144

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

Sz = Szpirglas Gou = Gourdon alg Goz = Gozard RB = Risler Boyer

Soit k un corps. Soit L une extension de k. Soit E un k-ev de dim finie

I. RACINES D'UN POLYNÔME + Gou + RB

1. Racines et multiplicités. Sz p540 Soit $P \in k[X]$

Def 1 = On dit que $a \in L$ est une racine de P si $P(a)=0$.

Ex 2 = $i \in \mathbb{C}$ est racine de X^2+1.

Ex 3 = Les racines du polynôme caractéristique d'un endomorphisme u sont des valeurs propres de u.

Prop 4 = $a \in k$ est racine de P ssi $X-a$ divise P.

Ex 5 = 1 est racine de $(X-1)(X-2)$

Def 6 = si $m \in \mathbb{N}^*$, on dit que $a \in k$ est racine d'ordre m de P si $(X-a)^m \mid P$ et $(X-a)^{m+1} \nmid P$.
Si $m=1$, on dit que a est racine simple de P.

Ex 7: 1 est racine double de $(X-1)^2$.

Prop 8 = Le nombre de racines de P, comptées avec leur multiplicité, est inférieur ou égal au degré de P, si $P \neq 0$

Rq 9 = C'est faux si on se place sur un anneau

C-ex 10 = Le polynôme $\bar{4}X \in \mathbb{Z}/8\mathbb{Z}[X]$ a 3 racines : $\bar{0}, \bar{2}, \bar{4}$ mais est de deg 1.

App 11: Les valeurs propres de $u \in \mathcal{L}(E)$, comptées avec multiplicité, sont en nombre inférieur à $\deg \chi_u = \dim E$

Prop 12 = Si k est un corps infini, tel que pour tout $x \in k$ $P(x)=0$ alors P est le polynôme nul.

Rq 13 = C'est faux si k est un corps fini

C-ex 14 = Si $k = \mathbb{F}_p$, où p est premier, $X^p - X$ est de degré p donc non nul or $\forall x \in \mathbb{F}_p$ $x^p = x$.

App 15 = Il existe un unique polynôme $L \in k[X]$ avec $\deg L \leq n-1$ tel que $\forall i$ $L(a_i) = b_i$, où les $a_i \in k$ sont deux à deux distincts, et $b_i \in k$
C'est le polynôme d'interpolation de Lagrange

Prop 16 = Si k est de caractéristique nulle, si $P \neq 0$, alors $a \in k$ est racine d'ordre m de P ssi
$\forall i \in [\![0, m-1]\!]$ $P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Rq 17 = Le sens réciproque est faux si $car(k) \neq 0$

C-ex 18 = $P = X^3 \in \mathbb{F}_3[X]$ a $\bar{0}$ pour racine d'ordre 3 et pourtant $P^{(3)}(\bar{0}) = \bar{0}$.

2. Polynômes irréductibles. Sz + Goz

Def 19 = $P \in k[X]$ est irréductible si P est non constant et toute décomposition $P = QR$ implique Q est constant ou R est constant.

Prop 20 = Tout polynôme de degré 1 est irréductible.

Thm 21 = d'Alembert Gauss : Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.

Coro 22 = Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Coro 23 = Les polynômes irréductibles de $\mathbb{R}[X]$, sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Prop 24 Tout polynôme * de degré strictement supérieur à 1 n'a pas de racine dans k. * irréductible

C-ex 25 = Réciproque fausse : $(X^2+1)^2 \in \mathbb{R}[X]$ n'est pas irréductible sur $\mathbb{R}$ sans racine réelle.

Prop 26 = Tout polynôme irréductible de degré 2 ou 3 sans racine est irréductible.

Ex 27 = $X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible

3. Adjonction de racines. Goz p57 + Sz

Def 28 = Si $\deg P \geq 1$, on appelle corps de rupture de P sur k, toute extension de corps $k \hookrightarrow L$ telle que
- P admette un zéro α dans L
- L soit exactement le sous corps $k[\alpha]$ de L

engendré par k et α.

Ex 29 = Si $\deg P = 1$ alors k est un corps de rupture de P.

