144

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

I. Factorisation d'un polynôme

A. Généralités sur les racines

Cadre: $\mathbb{B}$ anneau, et $\mathbb{A} \leq \mathbb{B}$ sous-anneau de $\mathbb{B}$

Def 1: Si $P \in \mathbb{A}[X]$, $\alpha \in \mathbb{B}$ est racine de P sur $\mathbb{B}$ si $P(\alpha)=0$. On note $Z_{\mathbb{B}}(P) := \{\alpha \in \mathbb{B};\ P(\alpha)=0\}$.

Prop. 2. Si $P \in \mathbb{A}[X]$, $\alpha \in Z_{\mathbb{B}}(P) \iff X-\alpha \mid P$.

Déf 3. Si $P \in \mathbb{A}[X]$, et $\alpha \in Z_{\mathbb{B}}(P)$, on appelle ordre (ou multiplicité) de α sur P la quantité:

$$\mathrm{ord}_\alpha P := \sup\{k \in \mathbb{N},\ (X-a)^k \mid P\}.$$

Ex 4: • $\mathrm{ord}_\alpha(0) = +\infty$, $\forall \alpha \in \mathbb{A}$

• Si $p \in \mathbb{P}$, et $P = X^p - 1 \in \mathbb{F}_p$, alors:

$$\mathrm{ord}_1(P) = p.$$

Prop. 5. Si $P \in \mathbb{A}[X]$, et $a_1, \dots, a_r \in Z_{\mathbb{B}}P$ 2 à 2 $\neq$, de multiplicités respectives m_i, alors:

$$P = \prod_{i=1}^{r} (X-a_i)^{m_i} \cdot Q, \quad \text{où} \begin{cases} Q \in \mathbb{B}[X] \\ \forall i,\ Q(a_i) \neq 0. \end{cases}$$

Cor. 6. Si $\mathbb{K}$ corps, et si $d°P = n \geq 0$, alors P admet au + n zéros.

Cor. 7. Si $\mathbb{K}$ infini, alors $\varphi : P \longrightarrow \tilde{P}$ qui, à $P \in \mathbb{K}[X]$ associe sa fonction polynômiale, est injective.

C-ex 8. ⚠ Faux si $\mathbb{K}$ fini ⚠ Si $p \in \mathbb{P}$, $\forall x \in \mathbb{F}_p$: $x^p - x = 0$ (petit théorème de Fermat)

Prop. 9: Soit $\mathbb{K} \hookrightarrow \mathbb{L}$ extension de corps, et $\alpha \in \mathbb{L}$, Π_α son polynôme minimal. Soit $p = \mathrm{car}\,\mathbb{K}$.

$$\mathrm{ord}_\alpha(\Pi_\alpha) = 1 \iff \Pi_\alpha \in \mathbb{K}[X^p]$$

Ex. 10: $\mathbb{K} = \mathbb{F}_p$: Soit a transcendant sur $\mathbb{F}_p$, $P = X^p - a$, α racine de P. $P = \Pi_\alpha$, et $P = X^p - \alpha^p = (X-\alpha)^p$.

B. Adjonction de racines

Cadre. $\mathbb{K}$ corps.

Def. 11: Si $P \in \mathbb{K}[X]$, un corps de rupture de P sur $\mathbb{K}$ est une extension $\mathbb{K} \hookrightarrow \mathbb{L}$ telle que: $\begin{cases} \exists\, \alpha \in Z_{\mathbb{L}}(P) \\ \mathbb{L} = \mathbb{K}(\alpha) \end{cases}$

(P non constant)

Prop. 12: Si $P \in \mathbb{K}[X]$, alors P admet un corps de rupture; unique à $\mathbb{K}$-isomorphisme près.

Ex. 13. $P = X^2 + 1$, • $\mathbb{K} = \mathbb{Q} \longrightarrow \mathbb{L} = \mathbb{Q}(i)$
• $\mathbb{K} = \mathbb{C} \longrightarrow \mathbb{L} = \mathbb{C}$.

Rmq 14: Le corps de rupture dépend du corps de base.

Def. 15: Soit $P \in \mathbb{K}[X]$. P est dit scindé sur l'ext. $\mathbb{K} \hookrightarrow \mathbb{L}$ si $P = a.\prod_{i=1}^{n} (X - z_i)$, où $z_1, \dots, z_n \in \mathbb{L}$.

Def. 16: Un corps de décomposition de $P \in \mathbb{K}[X]$ est une extension $\mathbb{K} \hookrightarrow \mathbb{L}$ telle que

$$\begin{cases} P \text{ scindé sur } \mathbb{L}, \quad P = a.\prod_{i=1}^{n} (X - z_i) \\ \mathbb{L} = \mathbb{K}(z_1, \dots, z_n) \end{cases}$$

Prop 17. Si $P \in \mathbb{K}[X]$, alors P admet un corps de décomposition, unique à $\mathbb{K}$-isomorphisme près.

