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

Développements :

Formes de Hankel, Théorème de Chevalley-Warning.

Bibliographie :

Rombaldi, Gourdon, Perrin, RDO, Gozard, Mignotte, Nourdin, H2G2.

Rapport du jury :

Dans cette leçon on peut présenter des méthodes de résolutions, de la théorie des corps, des notions de topologie (continuité des racines) ou même des formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). Notons le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices ; les valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois ou s'intéresser à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin.

1 Racines d'un polynôme

1.1 Premières définitions et propriétés

Définition 1 (Romb p359). *[Gourdon p59] Racine d'un polynôme.*

Exemple 2 (Romb p377). *Les $exp(2ik\pi/n)$ sont les racines de $X^n - 1$ sur $\mathbb{C}$.*

Proposition 3 (Gourdon p59). *[Romb p359] α racine de P si et seulement si $X - \alpha$ divise P.*

Définition 4 (Romb p360). *[Gourdon p59] Ordre d'une racine.*

Proposition 5 (Romb p360). *α racine de P de multiplicité m si et seulement si il existe Q tel que $P = Q(X - \alpha)^m$ et $Q(\alpha) \neq 0$.*

Exemple 6. *1 est racine double de $X^2 + 2X + 1$.*
Les racines nème sont simples sur $\mathbb{C}$.

Exemple 7 (Romb p404). *$\sum 1/k! X^k$.*

Corollaire 8 (Romb p361). *Le degré de P est $\geq$ à la somme des multiplicités des racines.*

Proposition 9 (Romb p361). *Un polynôme de degré n admet au plus n racines.*

Remarque 10 (Romb p361). *Faux dans un anneau commutatif unitaire : $\mathbb{Z}/6\mathbb{Z}$, $3X$ a deux racines, 0 et 2.*

Application 11. *Si 2 polynômes coïncident en $n + 1$ points, ils sont égaux. Interpolation de Lagrange.*

Application 12 (FGN). *Déterminant de Vandermonde.*

Corollaire 13 (Romb p361). *Si K est infini, le morphisme de K algèbres qui à P associe sa fonction polynomiale est injectif.*

Remarque 14 (Gourdon p58). *Si K est infini, on peut donc identifier polynôme et fonction polynomiale.*
Faux dans F_q, car $X^q - X$ est non nul, et sa fonction associée l'est. Ou prendre $\prod_{\alpha \in K)}(X - \lambda)$.

Définition 15 (Romb p362). *Polynôme scindé. Algébriquement clos.*

Proposition 16 (Gourdon p60). *Deux polynômes scindés sont premiers entre eux si et seulement si ils n'ont pas de racine commune.*

Proposition 17 (Romb p362). *[Gourdon p60] En caractéristique nulle, α racine de P d'ordre m si et seulement si $P^{(k)}(\alpha) = 0$ pour tout $k \in \{0, ..., m - 1\}$ et $P^{(m)}(\alpha) \neq 0$.*

Contre exemple 18 (Gourdon p60). *X^3 dans $\mathbb{Z}/3\mathbb{Z}$, 0 est racine d'ordre 3 mais en dérivant 3 le polynôme est nul. $X^p - 1$ ne possède que des racines de multiplicité 1. Pourtant, $P'(X) = 0$ donc toute racine de P annule aussi P'.*

Remarque 19 (Gourdon p60). *En caractéristique qcq, a est racine simple si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.*

Liens racines et irréductibilité

Définition 20 (Romb p368). *Polynôme irréductible. Si P est non constant et si $P = QR$ alors R ou Q est constant.*

Exemple 21 (Romb p368). *Les polynômes de degré 1 sont irréductibles.*

Proposition 22 (Romb p369). *Un polynôme de degré 2 ou 3 est irréductible si et seulement si il n'admet pas de racines.*

Proposition 23 (Romb p369). *Un polynôme de degré ≥ 2 irréductible n'a pas de racines.*

Contre exemple 24 (Perrin). *$(X^2+1)^2$ n'a pas de racines dans Q mais est réductible.*

Théorème 25 (Romb p379). *Théorème de d'Alembert Gauss.*

Corollaire 26 (Romb p379). *Irréductibles de $\mathbb{C}$ et de $\mathbb{R}$.*

Exemple 27. *X^2+X+1 est irréductible dans $F_2[X]$.*

Application 28. *Trigonalisation dans $M_n(\mathbb{C})$.*

Application 29 (Romb). *Tout $u \in L(E)$ admet un plan ou une droite stable.*

1.2 Propriétés topologiques

Proposition 30 (FG). *Continuité des racines de polynômes.*

Proposition 31 (OA). *Les racines dépendent localement de façon $\mathbb{C}^{+\infty}$ du polynôme, et l'ensemble des polynômes scindés à racines constitue un ouvert de $R_n[X]$.*

