

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

Cadre : \mathbb{K} est un corps.

1. Racines d'un polynôme. —

1. Définition et premières propriétés. —

- Def : Soit $P \in K[X]$. Un élément $\lambda \in \mathbb{K}$ est une racine de P ssi $P(\lambda) = 0$.
- Ex : Pour $n \geq 1$, les $e^{2i\pi \frac{k}{n}}$ sont des racines de $X^n - 1$.
- Pro : Le polynôme $X - \lambda$ divise P dans $\mathbb{K}[X]$ si et seulement si $P(\lambda) = 0$.
- Def : Pour λ une racine de P, la multiplicité de λ est le plus grand entier d tel que $(X - \lambda)^d$ divise P dans $\mathbb{K}[X]$.
- Pro : Un polynôme P de degré $n \geq 1$ admet au plus n racines comptées avec leurs multiplicités dans \mathbb{K} .
P admet exactement n racines dans \mathbb{K} ssi il est produit de polynômes de degré 1 dans $\mathbb{K}[X]$. On dit alors que P est scindé sur \mathbb{K} .
- Contre-ex : Dans $\mathbb{Z}/81\mathbb{Z}$, 0,9,27 sont racines de $P(X) = X^2$. Cela est dû au fait que cet anneau n'est pas intègre.
- Pro : Si $\text{car}(\mathbb{K}) = 0$, alors λ est une racine de P de multiplicité d ssi $P(\lambda) = P'(\lambda) = \dots = P^{(d-1)}(\lambda) = 0$, et $P^{(d)}(\lambda) \neq 0$.
- Contre-ex : Pour $\mathbb{K} = \mathbb{F}_p$, $P(X) = X^p - 1$ ne possède que des racines de multiplicité 1. Pourtant, $P'(X) = 0$, donc toute racine de P annule aussi P'.
- Pro : Pour $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ distincts, il existe un unique polynôme P unitaire de degré n qui s'annule en les λ_i . Il s'écrit $P(X) = \prod_i (X - \lambda_i)$.
- App : Pour $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ distincts, pour $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, il existe au moins un polynôme de degré $\leq n$ tel que $P(\lambda_i) = \alpha_i \forall i$.
- Pro : Si \mathbb{K} est infini, alors le seul polynôme P qui s'annule sur une \mathbb{K} tout entier (ou une partie infinie de \mathbb{K}) est le polynôme nul : Le morphisme $P \mapsto (x \mapsto P(x))$ est injectif.
- Contre-ex : Si \mathbb{K} est un corps fini, $P(X) = \prod_{\lambda \in \mathbb{K}} (X - \lambda)$ s'annule sur \mathbb{K} tout entier mais n'est pas le polynôme nul.
- Def : P est dit irréductible sur \mathbb{K} si il n'est pas constant et si $P = RQ$, $P, Q \in \mathbb{K}[X] \Rightarrow R$ ou Q est constant.
- Ex : Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.
- Pro : Soit P de degré ≥ 2 . Si P est irréductible sur \mathbb{K} , alors il n'admet pas de racines sur \mathbb{K} .
- Contre-ex : $P(X) = (X^2 + 1)^2$ n'admet pas de racines sur \mathbb{Q} mais est réductible.
La réciproque est cependant vraie pour les polynômes de degré 2 ou 3.

2. Extensions de corps par adjonction de racines. —

- Def : Soit $P \in \mathbb{K}[X]$ irréductible sur \mathbb{K} . Un corps de rupture de P sur \mathbb{K} est une extension de corps L sur \mathbb{K} telle que P admet une racine λ dans L, et telle que L est engendré par \mathbb{K} et λ .

