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

Soient $\mathbb{K}$ un corps commutatif et $\mathscr{A}$ une algèbre sur $\mathbb{K}$. À tout polynôme $P = \sum_{i=0}^{n} a_i X^i$ de $\mathscr{K}[X]$, on associe l'application

$$\widetilde{P} : \begin{array}{ccc} \mathscr{A} & \rightarrow & \mathscr{A} \\ x & \mapsto & \sum_{i=0}^{n} a_i x^i \end{array}$$

L'application $P \mapsto \widetilde{P}$ est un morphisme d'algèbres. On notera abusivement $P = \widetilde{P}$ par la suite s'il n'y a pas d'ambiguïté.

I - Polynômes

1. Racines

Soit $P \in \mathbb{K}[X]$.

[GOU21] p. 63

Définition 1. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ (cf. Section II). On dit que $a \in \mathbb{L}$ est une **racine** de P si $P(a) = 0$.

Proposition 2. $a \in \mathbb{K}$ est racine de P si et seulement si $X - a \mid P$.

Application 3 (Polynômes d'interpolation de Lagrange)**.** Soient $a_1, \dots, a_n \in \mathbb{K}$ deux à deux distincts et $b_1, \dots b_n \in \mathbb{K}$. Alors

$$\exists! L \in \mathbb{K}[X] \text{ tel que } \forall i \in [\![1, n]\!], L(a_i) = b_i$$

Définition 4. Soient $a \in \mathbb{K}$ et $h \in \mathbb{N}^*$. On dit que a est **racine de** P **d'ordre** h si $(X-a)^h \mid P$ mais $(X-a)^{h+1} \nmid P$.

Proposition 5. Soient $a_1, \dots, a_r \in \mathbb{K}$ des racines de P distinctes deux à deux et d'ordre $h_1, \dots, h_r$. Alors, $\exists Q \in \mathbb{K}[X]$ tel que

$$P = (X-a_1)^{h_1} \dots (X-a_r)^{h_r} Q(X) \quad \text{et} \quad Q(a_i) \neq 0 \, \forall i \in [\![1, n]\!]$$

Corollaire 6. Si $P \in \mathbb{K}[X]$ est de degré $n \geq 1$, alors P a au plus n racines (comptées avec leur ordre de multiplicité).

Contre-exemple 7. C'est faux en général dans un anneau. Par exemple, si $P = \overline{4}X \in \mathbb{Z}/8\mathbb{Z}[X]$, alors P a trois racines : $\overline{0}$, $\overline{1}$ et $\overline{4}$, mais $\deg(P) = 1$.

Proposition 8. Si $\mathbb{K}$ est infini et $P(x) = 0$ pour tout $x \in \mathbb{K}$, alors $P = 0$.

Contre-exemple 9. Si $\mathbb{K} = \{a_1, \dots, a_n\}$, le polynôme $(X - a_1) \dots (X - a_n)$ est non nul, mais son évaluation en tout élément de $\mathbb{K}$ vaut 0.

Définition 10. P est dit **scindé sur** $\mathbb{K}$ si on peut écrire

$$P = \lambda (X - a_1)^{h_1} \dots (X - a_r)^{h_r}$$

avec $\lambda \in \mathbb{K}$ et pour tout $i \in [\![1, n]\!]$, $a_i \in \mathbb{K}$ et $h_i \in \mathbb{N}^*$.

Définition 11. On appelle **polynôme dérivé** de P le polynôme

$$P' = a_1 + 2a_2 X + \dots + n a_n X^{n-1}$$

Remarque 12. L'application $P \to P'$ est linéaire, et les règles de dérivation coïncident avec les règles usuelles.

Théorème 13 (Formule de Taylor)**.** On suppose $\mathbb{K}$ de caractéristique nulle. Alors tout polynôme F de degré inférieur ou égal à n vérifie

$$\forall a \in \mathbb{K}, F(X) = \sum_{i=0}^{n} \frac{(X - a)^i}{i!} F^{(i)}(a)$$

Corollaire 14. On suppose $\mathbb{K}$ de caractéristique nulle et $P \neq 0$. Alors $a \in \mathbb{K}$ est racine d'ordre h de P si et seulement si

$$\forall i \in [\![1, h-1]\!], P^{(i)}(a) = 0 \quad \text{et} \quad P^{(h)}(a) \neq 0$$

Exemple 15. Le polynôme $P_n = \sum_{i=0}^{n} \frac{1}{i!} X^i$ n'a que des racines simples dans $\mathbb{C}$.

