

I Généralités

I.1 Racines d'un polynôme

[Rom21] Soit $\mathbb{K}$ un corps.

Thm 1. L'anneau $\mathbb{K}[X]$ est euclidien, et donc principal.

Lemme 2. Pour tout $\alpha \in \mathbb{K}$, l'application $ev_\alpha : \mathbb{K}[X] \rightarrow \mathbb{K}$, $P \mapsto P(\alpha)$ est un morphisme d'algèbre.

Déf 3. Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine de P , si $P(\alpha) = 0$.

Thm 4. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. α est une racine de P , si et seulement si, $(X - \alpha) \mid P$.

Déf 5. Soient $P \in \mathbb{K}[X]$ non constant et $\alpha \in \mathbb{K}$ une racine de P . On dit que α est une racine de multiplicité $m \in \mathbb{N}^*$ de P si $(X - \alpha)^m \mid P$, et $(X - \alpha)^{m+1} \nmid P$. On notera m_α la multiplicité d'une racine α de P . Si $m_\alpha = 1$, on dit que α est une racine simple.

Thm 6. Soient $P \in \mathbb{K}[X]$ non constant, $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distincts, et $m_1, \dots, m_r \in \mathbb{N}^*$. Les deux assertions suivantes sont équivalentes :

- i) Pour tout $i \in \llbracket 1, r \rrbracket$, α_i est une racine de P de multiplicité m_i .
- ii) Il existe $Q \in \mathbb{K}[X]$ tel que $P = Q \prod_{i=1}^r (X - \alpha_i)^{m_i}$, et pour tout $i \in \llbracket 1, r \rrbracket$, $Q(\alpha_i) \neq 0$.

Cor 7. Si $P \in \mathbb{K}[X]$ non constant admet $r \geq 1$ racines distincts $\alpha_1, \dots, \alpha_r$, alors $\deg P \geq \sum_{i=1}^r m_{\alpha_i}$.

Cor 8. Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 1$ racines distinctes ou confondues dans $\mathbb{K}$.

Cor 9. Si $\mathbb{K}$ est infini, l'application qui à un polynôme $P \in \mathbb{K}[X]$ lui associe sa fonction polynomiale $\tilde{P}$, est un morphisme de $\mathbb{K}$ -algèbre injectif de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$.

C-ex 10. Pour $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, le polynôme $P = X^p - X \in \mathbb{K}[X]$ n'est pas nul, alors que sa fonction polynôme associée est nulle.

I.2 Dérivation de polynômes

[Rom21]

Déf 11. Le polynôme dérivé de $P = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$ est le polynôme P' défini par : $P'(X) = 0$ si P est constant, $P'(X) = \sum_{i=1}^n i a_i X^{i-1}$.

Prop 12. L'application $D : \mathbb{K}[X] \rightarrow \mathbb{K}[X]$, $P \mapsto P'$ est linéaire. De plus, pour tout polynômes $P, Q \in \mathbb{K}[X]$, $(PQ)' = P'Q + PQ'$, et $(P \circ Q)' = Q'P' \circ Q$.

Thm 13 (Taylor polynomiale). On suppose que $\mathbb{K}$ est de caractéristique nulle. Alors pour tout $P \in \mathbb{K}[X]$ de degré n et pour tout $a \in \mathbb{K}$, $P = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X - a)^k$, où $P^{(k)} = D^k(P)$.

Cor 14. On suppose que $\mathbb{K}$ est de caractéristique nulle. Pour $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$, les propositions suivantes sont équivalents :

- i) α est une racine de P de multiplicité m .
- ii) Il existe $Q \in \mathbb{K}[X]$ tel que $Q(\alpha) \neq 0$ et $P(X) = Q(X)(X - \alpha)^m$.
- iii) Pour tout $k \in \llbracket 0, m - 1 \rrbracket$, $P^{(k)}(\alpha) = 0$, et $P^{(m)}(\alpha) \neq 0$.

Rq 15. Lorsque $\mathbb{K}$ est de caractéristique nulle, on dispose alors de deux définitions de la multiplicité d'un polynôme : une algébrique, et une analytique.

I.3 Polynômes symétriques

[Odi23] Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. On note $\mathfrak{S}_n$ le groupe des permutations.

Thm 16. Soit $\sigma \in \mathfrak{S}_n$. L'application $F_\sigma : \mathbb{K}[X_1, \dots, X_n] \rightarrow \mathbb{K}[X_1, \dots, X_n]$, $P(X_1, \dots, X_n) \mapsto P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ est un endomorphisme d'algèbre. Autrement dit, $\mathfrak{S}_n$ agit par automorphisme d'algèbre sur $\mathbb{K}[X_1, \dots, X_n]$.

