Leçon 144 Racines de polynômes, fonctions symétriques élementaires, exemples et applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
3. Algèbre de Xavier Gourdon
4. Cours d'algèbre de Daniel Perrin
5. Eléments d'analyse et d'algèbre de Pierre Colmez
6. Extensions de corps de Josette Calais
7. Oraux X-ENS Algèbre 1 et 2
8. Petit guide de calcul différentiel de François Rouvière

Développements.

1. Formes de Hankel
2. Irréductibilité des polynômes cyclotomiques
3. Théorème de l'élément primitif

Table des matières

1 Un premier lien entre un polynôme et ses racines

1.1 Racines d'un polynôme

(Chapitre 12.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère K un corps et $P \in K[X]$.

1. Définition : La fonction polynomiale associée à P est $p : x \in K \longmapsto P(x)$
2. Exemple : Si on note $P = \sum_{k=0}^{n} a_k X^k$ alors $p(0) = a_0$
3. Proposition : $P \longmapsto p$ est un morphisme de K-algèbres non injectif a priori
4. Exemple : Si $K = \mathbb{F}_2$ alors $P = X^2 - X \neq 0$ mais $p = 0$
5. Définition : Soit $a \in K$, alors on dit que a est racine de P si $P(a) = 0$
6. Exemple : Un polynôme constant non nul n'a pas de racines et le polynôme nul a tous les éléments de K comme racines
7. Proposition : Soit $a \in K$, alors a racine de P si et seulement si $X - a \mid P$

1.2 Relation degré-racines

(Chapitres 12.5 et 12.10 d'Algèbre et géométrie de Jean-Etienne Rombaldi et Exercice 5.D.26 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

1. Définition : Si P non constant, soit $a \in K$ et $m \in \mathbb{N}^*$, alors on dit que a est racine de multiplicité m de P si $(X-a)^m \mid P$ et $(X-a)^{m+1}$ ne divise pas P
2. Théorème : Si P non constant, soit $a_1, ..., a_r \in K$ deux à deux distincts, alors les assertions suivantes sont équivalentes :
   — Pour tout $k \in [\![1, r]\!]$, a_k est racine de P de multiplicité m_k
   — Il existe $Q \in K[X]$ tel que $P = Q \prod_{k=1}^{r} (X - a_k)^{m_k}$ et $\forall k \in [\![1, r]\!], Q(a_k) \neq 0$
3. Corollaire : Si P non constant admet r racines distinctes $a_1, ..., a_r \in K$ de multiplicité respectives $m_1, ..., m_r$ alors $deg(P) \geq \sum_{k=1}^{r} m_k$
4. Corollaire : Si $deg(P) \geq 1$ alors P admet au plus $deg(P)$ racines
5. Remarque : Le résultat précédent est faux si K est un anneau commutatif unitaire
6. Exemple : Si $K = \mathbb{Z}/6\mathbb{Z}$ et $P = 3X$ alors P admet 0 et 2 comme racines distinctes et $deg(P) = 1$
7. Application : Formes de Hankel : Si $P \in \mathbb{R}[X]$ de degré n et de racines complexes distinctes $x_1, ..., x_t$ $(t \leq n)$ de multiplicités respectives $m_1, ..., m_t$ et $s_k = m_1 x_1^k + ... m_t x_t^k$, alors $\sigma_{\mathbb{R}} := \sum_{0 \leq i,j \leq n-1} s_{i+j} x_i x_j$ est une forme quadratique sur $\mathbb{R}^n$, de plus si on note $(p, q) = sign(\sigma_{\mathbb{R}})$ alors le nombre de racines de P est $t = p + q$ et et le nombre de racines réelles distinctes de P est $p - q$
8. Proposition : Soit $Q \in K[X]$ de degré $deg(Q) \leq deg(P)$ et coïcinde avec P en $deg(P)+1$ points distincts, alors $P = Q$

9. Application : Soit $a_1, ..., a_n \in K$ distincts et $b_1, ..., b_n \in K$, alors il existe un unique polynôme $L \in K[X]$ de degré $deg(L) \leq n-1$, appelé polynôme interpolateur de Lagrange, tel que $\forall i \in [\![1, n]\!], L(a_i) = b_i$
10. Théorème : Si $|K| = +\infty$ alors $P \in K[X] \longmapsto p$ est injectif

2 Les polynômes symétriques pour un second lien

2.1 Fonctions symétriques élémentaires

(Chapitres 2.8.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 2.4.2 d'Algèbre de Xavier Gourdon)

On considère $P \in K[X_1, ..., X_n]$.

