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

Refs : [Go3] Gozard Théorie de Galois [Gou1] Gourdon Algèbre [Cal2] Calais Anneaux [RDO1] Ramis Deschamps Odoux Algèbre 1 [Per] Perrin Cours d'algèbre [OA] Objectif agrégation

Dev : Polynômes cyclotomiques [Per] ; Polynômes irréductibles $\mathbb{F}_q$ [Gou] ; Chevalley Warning & EGZ [OA]

Par défaut, K désigne un corps commutatif.

I Racine d'un polynôme.

1) Définitions et premières propriétés.

[Gou1] 59, 61

Def 1 : Pour $P \in K[X]$ on dit que $a \in K$ est racine de P si $(X-a)$ divise P dans $K[X]$.

Ex 2 : 1 et -1 sont racines de X^2-1.

Prop 3 : Les racines de $P \in K[X]$ dans K sont exactement les éléments (a) de K tels que $P(a)=0$

Ex 4 : Les racines de X^n-1 dans $\mathbb{C}$ sont les racines n-ièmes de l'unité

Def 5 : On dit que $a \in K$ est une racine de P d'ordre $h \in \mathbb{N}^*$ si $(X-a)^h$ divise P et $(X-a)^{h+1}$ ne le divise pas.

Prop 6 : Si $P \in K[X]$ est de degré n, alors P a au plus n racines dans K.

Rq 7 Ceci devient faux si K n'est qu'un anneau : dans $\mathcal{M}_2(\mathbb{R})$ X^2 admet toutes les matrices comme racines, soit une infinité.

Cor 8 : Si K est infini il y a une correspondance bijective entre les polynômes et les fonctions polynomiales associées.

Théo 9 : Si car $K=0$, $P \in K[X] \setminus \{0\}$, alors $a \in K$ est racine d'ordre h de P si et seulement si $\forall i \in [\![0, h-1]\!]$ $P^{(i)}(a)=0$ et $P^{(h)}(a) \neq 0$.

Rq 10 Le résultat précédent est vrai en caractéristique quelconque mais seulement pour les racines simples.

Cor 11 : Soient $a_1, \dots, a_n \in K$ deux à deux distincts. L'application
$\varphi : K_{n-1}[X] \longrightarrow K^n$, $P \longmapsto (P(a_i))$ est un isomorphisme d'espace vectoriel

Rq 12 L'antécédent d'un n-uplet est le polynôme d'interpolation de Lagrange associé à ce n-uplet

Appl 13 : Déterminant de Vandermonde.

[Gou1] 59, 61

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

Rq 15 : Deux polynômes scindés sont premiers entre eux si et seulement si ils n'ont aucune racine commune.

[Go3] 9

Def 16 : $P \in K[X]$ est dit irréductible si, pour tout produit $P=QR$ dans $K[X]$, on a Q ou R constant et $\deg P \geq 1$.

Prop 17 : Tout polynôme de degré 1 est irréductible. Tout polynôme irréductible sur K n'admet pas de racine

Pol. irréd. sur $\mathbb{F}_q$ DVP

Prop 18 : La réciproque est fausse (sauf pour $\deg P = 2$ ou 3) en effet $(X^2+1)^2$ est irréductible sans racine dans $\mathbb{Q}[X]$.

Etude des polynômes cyclotomiques DVP

Théo 19 (D'Alembert Gauss) Tout polynôme de $\mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}[X]$

62, 63

Appli 20 : Toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable

Cor 21 : Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Ceux de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racine.

2) Extension de corps par adjonction de racines.

[Go3] 57, 58

Def 22 : On dit que L est un corps de rupture pour $P \in K[X]$ si c'est une extension de K, engendrée par une racine de P (irréductible).

Ex 23 Si P est de degré 1, K est un corps de rupture de P.

Théo 24 : Si $P \in K[X]$ est irréductible, $K[X]/(P)$ est un corps de rupture de P et tout corps de rupture lui est K-isomorphe (morphisme de K-algèbre).

Ex 25 : $\mathbb{C}$ est le corps de rupture de X^2+1. $\mathbb{F}_4$ est le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$.

Cor 26 : Tout élément de $K[X]$ admet une racine dans une extension de K.

Prop27 : Un polynôme de degré n est irréductible si et seulement si il n'admet de racine dans aucune extension de K de degré $\leq \frac{n}{2}$

[Goz]

Appl28 : X^4+1 est réductible sur $\mathbb{F}_p$ ...

57

Def29 : Soit E une extension de K, $P\in K[X]$ de degré $n\geq 1$. On dit que E est un corps de décomposition de P sur K si : (i) P est scindé dans $E[X]$. (ii) Toute extension intermédiaire ne satisfait pas au premier point.

57

Théo30 : Tout polynôme de degré n admet un corps de décomposition de degré au plus $n!$ sur K. De plus deux corps de décomposition d'un même polynôme sont K-isomorphes.