2 Polynômes symétriques, fonctions symétriques élémentaires

2.1 Définitions et relations coefficients-racines

Proposition 32 (RDO p200). *S_n agit sur $A[X_1,..,X_n]$ par ....*

Définition 33 (RDO p200). *[Romb p57] Polynôme symétrique.*

Définition 34 (Romb p57). *Polynômes symétriques élémentaires.*

Exemple 35 (Romb p57). *$\Sigma_{1,n}$, $\Sigma_{2,n}, \Sigma_{n,n}$.*

Remarque 36. *$\Sigma_{k,n}$ est k homogène.*

Exemple 37. *Le déterminant de Vandermonde V_n n'est pas un polynôme symétrique en les coefficients, mais son carré si.*

Définition 38 (Romb p365). *Fonctions symétriques élémentaires.*

Théorème 39 (Romb p366). *Relation coefficients-racines en fonction des fonctions symétriques élémentaires.*

Application 40 (Romb p367). *Formule du crible de Poincaré.*

2.2 Structure des polynômes symétriques

Théorème 41 (Romb p57). *L'application $P \mapsto P(\Sigma_1,..,\Sigma_n)$ est un isomorphisme d'anneaux A-linéaire entre $A[X_1,..,X_n]$ et $A[X_1,..,X_n]^{\Sigma_n}$.*
Si P est symétrique, il existe un unique polynôme Q tel que $P(X_1,...X_n) = Q(\Sigma_{1,n},...,\Sigma_{n,n})$.

Proposition 42 (RDO p206). *Algorithme de factorisation d'un polynôme symétrique :*
Entrées : P.
Sortie : S tel que $P(\Sigma_1,..,\Sigma_n) = P$.
Initialisation : $S = 0$.
Pour P polynôme symétrique, tant que le monôme de plus haut degré pour l'ordre lexicographique n'est pas
Lorsque P est constant, renvoyer $S + P(0)$.

Proposition 43 (Romb p405). *[RDO p207][FG] Formules de Newton.*

Application 44 (H2G2). *Formule de Hankel.*

Application 45 (Nourdin p257). *A est nilpotente si et seulement si $tr(A^k) = 0$ pour tout k.*

Application 46. *Théorème de Kronecker.*

3 Existence de racines

3.1 Eléments algébriques et transcendants

Définition 47 (Romb p245). *[Perrin p66] Elément algébrique. Elément transcendant.*

Exemple 48 (Romb). *Nombres de Liouville.*

Définition 49 (Perrin p67). *Extension algébrique.*

Définition 50 (Romb p245). *Polynôme minimal.*

Exemple 51 (Perrin p66). *$\sqrt{2}$ i sont algébriques sur Q de polynômes minimaux X^2-2, X^2+1.*

Proposition 52 (Romb p246). *α est algébrique sur K si et seulement si $K[\alpha] = K(\alpha)$ si et seulement si $[K[\alpha] : K] = deg(\Pi_\alpha) < +\infty$.*

Proposition 53 (Romb p247). *Lemme des degrés (base télescopique).*

Exemple 54. *$Q(\sqrt{3},\sqrt{2})$.*

Théorème 55 (Romb p248). *L'ensemble des éléments de L algébriques sur K est un sous-corps de L qui contient K.*

Proposition 56 (Gozard p37). *[Romb p252] Une extension finie est algébrique.*

Exemple 57. $\mathbb{C}$ *est une extension algébrique de* $\mathbb{R}$. $\mathbb{R}$ *n'est pas une extension algébrique de* $\mathbb{C}$ *car* e *et* π *sont transcendants.* $K(T)$ *n'est pas une extension algébrique de* K *car* T *est transcendant sur* K.

Théorème 58. *Si* $x_1, .., x_n$ *sont algébriques sur* K, *alors* $K(x_1, .., x_n)$ *est une extension algébrique finie de* K, *avec* $[K(x_1, .., x_n) : K] \leq \prod [K(x_i) : K]$.

Théorème 59. *Théorème de l'élément primitif. Soit* K *un corps de caractéristique nulle, soit* L *extension de* K *de degré fini. Alors il existe* $x \in L$ *tel que* $L = K(x)$. *De plus,* L *extension de* K, *on a* $[L : K] \leq n$ *si et seulement si pour tout* $x \in L$, $[K(x) : K] \leq n$.

3.2 Corps de rupture et de décomposition

Définition 60 (Romb p418). *Corps de rupture.*

Théorème 61 (Romb p418). *Si* P *est irréductible dans* $K[X]$ *de degré* n *alors* $K[X]/(P)$ *est un corps de rupture de* P *et* P *est le polynôme minimal de* $w = \overline{X}$ *sur* K.

Théorème 62 (Romb p419). *Pour tout polynôme* $P \in K[X]$ *de degré* $n \geq 1$, *il existe un corps de rupture* L *de* P *tel que* $[L : K] \leq n$.

Proposition 63 (Gozard p56). *[Romb p422] Soit* $P \in K[X]$ *un polynôme irréductible et* $L = K(\alpha)$ *un corps de rupture de* P. *Alors* $[L : K] = deg(P)$ *et une base de* L *est formée de la famille* $(1, \alpha, ..\alpha^{deg(P)-1})$ *des classes modulo* (P) *de* $1, X...., X^{deg(P)-1}$.

