144

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

Contexte : k corps commutatif, $P \in k[X]$, E k espace vectoriel de dimension finie.

I - Généralités sur les racines, applications

I-1 Définitions, propriétés

Def 1 : On dit que $\alpha \in k$ est racine de P si $P(\alpha) = 0$.
La multiplicité de α est le plus grand entier m tel que $(X-\alpha)^m \mid P$. Si $m = 1$, on dit que α est racine simple.

Prop 2 : $\# \{\text{racines de } P\} \leq \deg P$

CE. 3 : Résultat faux si k non intègre. $k = \mathbb{Z}/4\mathbb{Z}$, $P = 2X$ possède 0 et 2 comme racines.

Prop 4 : α est racine de P, de multiplicité m ssi $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$.

Def 5 : On dit que $P \in k[X] \setminus k$ est scindé s'il est produit de polynômes de degré 1 dans $k[X]$.
• k est dit "algébriquement clos" si tout polynôme de degré ≥ 1 est scindé

Ex - Th 6 : [D'Alembert - Gauss]
$\mathbb{C}$ est algébriquement clos.

CE. 7 : $\mathbb{R}$ et $\mathbb{Q}$ ne sont pas algébriquement clos.

I-2 Fractions rationnelles :

Def 8 : Soit $F \in k(X)$; $\frac{P}{Q}$ un représentant de F.
On dit que α est un zéro (resp pôle) de F si $P(\alpha) = 0$ (resp $Q(\alpha) = 0$). La multiplicité du pôle α est le plus petit entier m, tel que $(X-\alpha)^m F(X)$ ne possède pas de pôle en α.

Th 9 : [Décomposition en éléments simples] Si k est algébriquement clos
• $\forall F \in k(X) : \exists ! (E, R_1 ; \dots ; R_m) \in k[X]^{m+1} : F(X) = E(X) + \sum_{i=1}^{m} \frac{R_i}{(X-\alpha_i)^{m_i}}$
avec $\deg R_i < m_i$.
De plus, $\forall i \in [\![1 ; m]\!] : \exists ! (a_{1,i} ; \dots ; a_{m_i,i}) \in k^{m_i} : \frac{R_i}{(X-\alpha_i)^{m_i}} = \sum_{k=1}^{m_i} \frac{a_{k,i}}{(X-\alpha_i)^k}$

Ex 10 : $\frac{X^2+1}{X^4-X^2} = -\frac{1}{X^2} + \frac{1}{X-1} + \frac{1}{X+1}$

App 11 : Calcul d'intégrales de fractions rationnelles.

I.3 Application à la réduction d'endomorphismes : $f \in L(E)$

Def 12 : P est un polynôme annulateur de f si $P(f) = 0_{L(E)}$

Ex 13 : Si f est une symétrie. $X^2 - 1$ est annulateur.

Th 14 [Cayley - Hamilton]
$\chi_f(f) = 0_{L(E)}$

Prop 15 : $\{\text{racines de } \chi_f\} = \{\text{racines de } \mu_f\} = \mathrm{Spec}_k(f)$

Th 16 : f est diagonalisable (resp trigonalisable) ssi il existe un polynôme annulateur de f scindé à racines simples (resp scindé).

II - Fonctions symétriques élémentaires. (A anneau commutatif)

Def 17 : • Soit $P(X_1 ; \dots ; X_n) \in A[X_1, \dots ; X_n]$. On dit que P est un polynôme symétrique si : $\forall \sigma \in S_n$ $P(X_{\sigma(1)} ; \dots ; X_{\sigma(n)}) = P(X_1 ; \dots ; X_n)$.
on note $A[X_1, \dots ; X_n]^{sym}$ leur ensemble.
• Soit $p \in [\![1 ; n]\!]$, on définit le polynôme symétrique élémentaire de degré p : $\Sigma_p := \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$

Ex 18 : $\Sigma_1 = X_1 + \dots + X_n$; $\Sigma_n = X_1 \dots X_n$.

Th 19 [Structure des polynômes symétriques]
(1) $\varphi : A[Y_1 ; \dots ; Y_n] \longrightarrow A[X_1 ; \dots ; X_n]^{sym}$, $F \longmapsto F(\Sigma_1 ; \dots ; \Sigma_n)$ est surjective.
(2) φ est injective.