[Perr] 78

Théo31 : Soit $p\in\mathbb{P}$, $n\in\mathbb{N}$, on pose $q=p^n$. Il existe un corps à q éléments construit comme corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^{p^n}-X$. Ce corps est unique à isomorphisme près et on le note $\mathbb{F}_q$.

3) Algébricité et transcendance.

[Goz] 63

Def32 : Soit L-K une extension de K, un élément $\alpha\in L$ est dit algébrique sur K s'il existe $P\in K[X]$ tel que $P(\alpha)=0$. Dans le cas contraire on dit que α est transcendant. Si L est composé exclusivement d'éléments algébriques on dit que L est une extension algébrique.

Def33 Un corps est dit algébriquement clos si tout polynôme y est scindé (par une récurrence immédiate, c'est équivalent à dire que tout polynôme non constant admet une racine).

Ex34 $\mathbb{C}$ est algébriquement clos, $\mathbb{Q}$ ne l'est pas.

Prop35 : Un corps fini n'est pas algébriquement clos.

Théo36 (Steinitz) Tout corps admet une clôture algébrique, une extension algébrique algébriquement close.

Ex37 : $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$. Une clôture algébrique de $\mathbb{F}_p$ est un corps infini de caractéristique p.

Prop38 : $\mathbb{R}\setminus\mathbb{Q}$ n'est pas algébrique : $l:=\sum_{n=0}^{\infty}10^{-n!}\in\mathbb{R}$ n'est pas algébrique sur $\mathbb{Q}$. [Gou] 90

Cor39 : $\mathbb{C}$ n'est pas la clôture algébrique de $\mathbb{Q}$.

II Polynômes symétriques. Fonctions symétriques élémentaires.

Dans cette partie, A désigne un anneau commutatif unitaire intègre, $n\in\mathbb{N}^*$

1) Définitions et relations coefficients racines.

[Gal 2]

Def40 : Le groupe symétrique $\mathfrak{S}_n$ agit sur $A[X_1,\dots,X_n]$ par $\sigma.P(X_1,\dots,X_n)=P(X_{\sigma(1)},\dots,X_{\sigma(n)})$. Les points fixes sous cette action sont notés $\mathfrak{S}[X_1,\dots,X_n]$ et sont appelés polynômes symétriques à n variables

Ex41 : Si $n=1$ Tout polynôme est symétrique. Dans le cas général, les polynômes $\sum_{1\leq i_1<\dots<i_k\leq n} X_{i_1}X_{i_2}\dots X_{i_k}=\Sigma_k$ pour $k\in[\![1,n]\!]$ sont symétriques. Ce sont les polynômes symétriques élémentaires.

[Gou] 60

Théo42 : Soit $P=a_0+a_1X+\dots+a_nX^n\in K[X]$, $a_n\neq 0$. Dans un corps de décomposition de P, on a $P=a_n(X-\alpha_0)\dots(X-\alpha_n)$. Et, pour $k\in[\![0,n]\!]$ on a $a_i=\Sigma_{n-i+1}(\alpha_0,\dots,\alpha_n)\times a_n(-1)^i$ C'est une équivalence

Appl43 : Le déterminant d'une matrice (resp sa trace) est un coeff de son polynôme caractéristique, prod (resp somme) de ses valeurs propres dans une clôture algébrique

[RDO]

Prop44 Formule de Newton : En posant $S_k=X_1^k+\dots+X_n^k$, on a

(a) $\forall k\in[\![1,n]\!]$ $\sum_{i=0}^{k}(-1)^i\Sigma_iS_{k-i}=0$ avec la convention $\Sigma_0=1$.

(b) $\forall k>n$, $\sum_{i=0}^{n}(-1)^i\Sigma_iS_{k-i}=0$

App45 : Caractérisation des matrices nilpotentes : $A\in\mathcal{M}_n(K)$ $A^n=0\iff \mathrm{tr}(A^k)=0\ \forall k\in[\![1,n]\!]$

2) Structure des polynômes symétriques.

Def46 : Soit $X_1^{\alpha_1}\dots X_n^{\alpha_n}\in A[X_1\dots X_n]$ un monôme, on définit le poids de ce monôme comme $\sum_{k=1}^{n}k\alpha_k$. On appelle poids d'un polynôme $P\in A[X_1\dots X_n]$ le max des poids des monômes dont il est la somme. (0 a $-\infty$ comme poids par convention).

Ex47 : Si $n=1$ le poids est le degré. Le poids de Σ_k est $nk-\frac{k(k-1)}{2}$

Théo49 : Soit $P\in\mathfrak{S}[X_1\dots X_n]$, il existe un unique $Q\in A[X_1\dots X_n]$ tel que $P=Q(\Sigma_1\dots\Sigma_n)$. Tout polynôme symétrique est polynôme en les pol sym élém. De plus, Q est de poids le degré de P.

