144

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

Soit $\mathbb{K}$ corps, $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$, A anneau commutatif unitaire

I] Racines d'un polynôme

1] Racine, multiplicité et polynôme scindé

[Rom] XII.5

Définition 1: On dit que $\alpha \in \mathbb{K}$ est racine de P si: $P(\alpha)=0$.

Proposition 2: $\alpha \in \mathbb{K}$ est racine de P ssi $X-\alpha \mid P$

Définition 3: Soit $P \in \mathbb{K}[X] \setminus \mathbb{K}$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est racine d'ordre (ou de multiplicité) m de P si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P.

Théorème 4: Soit $P \in \mathbb{K}[X] \setminus \mathbb{K}$, $\alpha_1, \dots, \alpha_r \in \mathbb{K}^r$ deux à deux distincts $m_1, \dots, m_r \in \mathbb{N}^*$

Alors: $\forall k \in [\![1;r]\!]$, α_k est racine de multiplicité m_k ssi $\exists Q \in \mathbb{K}[X] \mid P(X) = Q(X) \prod_{i=1}^{r} (X-\alpha_k)^{m_k}$ avec $\forall k \in [\![1;r]\!]$, $Q(\alpha_k) \neq 0$.

Corollaire 5: Un polynôme $P \in \mathbb{K}[X]$ de degré n admet au plus n racines distinctes dans $\mathbb{K}$.

Application 6: Si deux polynômes $P, Q \in \mathbb{K}[X]$ de degré au plus n coïncident en au moins $(n+1)$ points distincts, alors ils sont égaux.

Contrexemple 7: Le résultat est faux sur les anneaux ! $3X \in \mathbb{Z}/6\mathbb{Z}[X]$ est de degré 1 mais a deux racines: 0 et 2.

Proposition 8: Si le corps $\mathbb{K}$ est infini

Alors: le morphisme de $\mathbb{K}$-algèbres $\begin{array}{l}\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}} \\ P \mapsto \tilde{P}\end{array}$ qui a un polynôme associe sa fonction polynomiale est injectif.

Contrexemple 9: L'hypothèse sur $\mathbb{K}$ est vitale ! Dans $\mathbb{F}_{p^n}$, $\forall x \in \mathbb{F}_{p^n}$, $x^{p^n} = x$ et alors l'image de $X^{p^n} - X$ par le morphisme est $\begin{array}{l}\mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \\ x \mapsto 0\end{array}$ alors que $X^{p^n} - X \neq 0$.

XII.5 [Rom]

Définition 10: On dit que P est scindé sur $\mathbb{K}$ si P est constant ou s'il est de degré n et admet $\alpha_1 \neq \dots \neq \alpha_r$ racines de multiplicité $m_1, \dots, m_r$ tels que $\sum_{i=1}^{r} m_i = n$.

Si $m_1 = \dots = m_r = 1$, on dit que P est scindé à racines simples.

XII.6

Théorème 11: Si $car(\mathbb{K}) = 0$, $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

Alors: α est racine de P d'ordre m ssi $\forall k \in [\![0; m-1]\!]$, $P^{(k)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

2] Racines, polynômes irréductibles et application

XII.8 [Rom]

Définition 12: Un polynôme $P \in \mathbb{K}[X] \setminus \mathbb{K}$ est dit irréductible si: $P = AB \Rightarrow A \in \mathbb{K}$ ou $B \in \mathbb{K}$

Proposition 13: Un polynôme de degré 1, 2 ou 3 est irréductible dans $\mathbb{K}[X]$ ssi il admet au moins une racine dans $\mathbb{K}$.

Proposition 14: Soit $P \in \mathbb{K}[X]$ irréductible tel que $\deg(P) \geq 2$.

Alors: P n'a pas de racines dans $\mathbb{K}$

XII.11

Théorème 15: (de D'Alembert-Gauss) Les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1.

Théorème 16: Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 aX^2+bX+c tels que $b^2-4ac<0$.

[Per]

Définition 17: On note $\mu_n^\times = \{z \in \mathbb{C} \mid \forall p \mid n,\ p<n \Rightarrow z^p \neq 1,\ z^n = 1\}$ l'ensemble des racines primitives n-ièmes de l'unité. On appelle n-ième polynôme cyclotomique $\Phi_n(X) = \prod_{\xi \in \mu_n^\times} (X-\xi)$.

Théorème 18: $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Application 19: Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

3) Extensions de corps par adjonction de racines

I.1

Définition 20 : Soit $P\in\mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ engendrée par $\mathbb{K}$ et une racine α de P : i.e. $\mathbb{L}=\mathbb{K}(\alpha)$.

Théorème 21 : Soit $P\in\mathbb{K}[X]$ irréductible.
Alors : (1) il existe un corps de rupture de P sur $\mathbb{K}$
(2) Si $\mathbb{K}(\alpha)$ et $\mathbb{K}(\beta)$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $f:\mathbb{K}(\alpha)\to\mathbb{K}(\beta)$ tel que $f(\alpha)=\beta$.

