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

Références : Gourdon Algèbre, Rombaldi, Perrin, *Algèbre linéaire - Réduction des endomorphismes* Mansuy, X-ENS Algèbre 1.

Cadre : Soit $\mathbb{K}$ un corps commutatif.

1 Racines d'un polynôme

1.1 Définitions et premières propriétés

Définition 1. Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine de P si $P(\alpha) = 0$.

Proposition 2. *α racine de $P \iff (X - \alpha)$ divise P*

Définition 3. On dit que α est racine de multiplicité h de P si $(X-\alpha)^h$ divise P et $(X-\alpha)^{h+1}$ ne le divise pas.

Théorème 4. *Soit $P \in \mathbb{K}[X]$ et $(a_1, ..., a_r) \in \mathbb{K}^r$ avec $(m_1, ..., m_r) \in \mathbb{N}^{*r}$. Alors : $(a_1, ..., a_r)$ sont racines de P de multiplicité respectives $(m_1, ..., m_r) \iff$ il existe $\mathbb{Q}[X]$ tel que $P(X) = Q(X)\Pi_{k=1}^r (X - a_k)^{m_k}$.*

Corollaire 5. *Soit $P \in \mathbb{K}[X]$ de degré n. Si P admet plus de n racines, alors il est nul.*

Définition 6. On dit que $P \in \mathbb{K}[X]$ est scindé dans $\mathbb{K}[X]$ si il se met sous la forme $P(X) = \lambda \Pi_{k=1}^r (X - a_k)^{m_k}$ avec $\lambda \in \mathbb{K}^*$, $(a_1, ..., a_r) \in \mathbb{K}^r$ avec $(m_1, ..., m_r) \in \mathbb{N}^{*r}$.

Exemple 7. $X^2 + 1$ est scindé dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$.

Définition 8. $P \in \mathbb{K}[X]$ est dit irreductible si ses seuls diviseurs sont les polynômes constants et λP (λ constant).

Exemple 9. Un polynôme irreductible de degré plus grand que 1 n'admet pas de racine.

1.2 Lien avec le polynôme dérivé

Théorème 10 (Formule de Taylor pour les polynômes). *On suppose que $\mathbb{K}$ est de caractéristique nul. $\forall P \in \mathbb{K}[\mathbb{X}]$ de degré n et pour tout $a \in \urcorner$, on à :*

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(X)}{k!}(X-a)^k$$

Théorème 11. *On suppose que $\mathbb{K}$ est de caractéristique nul. a est racine de multiplicité h de $P \iff \forall i \in [|0, h-1|]$, $P^{(i)}(a) = 0$ et $P^{(h)}(a) \neq 0$*

$P = X^3$ dans $\mathbb{F}_3$. 0 est racine d'ordre 3, mais on a quand même $P^{(3)}(0) = 0$

Corollaire 12. *Soit P non-nul de $\mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est racine simple de $P \iff P'(a) \neq 0$.*
Ceci est vrai quel que soit la caractéristique du corps $\mathbb{K}$.

1.3 Relation coefficients-racines

Définition 13. Soit $n \in \mathbb{N}^*$ et k compris entre 0 et n. On définit les fonctions symétriques élémentaires

$$\begin{aligned} \sigma_{n,k} : \quad & \mathbb{K}^n \to \mathbb{K} \\ & a = (a_1, ..., a_n) \mapsto \sum_{1 \leq i_1 \leq ... \leq i_n \leq n} a_{i_1} ... a_{i_n} \end{aligned} \tag{1}$$

si $\neq 1$. (Sinon, $\sigma_{n,k} = 1$.

Lemme 14. *Pour tout entier $n > 1$ et tout $a = (a)_{1 \leq n} = (a', a_n) \in \mathbb{K}^n$, on à : $\sigma_{n,0}(a) = \sigma_{n-1,0}(a') = 1$, $\sigma_{n,k}(a) = \sigma_{n-1,k}(a') + a_n \sigma_{n_1,k-1}(a')$ $(1 \neq k \neq n-1)$, $\sigma_{n,n}(a) = a_n \sigma_{n-1,n-1}(a')$*

Théorème 15. *Soit P scindé de la forme $P(X) = \Pi_{k=1}^r (X - a_k)$ avec $(a_1, ..., a_r) \in \mathbb{K}^n$ ses racines. Alors avec l'écriture $P(X) = \sum_{k=0}^{n} b_k X^{n-k}$, on à les relations suivantes :*

$$\forall k \in [|0, n|], a_k = (-1)^k \sigma_{n,k}(a_1, ..., a_n)$$

Exemple 16. — En particulier, $\sum_{i=1}^{n} a_i = \frac{-b_1}{b_0}$, $\Pi_{i=1}^n a_i = (-1)^p \frac{a_p}{a_0}$

