

K désigne un corps commutatif.

I) Racines d'un polynôme.

1) Définitions et premières propriétés

Def 1: Soit $P \in K[X]$. On dit que $a \in K$ est une racine de P si $P(a) = 0$.

Ex 2: Les racines complexes de $X^n - 1$ sont les racines n -ième de l'unité.

Prop 3: Soit $a \in K$ et $P \in K[X]$.

$(a \text{ est une racine de } P) \Leftrightarrow (X-a \text{ divise } P)$

Def 4: Soit $P \in K[X]$, $a \in K$ et $k \in \mathbb{N}^*$. On dit que a est une racine d'ordre k de P si $(X-a)^k | P$ et $(X-a)^{k+1} \nmid P$.

Thm 5: Si K est de caractéristique 0, et si $P \in K[X]$, $P \neq 0$, alors $a \in K$ est une racine d'ordre k de $P \Leftrightarrow \forall 0 \leq i \leq k-1, P^{(i)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Cte-ex 6: Le théorème est faux en caractéristique non nulle, comme le montre le contre-exemple suivant:

$P = X^3 \in \mathbb{Z}/3\mathbb{Z}[X]$ et $a = \bar{0}$: a est racine d'ordre 3 et $P^{(3)}(a) = 0$.

Prop 7: Si $P \in K[X]$ est de degré $n \geq 1$, alors P a au plus n racines.

Cte-ex 8: Le résultat précédent est faux sur un anneau: $P = 4Z \in \mathbb{Z}/8\mathbb{Z}$ est de degré 1 et a 3 racines: $\bar{0}, \bar{2}, \bar{4}$.

Prop 9: Soit $P \in K[X]$ tel que $\forall x \in K, P(x) = 0$. Si K est infini, alors $P = 0$.

Cte-ex 10: Si K est fini, le résultat est faux:

Si $K = \{a_1, \dots, a_n\}$, alors $P = (X-a_1) \cdots (X-a_n)$ est non nul mais vérifie $P(x) = 0 \forall x \in K$.

App 11: Si K est infini, la prop 9 montre qu'il y a bijection entre $K[X]$ et les fonctions polynômes de K dans K .

Cor 12: Soient $a_1, \dots, a_n \in K$ deux à deux distincts.

$\varphi: K^{n-1}[X] \xrightarrow{P} K^n$
 $P \mapsto (P(a_1), \dots, P(a_n))$ est un isomorphisme.

App 13: $\begin{vmatrix} 1 & a_1 & \dots & a_1^{n-1} \\ 1 & a_2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_j - a_i)$ (déterminant de Vandermonde)

Def 14: $P \in K[X]$ est dit scindé sur K si on peut écrire $P = 1 \prod_{i=1}^n (X-a_i)^{m_i}$ avec $\lambda \in K, a_i \in K, m_i \in \mathbb{N}^*$.

Def 15: $P \in K[X]$ est dit irréductible si P n'est pas constant et si $P = QR \Rightarrow Q$ ou R est constant.

Prop 16: Tout polynôme de degré 1 est irréductible.
 • Tout polynôme irréductible de degré > 1 n'a pas de racine.

Cte-ex 17: $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$ mais est réductible dans $\mathbb{Q}[X]$.

Prop 18: Les polynômes irréductibles de degré 2 ou 3 sont exactement ceux qui n'ont pas de racine dans K .

Thm 19 (D'Alembert-Gauss)

Tout polynôme de $\mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$.

App 20: Toute matrice est trigonalisable dans $\mathbb{C}$.

Cor 21: Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

• Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

2) Adjonction de racines.

Def 22: Soit $P \in K[X]$ irréductible. On dit que L est un corps de rupture de P ssi L est une extension de K engendrée par K et une racine α de P . On a alors $L = K(\alpha)$.

Ex 23: Si $\deg P = 1$, alors K est un corps de rupture de P .

Thm 24: Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P , unique à isomorphisme près.

Ex 25: $\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$.

$\mathbb{F}_4$ est le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$.

Prop 26: Soit $P \in K[X]$ de degré n . Alors P est irréductible dans $K[X]$ ssi P n'a pas de racine dans les extensions L de K telles que $[L:K] \leq n/2$.

