

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

fefef

2025-2026

Table des matières

1	Racines d'un polynôme	1
1.1	Multiplicités	1
1.2	Polynômes scindés	2
2	Polynômes symétriques	2
3	Théorie des corps	3
3.1	Nombres algébriques	3
3.2	Adjonction de racines	3
3.3	Corps finis	4
4	Localisation de racines	4
5	Développements	5
	<i>A est un anneau commutatif unitaire, $\mathbb{K}$ est un corps.</i>	

1 Racines d'un polynôme

1.1 Multiplicités

[6] : Rombaldi ou [3] : Gourdon

Notation 1 (Fonction polynômiale). Pour $P = \sum_{k=0}^n a_k X^k \in A[X]$, on note $\tilde{P} : \alpha \in \mathbb{K} \mapsto \sum_{k=0}^n a_k \alpha^k$ sa fonction polynômiale associée. On notera souvent $P(\alpha)$ plutôt que $\tilde{P}(\alpha)$.

Définition 2 (Racine et multiplicité algébrique). $\alpha \in A$ est racine de $P \in A[X]$ si $P(\alpha) = 0$. Elle est de multiplicité $m \in \mathbb{N}$ si $(X - \alpha)^m \mid P$ et $(X - \alpha)^{m+1} \nmid P$.

Remarque 3. $P \in \mathbb{K}[X]$ de degré ≤ 3 est irréductible (sur $\mathbb{K}$) ssi il n'a pas de racines dans $\mathbb{K}$.

Théorème 4. Supposons que A est intègre. Soit $P \in A[X]$, $\alpha_1, \dots, \alpha_r \in A$ et $m_1, \dots, m_r \in \mathbb{N}$. Alors $\forall 1 \leq k \leq r, \alpha_k$ est racine de P de multiplicité m_k ssi $\exists Q \in A[X], P(X) = Q(X) \prod_{k=1}^r (X - \alpha_k)^{m_k}$ et $\forall 1 \leq k \leq r, Q(\alpha_k) \neq 0$.

Corollaire 5. Si A est intègre, $P \in A[X]$ de degré $n \in \mathbb{N}$ a au plus n racines (comptées avec multiplicités).

Exemple 6. C'est faux si A n'est pas intègre : $3X$ a pour racines 0 et 2 dans $\mathbb{Z}/6\mathbb{Z}[X]$.

Corollaire 7 (Fonction polynômiale). Si A est intègre et infini, alors $P \in A[X] \mapsto \tilde{P} \in A^A$ est injectif.

Exemple 8. Sur $\mathbb{Z}/p\mathbb{Z}$ avec p premier, $X^p - X$ et 0 ont mêmes fonctions polynômiales.

Théorème 9 (Taylor). Si $\mathbb{K}$ est de caractéristique nulle, et $P \in \mathbb{K}[X]$, alors $\forall \alpha \in \mathbb{K}, P = \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$.

Théorème 10 (Multiplicité analytique). Si $\mathbb{K}$ est de caractéristique nulle, $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$, les ASSE

- α est racine de P de multiplicité (algébrique) m
- $\exists Q \in \mathbb{K}[X], P(X) = Q(X)(X - \alpha)^m$ avec $Q(\alpha) \neq 0$
- $\forall 0 \leq k \leq m-1, P^{(k)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

Exemple 11. C'est faux en caractéristique finie p : 0 est racine de $F = X^p$ de multiplicité algébrique p mais $F^{(p)}(0) = 0$.

1.2 Polynômes scindés

Définition 12 (Polynôme scindé). $P \in A[X]$ de degré $n \in \mathbb{N}$ est scindé sur A s'il admet des racines distinctes $\alpha_1, \dots, \alpha_r \in A$ de multiplicités $m_1, \dots, m_r$ telles que $\sum_{k=1}^r m_i = n$. Il est dit scindé à racines simples si les m_i valent tous 1.

