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

Cadre : $\mathbb{K}$ est un corps commutatif et A un anneau intègre et commutatif.

1. Rapport du jury. — 2017 : *Dans cette leçon on peut présenter des méthodes de résolution, de la théorie des corps, des notions de topologie (continuité des racines) ou même des formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). Il est apprécié de faire apparaître le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices ; l'étude des valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois ou s'intéresser à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin..*

2. Racines d'un polynôme. —

1. *Généralités.* — *Définitions et propriétés :*

- Pro : $\mathbb{K}[X]$ est un anneau euclidien (donc factoriel et principal) dans lequel se plonge $\mathbb{K}$ et dont les inversibles sont les éléments de $\mathbb{K}^*$.
- Pro : on a donc les notions de PGCD et de PPCM.
- Pro : $\mathbb{K}[X]$ est une K-algèbre, de dimension infinie avec pour base canonique les monômes X^k.
- on a $deg(PQ) = deg(P) + deg(Q)$.
- Pro : Pour $i \in \{1, \cdots n\}, \lambda_i \in \mathbb{K}$ distincts et $\alpha_i \in \mathbb{K}$, il existe au moins un polynôme P de degré $\leq n$ tel que $P(\lambda_i) = \alpha_i \forall i$.
- Def : $a \in \mathbb{K}$ est une racine de $P(X) \in \mathbb{K}[X]$ ssi $P(a) = 0$.
- Pro : x est racine de P ssi $(X - a)$ divise $P(X)$.
- Def : $a \in \mathbb{K}$ est une racine double ou multiple de $P(X) \in \mathbb{K}[X]$ ssi $(X - a)^2$ divise P. Elle dite simple autrement. Elle est dite de multiplicité n ssi $(X - a)^n$ divise P et $(X - a)^{n+1}$ ne divise pas P.
- Def : un polynôme est dit scindé si sa décomposition en éléments irréductibles ne fait intervenir que des polynômes irréductibles de degré 1. Il est dit séparable si de plus ses racines sont simples.
- Pro : un polynôme P de degré n a au plus n racines. (Rem : ceci est faux sur des anneaux de polynômes à coefficients sur un anneau non-intègre.)

Polynômes dérivés :

- Pro : on peut définir une fonction polynomiale canonique $(x \to P(x))$ et un polynôme dérivé $P^{'}$ défini formellement et dont la fonction polynomiale correspond à la dérivée de la fonction polynomiale de P.Idem pour des dérivées multiples $P^{(m)}$.
- Pro : P a une racine double ssi $P^{'} \wedge P \neq 1$
- Pro : Si $car(\mathbb{K}) = 0$, alors "a est une racine de multiplicité n de $P(X)$" ssi "a est racine de $P^{(i)}$ où $i \leq n$ et $P^{(n+1)}(a) \neq 0$". Ce résultat reste vrai si $n \leq (car(\mathbb{K}) - 2$.
- Def :

Critères d'irréductibilité

- *Critère d'Einseinstein* : si p premier divise les coefficients autres que dominant et p^2 ne divise pas pour autant le coefficient du terme constant, le polynôme est irréductible. Ex : $X^n - pc$ avec p premier et premier avec c.
- Si $P(X)$ est irréductible, $P(X + 1)$ l'est aussi. Ex: $X^n + \cdots + 1$
- Soit $P(X) = \Sigma(a_k X)$ et si p ne divise a_n et si on considère $P_p$la réduction modulo p, alors si P_p est irréductible, P l'est aussi. Ex : $X^3 + 2712X^2 + 517X + 111$, qui se réduit à $X^3 + X + 1$ sur F_2 où il est irréductible car de degré 3 et sans racine.
- Si P de degré n il est irréductible qu'il n'a pas de racine de degré ≤ 2.
- Si P est irréductible sur $k[X]$, il l'est aussi sur toute extension K dont la dimension sur k est première avec le degré de P. Ex : YYY
- Dév. : BerlekampTrouver des facteurs d'un polynôme sur F_q

