NOM : PASCAL **Prénom :** Barbara **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et Applications.

Autre sujet :

Références : P. Tauvel, Corps commutatifs et théorie de Galois ; X. Gourdon, Algèbre ; D. Perrin, Cours d'Algèbre ; D. Serre, Les Matrices

Prasalor

1) Racines d'un polynôme de K[X]

Ici K désigne un corps commutatif

a) Définitions, propriétés algébriques

Déf 1 : L'application $K \to K$, $x \mapsto P(x)$ est appelée la fonction polynôme définie par $P \in K[X]$.
Dans la suite on confondra $P \in K[X]$ avec sa fonction polynôme.

Déf 2 : Soit $P \in K[X]$. On dit que $x \in K$ est une racine de P si $P(x) = 0$ dans K.

Ex 3 : Si $K = \mathbb{F}_2$, $\bar{1}$ est racine de $X^3+X^2+X+\bar{1}$.

Thm 4 : Soit $P \in K[X]$, $x \in K$
(i) Par division euclidienne, $\exists Q \in K[X]$ tq $P = (X-x)Q + P(x)$
(ii) x racine de $P \iff X - x \mid P$ dans $K[X]$

Ex 5 : Sur $\mathbb{F}_2$, $X^3+X^2+X+\bar{1} = (X-\bar{1})(X^2-\bar{1})$.

Coro : (i) Si $n \in \mathbb{N}$, $\deg(P) = n$ et si P a plus de n+1 racines dans K, alors P est nul.
(ii) Si $n \in \mathbb{N}^*$, $a_1, \dots, a_n \in K$, 2 à 2 distincts, $P \in K[X]$
$P(a_i) = 0$, $1 \leq i \leq n \iff (X-a_1)\dots(X-a_n) \mid P$ ds $K[X]$
(iii) Si K est infini, l'application qui à P associe sa fonction polynomiale est injective.

b) Application : étude des carrés

Déf : $K^{[2]}$ (resp. $K^{*[2]}$) désigne l'ensemble des carrés de K (resp. $K^* = K \setminus \{0\}$). Si $p \in \mathbb{N}^*$, $q, r \in \mathbb{Z}$, on note $q \equiv r \mod (p)$ pour dire que $q - r \in p\mathbb{Z}$.

Prop 8 : Si K est fini et $car(K) \neq 2$
(i) On note $q = card(K)$, on a alors
$-1 \in K^{[2]} \iff q \equiv 1 \mod [4]$
$-1 \notin K^{[2]} \iff q \equiv 3 \mod [4]$
$card(K^{[2]}) = \frac{q+1}{2}$, $card(K^{*[2]}) = \frac{q-1}{2}$.
(ii) Si $\alpha \in K^* \setminus K^{[2]}$ $x \mapsto \alpha x$ induit une bijection de l'ensemble $K^{*[2]}$ sur $K^* \setminus K^{[2]}$
(iii) Soient $\alpha, \beta \in K^*$, $\alpha\beta \in K^{[2]} \iff$ (α et $\beta \in K^{*[2]}$) ou (α et $\beta \notin K^{*[2]}$)

Thm 9 : Si K fini avec $q = card(K)$ impair, et si $x \in K^*$, on a
$x \in K^{*[2]} \iff x^{\frac{q-1}{2}} = 1$; $x \notin K^{*[2]} \iff x^{\frac{q-1}{2}} = -1$

c) Notion de multiplicité

Prop 10 : Soient $P \in K[X]$, $x \in K$, $h \in \mathbb{N}$. Les conditions suivantes sont équivalentes :
(i) P est divisible par $(X-x)^h$ mais pas par $(X-x)^{h+1}$
(ii) $\exists Q \in K[X]$ tq $P = (X-x)^h Q$ avec $Q(x) \neq 0$
Si $P \neq 0$, un tel h est unique. On l'appelle la multiplicité de x relativement à P.

Ex 11 : Sur $\mathbb{F}_2$, $X^3+X^2+X+\bar{1} = (X-\bar{1})^3$
$\bar{1}$ est racine de multiplicité 3 de $X^3+X^2+X+\bar{1}$.

Thm 12 : Si $P \neq 0$, $\deg(P) = n$
(i) Soient $\alpha_1, \dots, \alpha_p$ des racines distinctes

de P, de multiplicités $k_1, \dots, k_p$ resp. Si existe $Q \in K[X]$ tq $P = (X-\alpha_1)^{k_1} \dots (X-\alpha_p)^{k_p} Q$ et $Q(\alpha_i) \neq 0$, $1 \leq i \leq p$.
(ii) La somme des ordres des racines de P vaut au plus n.