Définition 13 (Corps algébriquement clos). $\mathbb{K}$ est algébriquement clos si tout $P \in \mathbb{K}[X] \setminus \{0\}$ est scindé (sur $\mathbb{K}$), ou de manière équivalente, tout $P \in \mathbb{K}[X]$ non constant admet une racine dans $\mathbb{K}$.

Théorème 14 (D'Alembert-Gauss). $\mathbb{C}$ est algébriquement clos.

Exemple 15. $X^n - 1 = \prod_{k=1}^n (X - e^{2i\pi k/n})$.

Corollaire 16. Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les $aX^2 + bX + c$ avec $a \neq 0$ et $b^2 - 4ac < 0$.

Proposition 17. Les valeurs propres de $M \in M_n(\mathbb{K})$ sont les racines de χ_M (polynôme caractéristique) et μ_M (polynôme minimal).

Théorème 18. M est trigonalisable (sur $\mathbb{K}$) ssi χ_M est scindé (sur $\mathbb{K}$). M est diagonalisable (sur $\mathbb{K}$) ssi μ_M est SARS (sur $\mathbb{K}$).

Remarque 19. Sur un corps algébriquement clos, tout endomorphisme est trigonalisable.

2 Polynômes symétriques

[3] : Gourdon

Définition 20 (Polynôme symétrique). $P \in A[X_1, \dots, X_n]$ est symétrique si $\forall \sigma \in \mathfrak{S}_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

Exemple 21 (Polynômes symétriques élémentaires et sommes de Newton). — $\forall 0 \leq k \leq n, \Sigma_k := \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$ est symétrique
— $\forall p \in \mathbb{N}, S_p := \sum_{i=1}^n X_i^p$ est symétrique

Proposition 22 (Relations racines/coefficients). Si $P = \sum_{k=0}^n a_k X^k = \prod_{i=1}^n (X - \alpha_i)$ est scindé sur A , alors $\forall 0 \leq k \leq n, a_k = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} \alpha_{i_1} \dots \alpha_{i_k}$.

Proposition 23 (Identités de Newton). $\forall k \geq 1, S_k + \sum_{j=1}^{k-1} (-1)^j \Sigma_j S_{k-j} + (-1)^k k \Sigma_k = 0$ (avec pour convention $\Sigma_p = 0$ pour $p > n$).

Corollaire 24. $\forall p \geq 1, \exists \Phi_p \in \mathbb{Z}[T_1, \dots, T_n], S_p = \Phi_p(\Sigma_1, \dots, \Sigma_n)$, et $\forall 1 \leq k \leq n, \exists \Psi_k \in \mathbb{Q}[T_1, \dots, T_n], \Sigma_k = \Psi_k(S_1, \dots, S_n)$.

Théorème 25 (Fondamental). Soit $P \in A[X_1, \dots, X_n]$ symétrique, alors il existe un unique $Q \in A[T_1, \dots, T_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$.

Exemple 26. $S_2 = \Sigma_1^2 - 2\Sigma_2, \sum_{i=1}^n \sum_{j \neq i} X_i^2 X_j = \Sigma_1 \Sigma_2 - 3\Sigma_3$.

[1] : Berhuy

Corollaire 27 (Entiers algébriques). L'ensemble des entiers algébriques $\overline{\mathbb{Z}} := \{x \in \mathbb{C} \mid \exists P \in \mathbb{Z}[X] \text{ unitaire}, P(x) = 0\}$ est un sous-anneau de $\mathbb{C}$.

Définition 28 (Discriminant). Soit $P = \sum_{k=0}^n a_k X^k = a_n \prod_{k=1}^n (X - \alpha_k) \in A[X]$ scindé. Le discriminant de P est $\text{disc}(P) = a_n^{2(n-1)} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 \in A$.

Proposition 29. Notons A_0 l'anneau engendré par 1_A . Il existe $Q \in A_0[T_0, \dots, T_n]$ tel que $\text{disc}(P) = Q(a_0, \dots, a_n)$. De plus, $\text{disc}(P) \neq 0$ ssi P est à racines simples.