Remarque 16. C'est encore vrai en caractéristique non nulle pour $h = 1$.

2. Polynômes symétriques

Soit A un anneau commutatif unitaire.

Définition 17. Soit $P \in A[X_1, \dots, X_n]$. On dit que P est **symétrique** si p. 83

$$\forall \sigma \in S_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

Exemple 18. Dans $\mathbb{R}[X]$, le polynôme $XY + YZ + ZX$ est symétrique.

Définition 19. On appelle **polynômes symétriques élémentaires** de $A[X_1, \dots, X_n]$ les polynômes noté Σ_p où $p \in [\![1, n]\!]$ définis par

$$\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$$

Exemple 20.
- $\Sigma_1 = X_1 + \dots + X_n$.
- $\Sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j$.
- $\Sigma_n = X_1 \dots X_n$.

Remarque 21. Si $P \in A[X_1, \dots, X_n]$, alors $P(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$ est symétrique. Et la réciproque est vraie.

Théorème 22 (Théorème fondamental des polynômes symétriques)**.** Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors,

$$\exists ! \Phi \in A[X_1, \dots, X_n] \text{ tel que } \Phi(\Sigma_1, \dots, \Sigma_n)$$

Exemple 23. $P = X^3 + Y^3 + Z^3$ s'écrit $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

Application 24 (Relations coefficients - racines)**.** Soit $P = a_0 X^n + \dots + a_n \in \mathbb{K}[X]$ avec $a_0 \neq 0$ scindé sur $\mathbb{K}$, dont les racines (comptées avec leur ordre de multiplicité) sont $x_1, \dots, x_n$. Alors p. 64

$$\forall p \in [\![1, n]\!], \Sigma_p(x_1, \dots, x_n) = (-1)^p \frac{a_p}{a_0}$$

En particulier,
- $\Sigma_1(x_1, \dots, x_n) = \sum_{i=1}^n x_i = -\frac{a_1}{a_0}$.
- $\Sigma_n(x_1, \dots, x_n) = \prod_{i=1}^n x_i = (-1)^n \frac{a_n}{a_0}$.

[DEV]

Application 25 (Théorème de Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité. [I-P] p. 279

Corollaire 26. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Définition 27. On appelle **identités de Newton** les polynômes [GOU21] p. 86

$$S_p = \sum_{i=1}^{n} X_i^p \in \mathbb{R}[X]$$

Proposition 28.
— $\forall k \in [\![1, n-1]\!]$, $S_k = (-1)^{k+1} k \Sigma_k + \sum_{i=1}^{k-1} (-1)^{i+1} \Sigma_i S_{n-k+i}$.
— $\forall p \in \mathbb{N}$, $S_{p+n} = \sum_{i=1}^{n} \Sigma_i S_{p+n-i}$.

[DEV]

Application 29 (Formes de Hankel)**.** On suppose $\mathbb{K} = \mathbb{R}$ et on note $x_1, \dots, x_t$ les racines complexes de P de multiplicités respectives $m_1, \dots, m_t$. On pose [C-G] p. 356

$$s_0 = n \text{ et } \forall k \geq 1,\ s_k = \sum_{i=1}^{t} m_i x_i^k$$

Alors :

(i) $\sigma = \sum_{i,j \in [\![0, n-1]\!]} s_{i+j} X_i X_j$ définit une forme quadratique sur $\mathbb{C}^n$ ainsi qu'une forme quadratique $\sigma_{\mathbb{R}}$ sur $\mathbb{R}^n$.

(ii) Si on note (p, q) la signature de $\sigma_{\mathbb{R}}$, on a :
  — $t = p + q$.
  — Le nombre de racines réelles distinctes de P est $p - q$.