Rmq 18 : Deux polynômes différents peuvent avoir un même corps de décomposition.

Ex 19 : $\mathbb{K} = \mathbb{Q}$; $P = X^2 - 5$, $Q = X^2 + X - 1$. $\mathbb{L} = \mathbb{Q}(\sqrt{5})$.

Déf 20 : Une clôture algébrique sur $\mathbb{K}$ est une extension $\mathbb{K} \hookrightarrow \mathbb{L}$ algébrique sur laquelle tout $P \in \mathbb{K}[X]$ est scindé.

Ex 21 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

C. Polynômes symétriques

Cadre : $\mathbb{A}$ anneau intègre, $n \in \mathbb{N}$; $\geq$ ordre lexicographique sur $\mathbb{N}^n$.

Déf 22 : Si $P \in \mathbb{A}[X_1, \dots, X_n]$, P est dit symétrique si $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) := P_\sigma = P(X_1, \dots, X_n)$.

Prop 23 : L'ensemble des éléments symétriques est une sous-$\mathbb{A}$ algèbre de $\mathbb{A}[X_1, \dots, X_n]$, noté $\mathbb{A}_S[X_1, \dots, X_n]$.

Ex 24 :
- $S_k = \sum_{i=1}^{n} X_i^k \in \mathbb{A}_S[X_1, \dots, X_n]$ si $k \in \mathbb{N}$.
- $\Sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k}$ (fonction symétrique élémentaire)

Thm 25 : [Structure des fonctions symétriques]. $\forall f \in \mathbb{A}_S[X_1, \dots, X_n]$, $\exists ! \phi \in \mathbb{A}[X_1, \dots, X_n]$; $f = \phi(\Sigma_1, \dots, \Sigma_n)$.

II. Existence, Dénombrement, Localisation des racines

A. Localisation des racines

Thm 26 : Soit $f \in \mathbb{C}[X]$ unitaire, $f = \sum_{j=0}^{n} a_j X^j$. Soit $m \in [\![0, n]\!]$. On trouve au moins m racines de f dans $\mathcal{D}(0, \max_{0 \leq \ell \leq m-1} |a_\ell|^{\frac{1}{n-\ell}})$.

Déf 27 : On notera, si $P \in \mathbb{C}[X]$, $P = \sum_{j=0}^{n} a_j X^j$, $\|P\| = \max_{0 \leq j \leq n} |a_j|$.

Thm 28 : [de Continuité] Soit $f \in \mathbb{C}[X]$, $f = \sum_{j=0}^{n} a_j X^j = \prod_{j=1}^{k} (X - z_j)^{m_j}$, où les z_j sont 2 à 2 distincts. Soit $\varepsilon < \frac{1}{2} \min_{1 \leq i < j \leq k} |z_i - z_j|$.

$\exists \delta > 0$; ($\|g - f\| < \delta \implies$ chaque $\mathcal{D}(z_j, \varepsilon)$ contient m_j racines de g)

Cor 29 : [Rouché polynômial] Soit $P_1, P_2 \in \mathbb{C}[X]$, $\Omega \subset \mathbb{C}$, et γ lacet dans Ω. Si $|P_1| < |P_2|$ sur $T = \gamma$, alors P_2 et $P_1 + P_2$ ont le même nombre de zéros, avec multiplicités, dans γ.

Thm 30 : [Rolle] Si $P \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$; $P(a) = P(b)$, alors P' s'annule sur $]a, b[$.

Thm 31 : [Ellipse de Steiner] Soit $\mathcal{P}$ le plan affine, $M_1(z_1), M_2(z_2), M_3(z_3)$ trois points non alignés de $\mathcal{P}$. Soit $P = (X - z_1)(X - z_2)(X - z_3)$, et $\mathcal{Z}_{\mathbb{C}}(P') = \{\omega_1, \omega_2\}$. Alors $F_1(\omega_1)$ et $F_2(\omega_2)$ sont les foyers d'une ellipse tangente aux milieux des 3 côtés de $M_1 M_2 M_3$. DEV 1

Cor 32 : [Gauß-Lucas] Soit $P \in \mathbb{C}[X]$ et C l'enveloppe convexe de ses racines. Alors C contient les racines de P'.

B. Dénombrement des racines

Thm 33 [Chevalley-Warning] Soit $p \in \mathbb{P}$, $f \in \mathbb{N}$ et $q = p^f$. Soient $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_n]$, tels que $\sum_{i=1}^{s} d^\circ f_i < n$. Alors, en notant $V := \bigcap_{i=1}^{s} \mathcal{Z}_{\mathbb{F}_q}(f_i)$, $\operatorname{card}(V) \equiv 0 \ [p]$ DEV 2

Thm 34 : [Formes de Hankel] Soit $P \in \mathbb{R}[X]$. Il existe une forme quadratique réelle q de signature (s, t) telle que
$$\begin{cases} \operatorname{card} \mathcal{Z}_{\mathbb{C}}(P) = s + t \\ \operatorname{card} \mathcal{Z}_{\mathbb{R}}(P) = s - t \end{cases}$$
DEV 3

III. Une application : réduction des endomorphismes

Cadre : E $\mathbb{K}$-ev de dim. finie $n \geq 1$, $u \in \mathcal{L}(E)$, $\mathbb{K}$ corps.