Prop13: Soit $P \in K[X]$ et $\alpha \in K$ une racine de P. Alors α racine simple de $P \iff \alpha$ n'est pas racine de P'

Cor14: Soit $P \in \mathbb{R}[X]$ irréductible. Dans $\mathbb{C}$, P n'a que des racines simples.

App15: (i) Soit $P \in \mathbb{R}[X]$ et $\lambda \in \mathbb{C}$ tq λ racine de P de multiplicité $\mu > \deg(P)/2$. Alors $\lambda \in \mathbb{R}$.
(ii) Soit $P \in \mathbb{R}[X]$, $\deg(P) = 2m+1$, $n \geq 2$ tel que P ait une racine complexe de multiplicité n. Alors P possède une racine dans $\mathbb{R}$.

Thm16: On suppose $\mathrm{car}(K) = 0$, $P \in K[X]$, $\alpha \in K$, $p \in \mathbb{N}$. Sont équivalentes les propositions suivantes :
(i) α racine d'ordre p de P
(ii) α racine de $P, P', \dots, P^{(p-1)}$ mais pas de $P^{(p)}$.

2) Relations coefficients-Racines

Def17: Soit $n \in \mathbb{N}^*$, $\alpha_1, \dots, \alpha_n \in K$. Pour $1 \leq k \leq n$, on pose

$$\sigma_k(\alpha_1, \dots, \alpha_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \dots \alpha_{i_k}.$$

Prop18: Si $\tau \in \mathfrak{S}_n$, alors $\sigma_k(\alpha_{\tau(1)}, \dots, \alpha_{\tau(n)}) = \sigma_k(\alpha_1, \dots, \alpha_n)$
Les $\sigma_k : K^n \to K$ sont appelées les fonctions symétriques élémentaires.

Thm19: Soit $P = a_n X^n + \dots + a_1 X + a_0 \in K[X]$, $\deg(P) = n \geq 1$ tel que $\exists \alpha_1, \dots, \alpha_n \in K$ et $P = a_n (X-\alpha_1) \dots (X-\alpha_n)$. On pose $\sigma_k = \sigma_k(\alpha_1, \dots, \alpha_n)$. Alors

$$\sigma_1 = \frac{-a_{n-1}}{a_n}, \dots, \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, \dots, \sigma_n = (-1)^n \frac{a_0}{a_n}$$

Thm20 [Relations de Newton]
Soient $n \in \mathbb{N}^*$, $\alpha_1, \dots, \alpha_n \in K$. On note $\sigma_k = \sigma_k(\alpha_1, \dots, \alpha_n)$ $1 \leq k \leq n$. Si $p \in \mathbb{N}^*$, on pose $S_p = S_p(\alpha_1, \dots, \alpha_n) = \alpha_1^p + \dots + \alpha_n^p$. On a alors
(i) Si $p > n$
$S_p - \sigma_1 S_{p-1} + \dots + (-1)^k \sigma_k S_{p-k} + \dots + (-1)^n \sigma_n S_{p-n} = 0$
(ii) Si $1 \leq p \leq n$,
$S_p - \sigma_1 S_{p-1} + \dots + (-1)^k \sigma_k S_{p-k} + \dots + (-1)^p p \sigma_p = 0$.

App21 [Théorème de Wilson] Un entier positif $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1 \ [n]$

3) Adjonction de racines

Def22: Si $P \in K[X]$ s'écrit $P = c(X-\alpha_1) \dots (X-\alpha_n)$, $c, \alpha_1, \dots \alpha_n \in K$ on dit que P est scindé.

Def23: Si $P \in K[X]$ est irréductible. On appelle corps de rupture de P une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

Thm24: $\forall P \in K[X]$ irréductible sur K, il existe un corps de rupture de P sur K, unique à isomorphisme près.

Def25: Soit $P \in K[X]$, $\deg(P) = n$. On appelle corps de décomposition de P sur K une extension L de K telle que:
(i) dans $L[X]$, $P = c(X-\alpha_1) \dots (X-\alpha_n)$, $c \in K$, $\alpha_1, \dots, \alpha_n \in L$
(ii) $L = K(\alpha_1, \dots, \alpha_n)$
sur son corps de décomposition P est scindé et L est minimal pour cette propriété.

Thm26: $\forall P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près

Ex27: Si $P = X^3 - 2 \in \mathbb{Q}[X]$
$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de P.
$\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de P.

Def28: K un corps est dit algébriquement clos si tout $P \in K[X]$ est scindé sur K.

Thm29 [D'Alembert-Gauss]: $\mathbb{C}$ est algébriquement clos.