Thm 30 = Si $P \in k[X]$ est irréductible dans $k[X]$ alors
- il existe un corps de rupture de P.
- si $k(\alpha)$ et $k(\beta)$ sont deux corps de rupture de P, alors il existe un k-isomorphisme $\varphi : k(\alpha) \to k(\beta)$ tel que $\varphi(\alpha) = \beta$.

Ex 31 : X^2+1 est irréductible sur $\mathbb{R}$. Le corps $\frac{\mathbb{R}[X]}{(X^2+1)}$ est un corps de rupture de X^2+1. On le note $\mathbb{C}$ et on note i la classe de X.

Ex 32 = Soit j une racine de $X^2+X+1 \in \mathbb{C}[X]$. Le polynôme $X^3-2 \in \mathbb{Q}[X]$ admet dans $\mathbb{C}$, les racines $\alpha = \sqrt[3]{2}$, $j\alpha$ et $j^2\alpha$. $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\alpha j)$ sont deux corps de rupture de X^3-2 qui sont distincts car $\mathbb{Q}(\alpha) \subset \mathbb{R}$ et $\mathbb{Q}(\alpha j) \not\subset \mathbb{R}$.

Coro 33 = Si $\deg P \geq 1$, il existe une extension L de k dans laquelle P possède au moins une racine.

Prop 34 = Si $\deg P = n$. P est irréductible dans $k[X]$ ssi P n'a pas de racine dans les extensions L de k telles que $[L:k] \leq \frac{n}{2}$.

Def 35 = Si $\deg P \geq 1$, on appelle corps de décomposition de P sur k toute extension $k \hookrightarrow L$ telle que
- P est scindé sur L.
- L est exactement le sous corps $k(\alpha_1, \dots, \alpha_n)$ de L engendré par k et les zéros $\alpha_1, \dots, \alpha_n$ de P dans L.

Thm 36 = Si $\deg P = n \geq 1$, alors
- il existe un corps de décomposition L de P sur k, avec $[L:k] \leq n!$
- Si L et L' sont deux corps de décomposition de P sur k alors il existe un k-isomorphisme de L sur L'.

Ex 37 = $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$.

Thm 38 = Soit p premier, $n \in \mathbb{N}^*$. On note $q = p^n$. Alors
- Il existe un corps fini à q éléments. Il est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.
- Si F et F' sont deux corps à q éléments, ils sont $\mathbb{F}_p$-isomorphes. On le note $\mathbb{F}_q$

Rq 39 = En fait $\mathbb{F}_q$ est exactement l'ensemble des racines de $X^q - X$.

App 40 : Soit p premier, $m \in \mathbb{N}^*$. $q = p^m$. On note $P_q(d)$, $d \in \mathbb{N}^*$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires et de degré d. Alors
- $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in P_q(d)} P$.
- $I_q(n) = \mathrm{Card}(P_q(d)) > 0$ pour tout $d \in \mathbb{N}^*$.
- $I_q(n) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

DVPT n°1

II POLYNÔMES SYMÉTRIQUES OU FONCTIONS SYMÉTRIQUES ÉLÉMENTAIRES. 52 + 602

Soit A un anneau commutatif

1. Polynômes symétriques et relation coefficients-racines.

On note $\mathfrak{S}_n$ le groupe symétrique d'ordre n.

Def 41 = Un polynôme $P \in A[X_1, \dots, X_n]$ est dit symétrique si pour tout $\sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Prop 42 . $P \in A[X_1, \dots, X_n]$ est symétrique ssi pour tout $i < j$, $P(X_1, \dots, X_i, \dots, X_j, \dots, X_n) = P(X_1, \dots, X_j, \dots, X_i, \dots, X_n)$.

Ex 43 =
- $XY + YZ + ZX \in \mathbb{R}[X,Y,Z]$ est symétrique
- $XY + X^2 \in \mathbb{R}[X,Y]$ n'est pas symétrique.

Def 44 = On appelle polynômes symétriques élémentaires de $A[X_1, \dots, X_n]$, les polynômes Σ_p $(1 \leq p \leq n)$ définis par $\Sigma_p = \sum_{i_1 < \dots < i_p} X_{i_1} \cdots X_{i_p}$.

Ex 45 : $\Sigma_1 = X_1 + \dots + X_n$, $\Sigma_n = X_1 \times \dots \times X_n$.