2. *Corps de rupture.* — *Prop. : adjonction d'une racine* Pour tout corps k dans lequel un polynôme f n'aurait pas de racine, on peut créer un sur-corps m/k de k-dimension finie de cette façon :

- (f) est maximal et donc $m = k[X]/f(X)$ est un corps.
- m vérifie que, si on note $\alpha = [X]$ alors $f(\alpha) = 0$.
- m est un k-e.v. et $[m : k] = deg(f)$
- on a $k \subseteq m$ via l'injection canonique d'un anneau dans son anneau des polynômes.
- *Nota :* on a donc "fabriqué" un nouvel élément α et un nouveau corps m de la forme $k(\alpha)$. Dans ce nouveau corps, f a une racine et n'est donc plus irréductible : on parle de "corps de rupture de f".
- Pro : les corps de rupture d'un même polynôme irréductible f sont isomorphes entre eux.
- Def : Soit L une extension de corps sur K et P un polynôme sur K de degré n. L est un corps de décomposition de P si P y est scindé et si L est engendré par les racines de P.
- Pro : Dans ce cas $[L : K] \leq n!$ et L est unique à isomorphisme de $\mathbb{K}$-algèbre près.
- App : $\forall m \in \mathbb{N}$ et p premier, $\exists F_q$, un corps à p^m éléments, construit comme le corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ du polynôme $X^{p^m} - X$.

3. *Algébricité et transcendance :* —

- Def : Un élément de M sur-corps de k est dit "algébrique sur k" s'il est racine d'un polynôme à coefficients dans k. Il est dit "transcendant" dans le cas contraire.
- Exe : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ mais e ne l'est pas.
- L est appelée extension algébrique de $\mathbb{K}$ si tous ses éléments sont algébriques sur $\mathbb{K}$.
- Pro : Toute extension de dimension finie est algébrique.
- Théorème de d'Alembert-Gauss : $\mathbb{C}$ est algébriquement clos.

4. *Applications à l'algèbre linéaire :* —

- App : Le Spectre d'un endomorphisme correspond aux racines sur $\mathbb{K}$ du polynôme caractéristique $det(A - XI)$ où A est une matrice associée à une base quelconque.
- Pro : si le polynôme caractéristique est scindé l'endomorphisme est trigonalisable. S'il est séparable, l'endomorphisme est diagonalisable.
- Cor : Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.

5. *Exemples divers.* —

- Pro : si $P \in \mathbb{R}[X]$ et λ est une racine complexe d'ordre k alors $\bar{\lambda}$ est également racine et d'ordre k.
- Pro : si $P \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$ alors P n'a que des racines simples sur C.

3. Fonctions symétriques. —

4. Localisation et comptage des racines. — Méthode de Newton polynomiale : Pour P un polynôme réel à racines réelles simples *Dans* $\mathbb{C}[X]$

- Pro : si $P(X) = \Sigma_0^n a_i X^i \in \mathbb{C}[X]$, unitaire de degré n, alors pour chaque racine λ on a : $|\lambda| \leq 1 + max_i(|a_i|)$
- The : Développement (*Théorème de Gauss-Lucas*) : Soit $P(X) \in \mathbb{C}[X]$ non-constant, alors toute racine de $P^{'}$ appartient à l'enveloppe convexe des racines de P.

galois ? valeurs propres ? continuite de la fonction ?

Développement 1 : *Berlekamp*

Développement 2 : *Théorème de Gauss-Lucas*

.

Sources :

- *D. Perrin "Algèbre Générale"*
- *Dany-Jack Mercier "Corps Finis"*
- *J. Calais "Extension des corps - Théorie de Galois"*
- *Jeanneret - Lines "Invitation à l'Algèbre"*
- *Hauchecorne*

November 24, 2017

Bruno Nitrosso, EPP et indépendant