- Pro : Pour tout $P \in \mathbb{K}[X]$ irréductible, le corps $\mathbb{K}[X]/(P)$ est un corps de rupture de P sur \mathbb{K} .
De plus, le corps de rupture de P sur \mathbb{K} est une extension finie de degré n sur \mathbb{K} et est unique à isomorphisme de \mathbb{K} – algèbre près.
- Ex : \mathbb{C} est le corps de rupture de $X^2 + 1$ sur \mathbb{R} . Les polynômes $X^p + X + 1$ sont irréductibles sur \mathbb{F}_p . Cela permet de construire des corps à p^p éléments.
- Pro : Soit $P \in \mathbb{K}[X]$ de degré $n \geq 2$. P est irréductible sur \mathbb{K} ssi P n'admet aucune racine dans toute extension de corps finie de degré $\leq \lceil \frac{n}{2} \rceil$.
- Def : Soit L une extension de corps sur \mathbb{K} , $P \in \mathbb{K}[X]$ de degré n. L est un corps de décomposition de P sur \mathbb{K} si P est scindé dans L et si L est engendré par \mathbb{K} et par les racines de P.
- Pro : Pour tout polynôme P de degré ≥ 1 , il existe un corps de décomposition de P sur \mathbb{K} . Ce corps de décomposition est une extension finie de degré $\leq n!$, et est unique à isomorphisme de \mathbb{K} – algèbre près.
- Ex : $\mathbb{Q}(\sqrt{2})$ est le corps de décomposition de $X^2 - 2$ sur \mathbb{Q} . $\mathbb{Q}(\sqrt{2}, i)$ est le corps de décomposition de $X^4 - 1$ sur \mathbb{Q} .
- Ex : $\mathbb{Q}(\sqrt[3]{2}, j)$ est le corps de décomposition de $X^3 - 2$ sur \mathbb{Q} , et est une extension de degré $3! = 6$ sur \mathbb{Q} .
- App : Pour tout p premier et pour tout $q = p^r$, il existe un corps fini à q éléments. Il est à isomorphisme près le corps de décomposition de $X^q - X$ sur \mathbb{F}_p . On le note \mathbb{F}_q .

3. Algébricité et transcendance. —

- Def : Soit L une extension de corps sur \mathbb{K} . Un $x \in L$ est dit algébrique sur \mathbb{K} s'il existe $P \in \mathbb{K}[X]$ tel que $P(x) = 0$. Il est dit transcendant sinon.
L est appelée extension algébrique de \mathbb{K} si tous ses éléments sont algébriques sur \mathbb{K} .
- Pro : Les extensions finies sont algébriques.
- Ex : \mathbb{C} est une extension algébrique de \mathbb{R} . \mathbb{R} n'est pas une extension algébrique de \mathbb{C} car e et π sont transcendants. $\mathbb{K}(T)$ n'est pas une extension algébrique de \mathbb{K} car T est transcendant sur \mathbb{K} .
- Ex : Pour p_n le n-ième nombre premier et $F_n := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$, $F = \cup_n F_n$ est une extension algébrique de \mathbb{Q} de degré infini.
Pour $q = p^r$, $F = \cup_n \mathbb{F}_{q^{n!}}$ est une extension algébrique de \mathbb{F}_q de degré infini.
- Def : Un corps \mathbb{K} est dit algébriquement clos ssi tout polynôme de degré ≥ 1 est scindé sur \mathbb{K} , ssi tout polynôme de degré ≥ 1 admet une racine sur \mathbb{K} , ssi les seuls irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1, ssi toute extension algébrique sur \mathbb{K} est triviale.
- Ex : $\mathbb{Q}, \mathbb{R}, \mathbb{F}_q$ ne sont pas algébriquement clos.
- Théorème de d'Alembert-Gauss : \mathbb{C} est algébriquement clos.
- Cor : Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine réelle.
- App : Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.

- Rem : \mathbb{Q} et \mathbb{F}_q admettent des polynômes irréductibles de degré aussi grand que l'on veut.
- Ex : $\cup_n \mathbb{F}_{p^n}$ est algébriquement clos.

2. Polynômes symétriques, fonctions symétriques élémentaires. —

Dans cette partie, A désigne un anneau commutatif unitaire.