— Si $P = X^2 + bX + c$ est de degré 2 dans $\mathbb{C}[X]$, ses racines (x_1 et x_2) sont solutions du système : $-b = x_1 + x_2$ et $a = x_1 x_2$

2 Adjonctions de racines

2.1 L'anneau $\frac{\mathbb{K}[X]}{(P)}$

Proposition 17. *Soit $P \in \mathbb{K}[X]$. L'anneau quotient $\frac{\mathbb{K}[X]}{(P)}$ est une $\mathbb{K}$-algèbre de dimension finie $n = deg(P)$. La famille $(\overline{1}, \overline{X}, ..., \overline{X^{n-1}})$ en est une base.*

Théorème 18. *$\frac{\mathbb{K}[X]}{(P)}$ est un corps $\iff$ $\frac{\mathbb{K}[X]}{(P)}$ est intègre $\iff$ P est un polynôme irreductible de $\mathbb{K}[X]$*

2.2 Algébricité

Définition 19. Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de corps de $\mathbb{K}$. On dit que $\alpha \in \mathbb{L}$ est algébrique dans $\mathbb{K}$ si il existe $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$

Théorème 20. *Si $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$, alors il existe un unique polynôme $P_\alpha \in \mathbb{K}[X]$ tel que $(P_\alpha) = \{Q \in \mathbb{K}[X] \mid Q(\alpha) = 0\}$ et ce polynôme est l'unique polynôme irreductible de $\mathbb{K}[X]$ qui annule α. On l'appelle polynôme minimal de α, son degré est noté $d(\alpha, \mathbb{K})$.*

Exemple 21. $\sqrt{2}$ est algébrique sur $\mathbb{Q}[X]$
i est algébrique sur $\mathbb{R}[X]$

2.3 Des extensions pour les polynômes

Définition 22. On dit que $\mathbb{K} \subset \mathbb{L}$ est un corps de rupture de $P \in \mathbb{K}[X]$ (non-constant) si le polynôme P a une racine α dans $\mathbb{L}$ et $\mathbb{L} = \mathbb{K}[\alpha]$

Théorème 23. *Si P est un polynôme irreductible de $\mathbb{K}[X]$ de degré n, alors $\frac{\mathbb{K}[X]}{(P)}$ est un corps de rupture de P et P est le polynôme minimal de $w = \overline{X}$ sur $\mathbb{K}$. Ce corps de rupture est unique à isomorphisme près.*

Exemple 24. $\frac{\mathbb{R}[X]}{X^2+1}$ est un corps de rupture pour $X^2 + 1$, en notant $i = \overline{X}$, on a construit le corps $\mathbb{C}$.

Proposition 25. *Pour tout polynôme $Q \in \mathbb{K}[X]$ de degré $n > 0$, il existe un corps de rupture $\mathbb{L}$ tel que $[\mathbb{L} : \mathbb{K}] \leq n$.*

Définition 26. Soit P un polynôme de $\mathbb{K}[X]$. $\mathbb{L}$ de degré n est un corps de décomposition de P sur $\mathbb{K}$ si P est scindé dans $\mathbb{L}[X]$, et, en notant $(a_1, ..., a_n)$ ses racines (comptées avec multiplicités), $\mathbb{L} = \mathbb{K}(1, ..., n)$.

Théorème 27. *Pour tout polynôme P, le corps de décomposition existe et est unique.*

Définition 28. On dit que $\mathbb{K}$ est un corps algébriquement clos si tout polynôme de $\mathbb{K}[X]$ y est scindé.

Théorème 29 (D'alembert-Gauss). *$\mathbb{C}$ est algébriquement clos.*

2.4 Construction des corps finis

Théorème 30.
— *1) Soit F un corps à q éléments. Alors il existe un nombre premier p et un entier naturel n tel que $\#(F) = p^n$*
— *2) Soit F le corps de décomposition du polynôme $P = X^{p^n} - X$ dans $\mathbb{F}_p$. Alors F est un corps à $q = p^n$ éléments.*
— *3) Il est unique à isomorphisme près*

Corollaire 31. *Soit F fini à $q = p^n$ éléments. A est un sous-corps de F à $\#(A) = l$ éléments ssi il existe d diviseur de n tel que $l = p^d$*

Exemple 32. Imbrication des sous-corps de $\mathbb{F}_{16}$ (dessin).

Exemple 33. Pour construire $\mathbb{F}_{\not\in}$, en vertu du théorème sur l'anneau $\frac{\mathbb{K}[X]}{P}$, on cherche un polynôme irreductible de degré 2 dans $\mathbb{F}_{\not\in}$. On prend : $P = X^2 + X + 1$, et on obtient $\mathbb{F}_{\not\in} = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}$ où $\overline{X}$ est racine de $P = X^2 + X + 1$.