Exemple 30. — $\text{disc}(aX^2 + bX + c) = b^2 - 4ac$
— $\text{disc}(X^3 + pX + q) = -4p^3 - 27q^2$

Remarque 31. Si $P \in \mathbb{K}[X]$ est de degré < 5 , ses racines s'expriment à l'aide de $\text{disc}(P)$ et de racines k -ième. Il n'existe pas de telle formule si $\deg P \geq 5$ (théorème d'Abel, admis).

3 Théorie des corps

[5] : Perrin ou [4] : Gozard

Dans cette partie, $\mathbb{L}$ est une extension de $\mathbb{K}$.

3.1 Nombres algébriques

Définition 32 (Nombre algébrique et transcendant). $\alpha \in \mathbb{L}$ est algébrique si $\text{eval}_\alpha : P \in \mathbb{K}[X] \mapsto P(\alpha) \in \mathbb{L}$ est non injectif, i.e. $\exists P \in \mathbb{K}[X] \setminus \{0\}, P(\alpha) = 0$.

Dans ce cas, $\ker(\text{eval}_\alpha) = (\mu_{\alpha, \mathbb{K}})$ avec un unique polynôme unitaire $\mu_{\alpha, \mathbb{K}} \in \mathbb{K}[X]$, appelé polynôme minimal de α (sur $\mathbb{K}$).

Si α n'est pas algébrique, il est dit transcendant.

Exemple 33. $\sqrt{2}, i, 2^{1/3}$ sont algébriques sur $\mathbb{Q}$, de polynômes minimaux $X^2 - 2, X^2 + 1, X^3 - 2$. e et π sont transcendants sur $\mathbb{Q}$ [admis].

Presque tous (pour la mesure de Lebesgue) les nombres complexes sont transcendants sur $\mathbb{Q}$.

Théorème 34. Soit $\alpha \in \mathbb{L}$. Les ASSE :

- α est algébrique sur $\mathbb{K}$
- $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$
- $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$

Lorsque c'est le cas, $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = [\mathbb{K}(\alpha) : \mathbb{K}] = \deg(\mu_{\alpha, \mathbb{K}})$.

Définition 35. $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}$ est algébriquement clos et $\forall \alpha \in \mathbb{L}, \alpha$ est algébrique sur $\mathbb{K}$.

Théorème 36 (Steinitz). [Admis] $\mathbb{K}$ admet une clôture algébrique, unique à isomorphisme près.

Proposition 37. Si $\mathbb{L}$ est algébriquement clos, alors $\bar{\mathbb{K}}_{\mathbb{L}} := \{x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K}\}$ est une clôture algébrique de $\mathbb{K}$.

3.2 Adjonction de racines

Définition 38 (Corps de rupture). Soit $P \in \mathbb{K}[X]$ irréductible (sur $\mathbb{K}$). $\mathbb{L}$ est un corps de rupture de P sur $\mathbb{K}$ s'il existe $\alpha \in \mathbb{L}$ tel que $P(\alpha) = 0$ et $\mathbb{L} = \mathbb{K}(\alpha)$.

Lemme 39 (Prolongement des isomorphismes). Soit $i : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ un isomorphisme (de corps), qui se prolonge en $\hat{i} : \mathbb{K}_1[X] \rightarrow \mathbb{K}_2[X], \sum a_k X^k \mapsto \sum i(a_k) X^k$, isomorphisme (d'anneaux).

- Si $P \in \mathbb{K}_1[X]$ est irréductible (sur $\mathbb{K}_1$), alors $\hat{i}(P)$ est irréductible (sur $\mathbb{K}_2$).
- Si $\mathbb{K}_1 \subset \mathbb{L}_1, \mathbb{K}_2 \subset \mathbb{L}_2, \alpha_1, \alpha_2$ racines resp. de P et $\hat{i}(P)$ dans $\mathbb{L}_1$ et $\mathbb{L}_2$, alors $\exists ! j : \mathbb{K}_1(\alpha_1) \rightarrow \mathbb{K}_2(\alpha_2)$ isomorphisme (de corps) qui prolonge i tel que $j(\alpha_1) = \alpha_2$.