App 27: Le polynôme X^4+1 est irréductible sur $\mathbb{Z}$, mais est réductible sur $\mathbb{F}_p$ pour tout nombre premier p .

Def 28: Soit $P \in K[X]$ de degré $n \in \mathbb{N}^*$. Soit E une extension de K . On dit que E est un corps de décomposition de P sur K si:
 (i) $\exists a \in E, \exists (x_1, \dots, x_n) \in E^n$ tq $P(X) = a(X-x_1) \dots (X-x_n)$ dans $E[X]$.
 (ii) $E = K(x_1, \dots, x_n)$.

Thm 29: Soit $P \in K[X]$ de degré $n \in \mathbb{N}^*$. Il existe un corps de décomposition Σ de P sur K , avec $[\Sigma:K] \leq n!$, et il est unique à isomorphisme près.

Ex 30: $\mathbb{C} = \mathbb{R}(i)$ est le corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.
 $\mathbb{Q}(\sqrt{2})$ est le corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$.

App 31: Construction des corps finis.

Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit $q = p^n$.
 Il existe un corps à q éléments: c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. En particulier il est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Def 32: K est algébriquement clos si tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K .

Ex 33: $X^2 - 2$ n'admet pas de racine dans $\mathbb{Q}$, donc $\mathbb{Q}$ n'est pas algébriquement clos.

$X^2 + 1$ n'admet pas de racine dans $\mathbb{R}$, donc $\mathbb{R}$ n'est pas algébriquement clos.

Prop 34: Tout corps algébriquement clos est infini.

Def 35: Soit L une extension de K . $a \in L$ est dit algébrique sur K si il existe $P \in K[X] \setminus \{0\}$ tel que $P(a) = 0$.
 L est une extension algébrique de K si tous les éléments de L sont algébriques sur K .

Def 36: Une extension L de K est une clôture algébrique de K si L est algébrique sur K et L est algébriquement close.

Ex 37: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

3) Résultant

Def 38: Soient $P, Q \in K[X]$, $P = \sum_{i=0}^m a_i X^i$, $Q = \sum_{i=0}^n b_i X^i$. On appelle résultant de P et Q le déterminant suivant:
 $\text{Res}(P, Q) = \det(X^{n-1}P, X^{n-2}P, \dots, P, X^{m-1}Q, X^{m-2}Q, \dots, Q)$.

Thm 39: Si P et Q ont une racine commune, alors $\text{Res}(P, Q) = 0$.
 La condition est suffisante si P ou Q est scindé dans K .

Prop 40: Si K est algébriquement clos et si $P = a \prod_{i=1}^n (X - x_i)$,
 $Q = b \prod_{j=1}^m (X - y_j)$ alors $\text{Res}(P, Q) = a^n b^m \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j)$.

Def 41: Si $P \in K[X]$ est unitaire de degré $n \geq 1$, alors on appelle discriminant de P la quantité $D(P) = (-1)^{\frac{n(n-1)}{2}} \text{Res}(P, P')$.

Prop 42: si $P \in K[X]$ unitaire a une racine simple, alors $D(P) \neq 0$. La réciproque est vraie si P ou P' est scindé.

Ex 43: $D(X^2 + bX + c) = b^2 - 4c$.
 $D(X^3 + pX + q) = -4p^3 - 27q^2$.

III) Polynômes symétriques, fonctions symétriques élémentaires

Def 44: Soit $P \in K[X_1, \dots, X_n]$. On dit que P est un polynôme symétrique si $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Ex 45: $\prod_{i \neq j} (X_i - X_j) = (-1)^{n(n-1)/2} \left(\prod_{i < j} (X_i - X_j) \right)^2$ est un polynôme symétrique.

Def 46: On appelle fonctions (ou polynômes) symétriques élémentaires de $K[X_1, \dots, X_n]$ les polynômes suivant:

$$\forall 1 \leq k \leq n, \Sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$$

Rq 47: Σ_k est homogène de degré k .

Def 48: Soit un monôme $aX_1^{\alpha_1} \dots X_n^{\alpha_n}$ où $a \in K^*$, $\alpha_i \in \mathbb{N}$. On appelle poids de ce monôme l'entier $\sum_{i=1}^n i \alpha_i$.

