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

I Racines d'un polynôme

A Racine, multiplicité et polynôme scindé Rom 12.5 et 12.6

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

Exemple 2 : Un polynôme constant non nul n'a pas de racine et le polynôme nul a tous les éléments de $\mathbb{K}$ comme racines.

Proposition 3 : Soit $a \in \mathbb{K}$, alors a est racine de P ssi $X - a \mid P$.

Définition 4 : Soient $P \in \mathbb{K}[X] \setminus \mathbb{K}$ un polynôme non constant, $\alpha \in \mathbb{K}$ 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 si $(X-\alpha)^{m+1}$ ne divise pas P.

Théorème 5 : Soient $P \in \mathbb{K}[X] \setminus \mathbb{K}$, $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distincts et $m_1, \dots, m_r$ des entiers naturels non nuls. On a équivalence entre :
i) $\forall k \in [\![1, r]\!]$, α_k est racine de P de multiplicité m_k.
ii) $\exists Q \in \mathbb{K}[X]$, $P(X) = Q(X) \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$ et $Q(\alpha_k) \neq 0$ $\forall k \in [\![1, r]\!]$.

Corollaire 6 : Si $P \in \mathbb{K}[X] \setminus \mathbb{K}$ admet $r \geq 1$ racines distinctes $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ de multiplicités respectives $m_1, \dots, m_r$ on a alors $d^\circ P \geq \sum_{k=1}^{r} m_k$.

Corollaire 7 : Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 1$ admet au plus n racines distinctes ou confondues dans $\mathbb{K}$.

Remarque 8 : Le résultat précédent n'est plus valable pour les polynômes à coefficients dans un anneau commutatif unitaire. Par exemple dans $\mathbb{Z}/6\mathbb{Z}[X]$, le polynôme $\bar{3}X$ qui est de degré 1 a deux racines distinctes $x_1 = \bar{0}$ et $x_2 = \bar{2}$.

Corollaire 9 : Si le corps $\mathbb{K}$ est infini, le morphisme de $\mathbb{K}$-algèbres : $P \mapsto \tilde{P}$ qui associe à $P \in \mathbb{K}[X]$ la fonction polynomiale $\tilde{P} \in \mathbb{K}^{\mathbb{K}}$ est injectif.

Remarque 10 : Si $\mathbb{K}$ est un corps fini à $q = p^n$ éléments, $p \in \mathbb{P}$, $n \in \mathbb{N}^*$, alors $|\mathbb{K}^\times| = q - 1$ et $x^{q-1} = 1$ et donc $x^q = x$. La fonction $\tilde{P}$ associée au polynôme $P(X) = X^q - X$ est la fonction nulle, c'est absurde.

Définition 11 : On dit qu'un polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$, s'il est constant ou de degré $n \geq 1$ et admet $r \geq 1$ racines distinctes $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ de multiplicités respectives $m_1, \dots, m_r$ avec $\sum_{k=1}^{r} m_k = n$. Dans ce cas où tous les m_i sont égaux à 1, on dit que le polynôme est scindé à racines simples.

Théorème 12 : On suppose que $\mathrm{car}(\mathbb{K}) = 0$. Pour $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :
i) α est racine d'ordre $m \geq 1$ de P,
ii) $\exists Q \in \mathbb{K}[X]$, $P(X) = Q(X)(X-\alpha)^m$ et $Q(\alpha) \neq 0$
iii) $P^{(k)}(\alpha) = 0$ $\forall k \in [\![0, m-1]\!]$ et $P^{(m)}(\alpha) \neq 0$

B Adjonction de racines (corps de rupture et corps de décomposition) Per X.6

Définition 13 : Soit K un corps, $P \in K[X]$ un polynôme irréductible. Une extension $L \supset K$ est appelée corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ $\alpha \in L$ et $P(\alpha) = 0$.

Exemple 14 : $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de $X^2 + 1$.

Théorème 15 : Soit $P \in \mathbb{K}[X]$, irréductible. Il existe un unique corps de rupture de P sur $\mathbb{K}$ (à isomorphisme près). Il s'agit de $\mathbb{K}[X]/(P)$.

Définition 16 : Soit $P \in \mathbb{K}[X]$ un polynôme irréductible non nul, de degré n. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension L de $\mathbb{K}$ telle que :
i) dans $L[X]$, P est produit de facteurs de degré 1 (ou encore les racines de P sont toutes dans L)
ii) le corps L est minimal pour cette propriété (ou encore les racines de P engendrent L).

Exemple 17 : Un corps de décomposition de $(X^2+2)(X^2+3)$ est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Théorème 18 : Pour tout $P \in \mathbb{K}[X]$, il existe un unique corps de décomposition de P sur $\mathbb{K}$ (à isomorphisme près). On le note $D_{\mathbb{K}}(P)$.

Application 19 : (Théorème de l'élément primitif) Si $\mathrm{car}(\mathbb{K}) = 0$ ou $\mathbb{K}$ fini, soit $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$. Alors il existe $\alpha \in L$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.

II Polynômes symétriques : fonctions symétriques élémentaires.