1. Définition : On dit que P est symétrique si $\forall \sigma \in S_n, P = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$
2. Exemple : Soit $k \in [\![1, n]\!]$, alors $\Sigma_{k,n} = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1}...X_{i_k}$ est un polynôme symétrique, appelé fonction symétrique élémentaire
3. Exemple : $\Sigma_{1,n} = \sum_{i=1}^{n} X_i, \Sigma_{n,n} = X_1...X_n$
4. Remarque : Les fonctions symétriques élémentaires vérifient $\prod_{k=1}^{n}(X - X_{k,n}) = X^n - \Sigma_{1,n}X^{n-1} + \Sigma_{2,n}X^{n-2} + ... + (-1)^{n-1}\Sigma_{n-1,n}X + (-1)^n\Sigma_{n,n}$
5. Théorème : Si P symétrique alors il existe un unique polynôme $Q \in K[X_1, ..., X_n]$ tel que $P = Q(\Sigma_{1,n}, ...\Sigma_{n,n})$
6. Exemple : Si $P = X^3 + Y^3 + Z^3$ alors $P = \Sigma_{1,3}^3 - 3\Sigma_{1,3}\Sigma_{2,3} + 3\Sigma_{3,3}$
7. Application : Soit $P \in \mathbb{Z}[X]$, $\alpha_1, ..., \alpha_n$ ses racines complexes et $Q \in \mathbb{Z}[X_1, ..., X_n]$ symétrique alors $Q(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$
8. Définition : Les sommes de Newton sont les polynômes $S_p = \sum_{i=1}^{p} X_i^p \in \mathbb{R}[X_1, ..., X_n]$
9. Proposition : $\forall k \in [\![1, n-1]\!], S_k - \Sigma_{1,n}S_{k-1} + ... + (-1)^{k-1}\Sigma_{k-1,n}S_1 + (-1)^k k\Sigma_{k,n} = 0$
10. Proposition : Soit $p \in \mathbb{N}$, alors $S_{p+n} - \Sigma_{1,n}S_{p+n-1} + ... + (-1)^{n-1}\Sigma_{n-1,n}S_{p+1} + (-1)^n\Sigma_{n,n}S_p = 0$
11. Application : Tout polynôme symétrique de $\mathbb{R}[X_1, ..., X_n]$ peut s'exprimer comme un polynôme en les sommes de Newton $S_1, ..., S_n$

2.2 Relation coefficients-racines

(Chapitres 0.4.4 de Eléménts d'analyse et d'algèbre de Pierre Colmez et 2.4.2 d'Algèbre de Xavier Gourdon)

1. Théorème : Soit $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \in K^*$ de racines $\alpha_1, ..., \alpha_n$ dans un corps contenant K, alors $\forall i \in [\![1, n]\!], a_{n-i} = (-1)^i a_n \Sigma_i(\alpha_1, ..., \alpha_n)$

2. Corollaire : Dans ce cas, $\sum_{i=1}^{n}\alpha_i = -\frac{a_{n-1}}{a_n}$ et $\prod_{i=1}^{n}\alpha_i = (-1)^n\frac{a_0}{a_n}$
3. Exemple : Si $P = X^3+aX^2+bX+c$ admet trois racines $\alpha_1, \alpha_2, \alpha_3$ alors $\alpha_1+\alpha_2+\alpha_3 = -a$ et $\alpha_1\alpha_2\alpha_3 = -c$
4. Corollaire : Soit $P = X^n + \sum_{i=0}^{n-1} a_k X^k \in A[X]$ unitaire de racines $\alpha_1, ..., \alpha_n$, alors $\forall i \in [\![0, n-1]\!], \Sigma_i(\alpha_1, ..., \alpha_n) = (-1)^i a_{n-i} \in A[X]$
5. Application : Les entiers algébriques $a \in \mathbb{C}$ (il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(a) = 0$) forment un anneau
6. Proposition : Soit $P = X^3 + pX + q \in \mathbb{R}[X]$ de racins complexes α, β, γ, alors $\Delta := (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-a)^2 = -(4p^3+27q^2)$
7. Application : Dans ce cas, P a trois racines réelles si et seulement si $\Delta \geq 0$
8. Exemple : Si $P = X^3 + X + 1$ alors $\Delta = -31$ donc P n'admet pas trois racines réelles