1. Définition et relations coefficients-racines. —

- Pro : Soit $n \geq 1$. Le groupe des permutations Σ_n agit sur $A[X_1, \dots, X_n]$ par $\sigma.P(X_1, \dots, X_n) := P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.
- Def : On appelle polynôme symétrique un polynôme P dans $A[X_1, \dots, X_n]^{\Sigma_n}$. On a $\sigma.P = P \forall \sigma \in \Sigma_n$.
- Def+Pro : Pour $1 \leq k \leq n$, on définit $\Sigma_k(X_1, \dots, X_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$. Ces polynômes sont symétriques, et sont appelés polynômes symétriques élémentaires.
- Ex : Pour $n=2$, $\Sigma_0 = 1$, $\Sigma_1 = X_1 + X_2$, $\Sigma_2 = X_1 X_2$.
- Ex : Le déterminant de Vandermonde V_n n'est pas un polynôme symétrique en les coefficients, mais son carré si.
- Thm : Relations coefficients-racines : Soit $P \in A[X]$ et $(\alpha_1, \dots, \alpha_n)$. On a l'équivalence :
 - $P(X) = (X - \alpha_1) \dots (X - \alpha_n)$.
 - $P(X) = X^n + a_{n-1} X^{n-1} + \dots + a_0$ avec $a_{n-i} = (-1)^i \Sigma_i(\alpha_1, \dots, \alpha_n)$.
- Pro : Formules de Newton : En posant $S_k(X_1, \dots, X_n) = X_1^k + \dots + X_n^k$, on a :
 - $\forall 1 \leq k \leq n$, $S_k - \Sigma_1.S_{k-1} + \dots + (-1)^{k-1} \Sigma_{k-1}.S_1 + (-1)^k k \Sigma_k = 0$.
 - $\forall k \geq n$, $S_k - \Sigma_1.S_{k-1} + \dots + (-1)^{k-1} \Sigma_{k-1}.S_1 + (-1)^n S_{k-n} \Sigma_n = 0$
- App : Caractérisation des matrices nilpotentes : Soit $A \in M_n(\mathbb{K})$. A est nilpotente sse $\forall 1 \leq k \leq n$, $Tr(A^k) = 0$.

2. Structure des polynômes symétriques. —

- Def : Poids d'un monôme.
- Théorème de structure des polynômes symétriques : L'application $P \mapsto P(\Sigma_1, \dots, \Sigma_n)$ est un isomorphisme d'anneaux A -linéaire entre $A[X_1, \dots, X_n]$ et $A[\Sigma_1, \dots, \Sigma_n]^{\Sigma_n}$. Ainsi, tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.
- Algorithme de factorisation d'un polynôme symétrique : Entrées : P . Sortie : S tel que $P(\Sigma_1, \dots, \Sigma_n) = P$. Initialisation : $S=0$. Pour P polynôme symétrique, tant que le monôme de plus haut degré pour l'ordre lexicographique n'est pas constant, regarder le monôme $X_1^{a_1} \dots X_n^{a_n}$, poser $Q = X_1^{a_1 - a_2} \dots X_2^{a_2 - a_3} \dots X_{n-1}^{a_{n-1} - a_n} \dots X_n^{a_n}$, poser $S = S + Q$, et $P = P - Q(\Sigma_1, \dots, \Sigma_n)$. Lorsque P est constant, renvoyer $S + P(0)$.
- Def : Comme A_n est un sous-groupe de Σ_n , on peut aussi définir l'ensemble des polynômes alternés $A[X_1, \dots, X_n]^{A_n}$

- Thm : Soit A intègre. Pour $V_n = \prod_{i < j} (X_i - X_j)$, $U_n = \prod_{i < j} (X_i + X_j)$, le polynôme $W_n := \frac{V_n + U_n}{2}$ est à coefficients entiers, et tout polynôme $P \in A[X_1, \dots, X_n]$ alterné s'écrit $P = Q + W_n.R$ avec Q, R symétriques.

3. Discriminant. —

- Def : Pour $P \in \mathbb{K}[X]$ de degré $n \geq 2$, pour L le corps de décomposition de P sur \mathbb{K} et $\alpha_1, \dots, \alpha_n$ les racines de P , on définit $disc(P) := a_n^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2$.
- Pro : $disc(P)$ est un polynôme symétrique en les $\alpha_1, \dots, \alpha_n$ à coefficients entiers. Il existe $Q \in \mathbb{Z}[X_1, \dots, X_n, X_{n+1}]$ tel que $disc(P) = Q(a_0, \dots, a_n)$ car les polynômes symétriques élémentaires en les α_i sont des polynômes en les a_i . Ainsi, $disc(P) \in \mathbb{K}$, et on peut étendre la définition du discriminant à tout anneau A intègre.
- Pro : $P \in K[X]$ est à racines simples ssi $disc(P) \neq 0$.
- Rem : Ce résultat s'étend à tout anneau intègre A grâce à l'injectivité du morphisme d'évaluation sur un corps infini.
- Ex : Pour $P(X) = aX^2 + bX + c$, $disc(P) = b^2 - 4ac$.