Rom X.6

On suppose ici $\mathbb{K}$ un corps tel que $\mathrm{car}(\mathbb{K}) \neq 2$ et $P \in \mathbb{K}[X_1, \dots, X_m]$.

Définition 20 : On dit qu'un polynôme $P \in \mathbb{K}[X_1, \dots, X_m]$ est symétrique si pour tout $\sigma \in S_m$, $P(X_{\sigma(1)}, \dots, X_{\sigma(m)}) = P(X_1, \dots, X_m)$.

Exemple 21 : les polynômes $\Sigma_{k,m} = \sum_{1 \leq i_1 < \dots < i_k \leq m} X_{i_1} \cdots X_{i_k}$ où $k \in [\![1, m]\!]$ sont des polynômes symétriques élémentaires.
On a $\Sigma_{1,m} = \sum_{i} X_i$, $\Sigma_{m,m} = X_1 \cdots X_m$.

Théorème 22 : Si P est symétrique, il existe alors un unique polynôme $Q \in \mathbb{K}[X_1, \dots, X_m]$ tel que : $P(X_1, \dots, X_m) = Q(\Sigma_{1,m}, \dots, \Sigma_{m,m})$.

Exemple 23 : Si $P = X^3 + Y^3 + Z^3$ alors $P = \Sigma_{1,3}^3 - 3\Sigma_{1,3}\Sigma_{2,3} + 3\Sigma_{3,3}$.

Application 24 : Soit $P \in \mathbb{Z}[X]$ unitaire. Les fonctions symétriques $\sigma_1, \dots, \sigma_m$ de ses racines $u_1, \dots, u_m$ sont entières. Si $F \in \mathbb{Z}[X_1, \dots, X_m]$ est symétrique, alors $F(u_1, \dots, u_m) \in \mathbb{Z}$.

Définition 25 : Soit $m \geq 2$. On appelle sommes de Newton les polynômes
$S_p = \sum_{i=1}^{m} X_i^p \in \mathbb{R}[X_1, \dots, X_m]$

Proposition 26 : $\forall k \in [\![1, m-1]\!]$, $S_k - \Sigma_1 S_{k-1} + \cdots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k k \Sigma_k = 0$

Proposition 27 : Soit $p \in \mathbb{N}$, $S_{p+m} - \Sigma_1 S_{p+m-1} + \dots + (-1)^{m-1} \Sigma_{m-1} S_{p+1} + (-1)^m \Sigma_m S_p = 0$

Application 28 : Tout polynôme symétrique de $\mathbb{R}[X_1, \dots, X_m]$ peut s'exprimer comme un polynôme en les sommes de Newton $S_1, \dots, S_m$.

Théorème 29 (relation coefficients racines) : Les polynômes symétriques élémentaires vérifient l'égalité fondamentale :
$(T - X_1) \cdots (T - X_m) = T^m - \Sigma_1 T^{m-1} + \Sigma_2 T^{m-2} + \cdots + (-1)^{m-1} \Sigma_{m-1} T + (-1)^m \Sigma_m$.
En particulier, si $P = X^m + a_1 X^{m-1} + \cdots + a_m$ est un polynôme de $\mathbb{K}[X]$ scindé sur $\mathbb{K}$ et si $u_1, \dots, u_m$ sont ses racines, alors $\forall i$, $1 \leq i \leq m$, $(-1)^i a_i = \Sigma_i(u_1, \dots, u_m)$.

III Applications

A Localisation de racines X. G

Théorème 30 (Gauss Lucas) Soit $P \in \mathbb{C}[X]$ non constant. Alors les racines de P' sont dans l'enveloppe convexe des racines de P.

Corollaire 31 : Si $P \in \mathbb{R}[X]$ dont toutes ses racines sont réelles et notées $\alpha_1 < \cdots < \alpha_m$ alors P' admet $m-1$ racines β_i telles que $\alpha_1 < \beta_1 < \alpha_2 < \cdots < \beta_{m-1} < \alpha_m$.

Exemple 32 : Si $P = (X-1)(X-2)(X-3) = X^3 - 6X^2 + 11X - 6$ alors $P' = 3X^2 - 12X + 11$ admet deux racines β_1 et β_2 telles que $1 < \beta_1 < 2 < \beta_2 < 3$.

Théorème 33 (Kronecker) : Si $P \in \mathbb{Z}[X]$ unitaire de degré $m \geq 1$ dont toutes les racines sont de module ≤ 1 et $P(0) \neq 0$ alors toutes les racines de P sont des racines de l'unité.

Lemme 34 : Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, alors : $\forall \varepsilon > 0, \exists m \in \mathbb{N}^*, |e^{2i\pi m\alpha} - 1| < \varepsilon$

Théorème 35 (Kronecker 2) : Si $P \in \mathbb{Z}[X]$ unitaire de racines complexes de modules strictement inférieurs à 1 alors $P = X^q$ ou il existe $k \in \mathbb{N}^*$ tel que $P \mid X^k - 1$.

Corollaire 36 : Dans ce cas $P = X$ ou P est égale à un polynôme cyclotomique Φ_m.