DV 1

3/2

Hyperplans tuteurs, Calcul scientifique

DV2

4) Applications choisies

a) Localisation de racines ($\mathbb{K}=\mathbb{C}$)

Prop 30 : Soit $P=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n\in\mathbb{C}[X]$, avec les a_i non tous nuls. On note $\rho=\max\{|\lambda|,\lambda\in\mathbb{C},P(\lambda)=0\}$.

(i) $\rho<\sup\{1,\sum_{i=1}^{n}|a_i|\}$

(ii) $\rho<1+\sup_{1\le i\le n}|a_i|$

Prop 31 : On pose $f(x)=x^n-|a_1|x^{n-1}-\cdots-|a_{n-1}|x-|a_0|$

(i) f admet une unique racine $\alpha\in\mathbb{R}_+^*$.
Si $0<x<\alpha$, $f(x)<0$ et si $x>\alpha$, $f(x)>0$.
De plus $(2^{1/n}-1)\alpha\le\rho\le\alpha$.

(ii) On pose $R=\sup_{1\le k\le n}|a_k|^{1/k}$. Alors $R/n\le\rho\le 2R$.
(Règle de Cauchy)

b) Diagonalisation dans $\mathcal{M}_n(\mathbb{K})$

Déf 32 : Soit $M\in\mathcal{M}_n(\mathbb{K})$, $\alpha\in\mathbb{K}$. On dit que α est valeur propre de M si $M-\alpha I_n$ est de rang $<n$.

Prop/Déf 33 : Si $M\in\mathcal{M}_n(\mathbb{K})$ on définit $\chi_M=\det(XI_n-M)$ le polynôme caractéristique de M.
α est valeur propre de $M\iff\chi_M(\alpha)=0$.

App 34 [Calcul de χ_M : Méthode de Leverrier] Soit $k=0$
Pour $m\ge 1$, on pose $s_m=\mathrm{tr}(M^m)$, on écrit

$$\chi_M=X^n+\Sigma_1X^{n-1}+\cdots+\Sigma_kX^{n-k}+\cdots+\Sigma_n$$

→ On pose $\Sigma_0=1$ et on a $\Sigma_1=-s_1$
Puis on calcule pour m croissants :
→ $\Sigma_m=-\frac{1}{m}(s_1\Sigma_{m-1}+\cdots+s_m\Sigma_0)$.
Cet algorithme permet de calculer χ_M en $O(n^4)$ opérations.

Prop 35 : Soit $M\in\mathcal{M}_n(\mathbb{K})$. Si χ_M est scindé à racines simples sur $\mathbb{K}$ alors M est diagonalisable (i.e. $\exists P\in GL_n(\mathbb{K})$ et D diagonale telles que $PDP^{-1}=M$).

Thm 36 : $M\in\mathcal{M}_n(\mathbb{K})$ est trigonalisable (i.e. $\exists P\in GL_n(\mathbb{K})$ et T triangulaire supérieure telles que $PTP^{-1}=M$) si et seulement si χ_M est scindé sur $\mathbb{K}$.

c) Localisation de valeurs propres

Thm 37 [Gershgörin] Soit $A=(a_{i,j})\in\mathcal{M}_n(\mathbb{C})$.
Le spectre de A est inclus dans la réunion des disques de Gershgörin $D_i=D(a_{ii},\sum_{j\ne i}|a_{ij}|)$.
On appelle cette réunion le domaine de Gershgörin.

Prop 38 : Soit $P\in\mathbb{C}[X]$, $P=X^n+a_{n-1}X^{n-1}+\cdots+a_0$.
On note $C_P=\begin{pmatrix}0 & \cdots & 0 & -a_0\\ 1 & \ddots & & \vdots\\ & \ddots & 0 & \vdots\\ 0 & & 1 & -a_{n-1}\end{pmatrix}$ la matrice compagnon du polynôme P.
On a alors $\chi_{C_P}=P$.

App 39 : Soit z une racine complexe du polynôme $P=X^n+a_{n-1}X^{n-1}+\cdots+a_0\in\mathbb{C}[X]$
Alors $|z|\le\max(|a_0|,(1+|a_1|),\ldots,(1+|a_{n-1}|))$.

Polynômes à coefficients rationnels et racines dans $\mathbb{Q}$ | X. Gourdon, Algèbre p65

Proposition : Soit $P \in \mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$. Alors P n'a que des racines simples dans $\mathbb{C}$

Démonstration : Comme P est irréductible dans $\mathbb{Q}[X]$ et que $\deg(P') < \deg(P)$, $PGCD(P,P') = 1$. Donc par le thm de Bézout il existe $(U,V) \in \mathbb{Q}[X]^2$ tels que $UP + VP' = 1$. Par la réciproque du théorème de Bézout cela implique que P et P' sont premiers entre eux dans $\mathbb{C}[X]$. Donc, sur $\mathbb{C}$, P est scindé à racines simples. □

Proposition : Si P appartenant à $\mathbb{Q}[X]$ admet une racine $\lambda \in \mathbb{C}$ de multiplicité $\mu > \deg(P)/2$, alors $\lambda \in \mathbb{Q}$.