Proposition 34. *Soit p un nombre premier impair et $\mathbb{F}_q$ un corps à $q = p^n$ éléments.*
— *L'ensemble $P_2 = \{x^2, x \in \mathbb{F}_q\}$ est un sous-groupe de $\mathbb{F}_q^*$, de cardinal $\frac{q-1}{2}$. (Il y a donc $\frac{q+1}{2}$ dans $\mathbb{F}_q$.*
— *Il y a $\frac{q-1}{2}$ non-carrés dans $\mathbb{F}_q^*$.*
— *Les carrés de $\mathbb{F}_q^*$ sont les racines du polynômes $X^{\frac{q-1}{2}} - 1$. Les non-carrés de $\mathbb{F}_q^*$ sont les racines du polynômes $X^{\frac{q-1}{2}} + 1$.*

3 Applications

3.1 Lien avec l'algèbre linéaire

Cadre : Soit E un $\mathbb{K}$-e.v de dimension finie n.

Définition 35. Soit f un endomorphisme de E. On appelle polynôme minimal μ_f le polynôme qui engendre l'idéal principal $\{P \in \mathbb{K}[X] \mid P(f) = 0\}$. On appelle polynôme caractéristique de f le polynôme $\chi_f(X) = det(XI_n - M)$, avec M la matrice de f dans n'importe quelle base de E.

Remarque 36. L'espace vectoriel $\mathbb{K}[u]$ est isomorphe à $\frac{\mathbb{K}[X]}{(\mu_f)}$, et est de dimension $\deg(\mu_f)$.

Proposition 37. *Les valeurs propres de f sont exactement les racines de χ_f et μ_f.*

Exemple 38. En dimension 2, $\chi_f(X) = X^2 + tr(f)X + det(A)$, et si f est trigonalisable, $tr(f) = \lambda_1 + \lambda_2$ et $det(f) = \lambda_1\lambda_2$, avec λ_1 et λ_2 les valeurs propres de f.

Théorème 39. *f est diagonalisable $\iff$ il existe un polynôme annulateur de f scindé sur $\mathbb{K}$ à racine simple $\iff$ μ_f est scindé sur $\mathbb{K}$ à racine simple.*

Théorème 40. *f est trigonalisable $\iff$ il existe un polynôme annulateur de f scindé sur $\mathbb{K}$ $\iff$ μ_f est scindé sur $\mathbb{K}$*

Exemple 41. Comme $\mathbb{C}$ est algébriquement clos, tout endomorphisme d'un $\mathbb{C}$-ev est trigonalisable.

3.2 Localisation des racines

Cadre : On se place dans $\mathbb{R}$ où $\mathbb{C}$.

Remarque 42. Pour trouver le 0 d'un polynôme, on peut appliquer l'algorithme de Newton

Définition 43. On définit la matrice compagnon d'un polynôme $P \in \mathbb{K}[X]$.

Théorème 44. *Les valeurs propres de la matrices compagnons sont exactement les racines de P, avec la même multiplicité.*
Concrètement, la recherche de racine est maintenant devenu une recherche de racine.

Remarque 45. Pour trouver la plus grande valeur racine de P en valeur absolue, on peut donc appliquer la méthode de la puissance.

Lemme 46 (Hadamard). *Si M est une matrice à coefficient complexe à diagonale dominante, alors M est inversible.*

Définition 47. Soit $A = (a_{i,j}) \in \mathbb{M}_n(\mathbb{C})$. Le ième disque de Gerschgorin est le disque fermé de centre $a_{i,i}$ et de rayon $r_i = \sum_{j=1, j\neq i}^{n} |a_{i,j}|$.

Théorème 48. *Les valeurs propres d'une matrice complexe sont situés dans la réunion des disques de Gerschgorin.*

3.3 Polynômes cyclotomiques

Définition 49. On définit le nème polynôme cyclotomique Φ_n tout en introduisant les racines nèmes primitives de l'unité. Le degré de Φ_n est $\varphi(n)$

Théorème 50. *On a $X^n - 1 = \Pi_{d|n}\Phi_d(X)$ et $\Phi_n(X)$ est unitaire dans $\mathbb{Z}[X]$*

Application 51 (Progression arithmétique de Dirichlet)**.** *Soit a, n tel que $a \wedge n = 1$. Alors il existe une infinité de nombres premiers tel que $p \equiv a \pmod{n}$*

Théorème 52. *Pour tout entier naturel n plus grand que 1, Φ_n est irreductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$*

Application 53. *Degré de l'extension cyclotomique. Soit ω une racine nème première de l'unité, on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$*