P. Maurer
ENS Rennes

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

Devs :

- Théorème de Gauss-Wantzel
- Etude des polynômes cyclotomiques

Références :

1. Gozard, Théorie de Galois
2. Perrin, Cours d'algèbre
3. Gourdon, Algèbre

Dans ce qui suit, K désigne un corps commutatif.

1 Racines d'un polynôme

1.1 Définitions et propriétés

On se donne $P \in K[X]$.

Définition 1. *Soit L/K une extension de K. On dit que $a \in L$ est racine de P si $P(a) = 0$.*

Proposition 2. *Soit $a \in K$. Alors a est une racine de P si et seulement si $X - a | P$.*

Définition 3. *Soit $a \in K$ et $h \in \mathbb{N}^*$. On dit que a est une racine d'ordre h de P si $(X-a)^h | P$ et $(X-a)^{h+1} \nmid P$.*

Proposition 4. *Soit $a_1, \dots, a_r \in K$ des racines (deux à deux distinctes) de P d'ordre $h_1, \dots, h_r$. Il existe $Q \in K[X]$ tel que $P = (X-a_1)^{h_1} \cdots (X-a_r)^{h_r} Q(X)$, et $\forall i \in [\![1, r]\!]$ $Q(a_i) \neq 0$.*

Corollaire 5. *Si P est de degré $n \geq 1$, alors P a au plus n racines (comptées avec leur ordre de multiplicité).*

Remarque 6. Le corollaire 5 est faux si K est seulement un anneau. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, le polynôme $P = 4X$ a trois racines qui sont $\overline{0}$, $\overline{2}$ et $\overline{4}$ mais $\deg(P) = 1$.

Corollaire 7. *Soit A une partie infinie de K. Si $\forall a \in A \quad P(a) = 0$, alors P est le polynôme nul.*

Remarque 8. Sur un corps fini, cela n'est pas vrai : $P = (X - \overline{0}) \cdots (X - \overline{p-1}) \in \mathbb{F}_p[X]$ n'est pas le polynôme nul, pourtant il vérifie $P(x) = 0$ pour tout $x \in \mathbb{F}_p$.

Corollaire 9. *Si K est infini, alors il y a une bijection entre $K[X]$ et les fonctions polynomiales de $\mathbb{K}$ vers $\mathbb{K}$.*

Définition 10. *Un polynôme $P \in K[X]$ est dit scindé sur K si on peut écrire*

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

avec $\lambda \in K$, $r \in \mathbb{N}$ et $\forall i \in [\![1, r]\!] \quad a_i \in K$ et $h_i \in \mathbb{N}^*$.

Remarque 11. Deux polynômes de $K[X]$ scindés sur K sont premiers entre eux si et seulement si ils n'ont pas de racine commune.

Théorème 12. *(Formule de Taylor). Si K est de caractéristique nulle, tout polynôme $P \in K[X]$ de degré inférieur à $n \in \mathbb{N}$ vérifie*

$$\forall a \in K \quad P(X) = \sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a).$$

Théorème 13. *Si K est de caractéristique nulle et $P \in K[X]$ est non nul, alors $a \in K$ est racine d'ordre h de P si et seulement si $\forall i \in [\![0, r-1]\!] \quad P^{(i)}(a) = 0$ et $P^{(h)}(a) \neq 0$.*

Remarque 14. Le polynôme $X^3 \in \mathbb{F}_3[X]$ admet 0 pour racine de mulitplicité 3, pourtant $P^{(3)}(0) = 0$. Le théorème 13 est faux en caractéristique quelconque. En revanche, le résultat subsiste pour caractériser les racines simples.

Proposition 15. *(Interpolation de Lagrange). Soit $a_1, \dots, a_n \in K$ deux à deux distincts et $b_1, \dots, b_n \in K$. Il existe un unique polynôme $L \in K[X]$ tel que $\deg(L) \leq n-1$ et $\forall i \in [\![1, n]\!] \quad L(a_i) = b_i$. On l'appelle le polynôme interpolateur de Lagrange associé à $(a_1, \dots, b_n)$ et $(b_1, \dots, b_n)$.*

1.2 Adjonction de racines

Définition 16. *Soit $P \in K[X]$ un polynôme irréductible dans $K[X]$. On dit que L est un corps de rupture de P si et seulement si L est une extension monogène de K engendrée par K et une racine, notée α, de P.*

Remarque 17. L est alors une extension de K de degré $\deg(P)$.

Exemple 18. Si $\deg(P) = 1$, K est un corps de rupture de P.