B Polynômes irréductibles et cyclotomie Rom Per

Définition 37 : Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit irréductible s'il est non constant et n'est divisible que par les constantes non nulles ou les polynômes λP avec $\lambda \in \mathbb{K}^*$.

Exemple 38 : Un polynôme de degré 1 : $P(X) = aX + b$ avec $a \neq 0$ est irréductible.

Proposition 39 : Un polynôme de degré 1, 2 ou 3 est réductible dans $\mathbb{K}[X]$ si et seulement si il admet au moins une racine dans $\mathbb{K}$.

Proposition 40 : Un polynôme de degré ≥ 2 et irréductible dans $\mathbb{K}[X]$ n'a pas de racines dans $\mathbb{K}$ (si non il serait divisible par un polynôme de degré 1).

Théorème 41 (d'Alembert Gauss) Les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1.

Théorème 42 : Les polynômes réels irréductibles sont les polynômes de degré 1 et les polynômes de degré 2, $P(X) = aX^2 + bX + c$ tels que $b^2 - 4ac < 0$.

Définition 43 : On définit pour $m \in \mathbb{N}^*$, $\mu_m = \{ z \in \mathbb{C},\ z^m = 1 \}$ l'ensemble des racines $m^{ième}$ de l'unité. On définit de même l'ensemble des racines primitives de l'unité $\mu_m^* = \{ z \in \mathbb{C},\ z^m = 1 \ \forall d < m \ z^d \neq 1 \}$

Définition 44 : On définit le $n^{ième}$ polynôme cyclotomique $\Phi_n(X) = \prod_{u \in \mu_n^*} (X - u)$.

Proposition 45 : On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Remarque 46 : En comparant les degrés on retrouve que $n = \sum_{d|n} \varphi(d)$

Exemple 47 : $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$ ...

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

C Algèbre linéaire / Réduction des endomorphismes X.G BHP

On désignera par E un $\mathbb{K}$-ev de dimension $n \in \mathbb{N}^*$ et soit $u \in \mathcal{L}(E)$.

Définition 48 : Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle polynôme caractéristique de A le polynôme $\chi_A(X) = \det(X I_n - A) \in \mathbb{K}[X]$

Proposition 49 : Soit $A \in \mathcal{M}_n(\mathbb{K})$. On peut écrire :
$\chi_A(X) = X^n - \operatorname{tr} A \, X^{n-1} + \dots + (-1)^n \det A$.

Théorème 50 (Cayley - Hamilton) On a $\chi_u(u) = 0$.

Corollaire 51 : λ est valeur propre de u si et seulement si $\chi_u(\lambda) = 0$.

Proposition 52 (conditions de diagonalisabilité) On a équivalence entre :
i) u est diagonalisable ;
ii) Il existe un polynôme annulateur de u scindés à racines simples ;
iii) π_u est scindé à racines simples
iv) χ_u est scindé et pour toute valeur propre λ, $\dim E_\lambda = \text{multiplicité}(\lambda)$ en tant que racine de χ_u.

Exemple 53 :
- Soit p un projecteur. Alors $X^2 - X$ est un polynôme annulateur de p scindé à racines simples. Les projecteurs sont donc toujours diagonalisables et à valeurs propres dans $\{0, 1\}$.
- Soit s une symétrie. Alors $X^2 - 1$ est un polynôme annulateur de s scindé à racines simples. Les symétries sont donc toujours diagonalisables et à valeurs propres dans $\{-1, 1\}$

Proposition 54 (conditions de trigonalisation) On a équivalence entre :
i) u est trigonalisable
ii) il existe un polynôme annulateur scindé
iii) π_u est scindé
iv) χ_u est scindé

Corollaire 55 : Tout endomorphisme est trigonalisable si $\mathbb{K}$ est algébriquement clos (sur $\mathbb{C}$ par exemple).

Développement (déterminant circulant).
Soient $a_1, \dots, a_n \in \mathbb{C}$. Alors :

$$\det A = \begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & & \\ a_2 & a_3 & \cdots & a_1 \end{vmatrix} = \prod_{k=0}^{n-1} \sum_{i=0}^{n-1} a_{i+1} \omega^{ki} \quad \text{où } \omega = e^{\frac{2i\pi}{n}}$$

On définit par récurrence une suite $(p^{(k)})_{k \in \mathbb{N}}$ par $p^{(0)} = (z_{1,0}, \dots, z_{n,0}) \in \mathbb{C}^n$ et $p^{(k+1)} = \left(\frac{z_{1,k} + z_{2,k}}{2}, \dots, \frac{z_{n-1,k} + z_{n,k}}{2}, \frac{z_{n,k} + z_{1,k}}{2} \right)_{k \in \mathbb{N}}$

Alors $p^{(k)} \to (g, \dots, g)$ où $g = \text{isobar}(z_{1,0}, \dots, z_{n,0})$.

Références

Xavier Gourdon Algèbre X.G

D Perrin Cours d'Algèbre Per

Rombaldi Mathématiques pour l'agrégation Rom

Objectif agrégation Beck BMP