A. Polynôme et diagonalisation

Déf 35 Le polynôme caractéristique de u est le polynôme de $\mathbb{K}[X]$ défini par : $\chi_u := \det(u - X \cdot I_n)$

Prop 36. $\mathcal{Z}_{\mathbb{K}}(\chi_u) = Sp(u)$. [spectre de u]

Ex. 37 : $f : \mathbb{R}^2 \to \mathbb{R}^2$ de matrice canonique $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

$\chi_f = X^2 - 1$.

Prop 38 : $\chi_u = (-1)^n \left(\sum_{j=1}^{n} \sigma_j (-1)^j X^{n-j} + X^n \right)$

σ_j est $\begin{cases} \cdot \text{ le polynôme symétrique élémentaire } j\text{-ième de } \chi_u \\ \cdot \text{ le mineur principal d'ordre } j \text{ de (la matrice canonique de) } u. \end{cases}$

En particulier, $\sigma_1 = \mathrm{Tr}\, u$ et $\sigma_n = \det u$.

Rmq 39 : Si $\mathbb{K}$ alg. clos, alors $Sp(u) \neq \emptyset$.

En particulier, si $\mathbb{K} \hookrightarrow \mathbb{L}$ contient un corps de rupture de χ_u sur $\mathbb{K}$, alors $Sp(u) \neq \emptyset$.

Thm 40 Les assertions suivantes sont équivalentes :

(i) u diagonalisable (sur $\mathbb{K}$)

(ii) χ_u scindé sur $\mathbb{K}$, et $\forall \lambda \in \mathcal{Z}(\chi_u)$; $\mathrm{ord}_\lambda(\chi_u) = \dim E_\lambda(u)$

(iii) $\exists \lambda_1, \dots, \lambda_p \in Sp\, u$ tels que : $E = \bigoplus_{i=1}^{p} E_{\lambda_i}(u)$

Cex 41. $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ diagonalisable sur $\mathbb{R}$, mais pas sur $\mathbb{Q}$

Thm 42. u trigonalisable sur $\mathbb{K} \iff \chi_u$ scindé (sur $\mathbb{K}$)

Cex 43. $\begin{pmatrix} 1 & 1 \\ a & 1 \end{pmatrix}$ trigonalisable sur $\mathbb{R} \iff a \geq 0$

B. Polynôme minimal

Déf 44 : Le morphisme d'algèbre $\varphi_u : \mathbb{K}[X] \to \mathcal{L}(E)$, $P \mapsto P(u)$ n'est pas injectif, son idéal-noyau est engendré par un unique polynôme unitaire (irréductible), appelé polynôme minimal de u, et noté μ_u.

Prop 45. $Sp\, u = \mathcal{Z}(\mu_u)$.

Thm 46 : [Lemme des noyaux] Si $I \neq \emptyset$, et $(P_i)_i \in \mathbb{K}[X]^I$, avec P_i 2 à 2 premiers entre eux. (I fini). Soit $P = \prod_{i \in I} P_i$

Alors $\mathrm{Ker}\, P(u) = \bigoplus_{i \in I} \mathrm{Ker}\, P_i(u)$

Thm 47 : u diagonalisable sur $\mathbb{K} \iff \exists P \in \mathbb{K}[X]$ scindé à racines simples sur $\mathbb{K}$ tel que $P(u) = 0$.

Thm 48 : [Théorème de Cayley-Hamilton] $\chi_u(u) = 0$

C. Localisation de racines

Thm 49 [Lemme de Hadamard]

Si $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\forall i, |a_{ii}| > \sum_{j \neq i} |a_{ij}|$, alors A inversible.

Déf 50. Si $A \in \mathcal{M}_n(\mathbb{C})$ et $i \in [\![1,n]\!]$, le i-ème disque de Gersgorin l'ensemble $\overline{\mathcal{D}}(a_{ii}, \sum_{j \neq i} |a_{ij}|) =: D_i$

Thm 51 [Théorème de Gersgorin]

Si $A \in \mathcal{M}_n(\mathbb{C})$; $Sp\, A \subset \bigcup_{i=1}^{n} D_i$

Mansuy-Mneimné, Algèbre linéaire. Réduction des endomorphismes
Rahman-Schmeisser, Analytic Theory of Polynomials
X. Gourdon, Algèbre
Josette Calais, Éléments de théorie des anneaux
Calderon-Germoni, Nouvelles histoires hédonistes de groupes et de géométries
Guin-Hausberger, Algèbre I - Groupes, Corps et Théorie de Galois