Théorème 19. *Soit $P \in K[X]$ irréductible.*

1. *Il existe un corps de rupture de P.*

2. *Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de P, alors L et L' sont K-isomorphes : il existe un unique K-isomorphisme $t : L \to L'$ tel que $t(\alpha) = \beta$.*

Définition 20. *Soit L une extension de K. Soit $P \in K[X]$, avec $\deg(P) = n \in \mathbb{N}^*$. On dit que L est un corps de décomposition de P sur K si P s'écrit $P(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L$ et si $L = K(\alpha_1, \ldots, \alpha_n)$.*

Exemple 21. $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$, et $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$.
$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $\sqrt[3]{2}$ sur $\mathbb{Q}$ mais pas un corps de décomposition.

Théorème 22. *Soit $P \in K[X]$ de degré $n \geq 1$.*

1. *Il existe un corps de décomposition L de P sur K, avec $[L : K] \leq n!$*
2. *Si L et L' sont deux corps de décomposition de P sur K, alors il existe un K-isomorphisme de L dans L'.*

Théorème 23.
Soit p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.

1. *Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*
2. *En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.*

1.3 Extension algébrique et clotûre

Définition 24. *Soit L/K une extension, et $A \subset L$. On dit que A engendre L, et on écrit $L = K(A)$ si L est le plus petit sous-corps de L contenant A et K. Si A est fini et $A = \{\alpha_1, \ldots, \alpha_n\}$, on note $L = K(\alpha_1, \ldots, \alpha_n)$.*

Définition 25. *Soit K un corps et L une extension de K. Soit $\varphi : K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = \mathrm{id}_K$ et $\varphi(T) = \alpha$.*

Si φ est injectif, on dit que α est transcendant sur K. Sinon, on dit que α est algébrique sur K, et l'idéal $I = \mathrm{Ker}\,\varphi$ étant principal, on a $I = (P)$ avec P irréductible (que l'on peut supposer unitaire). Le polynôme P est, par définition, le polynôme minimal de α sur K, et on le note μ_α.

Exemple 26. $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$, mais pas π ni e.

Remarque 27. Le polynôme minimal d'un élément α algébrique sur K est l'unique polynôme unitaire irréductible de $K[X]$ qui annule α.

Exemple 28. $X^2 + 1$ est le polynôme minimal de i sur $\mathbb{Q}$. $X - i$ est le polynôme minimal de i sur $\mathbb{C}$.

Théorème 29. *Soit $K \subset L$ une extension et $\alpha \in L$. Les propriétés suivantes sont équivalentes :*

- *α est algébrique sur K*
- *On a $K[\alpha] = K(\alpha)$*
- *On a $\dim_K K[\alpha] < \infty$*

Dans ce cas, on a $\deg(\mu_\alpha) = [K(\alpha) : K]$.

Définition 30. *Une extension L/K est dite finie si on a $[L : K] < \infty$. Elle est dite algébrique si tous les éléments de L sont algébriques sur K.*

Définition 31. *Les conditions suivantes sont équivalentes :*

1. *Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K*
2. *Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine sur K*
3. *Les seuls polynômes irréductibles de $K[X]$ sont de degré 1*
4. *Toute extension algébrique de K est identique à K lui-même.*

On dit que K est algébriquement clos.

Exemple 32. $\mathbb{Q}$ n'est pas algébriquement clos, car $X^2 - 2$ et $X^3 - 2$ n'ont pas de racines dans $\mathbb{Q}$.
$\mathbb{R}$ n'est pas algébriquement clos, car $X^2 + 1$ et $X^2 + X + 1$ n'ont pas de racine dans $\mathbb{R}$.

Proposition 33. *Tout corps algébriquement clos est infini.*

Théorème 34. *(D'Alembert-Gauss)*
$\mathbb{C}$ est algébriquement clos.

Définition 35. *Soit K un corps, L une extension de K. On dit que L est une clotûre algébrique de K si L est algébrique sur K et si L est algébriquement clos.*

Exemple 36. $\mathbb{C}$ est une clotûre algébrique de $\mathbb{R}$.

2 Polynômes symétriques et fonctions symétriques élémentaires

Soit A un anneau commutatif unitaire, et $n \in \mathbb{N}$.

2.1 Relations coefficients et racines

Proposition 37. *Le groupe $\mathcal{S}_n$ agit sur l'anneau (ou la A-algèbre) $A[X_1, \ldots, X_n]$ via*

$$(\sigma P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Définition 38. *Soit $P \in A[X_1, \ldots, X_n]$. Les conditions suivantes sont équivalentes :*

- *Pour tout $\sigma \in \mathcal{S}_n$, $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$.*

- *Pour tout* $(i,j)\in[\![1,n]\!]^2$ *avec* $i<j$, *on a*

$$P(X_1,\dots,X_i,\dots,X_j,\dots,X_n)=P(X_1,\dots,X_j,\dots,X_i,\dots,X_n).$$

On dit que P *est un polynôme symétrique et on note* $A[X_1,\dots,X_n]^{\mathcal{S}_n}$ *l'ensemble des polynômes symétriques sur* A. *C'est une sous-algèbre de* $A[X_1,\dots,X_n]$.