Déf 17. Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. On dit que P est symétrique s'il est invariant par l'action de $\mathfrak{S}_n$ par automorphisme d'algèbre sur $\mathbb{K}[X_1, \dots, X_n]$. Autrement dit, pour tout $\sigma \in \mathfrak{S}_n$, $F_\sigma(P) = P$. On note $\mathbb{K}[X_1, \dots, X_n]^{\mathfrak{S}_n}$ l'ensemble des polynômes symétriques.

Ex 18. (Somme de Newton) Pour tout $k \geq 0$, $S_k^n = X_1^k + \dots + X_n^k$ est symétrique.

Déf 19. Pour $1 \leq k \leq n$, on définit le k -ième polynôme symétrique élémentaire comme étant $\sigma_k^n = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k} \in \mathbb{K}[X_1, \dots, X_n]$.

Prop 20. Pour tout k , $\sigma_k^n \in \mathbb{K}[X_1, \dots, X_n]^{\mathfrak{S}_n}$.

Ex 21. Pour $n = 3$, $\sigma_1^3 = X_1 + X_2 + X_3$, $\sigma_2^3 = X_1X_2 + X_1X_3 + X_2X_3$ et $\sigma_3^3 = X_1X_2X_3$

Rq 22. Pour tout $0 \leq k < n$, $\sigma_k^n(X_1, \dots, X_{n-1}, 0) = \sigma_k^{n-1}$.

Thm 23 (Relations coefficients-racines). Dans l'algèbre des polynômes

$$\mathbb{K}[X_1, \dots, X_n, T] : \prod_{i=1}^n (T - X_i) = T^n - \sigma_1^n T^{n-1} + \sigma_2^n T^{n-2} + \dots + (-1)^n \sigma_n^n$$

Cor 24. Soit $P \in \mathbb{K}[X]$ tel que $P = a_0X^n + a_1X^{n-1} + \dots + a_n$, $a_0 \neq 0$. Si P se factorise de la forme $P = a_0(X - \alpha_1) \dots (X - \alpha_n)$, alors $a_n = a_0(-1)^n \alpha_1 \dots \alpha_n$, $a_1 = -a_0(\alpha_1 + \dots + \alpha_n)$, et plus généralement, pour tout $i \in \llbracket 1, n \rrbracket$, $a_i = a_0(-1)^i \sigma_i^n(\alpha_1, \dots, \alpha_n)$.

Ex 25. Soit $P = aX^2 + bX + c$, $a \neq 0$. Soit x_1 et x_2 ses racines. Alors $\frac{c}{a} = x_1x_2$ et $\frac{b}{a} = x_1 + x_2$.

Thm 26. Soit $P \in \mathbb{K}[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Il existe un unique polynôme $Q \in \mathbb{K}[Y_1, \dots, Y_n]$, tel que $P = Q(\sigma_1^n, \dots, \sigma_n^n)$.

Ex 27. Pour $n = 2$, $S_1^2 = X_1 + X_2 = \sigma_1^2$, $S_2^2 = X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = \sigma_1^2(X_1, X_2)^2 - 2\sigma_1^2(X_1, X_2) = Q(\sigma_1^2, \sigma_2^2)$, pour $Q(X, Y) = Y^2 - 2X$.

II Etude des racines dans des corps particuliers

II.1 Dans $\mathbb{C}[X]$

Thm 28 (D'Alembert-Gauss). Tout polynôme $P \in \mathbb{C}[X]$ est scindé.

Prop 29. Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X]$. Si $\alpha > 0$ vérifie $\alpha^n \geq \sum_{k=0}^{n-1} |a_k| \alpha^k$, alors si l'on note $M = \max\{|z| : P(z) = 0\}$, on a que $M \leq \alpha$

Prop 30. Avec les mêmes notations :

- (Borne de Cauchy) $M \leq \max\{1, \sum_{k=0}^{n-1} |a_k|\}$

- $M < 1 + \max_{0 \leq k \leq n-1} |a_k|$

Prop 31 (Gauss-Lucas). Soit $P \in \mathbb{C}[X]$ et $Z = \{z : P(z) = 0\}$ l'ensemble des racines. Alors les racines de P' sont toutes dans l'enveloppe convexe de Z .

II.2 Dans $\mathbb{R}[X]$

Prop 32. Soit $P \in \mathbb{R}[X]$. Si $z \in \mathbb{C}$ est une racine de P , alors $\bar{z}$ est une racine de P .

Thm 33 (DEV 1 - Formes de Hankel). Soit $P \in \mathbb{R}[X]$. Il existe une forme quadratique réelle de signature (p, q) telle que le nombre de racines distinctes de P est $p + q$, et le nombre de racines réelles distinctes de P est $p - q$.

App 34. Soit $P = aX^2 + bX + c$, $a \neq 0$. Soient $\Delta = b^2 - 4ac$ et Q la forme de Hankel de P .

- Si $\Delta > 0$, Q est de signature $(2, 0)$ et donc P admet 2 racines réelles.
- Si $\Delta = 0$, Q est de signature $(1, 0)$ et donc P admet 1 racine réelle de multiplicité 2.
- Si $\Delta < 0$, Q est de signature $(1, 1)$ et donc P admet 0 racine réelle.