Ex 20 : $X^3 + Y^3 + Z^3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$

Prop 21. [Relations racines/coefficients]
Soit $P = a_n X^n + \dots + a_1 X + a_0$, scindé, $(\alpha_1;\dots;\alpha_n)$ ses racines.
On pose $\sigma_k := \Sigma_k(\alpha_1;\dots;\alpha_n)$, appelée fonction symétrique élémentaire
alors: $\sigma_1 = \frac{-a_{n-1}}{a_n}$; ... ; $\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$; ... ; $\sigma_n = (-1)^n \frac{a_0}{a_n}$.

Ex 22: $\chi_f = (X-\alpha)(X-\beta)$; $\sigma_1 = -\mathrm{tr}(f)$; $\sigma_2 = \det(f)$

Prop 23: [Relations de Newton] Soient $(\alpha_1;\dots;\alpha_n) \in k^n$, $p \in \mathbb{N}^*$
On note $S_p(\alpha_1;\dots;\alpha_n) := \alpha_1^p + \dots + \alpha_n^p$
- Si $p > n$: $S_p - \sigma_1 S_{p-1} + \dots + (-1)^k \sigma_k S_{p-k} + \dots + (-1)^n \sigma_n S_{p-n} = 0$
- Si $1 \leq p \leq n$: $S_p - \sigma_1 S_{p-1} + \dots + (-1)^k \sigma_k S_{p-k} + \dots + (-1)^{p-1} \sigma_{p-1} S_1 + (-1)^p p S_p = 0$

App 24 (prop 21):
Si p est premier alors $(p-1)! = -1 \mod p$ (théorème de Wilson)

App 25: Résolution de l'équation $z^3 + pz + q = 0$ par la méthode de Lagrange.

III - Caractérisation et localisation des racines

III-1 Localisation.

Prop 26: [Test racines rationnelles]. Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$
Si $\alpha = \frac{p}{q} \in \mathbb{Q}$ est une racine de P alors : $q \mid a_n$ et $p \mid a_0$.
$(p \wedge q = 1)$

Ex 27 : $X^4 + X^2 + 2X - 2$ ne possède pas de racines rationnelles.

Th 28 [Kronecker]
Soit $P \in \mathbb{Z}[X]$ unitaire, $\deg P \geq 1$, irréductible dans $\mathbb{Q}[X]$. Si toutes les racines de P sont de module ≤ 1 dans $\mathbb{C}$. Alors : $P = X$ ou P est un polynôme cyclotomique

Th 29 [Sturm]
Soit $P \in \mathbb{R}[X]$. On pose $S_0 = P$, $S_1 = P'$, $S_{i-1} = A_i S_i - S_{i+1}$
$\deg(S_{i+1}) < \deg S_i$. Soit $x \in \mathbb{R}$, $V(x)$ le nombre de changements de signe de la suite $S_0(x), S_1(x), \dots, S_p(x)$
Si $a < b$ alors P possède $V(b) - V(a)$ racines dans $[a;b]$.

III - 2 Résultant et discriminant :

Def 30 : Soit $P = a_p X^p + \dots + a_0$, $Q = b_q X^q + \dots + b_0$

$$\varphi_{P,Q} : \begin{array}{ccc} k_{q-1}[X] \times k_{p-1}[X] & \longrightarrow & k_{p+q-1}[X] \\ (U,V) & \longmapsto & UP + VQ \end{array}$$

$\mathcal{D} = ((X^{q-1},0);\dots;(1,0);(0,X^{p-1});\dots;(0,1))$, $\mathcal{F} = (X^{p+q-1};\dots;1)$

$A := \mathrm{Mat}_{\mathcal{D},\mathcal{F}}(\varphi_{P,Q})$. On définit le résultant de P et Q par

$$\mathrm{Res}(P,Q) = \det(A).$$

Th 31 : Les conditions suivantes sont équivalentes
(i) P et Q possèdent un diviseur commun non constant.
(ii) $\mathrm{Res}(P,Q) = 0$
(iii) $\exists U \in k_{q-1}[X] \setminus \{0\}$; $\exists V \in k_{p-1}[X] \setminus \{0\}$: $UP = VQ$.