Soit $P \in K[X_1, \dots, X_n]$. On appelle poids de P le maximum des poids des monômes non nuls dont il est la somme.

Ex 49: Le poids de Σ_k est $nk - \frac{k(k-1)}{2}$.

Thm 50: (Théorème de structure des polynômes symétriques).

Soit $P \in K[X_1, \dots, X_n]$ un polynôme symétrique de degré p . Il existe un unique polynôme $Q \in K[\Sigma_1, \dots, \Sigma_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$.

Q est de poids p et de degré égal au degré partiel de P par rapport à l'une des indéterminées $X_1, \dots, X_n$.

Rq 51: Ce théorème reste vrai sur un anneau.

Algorithme pour déterminer Q

On écrit $P = \sum_{i=0}^n a_i X^i - X_n^{in}$.

Soit $k = (k_1, \dots, k_n)$ le plus grand (pour l'ordre lexicographique) n-uplet tel que $a_k \neq 0$.

On pose $R = P - a_k (Z_1)^{k_1-k_2} (Z_2)^{k_2-k_3} \dots (Z_{n-1})^{k_{n-1}-k_n} (Z_n)^{k_n}$.

R est un polynôme symétrique homogène de degré strictement inférieur à k pour l'ordre lexicographique.

Si $R = 0$, l'algorithme est terminé.

Sinon on recommence avec R, et l'algorithme termine en un nombre fini de cette opération.

Ex 52: $\sum_{i \neq j} x_i x_j = Z_2^2 - 2Z_1 Z_3 + 2Z_4$.

Thm 53 (Relations coefficients-racines)

Soit $P \in K[X]$. Soit $(\alpha_1, \dots, \alpha_n) \in K^n$. Il y a équivalence entre

(i) $P(X) = (X - \alpha_1) \dots (X - \alpha_n)$

(ii) $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ où $\forall i \in \{1, \dots, n\}, a_{n-i} = (-1)^i Z_i(\alpha_1, \dots, \alpha_n)$

Thm 54 (Théorème de Kronecker)

Soit $P \in \mathbb{Z}[X]$ unitaire, de degré n, dont les racines dans $\mathbb{C}$ sont de module ≤ 1 . Si $P(0) \neq 0$, alors les racines de P sont des racines de l'unité.

Cor 55: Soit $P \in \mathbb{Z}[X]$ unitaire, irréductible, dont les racines complexes sont de module ≤ 1 . Alors $P = X$ ou P est un polynôme cyclotomique.

App 56 (app du thm 53)

Résolution du système $\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=2 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \end{cases}$

Thm 57 (Formules de Newton)

Soit $n \geq 2$, soient $x_1, \dots, x_n \in K$. On note $S_p = \sum_{i=1}^n x_i^p$, pour $p \in \mathbb{N}$.

(i) $S_p - Z_1 S_{p-1} + \dots + (-1)^{n-1} Z_{n-1} S_{p-n} + (-1)^n Z_n S_{p-n} = 0 \quad \forall p \geq n$.

(ii) $S_p - Z_1 S_{p-1} + \dots + (-1)^{p-1} Z_{p-1} S_1 + (-1)^p Z_p = 0 \quad \forall 1 \leq p \leq n-1$.

III Localisation et comptage des racines

1) Localisation

Prop 58: Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Alors les racines rationnelles de P sont contenues dans l'ensemble $\left\{ \frac{p}{q} \in \mathbb{Q} / p \wedge q = 1, p \mid a_0, q \mid a_n \right\}$.

Prop 59: Soit $P = X^n + a_{n-1}X^{n-1} + \dots + a_n \in \mathbb{C}[X]$. Soit $p \geq 0$ le plus grand des modules des racines de P. Alors: $p \leq \sup \{1, \sum_{i=1}^n |a_i|\}$ et $p \leq 1 + \sup_{1 \leq i \leq n} |a_i|$.

Thm 60 (Gauss-Lucas)

Soit $P \in \mathbb{C}[X]$ un polynôme de degré ≥ 2 . Alors les racines de P' sont dans l'enveloppe convexe des racines de P.