3 Localisation des racines

3.1 Premiers résultats avec P' et Kronecker

(Exercices 2.2.6 d'Algèbre de Xavier Gourdon, 5.28 de Oraux X-ENS Algèbre 1 et 2.5.7 d(Algèbre de Xavier Gourdon)

1. Proposition : Si $P \in \mathbb{C}[X]$ de degré $deg(P) \geq 2$ alors les racines de P' appartiennent à l'enveloppe convexe des racines de P
2. Corollaire : Si $P \in \mathbb{R}[X]$ dont toutes ses racines sont réelles et notées $\alpha_1 < ... < \alpha_n$ alors P' admet $n-1$ racines β_i tel que $\alpha_1 < \beta_1 < \alpha_2 < ... < \beta_{n-1} < \alpha_n$
3. Exemple : Si $P = (X-1)(X-2)(X-3) = X^3-6X^2+13X-6$ alors $P' = 3X^2-12X+13$ admet deux racines β_1 et β_2 telles que $1 < \beta_1 < 2 < \beta_2 < 3$
4. Théorème de Kronecker (version 1) : Si $P \in \mathbb{Z}[X]$ unitaire de racines complexes de modules inférieurs à 1 et $P(0) \neq 0$ alors toutes les racines de P sont des racines de l'unité
5. Lemme : Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, alors $\forall \varepsilon \in \mathbb{R}_+^*, |e^{2i\pi n\alpha} - 1| < \varepsilon$
6. Théorème de Kronecker (version 2) : Si $P \in \mathbb{Z}[X]$ unitaire de racines complexes de modules strictement inférieurs à 1 alors $P = X$ ou il existe $k \in \mathbb{N}^*$ tel que $P \mid X^k - 1$
7. Corollaire : Dans ce cas, $P = X$ ou P est égale à un polynôme cyclotomique ϕ_n

3.2 Utilisation des matrices compagnons avec les disques de Gehrshgörin

(Chapitres 20.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 4.2 d'Algèbre de Xaiver Gourdon et Exercice 2.5 des Oraux X-ENS Algèbre 2)

1. Définition : Si $P = X^n - \sum_{k=0}^{n} a_k X^k$ alors on lui associe sa matrice compagnon $C_P = \begin{pmatrix} 0 & \dots & 0 & a_0 \\ 1 & \ddots & \vdots & a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \dots & 1 & a_{n-1} \end{pmatrix}$
2. Exemple : Si $P = X^3 + aX^2 + bX + c$ alors $C_P = \begin{pmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{pmatrix}$
3. Théorème : Les polynômes minimal et caractéristique de C_P sont égaux à P
4. Corollaire : Les racines de P sont exactement les valeurs propres de C_P avec les mêmes multiplicités
5. Définition : Soit $A \in M_n(\mathbb{C})$, alors on dit que A est à diagonale strictement dominante si $\forall i \in [\![1, n]\!], |a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}| =: R_i$
6. Lemme d'Hadamard : Soit $A \in M_n(\mathbb{C})$ à diagonale strictement dominante, alors $A \in GL_n(\mathbb{C})$
7. Théorème de Gehrshgörin : Soit $A \in M_n(\mathbb{C})$, alors $Sp(A) \subset \bigcup_{i=1}^{n} D(a_{ii}, R_i)$
8. Remarque : Les $D(a_{ii}, R_i)$ sont appelés les disques de Gehrshgörin
9. Corollaire : Les racines de $P \in \mathbb{C}[X]$ sont incluses dans $\bigcup_{i=1}^{n-1} D(0, R_i) \cup D(a_{n-1}, R_n)$ avec $\forall i \in [\![2, n]\!], R_i = 1 + |a_{i-1}|$ et $R_1 = |a_0|$
10. Exemple : Si $P = X^3 + aX^2 + bX + c$ alors les racines de P sont incluses dans $D(0, |c|) \cup D(0, 1 + |b|) \cup D(a, 1 + |a|)$

3.3 Approche des racines réelles par la méthode de Newton

(Exercice 4.49 du Petit guide de calcul différentiel de François Rouvière)