Def 32 : On suppose que $n := \deg P \geq 2$. Le discriminant de P est défini par $\mathrm{dis}(P) = \frac{(-1)^{n(n-1)/2}}{a_n} \mathrm{Res}(P,P')$

Ex 33 :
- $P = aX^2 + bX + c$ $\quad \mathrm{dis}(P) = b^2 - 4ac$
- $P = X^3 + pX + q$ $\quad \mathrm{dis}(P) = 4p^3 + 27q^2$

Prop 34 : Avec les mêmes hypothèses que déf 32.
(i) $P \wedge P' = 1 \iff \mathrm{dis}(P) \neq 0$
(ii) Si P est scindé, alors P est à racines simples ssi $\mathrm{dis}(P) \neq 0$
de plus si $(\alpha_1;\dots;\alpha_n)$ sont les racines de P, alors

$$\mathrm{dis}(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

App 34 bis Résolution de l'équation $z^3 + pz + q = 0$ par la méthode de Cardan.

IV - Racines d'un polynôme et théorie des corps.

IV - 1 - Corps de décomposition.

Def 35. On appelle corps de décomposition de $P \in k[X]$, le plus petit surcorps K de k, tel que P est scindé K.

[de degré $\leq n!$ où $n := \deg P$.]

Ex 36 : $\mathbb{Q}(i)$ est le corps de décomposition de X^2+1 sur $\mathbb{Q}$.

Def 37 : Un polynôme est dit séparable si toutes ses racines sont distinctes dans son corps de décomposition.

Ex 38 : $X^n - 1$ est séparable sur $\mathbb{Q}(\zeta)$; où ζ est une racine n ième de l'unité.

Prop 39 : Si k est de caractéristique nulle ou fini, alors si P est irréductible, P est séparable.

Th 40 : Si K est un corps de décomposition pour $X^{p^n} - X$, sur $\mathbb{F}_p[X]$, (p premier) ; alors $|K| = p^n$.

Ex 41 : $\mathbb{F}_p$ est le corps de décomposition de $X^p - X$, sur $\mathbb{F}_p$.

IV - 2 Nombres algébriques.

Def 42 : Soit $\alpha \in K$, K/k une extension de corps. On dit que α est algébrique sur k si : $\exists f \in k[X] \setminus \{0\} : f(\alpha) = 0$

Une extension est dite algébrique si tout élément est algébrique. Un nombre non algébrique est dit transcendant.

Ex 43 : · $\sqrt{2}$, $\sqrt[3]{3}$ sont algébriques $/ \mathbb{Q}$.

· e, π sont transcendants $/ \mathbb{Q}$.

Th 44 : Si α est algébrique, on construit le plus petit sur corps de k contenant α comme $k[X]/(m_{\alpha,k})$.
($m_{\alpha,k}$ polynôme minimal sur k).

Cor 45 : Si α algébrique $[k(\alpha) : k] = \deg m_{\alpha,k} < +\infty$

Prop 46 : Si K/F est finie, alors K/F est algébrique.

Ex 47 : $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[X]/(X^2+1)$ est une extension de degré 2.

Prop 48 : Si $\begin{array}{c} K \\ | \\ L \\ | \\ F \end{array}$, et K/L et $\begin{array}{c} L \\ | \\ F \end{array}$ sont algébriques, alors K/F est algébrique.

App 49 : $\overline{\mathbb{Q}} := \{ \alpha \in \mathbb{C} \mid$ algébrique sur $\mathbb{Q} \}$ est un corps. (algébriquement clos).

Références : . Oraux X-ENS, algèbre 1, Cassini
· Corps commutatifs et théorie de Galois, P. Tauvel Calvage et Mounet
· Gourdon, les maths en tête, algèbre.
· Dictionnaire des mathématiques, A. Bouvier M. George F. Le Lionnais

THÉORÈME DE D'ALEMBERT-GAUSS

Théorème:

Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos

Etape 1 Afin de démontrer le théorème, nous utiliserons la définition : tout polynôme $P(X) \in \mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$.

En considérant $F(X) = P(X)\overline{P}(X)$, où $\overline{P}$ est le polynôme dont les coefficients sont les complexes conjugués de ceux de P, on se ramène au cas d'un polynôme à coefficients réels : en effet, si $a \in \mathbb{C}$ est une racine de $F(X)$, alors ou bien a est une racine de P, ou bien a est une racine $\overline{P}(X)$, et $\overline{a}$ est une racine de $P(X)$. On a alors $\deg(F) = d = 2^n q$ où q est impair.