Théorème 40 (Existence et unicité du corps de rupture). Soit $P \in \mathbb{K}[X]$ irréductible (sur $\mathbb{K}$). Il existe un corps de rupture de P , unique à isomorphisme près (c'est $\mathbb{K}[X]/(P)$).

Application 41. $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$ est irréductible sur $\mathbb{K}$ ssi P n'a pas de racines dans les extensions $\mathbb{L}$ telles que $[\mathbb{L} : \mathbb{K}] \leq n/2$.

Définition 42 (Corps de décomposition). Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$. $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si $\exists \alpha_1, \dots, \alpha_n \in \mathbb{L}, P = a(X - \alpha_1) \dots (X - \alpha_n)$ et $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$.

Théorème 43 (Existence et unicité du corps de décomposition). Il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près, noté $D_{\mathbb{K}}(P)$.

Exemple 44. $\mathbb{C} = \mathbb{R}(i)$ est le corps de rupture et de décomposition de $X^2 + 1$ sur $\mathbb{R}$. $\mathbb{Q}(2^{1/3})$ est le corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$, mais pas de décomposition, qui est $\mathbb{Q}(2^{1/3}, j)$.

3.3 Corps finis

Dans cette sous-partie, $\mathbb{K}$ est un corps de caractéristique p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

Lemme 45 (Morphisme de Frobenius). $F : x \in \mathbb{K} \mapsto x^p \in \mathbb{K}$ est un morphisme de corps appelé morphisme de Frobenius. Si $\mathbb{K}$ est fini, c'est un automorphisme.

Théorème 46 (Existence et unicité des corps finis). Il existe un corps à q éléments, c'est $D_{\mathbb{Z}/p\mathbb{Z}}(X^q - X)$. Il est unique à isomorphisme près, on le note $\mathbb{F}_q$.

Remarque 47. Plus précisément, si $\overline{\mathbb{F}_p}$ est une clôture algébrique de $\mathbb{F}_p$, il y a dans $\overline{\mathbb{F}_p}$ un unique corps à q éléments, c'est l'ensemble des racines de $X^q - X$.

Proposition 48. Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. En particulier $\mathbb{F}_q^*$ est cyclique.

Remarque 49. On peut aussi construire $\mathbb{F}_q$ si on a $P \in \mathbb{F}_p[X]$ irréductible de degré n avec $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ (corps de rupture de P sur $\mathbb{F}_p$). Par exemple $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. Cela permet d'obtenir les tables d'opérations de $\mathbb{F}_q$ (cf annexe).

Théorème 50 (Chevalley-Warning). [DEV] Soit $P_1, \dots, P_r \in \mathbb{F}_q[X_1, \dots, X_m]$ tels que $\sum_{i=1}^r \deg(P_i) < m$. Si $V := \{(x_1, \dots, x_m) \in \mathbb{F}_q^m \mid \forall 1 \leq i \leq r, P_i(x_1, \dots, x_m) = 0\}$, alors $\#V \equiv 0 \pmod p$.

Application 51 (Erdős-Ginzburg-Ziv). [DEV] Parmi $2n - 1$ entiers on peut en trouver n dont la somme est divisible par n .

4 Localisation de racines

[3] : Gourdon

Proposition 52 (Rolle). Si $P = a(X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r} \in \mathbb{R}[X]$ est scindé, alors $\forall 1 \leq j \leq r-1, \exists! \beta_j \in]\alpha_j, \alpha_{j+1}[$ tels que les racines de P' sont les α_i avec multiplicités $m_i - 1$ ($1 \leq i \leq r$) et les β_j ($1 \leq j \leq r-1$).