1. Lemme : Soit $f : [c, d] \subset \mathbb{R} \longrightarrow \mathbb{R}$ de classe C^2 avec $f(c) < 0 < f(d)$ et $f' > 0$, alors f admet un admet un unique point fixe $a \in]c, d[$ et pour tout $x \in [c, d]$, il existe $z \in [a, x]$ tel que $F(x) - a := x - \frac{f(x)}{f'(x)} - a = \frac{1}{2} \frac{f''(z)}{f'(x)} (x - a)^2$
2. Exemple : Si $p(x) = x^2 - y$ avec $y \in \mathbb{R}_+^*$ alors p est de classe $C^2, p(0) = -y < 0 < p(d)$ pour d assez grand
3. Lemme : Dans ce cas il existe $C \in \mathbb{R}_+^*$ tel que $\forall x \in [c, d], |F(x) - a| \leq C|x - a|^2$ et il existe $\alpha \in \mathbb{R}_+^*$ tel que $I = [a - \alpha, a + \alpha]$ soit stable par F
4. Théorème : Méthode de Newton : Dans ce cas, soit $x_0 \in I$, alors $x_n \underset{n \to +\infty}{\longrightarrow} a$ avec $x_{n+1} = F(x_n)$

5. Corollaire : Si de plus $f'' > 0$ alors $I = [a, d]$ est stable par F et pour tout $x_0 \in I$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante (ou constante) avec $0 \leq x_{n+1} - a \leq C(x_n - a)^2$ et $x_{n+1} - a \underset{n\to+\infty}{\sim} \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n - a)^2$
6. Exemple : C'est le cas de $p(x) = x^2 - y$ avec $y \in \mathbb{R}_+^*$
7. Application : Soit $y \in \mathbb{R}_+^*$ et $f(x) = x^2 - y$, alors la méthode de Newton permet d'approcher $\sqrt{y}$

4 Adjonction de racines

4.1 Polynômes irréductibles

(Chapitre 12.8 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On dit que $P \neq 0$ est irréductible s'il est non constant et n'est divisible qur pas les constantes non nulles ou les polynômes λP avec $\lambda \in K^*$
2. Exemple : Si $P = aX + b$ avec $a \in K^*, b \in K$ alors P est irréductible, de plus si K algébriquement clos alors les polynômes de degré 1 sont les seuls polynômes irréductibles
3. Théorème de d'Alembert-Gauss : $\mathbb{C}$ est algébriquement clos, autrement dit si $P \in \mathbb{C}[X]$ non constant alors P admet une racine dans $\mathbb{C}$
4. Proposition : Les polynômes cyclotomiqes $\phi_n \in \mathbb{Z}[X]$ sont irréductibles
5. Proposition : Un polynôme de degré $1, 2$ ou 3 est réductible dans $K[X]$ si et seulement s'il admet au moins une racine dans K
6. Théorème d'Euclide : Si P irréductible et $P \mid \prod_{k=1}^{r} A_k$ avec $A_1, ..., A_r \in K[X]$ alors P divise l'un des A_k
7. Théorème : P se décompose en produit de polynômes irréductibles et une telle décomposition est unique à l'ordre et constante multiplicative près
8. Corollaire : L'ensemble des polynômes unitaires irréductibles de $K[X]$ est infini

4.2 Corps de rupture et de décomposition

(Chapitres 2.3.A et 2.3.C de Extensions de corps de Josette Calais, 13.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et III.1.c et III.2.b du Cours d'algèbre de Daniel Perrin)

1. Définition : Si P irréductible, soit L extension de K, alors on dit que L est un corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$
2. Exemple : Un corps de rupture de $X^2 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2})$
3. Théorème : Si P irréductible alors il existe un corps de rupture de P sur K unique à isomorphisme près, il s'agit de $K[X]/(P)$
4. Définition : Soit L extension de K, alors on dit que L est un corps de décomposition de P sur K si dans $L[X]$ P est produit de facteurs de degré 1 et L est minimal pour cette propriété

5. Exemple : Un corps de décomposition de $X^3 - 2$ est $\mathbb{Q}(\sqrt[3]{2}, j)$
6. Théorème : Il existe un corps de décomposition de P sur K unique à isomorphisme près
7. Application : Théorème de l'élément primitif : Si K de caractéristique nulle ou fini, soit L extension de degré fini de K, alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ (Problème 2.5.8 d'Algèbre de Xavier Gourdon)
8. Application : Soit $p \in \mathbb{N}$ premier et $q = p^n$, alors il existe un corps à q éléments, unique à isomorphisme près, il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$