[Goz]

Exemple 22 : $\mathbb{C}\simeq\mathbb{R}[X]/\langle X^2+1\rangle$; $\mathbb{F}_4\simeq\mathbb{F}_2[X]/\langle X^2+X+1\rangle$

I.2

Définition 23 : Soit $\mathbb{L}$ une extension de $\mathbb{K}$, $P\in\mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si : $\exists a,x_1,\dots,x_n\in\mathbb{L}^{n+1}\ |\ P(X)=a(X-\alpha_1)\times\dots\times(X-\alpha_n)$ et $\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_n)$.

Théorème 24 : Soit $P\in\mathbb{K}[X]\setminus\mathbb{K}$.
Alors : (1) il existe un corps de décomposition Σ de P tq : $[\Sigma:\mathbb{K}]\le n!$
(2) Si Σ et Σ' sont deux corps de décomposition de P alors il existe un $\mathbb{K}$-isomorphisme de Σ dans Σ'.

Exemple 25 : (1) $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$
(2) $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de X^2-1 sur $\mathbb{Q}$.

II) Polynômes symétriques ; fonctions symétriques élémentaires

1) Relations coefficients – racines

I.4

Définition 26 : On dit que $P\in A[X_1,\dots,X_n]$ est symétrique si : $\forall\sigma\in S_n$, $P(X_{\sigma(1)},\dots,X_{\sigma(n)})=P(X_1,\dots,X_n)$

Exemple 27 : (1) $\prod_{i\neq j}(X_i-X_j)=(-1)^{\frac{n(n-1)}{2}}\left(\prod_{i<j}X_i-X_j\right)^2$ est symétrique
(2) $\forall e\in\mathbb{N}$, $X_1^e+\dots+X_n^e$ est un polynôme symétrique

[Goz]

Définition 28 : Les fonctions symétriques élémentaires de $A[X_1,\dots,X_n]$:
$\Sigma_1=\sum_{i=1}^n X_i$; $\Sigma_2=\sum_{i<j}X_iX_j$; … ; $\Sigma_k=\sum_{1\le i_1<\dots<i_k\le n}X_{i_1}\times\dots\times X_{i_k}$; … ; $\Sigma_n=X_1\times\dots\times X_n$

Théorème 29 : (relations coefficients – racines) Soit $P\in A[X]$, $(\alpha_1,\dots,\alpha_n)\in A$
Alors : $P(X)=(X-\alpha_1)\times\dots\times(X-\alpha_n)$ ssi $P(X)=X^n+a_{n-1}X^{n-1}+\dots+a_0$ avec : $\forall i\in[\![1,n]\!]$,
$a_{n-i}=(-1)^i\Sigma_i(\alpha_1,\dots,\alpha_n)$

I.4 [Goz]

2) Structure des polynômes symétriques

I.4

Définition 30 : Soit $aX_1^{\alpha_1}\times\dots\times X_n^{\alpha_n}$ monôme avec $a\in A^\times$ et $\alpha_i\in\mathbb{N}$. On appelle poids de ce monôme l'entier $\sum_{i=1}^n i\alpha_i$. On appelle poids de $P\in A[X_1,\dots,X_n]$ le max des poids de ses monômes.

Exemple 31 : Le poids de Σ_k est : $nk-\frac{k(k-1)}{2}$.

Théorème 32 : Soit $P\in A[X_1,\dots,X_n]$ polynôme symétrique de degré k.
Alors : $\exists!\, Q\in A[X_1,\dots,X_n]\ |\ P(X_1,\dots,X_n)=Q(\Sigma_1,\dots,\Sigma_n)$ avec Q de poids k et de degré le degré partiel de P par rapport à X_1.

[Goz]

Remarque 33 : Ceci montre que les polynômes symétriques élémentaires permettent d'obtenir tous les polynômes symétriques de $A[X_1,\dots,X_n]$.

Exemple 34 : $X_1^2+\dots+X_n^2=\Sigma_1^2-2\Sigma_2$ avec $Q(X_1,\dots,X_n)=X_1^2-2X_2$.

3) Racines et discriminant

IX.5

Définition 35 : Soit $P(X)=\lambda\prod_{i=1}^n(X-r_i)\in\mathbb{K}[X]$, $r_i\in\tilde{\mathbb{K}}$ un corps de décomposition de P sur $\mathbb{K}$ et $n\ge 2$. Le discriminant de P est :
$$Disc(P)=\lambda^{2(n-1)}\left[\prod_{i<j}(r_j-r_i)\right]^2=(-1)^{\frac{n(n-1)}{2}}\lambda^{2(n-1)}\prod_{i\neq j}(r_i-r_j)$$

Proposition 36 : $Disc(P)$ est un polynôme symétrique de $\mathbb{K}[X_1,\dots,X_n]$

[Goz]

Corollaire 37 : $Disc(P)\in\mathbb{K}$

Exemple 38 : $Disc(\Phi_n)=(-1)^{\frac{n-1}{2}}n^{n-2}$

Proposition 39 : $P\in\mathbb{K}[X]$ est à racines simples ssi $Disc(P)\neq 0$.