Théorème 53 (Gauss-Lucas). Soit $P \in \mathbb{C}[X]$ non constant, alors $Z(P') \subset \text{Conv}(Z(P))$.

[2] : Caldéro

Lemme 54 (Gerschgorin-Hadamard). Soit $M \in M_n(\mathbb{C})$, et $\forall 1 \leq i \leq n, D_i(M) := D(m_{i,i}, \sum_{j \neq i} |m_{i,j}|)$. Alors $\text{Sp}(M) \subset \mathcal{D}(M) := \bigcup_{i=1}^n D_i(M)$.

Proposition 55 (Borne de Cauchy). [Source ?] Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{C}[X]$ unitaire et $\alpha \in \mathbb{C}$ une racine de P . Alors $|\alpha| \leq 1 + \max_{0 \leq k \leq n-1} |a_k|$.

Théorème 56 (Continuité des racines). [DEV] Soit $(P_k)_{k \in \mathbb{N}} \in \mathbb{C}_n[X]^{\mathbb{N}}$ tous de degré n , tel que $P_k \xrightarrow[k \rightarrow +\infty]{} P \in \mathbb{C}[X]$. On note $\lambda_{k,i}$ (resp. λ_i) pour $1 \leq i \leq n$ les racines de P_k (resp. P). Alors on peut permuter pour tout $k \in \mathbb{N}$ les $\lambda_{k,i}$ pour que $\forall 1 \leq i \leq n, \lambda_{k,i} \xrightarrow[k \rightarrow +\infty]{} \lambda_i$.

Application 57 (Composantes connexes des disques de Gershgorin). [DEV] Notons $\bigcup_{j=1}^k C_j$ la décomposition de $\mathcal{D}(M)$ en composantes connexes, et pour tout $1 \leq j \leq k, n_j$ le nombre de disques $D_i(M)$ inclus dans C_j . Alors il y a exactement n_j valeurs propres de M (avec multiplicités) dans C_j .

Exemple 58. $M = \begin{pmatrix} 0 & 6 \\ 1 & 1 \end{pmatrix}$ a ses deux valeurs propres -2 et 3 dans $D_1(M) = D(0, 6)$.

[7] : Beck, Malick, Peyré

Théorème 59 (Régularité des racines d'un polynôme SARS). Soit $P_0 \in \mathbb{R}_n[X]$ SARS et $x_0 \in \mathbb{R}$ une racine simple de P_0 . Alors il existe un voisinage U de P_0 dans $\mathbb{R}_n[X]$, un voisinage V de x_0 dans $\mathbb{R}$ et $\varphi : U \longrightarrow V$ de classe C^∞ telle que $\forall P \in U, \forall x \in V, x = \varphi(P) \iff P(x) = 0$.

Application 60. L'ensemble des polynômes de $\mathbb{R}_n[X]$ scindés à n racines simples est un ouvert de $\mathbb{R}_n[X]$.

5 Développements

- Disques de Gershgorin connexité, [2]
- Théorème de Chevalley-Waring + EGZ, [8]

Références

- [1] Grégory Berhuy. *Algèbre, le grand combat*. Calvage and Mounet, 2020.
- [2] Philippe Caldero and Marie Peronnier. *Carnet de voyage en Algèbre, nouvelle édition revue et enrichie*. Calvage and Mounet, 2022.
- [3] Xavier Gourdon. *Algèbre*. ellipses, 2009.
- [4] Ivan Gozard. *Théorie de Galois, 2e édition*. ellipses, 2009.
- [5] Daniel Perrin. *Cours d'algèbre*. ellipses, 1996.
- [6] Jean-Etienne Rombaldi. *Mathématiques pour l'agrégation, Algèbre et géométrie*. deboeck supérieur, 2021.
- [7] Gabriel Peyré Vincent Beck, Jérôme Malick. *Objectif Agrégation*. HK, 2005.
- [8] Maxime Zavidovique. *Un max de maths*. Calvage and Mounet, 2013.