Exemple 39. Le polynôme $\prod_{i\neq j}(X_i-X_j)$ est symétrique. $X_1+X_2+X_3+X_4$ est symétrique.

Définition 40. *(Polynômes symétriques élémentaires)*
Soit $k\in[\![1,n]\!]$. *On note* $\sum_k$, *et on appelle* $k^{\text{ème}}$ *fonction (ou polynôme) symétrique élémentaire, le polynôme* $\displaystyle\sum_{1\leq i_1<\dots<i_k<n} X_{i_1}\cdots X_{i_k}\in A[X_1,\dots,X_n]$.

Proposition 41. *Pour tout* $k\in[\![1,n]\!]$, $\sum_n\in A[X_1,\dots,X_n]^{\mathcal{S}_n}$.

Exemple 42. On a $\Sigma_1=X_1+\dots+X_n$, $\Sigma_2=\displaystyle\sum_{1\leq i<j\leq n}X_iX_j$ et $\Sigma_n=X_1\cdots X_n$.

Théorème 43. *(Relations coefficients-racines). Soit* $P\in A[X]$, *et* $(\alpha_1,\dots,\alpha_n)\in A^n$. *Les conditions suivantes sont équivalentes :*

- $P(X)=(X-\alpha_1)\cdots(X-\alpha_n)$
- $P(X)=X^n+a_{n-1}X^{n-1}+\dots+a_0$, *où*

$$\forall i\in[\![1,n]\!]\quad a_{n-i}=(-1)^i\textstyle\sum_i(\alpha_1,\dots,\alpha_n).$$

Exemple 44. En particulier, les racines de P vérifient $\alpha_1+\dots+\alpha_n=-a_{n-1}$ et $\alpha_1\cdots\alpha_n=(-1)^n a_0$.

2.2 Structure des polynômes symétriques

Définition 45. *Soit un monôme* $aX_1^{\alpha_1}\cdots X_n^{\alpha_n}$, *où* $a\in A^*$ *et* $\alpha_i\in\mathbb{N}$. *On appelle poids de ce monôme l'entier* $\displaystyle\sum_{i=1}^n i\alpha_i$. *Pour* $P\in A[X_1,\dots,X_n]$ *non nul, on appelle poids de* P *le maximum des poids des monômes dont il est somme.*

Exemple 46. Le poids de $\sum_k$ est $nk-k(k-1)/2$.

Proposition 47. *Soit* P *un polynôme non nul de* $A[X_1,\dots,X_n]$ *et* π *son poids. Alors le polynôme* Q *défini par* $Q(X_1,\dots,X_n)=P(\Sigma_1,\dots,\Sigma_n)$ *est un polynôme symétrique de degré* $\leq\pi$.

Lemme 48. *Soit* $P\in A[X_1,\dots,X_n]$ *tel que pour tout* $j\in[\![1,n]\!]$, $P(X_1,\dots,X_{j-1},0,X_{j+1},\dots,X_n)=0$. *Alors* P *est divisible par* $\Sigma_n=X_1\cdots X_n$ *dans* $A[X_1,\dots,X_n]$.

Théorème 49. *Soit* $P\in A[X_1,\dots,X_n]$ *un polynôme symétrique de degré* k. *Il existe un unique polynôme* $Q\in A[X_1,\dots,X_n]$ *tel que* $P(X_1,\dots,X_n)=Q(\Sigma_1,\dots,\Sigma_n)$. *Ce polynôme* Q *est de poids* k *et de degré égal au degré partiel de* P *par rapport à l'une des indéterminées* $X_1,\dots,X_n$.

2.3 Discriminant

Dans cette partie, on se place de nouveau sur un corps K.

Définition 50. *Soit* $P\in K[X]$ *un polynôme de degré* $n\geq 2$, *et* $\alpha_1,\dots,\alpha_n$ *les racines de* P *dans son corps de décomposition sur* K. *On appelle discriminant de* P *sur* K *et on note* $\operatorname{disc}(P)$ *l'élément*

$$\operatorname{disc}(P):={a_n}^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2,$$

où a_n *est le coefficient dominant de* P.