Déf 35. [Ulm18] Soit $f \in \mathbb{R}[X]$, et $a, b \in \mathbb{R}$ avec $f(a), f(b) \neq 0$. Une suite de Sturm sur $[a, b]$ est une suite $f_0 = f, f_1, \dots, f_r$ avec $f_i \in \mathbb{R}$ telle que :

- f_r n'a pas de racines dans $[a, b]$.
- $\forall i \in \llbracket 1, r-1 \rrbracket, \forall \gamma \in [a, b]$, si $f_i(\gamma) = 0$, alors $f_{i-1}(\gamma)f_{i+1}(\gamma) < 0$.
- Si pour $\gamma \in]a, b[$, $f_0(\gamma) = 0$, alors f_0f_1 est une fonction strictement croissante sur un voisinage de γ .

Le nombre de changements de signes dans une suite de réels est le nombre de changement de négatif à positif, ou vice versa, ignorant les zéros. Notons $\delta_{f_i}(\gamma)$ le nombre de changements de signes dans $f_0(\gamma), f_1(\gamma), \dots, f_r(\gamma)$.

Ex 36. Soit $f \in \mathbb{R}[X]$ sans facteurs carrés, $b > a \in \mathbb{R}$ qui ne sont pas des zéros de f . On considère la suite $f_0 = f, f_1, \dots, f_r \in \mathbb{R}[X]$ définie par : $f_0 = f$, $f_1 = f'$, pour f_i non constant, $f_{i-1} = f_i q_i - f_{i+1}$, avec $\deg(f_{i+1}) < \deg(f_{i-1})$, et f_r constant. Alors $(f_0, f_1, \dots, f_r)$ est une suite de Sturm.

Thm 37 (Sturm). Soit $f \in \mathbb{R}[X]$, $b > a \in \mathbb{R}$ tels que $f(a), f(b) \neq 0$ et $f_0 = f, f_1, \dots, f_r$ une suite de Sturm pour f sur $[a, b]$. Le nombre de racines réelles distinctes de $f \in \mathbb{R}[X]$ dans l'intervalle $[a, b]$ est $\delta_{f_i}(a) - \delta_{f_i}(b)$.

Ex 38. Le polynôme $X^4 + X + 1$ possède deux racines réelles distinctes dans $] - 2, 2[$.

III Applications

III.1 Lien avec la réduction

Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$.

Déf 39. On appelle polynôme caractéristique de A le polynôme $\chi_A = \det(XI_n - A) \in \mathbb{K}[X]$.

Thm 40. λ est une valeur propre de A , si et seulement si, $\chi_A(\lambda) = 0$.

Cor 41. On suppose $\mathbb{K} = \mathbb{C}$. Si l'on note $\chi_A = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X]$, alors $a_{n-1} = \text{Tr } A$ et $a_0 = \det A$. Plus généralement, pour tout $k \in \llbracket 0, n-1 \rrbracket$, a_k est la somme des mineurs diagonaux d'ordre $n-k$ de A .

Déf 42. Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}[X]$, on appelle matrice compagnon

associée à P la matrice $C_P := \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & \dots & 1 & -a_{n-1} \end{pmatrix}$

Thm 43. $\chi_{C_P} = P$.

Rq 44. Étudier les racines d'un polynôme revient à rechercher les valeurs propres de sa matrice compagnon associée.

III.2 Irréductibilité du polynôme cyclotomique

Soit $n \in \mathbb{N}^*$.

Déf 45. On note $\mathbb{U}_n := \{z \in \mathbb{C} : z^n = 1\}$ l'ensemble des racines n -ième de l'unité. On note $\mathbb{V}_n = \{\zeta \in \mathbb{U}_n : \text{ord}(\zeta) = n\}$ l'ensemble des racines $n^{\text{ième}}$ primitives de l'unité.

Déf 46. Le n -ième polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est défini par : $\Phi_n(X) = \prod_{\zeta \in \mathbb{V}_n} (X - \zeta)$. On a $\deg(\Phi_n) = \varphi(n)$.

Thm 47 (DEV 2). $X^n - 1 = \prod_{d|n} \Phi_d$, $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

C-ex 48. $\Phi_8 = X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout p premier.

Cor 49. Soit m premier avec n , $\zeta \in \mathbb{V}_n$ et $\zeta' \in \mathbb{V}_m$. On a alors :

1. Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$. En particulier, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. On appelle extension cyclotomique une telle extension.
2. $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\zeta') = \mathbb{Q}$

Bibliographie

- [Odi23] Alain Ninet ODILE FLEURY Loic Foissy. *Algèbre et calcul formel*. 2eme edition. ellipses, 2023.
- [Rom21] Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation : Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 2021.
- [Ulm18] Felix ULMER. *Anneaux, corps, résultants*. ellipses, 2018.