Algorithme pour déterminer Q en partant de P. On écrit $P=\sum_{|i|=p} a_i X_{i_1}^{i_1}\dots X_{i_p}^{i_m}$ (on suppose P homogène, on somma les composantes homogènes de P pour le cas général). Soit $k=(k_1\dots k_n)$ le plus grand (ordre lexicographique) n-uplet tel que $a_k\neq 0$. On pose $R=P-a_k\Sigma_1^{k_1-k_2}\Sigma_2^{k_2-k_3}\dots\Sigma_m^{k_m}$. R est symétrique homogène de degré strictement inf à k pour l'ordre lexico. Si $R=0$ ok, sinon on recommence sur R, ça termine en temps fini.

Ex 57 : $\sum_{i\neq j} X_i^2 X_j = \Sigma_2^2 - 2\Sigma_1\Sigma_3 + 2\Sigma_4$.

3) Discriminant. Retour à K corps.

Def 58 : Pour $P\in K[X]$ de degré $n\geq 2$, L corps de décomposition de P sur K, $\alpha_1\dots\alpha_n$ les racines de P. On définit $\operatorname{disc} P = a_n^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2$.

Prop 59 : Le discriminant est un polynôme symétrique en les racines de P. donc c'est un polynome en les coefficients de P. Ainsi $\operatorname{disc}(P)$ peut être défini sur un anneau commutatif unitaire intègre.

Prop 60 : $P\in K[X]$ est à racines simples ssi $\operatorname{disc} P\neq 0$.

Ex 61 : $P(X)=aX^2+bX+c$ $\operatorname{disc} P = b^2-4ac$.

III Localisation et comptage des racines.

1) Localisation.

Prop 62 : Soit $P=\sum_0^n a_iX^i\in\mathbb{Z}[X]$ de degré $n\geq 1$. Alors les racines rationnelles de P sont contenues dans l'ensemble $\{\frac{p}{q}\in\mathbb{Q} \mid p\wedge q=1,\ p|a_0 \text{ et } q|a_n\}$.

Prop 63 : Soit $P=X^n+a_1X^{n-1}+\dots+a_{n+1}\in\mathbb{C}[X]$ et soit $\rho>0$ le plus grand module des racines de P. Alors $\rho\leq \sup(1,\|a_i\|_1)$ $\rho\leq 1+\|a_i\|_\infty$.

Rq 64 : Ceci a à voir avec les disques de Gershgörin de la matrice compagnon de P.

Théo 65 (Gauss Lucas) Soit $P\in\mathbb{C}[X]$ de degré $n\geq 2$. Les racines de P' sont contenues dans l'enveloppe convexe de celles de P.

2) Comptage.

[2av] Théo 66 Chevalley Warning. Soit $(f_\alpha)_{\alpha\in A}$ une famille de polynomes de $\mathbb{F}_q[X_1\dots X_n]$ telle que $\sum d^\circ f_\alpha < n$. On pose V l'ensemble des racines commun aux f_α, alors $|V|\equiv 0[p]$

Cor 67 (Ginzburg Erdös Ziv) Soit $n\geq 1$, parmi $2n-1$ entiers, on peut en choisir n dont la somme est divisible par n. DVP [2av]

Théo 68 : Soit P_m une suite convergente de polynômes (dans $\mathbb{C}_n[X]$) alors la suite de racines est convergente dans $\mathbb{C}^n$ ($n=\deg\lim$).

Théo 69 : Soit $P_0\in\mathbb{R}_n[X]$, x_0 racine simple de P_0. $\exists\, U$ voisin de P_0 dans $\mathbb{R}_n[X]$ et V vois de $x_0\in\mathbb{R}$ $\varphi: U\to V$ C^∞ tq $\forall P\in U, x\in V. x=\varphi(P) \Leftrightarrow p(x)=0$.

Théo 70 : Soit $P=\sum a_iX^i\in\mathbb{R}[X]$, $a_n a_0\neq 0$. v le nombre de changements de signe dans $(a_0\dots a_n)$, r le nb de rac réelles positives de P ac multip. alors $\exists m\in\mathbb{N} / r=v-2m$.

Ex 71 : $P=X^6-X^4+2X^2-3X-1$, $v=3$ donc $r=1$ ou 3. En fait 1.

Cor 72 : Un polynôme à coeffs réels comportant m coeffs $\neq 0$ a au plus $m-1$ rac réels >0 et $m-1$ rac <0.

Théo 73 (Rouché) [OA 67]

Soit $z_0\in\mathbb{C}$, $r>0$, $P,Q\in\mathbb{C}[X]$ tq $|Q|<|P|$ sur $C(z_0,r)$ Alors P et $P+Q$ ont même nb de zéros comptés avec multiplicité dans le disque $D(z_0,r)$.

Ex 74 : $P=X^8-5X^3+X-2$ $Q=-5X^3$, P possède 3 zéros dans $D(0,1)$.