3. Localisation et comptage des racines. —

- Pro : Soit P unitaire de degré n dans $\mathbb{C}[X]$. Alors, pour toute racine $|\lambda|$ de P , on a $|\lambda| \leq 1 + \max_i |a_i|$.
- Théorème de Gauss-Lucas : Soit $P \in \mathbb{C}[X]$ non-constant. Alors toute racine de P' appartient à l'enveloppe convexe des racines de P .
- Dev : Comptage des racines réelles : Soit $P \in \mathbb{R}[X]$ de degré n , et de racines complexes $\lambda_1, \dots, \lambda_r$, de multiplicités $\alpha_1, \dots, \alpha_r$. On pose $s_l := \sum_{i \geq r} \alpha_i \lambda_i^l$ pour $l \geq 0$, et $S_n((x_1, \dots, x_n)) := \sum_{i, k \leq n} s_{i+k} x_i \dots x_k$, qui est une forme quadratique sur \mathbb{R}^n . Si (p, q) est la signature de S_n , alors P possède $p + q$ racines distinctes, dont $p - q$ exactement sont réelles.
- Méthode de Newton polynomiale : Pour P un polynôme réel à racines réelles simples $\lambda_1 < \dots < \lambda_r$, la fonction $\Phi : x \in [\lambda_r, +\infty[\mapsto x - \frac{P(x)}{P'(x)} \in [\lambda_r, +\infty[$ est bien définie. Pour tout $x_0 \in [\lambda_r, +\infty[$, la suite récurrente définie par $x_{n+1} = \Phi(x_n)$ converge linéairement vers λ_r et quadratiquement à pr.
- App : Cela permet d'approcher rapidement des zéros de polynômes comme $x^2 - a$. Si P est un polynôme à coefficients rationnels, alors $x_n \in \mathbb{Q}$.
- Rem : On peut adapter cette méthode pour les polynômes réels à racines non forcément simples, afin de localiser les racines réelles pour pouvoir ensuite déduire la multiplicité de chaque racine en calculant les dérivées de P évaluées en ces racines de façon approchée.
- Dev : Théorème de Chevalley-Waring : Soit p premier, q une puissance de p , $n \geq 1$. Soient $P_1, \dots, P_r \in \mathbb{F}_q[X_1, \dots, X_n]$ tels que $\sum_{i \leq r} \deg_{tot}(P_i) < n$, et soit $V := \cup_i P_i^{-1}(\{0\})$. Alors $Card(V) \equiv 0 \pmod{p}$.
- App : Théorème de Ginszbourg-Erdős-Sziv : Soit $n \geq 1$ et soient $a_1, \dots, a_{2n-1} \in \mathbb{Z}$. Alors il existe $1 \leq i_1 < i_2 < \dots < i_n \leq 2n - 1$ tels que $a_{i_1} + \dots + a_{i_n} \equiv 0 \pmod{n}$.

Références

- Gourdon : Racines d'un polynôme, multiplicité, interpolation, irréductibilité, exemples.
Gozard : Corps de rupture, corps de décomposition, éléments algébriques/transcendants, exemples.
Perrin : Construction des corps finis.
Nourdin : Résultant, discriminant. Localisation des racines, Th de Gauss-Lucas.
Ramis, Deschamps, Odoux : Polynômes symétriques, Th de structure, exemples, algorithme.
Zavidovique : Th de Chevalley-Waring et de Erdős-Ginzburg-Sziv.(Dev)
Gantmacher (Tome 2) : Nombre de racines réelles d'un polynôme.(Dev)
Mignotte : Suites de Sturm.

May 20, 2017

Vidal Agniel, École normale supérieure de Rennes