2) Comptage

• Continuité, régularité

Thm 61: Soit $P(X) = \prod_{i=1}^n (X - \lambda_i) \in \mathbb{C}[X]$. Soit $(P_m)_{m \in \mathbb{N}}$ une suite de polynômes unitaires de degré n telle que $P_m \xrightarrow{m \rightarrow \infty} P$. Alors $\forall m \in \mathbb{N}, P_m = (X - \lambda_{1,m}) \dots (X - \lambda_{n,m})$ avec $\lambda_{i,m} \xrightarrow{m \rightarrow \infty} \lambda_i \quad \forall i \in \{1, \dots, n\}$.

Thm 62: Soit $P_0 \in \mathbb{R}[X]$ et x_0 une racine simple de P_0 . Alors la racine dépend localement du polynôme de manière C^∞ , i.e. $\exists \varphi \in C^\infty(U, V)$ avec U voisinage de P_0 dans $\mathbb{R}[X]$ et V voisinage de x_0 dans $\mathbb{R}$ telle que $\forall P \in U, \forall x \in V, x = \varphi(P) \Leftrightarrow P(x) = 0$.

• Comptage par l'analyse réelle

Thm 63: Soit $P = \sum_{i=1}^n a_i X^i \in \mathbb{R}[X]$ avec $a_n a_0 \neq 0$. Soit v le nombre de changement de signes dans $(a_0, a_1, \dots, a_n)$. Soit n le nombre de racines réelles positives de P, comptées avec multiplicité. Alors il existe $m \in \mathbb{N}$ tel que $n = v - 2m$.

Ex 64: $P = X^6 - X^4 + 2X^2 - 3X - 1$. On a $v = 3$ donc $n = 1$ ou 3. On trouve finalement que P possède une racine réelle positive.

Cor 65: Un polynôme à coefficients réels qui comporte m coefficients non nuls au plus m-1 racines réelles > 0 et au plus m-1 racines < 0 .

DVPT
 p. 159
 ↳
 [GOS] p. 512
 ↳
 [COA] p. 67

• Utilisation des formes quadratiques

Soit $P(X) = a_0 (X - \alpha_1)^{n_1} \dots (X - \alpha_q)^{n_q}$.

Soit $S_p = \sum_{j=1}^q n_j \alpha_j^p$, $p \geq 0$: sommes de Newton.

On pose $S_n(x, x) = \sum_{i,k=0}^{n-1} S_{i+k} x_i x_k$ où $n \geq q$: formes de Hankel

Thm 66 : Le nombre de racines distinctes de P et le nombre de toutes les racines réelles distinctes sont respectivement égaux au rang et à la signature de la forme $S_n(x, x)$.

• Comptage par l'analyse complexe

Thm 67 (Thm de Rouché)

Soit $g_0 \in \mathbb{C}$ et $r > 0$. Soient $P, Q \in \mathbb{C}[X]$ tq $|Q(z)| < |P(z)|$ $\forall z \in C(g_0, r)$.

Alors P et $P+Q$ possèdent le même nombre de zéros comptés avec multiplicité dans le disque ouvert $D(g_0, r)$.

Ex 68 : $P = X^5 - 5X^3 + X - 2$. On pose $Q = -5X^3$

$\forall z \in C(0, 1)$, $|P(z) - Q(z)| \leq |z|^8 + |z| + 2 \leq 4 < 5 = |Q(z)|$

Donc P possède 3 zéros dans l'intérieur du disque $D(0, 1)$.

Références

[OAT] : Beck, Talick, Peyre, Objectif Agrégation, 2ème édition.

[GOU] : Gourdon, Algèbre, 2ème édition

[NOU] : Nourdin, Agrégation de mathématiques épreuve orale, 2ème édition

[Per] : Perin, Cours d'algèbre

[Goz] : Gozard, Théorie de Galois, 2ème édition

[RDO] : Ramis, Deschamps, Odoux, Mathématiques spéciales, algèbre, 2ème édition

[FG] : Francinou, Gianella, Exercices de mathématiques pour l'agrégation, algèbre 1

[Test] : Testard, Analyse mathématique

[Tign] : Tignolte, Mathématiques pour le calcul formel.