Exemple 40 : $Disc(ax^2+bx+c)=b^2-4ac$

III] Localisation de racines

1] Suites de Sturm et estimation du nombre de racines

[FGN AI1]

Théorème 41 : (de Sturm) Soit $P \in \mathbb{R}[X]$; $S_0 = P$, $S_1 = P'$ puis, aussi longtemps que possible, $S_{i-1} = A_i S_i - S_{i+1}$ avec $\deg(S_{i+1}) < \deg(S_i)$. Pour $x \in \mathbb{R}$, on note $V(x)$ le nombre de changements de signes (stricts) de la suite $S_0(x); \dots; S_p(x)$ lorsque $S_{p+1} = 0$ i.e. $V(x) = \mathrm{card}\left(\{(i;j) \mid 0 \leq i < j \leq p,\ S_i(x)S_j(x) < 0 \text{ et } S_k(x) = 0 \text{ si } i < k < j\}\right)$

Soit $a < b$ tels que $P(a)P(b) \neq 0$.

Alors : le nombre de racines distinctes de P dans $[a;b]$ est égal à $V(a) - V(b)$.

Exemple 42 : $X^4 + X^3 - X - 1$ a 2 racines réelles sur $\mathbb{R}$.

[FGN An2]

Théorème 43 : Soit $(a_1; \dots; a_k) \in \mathbb{N}^*$ premiers entre eux et soit $\left(u_n := \mathrm{card}\left(\{(x_1; \dots; x_k) \in \mathbb{N}^k \mid a_1x_1 + \dots + a_kx_k = n\}\right)\right)_{n \in \mathbb{N}}$.

Alors : $u_n \underset{+\infty}{\sim} \dfrac{1}{a_1 \times \dots \times a_k} \times \dfrac{n^{k-1}}{(k-1)!}$

2] Matrices compagnon et disques de Gershgorin

[FGN Al2]

Définition 44 : Soit $P = X^n - \sum_{k=0}^{n} a_k X^k$. On appelle matrice compagnon de P : $C(P) = \begin{pmatrix} 0 & & (0) & a_0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & & \\ (0) & & 1 & a_{n-1} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$

Exemple 45 : Pour $P = X^3 - aX^2 - bX - c$, $C(P) = \begin{pmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{pmatrix}$

Théorème 46 : Les polynômes minimal et caractéristique de $C(P)$ sont P

Corollaire 47 : Les racines de P sont exactement les valeurs propres de $C(P)$ avec les mêmes multiplicités.

Définition 48 : Soit $A \in \mathcal{M}_n(\mathbb{C})$. On dit que A est à diagonale strictement dominante si : $\forall i \in [\![1;n]\!]$, $|a_{i,i}| > \sum_{j \neq i} |a_{i,j}| =: R_i$

[FGN Al2]

Lemme 49 : (de Hadamard) Soit $A \in \mathcal{M}_n(\mathbb{C})$ à diagonale strictement dominante.

Alors : $A \in GL_n(\mathbb{C})$.

Théorème 50 : (de Gerschgorin) Soit $A \in \mathcal{M}_n(\mathbb{C})$ à diagonale strictement dominante.

Alors : $Sp(A) \subseteq \bigcup_{i=1}^{n} \underbrace{\{z \in \mathbb{C} \mid |z - a_{i,i}| \leq R_i\}}_{D(a_{i,i};\, R_i)}$

Corollaire 51 : Les racines de $P \in \mathbb{C}[X]$ sont incluses dans $\bigcup_{i=1}^{n-2} D(0; R_i) \cup D(a_{n-1}; R_n)$ avec $R_i = \begin{cases} 1 + |a_{i-1}| & \text{si } i \in [\![2;n]\!] \\ |a_0| & \text{si } i = 1 \end{cases}$

Exemple 52 : Pour $P = X^3 - aX^2 - bX - c$, les racines sont dans $D(0; |c|) \cup D(0; 1 + |b|) \cup D(a; 1 + |a|)$

Références :

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi
[Per] Cours d'algèbre - Perrin
[Goz] Théorie de Galois - Gozard
[FGNAl1] Exercices de mathématiques oraux X-ENS Algèbre 1 - Francinou
[FGNAn2] Exercices de mathématiques oraux X-ENS Analyse 2 - Francinou
[FGNAl2] Exercices de mathématiques oraux X-ENS Algèbre 2 - Francinou