Corollaire 64 (Gozard p58). *Soit* $P \in K[X]$. *Il existe une extension algébrique simple dans laquelle* P *possède au moins une racine.*

Proposition 65 (Perrin p70). *Soit* $P \in K[X]$ *irréductible. Il existe un corps de rupture sur* K, *unique à isomorphisme de* K*-algèbres près.*

Exemple 66 (Gozard p58). $X^2 - 2$ *a pour corps de rupture* $Q(\sqrt{2})$. $X^3 - 2$ *a pour corps de rupture* $Q(\sqrt[3]{2})$ *mais aussi* $Q(j\sqrt[3]{2})$.
$\mathbb{C}$ *est le corps de rupture de* $X^2 + 1$ *sur* $\mathbb{R}$.

Proposition 67 (Perrin p78). P *est irréductible si et seulement si* P *n'a pas de racines dans les extensions d'indice* $\leq n/2$.

Exemple 68 (Perrin p78). $X^4 + 1$ *est irréductible dans* $\mathbb{Z}[X]$ *mais est pourtant réductible dans tous les* $F_p[X]$. *Cela montre que la méthode de réduction modulo un idéal premier ne couvre pas tous les cas d'irréductibilité.*

Définition 69 (Gozard p59). *Corps de décomposition.*

Exemple 70 (Gozard p60). $\mathbb{C}$ *est un corps de décomposition sur* $\mathbb{R}$ *de* X^2+1. $Q(\sqrt{2})$ *est un corps de décomposition sur* Q *de* $X^2 - 2$.

Contre exemple 71. $Q(\sqrt[3]{2})$ *n'est pas un corps de décomposition sur* Q *de* $X^3 - 2$ *mais simplement un corps de rupture. Son corps de décomposition est* $Q(\sqrt[3]{2}, j\sqrt[3]{2})$ *extension de degré* 6.

Proposition 72 (Gozard p60). *Existence et unicité du corps de décomposition.*

Application 73 (Perrin p73). *Il existe un corps à* $q = p^n$ *éléments, c'est le corps de décomposition de* $X^q - X$ *sur* F_p. *Il est unique à isomorphisme près, noté* F_q.

Application 74. $X^p + X + 1$ *est irréductible dans* $F_p[X]$ *et dans* $\mathbb{Z}[X]$.

Application 75 (Gourdon). *Une démonstration du théorème de Cayley-Hamilton sur un corps quelconque.*

Définition 76 (Gozard p62). *Corps algébriquement clos.*

Exemple 77 (Gozard p62). Q, $\mathbb{R}$ *ne sont pas algébriquement clos.*

Proposition 78 (Gozard p62). *Tout corps algébriquement clos est infini.*

Théorème 79. *(Gozard p62] Théorème de d'Alembert Gauss.* $\mathbb{C}$ *est algébriquement clos.*

Remarque 80. Q *et* F_p *admettent des polynômes irréductibles de tout degré.*

4 Localisation et comptage des racines

4.1 Motivations

u est diagonalisable si et seulement si χ_u est scindé à racines simples.
u est trigonalisable sur $\mathbb{R}$ si et seulement si $sp(u) \subset \mathbb{R}$.
A est définie positive si et seulement si $sp(A) \subset \mathbb{R}_+^*$.
Méthodes itératives avec $\rho(M^{-1}N) < 1$.

4.2 Localisation et approximation des racines réelles

Proposition 81. *Dichotomie pour approximer la racine.*

Théorème 82 (Rombaldi analyse p137). *[Mignotte] Théorème de Rolle.*

Application 83. *Si* P *est un polynôme scindé sur* $\mathbb{R}$, *alors* P' *aussi.*

Proposition 84 (FG p230). *Suites de Sturm pour localiser et approcher les racines réelles.*

Proposition 85. *Méthode de Newton pour approcher les racines d'un polynôme scindé sur* $\mathbb{R}$.

Proposition 86 (Nourdin p259)**.** *Si P est un polynôme à coefficients entiers alors les racines rationnelles de P sont contenues dans* $\{p/q \in Q, pgcd(p,q) = 1, p|a_0, q|a_n\}$.

Proposition 87 (Mignotte p203)**.** *Suites de Strum.*

Proposition 88 (Mignotte)**.** *Règle de Descartes, règle de Newton.*

4.3 Etude des racines complexes

Proposition 89 (Nourdin p259)**.** *[Gourdon p66] Théorème de Gauss-Lucas. Les racines de P' sont dans l'enveloppe convexe des racines de P.*

Proposition 90. *Soit P unitaire de degré n dans $\mathbb{C}[X]$. Alors, pour toute racine $|\lambda|$ de P, on a $|\lambda| \leq 1 + max(|a_i|)$.*

4.4 Racines et valeurs propres

Définition 91 (Nourdin p260)**.** *Matrice compagnon d'un polynome.*

Proposition 92 (FGN AL2)**.** *[Rombaldi] Disques de Gershgorin.*

4.5 Comptage

Proposition 93. *Théorème de Chevalley Warning et EGZ.*

Proposition 94. *Formes de Hankel.*

Proposition 95. *Théorème de Rouché.*