une action de $\mathfrak{S}_n$ sur $A[X_1, ..., X_n]$ via*

$$\sigma \cdot P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$$

On dit que $P \in A[X_1, ..., X_n]$ est symétrique s'il est invariant sous l'action de $\mathfrak{S}_n$.

Exemples 35 : σ_p et S_p définissent des polynômes symétriques.

Théorème 36 (Admis). *Soit $P \in A[X_1, ..., X_n]$ symétrique, alors il existe $Q \in A[X_1, ..., X_n]$ tel que*

$$P(X_1, ..., X_n) = Q(\Sigma_1, ..., \Sigma_n)$$

DEVELOPPEMENT 1

Théorème 37. *Soit $P \in \mathbb{Z}[X]$ unitaire, dont toutes les racines sont de module $\leqslant 1$ et $P(0) \neq 0$. Alors, les racines de P sont des racines de l'unité.*

Application 38 : Il n'y a qu'un nombre fini de sous-groupes de $GL_n(\mathbb{Z})$ à isomorphisme près.

3 Localisation des racines

3.1 Application à l'irréductibilité

Proposition 39.
1. *Un polynôme irréductible sur K n'a pas de racines dans K.*
2. *Les polynômes irréductibles de $K[X]$ de degré $\leqslant 3$ sont exactement ceux qui ont une racine dans K.*

Remarque 40 : La réciproque de 1. est fausse : $(X^2+1)^2$ est réductible et n'a pas de racines dans $\mathbb{R}$.

Théorème 41 (Gauss-Lucas). *Soit $P \in \mathbb{C}[X]$, alors les racines de P' sont dans l'enveloppe convexe de l'ensemble des racines de P.*

DEVELOPPEMENT 1

Lemme 42. *Soit $P(X) = a_m X^m + ... + a_1 X + a_0 \in \mathbb{Z}[X]$, on suppose que a_m et a_{m-1} sont positifs et on note $M = \sup_{i \leqslant m-2} |a_i|$. Alors, les racines α de P vérifient*

$$\mathrm{Re}(\alpha) \leqslant 0 \qquad ou \qquad |\alpha| < \frac{1+\sqrt{1+4M}}{2}$$

Théorème 43 (Critère de Cohn). *Soit $b \geqslant 3$, p un nombre premier dont l'écriture en base b est $a_m b^m + ... + a_1 b + a_0$, alors le polynôme $P(X) = a_m X^m + ... + a_1 X + a_0$ est irréductible dans $\mathbb{Z}[X]$.*

Application 44 :
- $6X^4 + 5X^3 + 5X^2 + 3X + 7$ est irréductible sur $\mathbb{Z}[X]$.
- $X^4 + 1$ est irréductible sur $\mathbb{Z}[X]$ car 257 en base 4 s'écrit $\overline{10001}^4$.

3.2 Application à la réduction

Proposition 45. *Les racines de χ_A sont exactement les valeurs propres de A.*

Application 46 : Si A a n valeurs propres distinctes, alors A est diagonalisable.

Théorème 47. *χ_A est scindé sur K si, et seulement si, A est trigonalisable.*

Corollaire 48. *Dans $M_n(\mathbb{C})$, toute matrice est trigonalisable.*

Application 49 : L'ensemble des matrices diagonalisables est dense dans $M_n(\mathbb{C})$.

Théorème 50. *A est diagonalisable si, et seulement s'il est annulé par un polynôme scindé à racines simples.*

Proposition 51. *Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in M_n(\mathbb{C})$ et $R_i = \sum_{j \neq i} |a_{i,j}|$. Alors, on a*

$$\mathrm{Sp}(A) \subset \bigcup_{i=1}^{n} \{z \in \mathbb{C}, |z - a_{i,i}| \leqslant R_i\}$$

3.3 Résultant et discriminant

Définition 52. *Soit $P \in \mathbb{C}_p[X]$ et $Q \in \mathbb{C}_q[X]$. La matrice de l'application linéaire*

$$(U,V) \in \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X] \longmapsto UP + VQ \in \mathbb{C}_{p+q-1}[X]$$

dans les bases canoniques $(1,...,X^p)$ et $(1,...,X^q)$ est appelée matrice de Sylvester. Son déterminant, noté $\mathrm{Res}(P,Q)$, est appelé le résultant de P et Q.

Théorème 53. *$\mathrm{Res}(P,Q) = 0$ si, et seulement si, P et Q ont une racine commune.*

Proposition 54. *Soit $P, Q \in \mathbb{C}[X]$ tel que Q ne divise pas P, soit R le reste de la division de P par Q, on note $r = \deg(R)$, alors*

$$\mathrm{Res}(P,Q) = (-1)^{pq} b_q^{p-r} \mathrm{Res}(Q,R)$$

Remarque 55 : L'algorithme d'Euclide permet donc de calculer le résultant de deux polynômes.

Définition 56. *Le discriminant de P, noté $\mathrm{disc}(P)$ est défini comme*

$$\delta(P) = (-1)^{\frac{p(p-1)}{2}} \frac{\mathrm{Res}(P,P')}{a_p}$$

Exemple 57 :
- Si $P = aX^2 + bX + c$, alors $\delta(P) = b^2 - 4ac$.
- Si $P = X^3 + pX + q$, alors $\delta(P) = -4p^3 - 27q^2$.

Proposition 58. *Si $P = \lambda(X - \alpha_1)...(X - \alpha_p)$, alors*

$$\delta(P) = \lambda^{2p-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Application 59 : Soit $P = a_d X^d + ... + a_0 \in \mathbb{Z}[X]$, on note $C = |a_d| + \max_{1 \leqslant i \leqslant d-1} |a_i|$ et α_i les racines de P Alors,

$$\forall d \geqslant 3, \inf_{\alpha_i \neq \alpha_j} |\alpha_i - \alpha_j| \geqslant (2C)^{-\frac{d(d-1)}{2}+1}$$

Références :

- FGN, Algèbre 1 et 2.
- Gourdon, Algèbre.
- Gozard, Théorie de Galois.
- Perrin, Cours d'algèbre.
- Risler, Algèbre pour la L3.
- Tauvel, Algèbre pour l'Agrégation.