Proposition 51. *Soit* $\lambda\in K$. *Le polynôme* $S=\lambda^{2n-2}\prod_{i<j}(X_i-X_j)^2=(-1)^{n(n-1)/2}\lambda^{2n-2}\prod_{i<j}X_i-X_j$ *est symétrique.*

Corollaire 52. *Soit* $P\in K[X]$ *un polynôme de degré* $n\geq 2$, *et* $\alpha_1,\dots,\alpha_n$ *les racines de* P *dans son corps de décomposition sur* K. *Il existe* $Q\in K[X_1,\dots,X_n]$ *tel que* $\operatorname{disc}(P)=Q(\sigma_1,\dots,\sigma_n)$, *où* $\sigma_k=\sum_k(\alpha_1,\dots,\alpha_n)$.

Corollaire 53. $P\in K[X]$ *est à racines simples ssi* $\operatorname{disc}(P)\neq 0$.

Exemple 54. Si $P(X)=aX^2+bX+c$ est de degré 2, $\operatorname{disc}(P)=\Delta=b^2-4ac$.

3 Applications

3.1 Racine primitives $n^{\text{èmes}}$ et cyclotomie

Dans ce qui suit, K est un corps et $n\in\mathbb{N}^*$ est un entier tel que $\operatorname{car}(K)\nmid n$.

Définition 55. *On appelle groupe des racines* $n^{\text{èmes}}$ *de l'unité dans* K, *et on note* $\mu_n(K)$ *l'ensemble* $\{\zeta\in K:\zeta^n=1\}$. *Une racine* $n^{\text{ème}}$ *de l'unité est dite primitive si de plus, pour tout* k *divisant* n, *on a* $\zeta^k\neq 1$. *On note* $\mu_n^*(K)$ *l'ensemble des racines primitives* $n^{\text{èmes}}$ *de l'unité.*

Définition 56. *Le* $n^{\text{ème}}$ *polynôme cyclotomique sur* K *est défini par :*

$$\Phi_{n,K}(X):=\prod_{\zeta\in\mu_n^*(K)}X-\zeta.$$

Lemme 57. *$\Phi_{n,K}(X)$ est unitaire, de degré $\varphi(n)$, et vérifie $X^n - 1 = \prod_{d|n} \Phi_{d,K}(X)$.*

Développement 1 :

Théorème 58. *(Polynômes cyclotomiques rationnels)*

i. $\Phi_{n,\mathbb{Q}}(X)$ est à coefficients dans $\mathbb{Z}$.

ii. $\Phi_{n,\mathbb{Q}}(X)$ est irréductible sur $\mathbb{Z}$.

Théorème 59. *(Cas des corps finis)*

Les propositions suivantes sont équivalentes :

i. Il existe p premier, avec $p \wedge n = 1$, tel que $\Phi_{n,\mathbb{F}_p}(X)$ soit irréductible sur $\mathbb{F}_p$.

ii. $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Développement 2 :

Théorème 60. *(Gauss-Wantzel)*

Soit p un nombre premier impair, et $\alpha \in \mathbb{N}^*$. Alors l'angle $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat, c'est-à-dire $p = 1 + 2^{2^\beta}$ pour un certain $\beta \in \mathbb{N}$.

3.2 Racines et réduction des endomorphismes

Soit E un espace vectoriel sur un corps commutatif K, et $A \in \mathcal{M}_n(K)$.

Définition 61. *On appelle polynôme caractéristique de A (resp. de f) le polynôme de $K[X]$ défini par $\chi_A(X) = \det(A - XI_n)$ (resp. $\chi_f(X) = \det(f - X\,\mathrm{Id})$).*

Proposition 62. *χ_A est un polynôme de degré n. Si $\chi_A = (-1)^n \sum_{k=0}^{n} a_k X^k$, alors on a $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(A)$ et $a_0 = (-1)^n \det(A)$.*

Théorème 63. *(Cayley-Hamilton)*

On a $\chi_f(f) = 0$. Autrement dit, le polynôme minimal divise le polynôme caractéristique.

Corollaire 64. *Les valeurs propres de f sont racines de son polynôme caractéristique (en fait, ce sont les seules).*

Proposition 65. *(Condition suffisante de diagonalisabilité)*

Si χ_f est scindé à racines simples, alors f est diagonalisable.

Théorème 66. *Les propositions suivantes sont équivalents :*

- *f est diagonalisable.*
- *μ_f est scindé à racines simples dans k.*
- *χ_f est scindé dans k et $\dim(E_\lambda) = v_\lambda$, où v_λ désigne la multiplicité de λ en tant que racine de χ_f.*
- *$E = \bigoplus_{\lambda \in \mathrm{Sp}(f)} E_\lambda$.*

Corollaire 67. *Si f possède n valeurs propres distinctes, alors f est diagonalisable.*