Etape 2 Procédons par récurrence sur n :

- Pour $n = 0$, d est impair et $F(X)$ a une racine dans $\mathbb{R}$, en utilisant le Théorème des Valeurs Intermédiaires.
- Supposons $n \geq 1$. Il existe alors une extension $\mathbb{K}'$ de $\mathbb{C}$ et $x_1, ..., x_d \in \mathbb{K}'$ tels que $F(X) = \prod_{i=1}^{d} (X - x_i)$ (en supposant F unitaire, sans perte de généralité). Soit c un élément arbitraire de $\mathbb{R}$. Considérons les éléments $y_{ij} = x_i + x_j + cx_ix_j$ de $\mathbb{K}'$ (avec $i \leq j$); leur nombre est : $\frac{1}{2}d(d+1) = 2^{n-1}q(d+1)$ et $q(d+1)$ est impair.

  Le polynôme $G(X) = \prod_{i \leq j}^{d} (X - y_{ij})$ a pour coefficients les polynômes symétriques à coefficients réels en les x_i. En utilisant le théorème fondamental, ce sont donc des polynômes à coefficients réels en les polynômes symétriques élémentaires des x_i. Ainsi, en utilisant les relations coefficients racines (ie $\sum_k = \frac{(-1)^n a^{n-k}}{a^n}$), les coefficients de $G(X)$ sont réels.

  Comme son degré est de la forme $2^{n-1}q'$ où q' est impair, l'hypothèse de récurrence montre qu'il admet une racine $z_c \in \mathbb{C}$ et l'un des y_{ij}, soit $y_{i(c)j(c)} = x_{i(c)} + x_{j(c)} + cx_{i(c)}y_{j(c)}$ est donc égal à z_c.

  Or comme $\mathbb{R}$ est infini, et l'ensemble des couple $(i,j)/(i \leq j)$ est fini, il existe deux nombres réels distincts c, c' tels que $i(c) = i(c')$ et $j(c) = j(c')$. Notons r, s ces indices. Alors:

$$\begin{cases} x_r + x_s + cx_rx_s &= z_c \quad \in \mathbb{C} \\ x_r + x_s + c'x_rx_s &= z_{c'} \quad \in \mathbb{C} \end{cases}$$

  Par combinaison linéaire, on obtient:

$$\begin{cases} x_r + x_s & \in \quad \mathbb{C} \\ x_sx_r & \in \quad \mathbb{C} \end{cases}$$

  Donc comme x_r et x_s sont racines de l'équation du second degré à coefficients dans $\mathbb{C}$ ($X^2 - SX + P \in \mathbb{C}[X]$), $x_r \in \mathbb{C}$ et $x_s \in \mathbb{C}$. Ainsi $F(X)$ a une racine dans $\mathbb{C}$, et le théorème est démontré.

Référence : P.SAMUEL, *Théorie algébrique des nombres*, HERMANN, APPENDICE P53

THÉORÈME DE KRONECKER

Théorème:

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$ et irréductible dans $\mathbb{Q}[X]$, tel que toutes ses racines sont de module ≤ 1. Alors soit $P = X$ soit $\exists k \in \mathbb{N}^*$ tel que $P | X^k - 1$.

Proposition n° 1 :
Soit $P \in \mathbb{Z}\,[X]$ un polynôme **unitaire**, dont on note les racines $\alpha_1, ..., \alpha_n$.
Alors Les fonctions symétriques $\sum_1, ..., \sum_n$ de ses racines $\alpha_1, ..., \alpha_n$ sont entières. Et si $F \in \mathbb{Z}[X_1, ..., X_n]$ est symétrique, alors $F(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$

Démonstration de la proposition n° 1 :
Si on note $P = \sum\limits_{k=0}^{n} a_k X^k$ étant unitaire $a_n = 1$, et les relations entre polynôme symétrique et coefficients donnent : $\sum_k = (-1)^k \frac{a_{n-k}}{a_n}$. Donc $\forall k \in [1, n] \sum_k \in \mathbb{Z}$.
On a alors le théorème fondmental qui nous permet d'écire qu'il existe un polynôme $G \in \mathbb{Z}[X_1, ..., X_n]$ tel que $F = G(\sum_1, ..., \sum_n)$ et de conclure.