Prop 46 : Relations coefficients-racines : Si $P \in K[X]$ est scindé sur K, $P = X^n + a_1 X^{n-1} + \dots + a_n$ alors $a_i = (-1)^i \Sigma_i (u_1, \dots, u_n)$ où les u_i sont les racines de P.

Ex 47 : $(X - x_1)(X - x_2) = X^2 - (x_1 + x_2) X + x_1 x_2$
$= X^2 - \Sigma_1(x_1, x_2) + \Sigma_2(x_1, x_2)$.

2. Thm de structure

Def 48 : On appelle poids du monôme $X_1^{c_1} \dots X_n^{c_n}$: $c_1 + 2c_2 + \dots + nc_n$.

• Le poids d'un polynôme $P \in A[X_1, \dots, X_n]$ est le maximum des poids des monômes qui interviennent dans P. On le note $\omega(P)$.

Thm 49 (de structure) : Si $P \in A[X_1, \dots, X_n]$ est symétrique de degré d alors il existe un polynôme $Q \in A[X_1, \dots, X_n]$ de poids $\omega(Q) \leq d$ tel que
$P(X_1, \dots, X_n) = Q(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$.
Ce polynôme est unique.

Algorithme en annexe.

Ex 50 : $\sum_{i \neq j} X_i^2 X_j \in \mathbb{R}[X_1, X_2, X_3]$ s'écrit $\Sigma_1 \Sigma_2 - 3\Sigma_3$.

DVLPT n°2

App 51 : • Si P est un polynôme unitaire, $P \in \mathbb{Z}[X]$ dont les racines sont toutes de module inférieur ou égal à 1. Si $P(0) \neq 0$. Alors les racines de P sont des racines de l'unité.

• Si $P \in \mathbb{Z}[X]$, unitaire irréductible dont les racines complexes sont de module inférieur ou égal à 1 alors $P = X$ ou P est un polynôme cyclotomique.

III LOCALISATION, COMPTAGE

1. Localisation.

Prop 52 : Si $P(X) = X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{C}[X]$. On note $R = \max(1, |a_0| + \dots + |a_{n-1}|)$. Alors P admet n racines (comptées avec leur multiplicité) dans le disque fermé $\bar{D}(0, R)$. Sz

Prop 53 : Gauss Lucas : Si $P \in \mathbb{C}[X]$, $\deg P \geq 2$. Alors les racines de P' sont dans l'enveloppe convexe des racines de P. Sz

Ex 54 : Si les racines de $P \in \mathbb{C}[X]$ sont réelles, alors les racines de P' aussi.

2. Comptage.

Thm 55 (Rouché) : Soient U un ouvert de $\mathbb{C}$, $a \in U$ et $r > 0$ tels que $\bar{B}(a, r) \subset U$. Soient $P, Q \in \mathbb{C}[X]$ tels que $\forall z \in \mathcal{C}(a, r)$ $|P(z) - Q(z)| < |P(z)|$ alors P et Q ont le même nombre de racines comptées avec multiplicité dans $B(a, r)$. Tauv

Ex 56 : Nb de racines de $P = X^8 - 5X^3 + X - 2$ dans $D(0,1)$: OA
3 racines dans $D(0,1)$. $(Q = -5X^3)$.

l'algorithme ne peut pas être en annexe. Exclusivement les figures.

Si P est symétrique, détermination pratique de Q tel que
$P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$.

On note $P = \sum_{|i|=p} a_i X_1^{i_1} \dots X_n^{i_n}$.

- On prend $k = (k_1, \dots, k_n)$ ~~le~~ plus grand (ordre lexicographique) tel que $a_i \neq 0$. On a alors $k_1 \geq k_2 \geq \dots \geq k_n$.
  On forme $P - a_k (\Sigma_1)^{k_1 - k_2} (\Sigma_2)^{k_2 - k_3} \dots (\Sigma_{n-1})^{k_{n-1} - k_n} \Sigma_n^{k_n}$
  est symétrique homogène. ~~Le~~ monôme $a_k X_1^{k_1} \dots X_n^{k_n}$ n'y figure plus et son degré est strictement inférieur à k.
- On recommence jusqu'à obtenir un polynôme nul.

↳ algorithme dans ~~le~~ RDO - maths spéciales algèbre 2° edition.