II - Adjonction de racines

Définition 30. On appelle **extension** de $\mathbb{K}$ tout corps $\mathbb{L}$ tel qu'il existe un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$. On notera $\mathbb{L}/\mathbb{K}$ pour signifier que $\mathbb{L}$ est une extension de $\mathbb{K}$ par la suite. [GOZ] p. 21

Remarque 31.
— Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors $\mathbb{L}$ est une extension de $\mathbb{K}$.
— Un morphisme de corps est forcément injectif, donc on peut identifier $\mathbb{K}$ à son image

et dire que $\mathbb{K} \subseteq \mathbb{L}$ de manière abusive.

Exemple 32. $\mathbb{C}$ est une extension de $\mathbb{R}$.

L'idée dans la suite va être de chercher comment “rajouter” des racines à des polynômes pourtant irréductibles sur un corps.

1. Corps de rupture

p. 57

Définition 33. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $P \in \mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P.

Exemple 34.
— Avec les notations précédentes, si $\deg(P) = 1$, $\mathbb{K}$ est un corps de rupture de P.
— $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.
— $\mathbb{F}_4$ est un corps de rupture de $X^2 + X + 1$ sur $\mathbb{F}_2$.

Théorème 35. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$.
— Il existe un corps de rupture de P.
— Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

2. Corps de décomposition

Définition 36. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que $\mathbb{L}$ est un **corps de décomposition** de P si :
— Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1)\dots(X - \alpha_n)$.
— $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

Exemple 37.
— $\mathbb{K}$ est un corps de décomposition de tout polynôme de degré 1 sur $\mathbb{K}$.
— $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.
— Soit $\xi \in \mu_n^*$, alors $\mathbb{Q}[\xi]$ est un corps de décomposition de Φ_n (le n-ième polynôme cyclotomique) sur $\mathbb{Q}$.

Théorème 38. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.
— Il existe un corps de décomposition de P.

— Deux corps de décomposition de P sont $\mathbb{K}$-isomorphes.

3. Clôture algébrique

Définition 39. $\mathbb{K}$ est **algébriquement clos** si tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{K}$.

Exemple 40. — $\mathbb{Q}$ n'est pas algébriquement clos.
— $\mathbb{R}$ non plus.

Proposition 41. Tout corps algébriquement clos est infini.

Théorème 42 (D'Alembert-Gauss)**.** $\mathbb{C}$ est algébriquement clos.

Définition 43. On dit que $\mathbb{L}$ est une **clôture algébrique** de $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 44. — $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
— $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] \setminus \{0\} \text{ tel que } P(\alpha) = 0\}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 45 (Steinitz)**.** (i) Il existe une clôture algébrique de $\mathbb{K}$.
(ii) Deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes.

III - Application en algèbre linéaire

Définition 46. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On appelle : [GOU21] p. 171

— **Polynôme caractéristique** de A le polynôme $\chi_A = \det(A - XI_n)$.

— **Polynôme minimal** de A l'unique polynôme unitaire π_A qui engendre l'idéal $\mathrm{Ann}(A) = \{Q \in \mathbb{K}[X] \mid Q(A) = 0\}$. p. 186

Proposition 47. p. 172

$$\lambda \text{ est valeur propre de } A \iff \chi_A(\lambda) = 0 \iff \pi_A(\lambda) = 0$$

Proposition 48. — A est trigonalisable si et seulement si χ_A est scindé sur $\mathbb{K}$. p. 185

— A est diagonalisable si et seulement si π_A est scindé à racines simples sur $\mathbb{K}$.

Corollaire 49. Si $\mathbb{K} = \mathbb{F}_q$, A est diagonalisable si et seulement si $A^q = A$.

Bibliographie

Nouvelles histoires hédonistes de groupes et de géométries **[C-G]**

Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome 1*. Calvage & Mounet, 13 mai 2017.
`http://www.calvage-et-mounet.fr/2022/05/09/nouvelles-histoires-hedoniste-de-groupes-et-de-geometrie/`.

Les maths en tête **[GOU21]**

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
`https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html`.

Théorie de Galois **[GOZ]**

Ivan Gozard. *Théorie de Galois. Niveau L3-M1*. 2e éd. Ellipses, 1er avr. 2009.
`https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html`.

L'oral à l'agrégation de mathématiques **[I-P]**

Lucas Isenmann et Timothée Pecatte. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2e éd. Ellipses, 26 mars 2024.
`https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html`.