Proposition n° 2 :
Soit $\theta \in \mathbb{R} \setminus \mathbb{Q}$, alors $\forall \varepsilon > 0, \exists k \in \mathbb{N}^*, \ |e^{2ik\pi\theta k} - 1| < \varepsilon$

Démonstration de la proposition n° 2 :

$$\begin{array}{rcll}
e^{i\theta} - 1 & = & 2i\sin(\frac{\theta}{2})e^{i\frac{\theta}{2}} & \text{donc :} \\
|e^{i\theta} - 1| & = & |2\sin(\frac{\theta}{2})| & \\
|e^{i\theta} - 1| & \leq & |\theta| & \text{soit :} \\
|e^{i\theta} - e^{i\theta'}| & \leq & |\theta - \theta'| &
\end{array}$$

Comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, on peut approcher θ par un rationnel à ε près, et on a l'inégalité souhaitée.

Démonstration du théorème :
Soient $\alpha_1, ..., \alpha_n$ les racines de P. Notons $a \in \mathbb{Z}$ le terme constant de P.
Le polynôme P étant unitaire on a : $\prod_{i=1}^{n} \alpha_i = (-1)^n a$.

1. S'il existe i tel que $|\alpha_i| < 1$, par exemple $|\alpha_1| < 1$, alors $|a| = |\alpha_1| \cdot |\prod_{i=2}^{n} \alpha_i| \leq |\alpha_1| < 1$, et comme $a \in \mathbb{Z}$, $a = 0$. Donc $X|P$, et P étant irréducctible et unitaire, $P = X$.
2. Dans le cas contraire, on a $|\alpha_i| = 1$ pour tout i. Considérons pour tout entier $k \geq 1$

$$\pi_k = (\alpha_1^k - 1)(\alpha_2^k - 1)...(\alpha_n^k - 1)$$

   Pour tout k, π_k s'écrit comme un polynôme à coefficients entiers symétrique en les α_i, et donc d'après la proposition n° 1, on a $\pi_k \in \mathbb{Z}$.
   (a) Nous allons montrer qu'il existe k tel que $\pi_k = 0$.
   Comme $|\alpha_1| = 1$, il existe $\theta \in \mathbb{R}$ tel que $\alpha_1 = e^{2i\pi\theta}$. Deux cas se présentent:
      i. Si $\theta \in \mathbb{Q}$, alors il existe $k \in \mathbb{N}^*$ tel que $k\theta \in \mathbb{Z}$, donc $\alpha_1^k = e^{2i\pi k\theta} = 1$, donc $\pi_k = 0$.
      ii. Si $\theta \in \mathbb{R} \setminus \mathbb{Q}$. Compte tenu de la majoration $|\alpha_i^k - 1| \leq 2$ pour tout i, l'expression de π_k entraîne $|\pi_k| \leq |\alpha_1^k - 1| \cdot 2^{n-1}$. Or si $\theta \in \mathbb{R} \setminus \mathbb{Q}$, d'après la proposition n° 2, il existe $k \in \mathbb{N}^*$ tel que $|\alpha_1^k - 1| < 2^{1-n}$, ce qui entraîne que $|\pi_k| < 1$, et comme π_k est un entier, on a forcément $\pi_k = 0$.
   (b) Il existe donc $k \in \mathbb{N}^*$ tel que $\pi_k = 0$, ce qui entraîne l'existence de i tel que $\alpha_i^k = 1$, par exemple $\alpha_1^k = 1$.
   Soit $X^k - 1 = P_1...P_r$ la décomposition de $X^k - 1$ en polynômes irréductibles unitaires de $\mathbb{Q}[X]$.
   Comme α_1 est racine de $X^k - 1$, il existe i tel que $P_i(\alpha_1) = 0$, par exemple $P_1(\alpha_1) = 0$.
   Ainsi, P_1 et P ont une racine commune et ne sont donc pas premiers entre eux dans $\mathbb{Q}[X]$ (l'égalité de Bezout $UP_1 + VP = 1$ appliqué à α_1 mène à une contradiction).
   Ces deux polynômes étant de plus irréductibles et unitaires, ils sont donc égaux.
   En définitive, $P = P_1$ et $P|X^k - 1$

Référence : X.GOURDON, *Les maths en tête, Algèbre*, ELLIPSES, PROBLÈME N° 7 P89