Démonstration : Soit $P = cP_1 \dots P_k$ la décomposition de P en facteurs irréductibles de $\mathbb{Q}[X]$. λ est racine de r polynômes parmi les P_i, supposons λ racine de $P_1, \dots, P_r$.
Si $\lambda \notin \mathbb{Q}$, alors $\forall 1 \leq i \leq r$, $\deg(P_i) \geq 2$.
Mais alors $\deg(P) = \sum_{i=1}^{k} \deg(P_i)$

$$\geq \sum_{i=1}^{r} \deg(P_i)$$

$$\geq 2r$$

Or on sait aussi que $\lambda \in \mathbb{C}$ est racine de P_i irréductible dans $\mathbb{Q}[X]$ donc λ racine simple de P_i pour $1 \leq i \leq r$. Donc $\mu = r$ d'où $\deg(P) \geq 2\mu$. Absurde. $\lambda \in \mathbb{Q}$. □

$R \neq 0$ car P_1 est irréductible et $\deg P_2 < \deg P_1$

donc $P_1(\lambda) = Q(\lambda) P_2(\lambda) + R(\lambda)$

$\Rightarrow R(\lambda) = 0$

Mais comme $\deg R < 1$ on en déduit $\lambda \in \mathbb{R}$

$R = c(X - \lambda)$, $c \neq 0$ ce qui est contradictoire

Le polynôme P admet donc une racine rationnelle.

Contre-exemple : si $n = 1$ ce dernier résultat est faux : le polynôme $X^3 - 2$ admet pour racines dans $\mathbb{C}$: $\sqrt[3]{2}, j\sqrt[3]{2}, \bar{j}\sqrt[3]{2}$: $\notin \mathbb{Q}$.

Localisation des racines, Gourdon, Algèbre p83

Proposition : Soit $P = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in \mathbb{C}[X]$. On note $\rho = \max_{\lambda \text{ racine de } P} |\lambda|$. On suppose les a_i non tous nuls de sorte que $\rho \neq 0$

(i) $\rho \leq \sup\left(1, \sum_{i=1}^{n} |a_i|\right)$

(ii) $\rho \leq 1 + \sup_{1 \leq i \leq n} |a_i|$

Démonstration

(i) Si $\rho \leq 1$ c'est direct

Si $\rho > 1$, soit $\alpha \in \mathbb{C}$ tel que $\begin{cases} |\alpha| = \rho \\ P(\alpha) = 0 \end{cases}$

ce qui s'écrit

$$\alpha^n = -(a_1 \alpha^{n-1} + \dots + a_n)$$

ou encore comme $\alpha \neq 0$

$$\alpha = -\left(a_1 + \frac{a_2}{\alpha} + \dots + \frac{a_n}{\alpha^{n-1}}\right)$$

D'où $|\alpha| = \rho \leq |a_1| + \dfrac{|a_2|}{\rho} + \dots + \dfrac{|a_n|}{\rho^{n-1}}$ (Δ)

$$\leq \sum_{i=1}^{n} |a_i| \quad \text{car } \rho > 1 \Rightarrow \frac{1}{\rho^k} < 1$$

(ii) Si $\rho \leq 1$, l'inégalité est vérifiée.

Si $\rho > 1$, en utilisant (Δ) on obtient que

$\rho \leq a + \dfrac{a}{\rho} + \dots + \dfrac{a}{\rho^{n-1}}$ où $a = \sup_{1 \leq i \leq n} |a_i|$

or $0 < \dfrac{1}{\rho} < 1$ donc $\rho \leq a \sum_{k=0}^{+\infty} \dfrac{1}{\rho^k}$

$$\rho \leq \frac{\rho a}{\rho - 1}$$

i.e. $\rho - 1 \leq a$ □.

Applications (i) On pose $f(x) = x^n - (|a_1| x^{n-1} + \dots + |a_{n-1}| x + |a_n|)$

donc $f\left(\frac{\rho}{2^{1/n}-1}\right) \geq 0$ d'où $\rho \geq (2^{1/n}-1)\alpha$

(ii). Montrons que $\alpha \leq 2R$, ce qui se ramène à $f(2R) \geq 0$. Par définition de R, on a $|a_k| \leq R^k \quad \forall\, 1 \leq k \leq n$. Si $r = 2R$ on a donc $|a_k| r^{n-k} \leq \frac{r^n}{2^k}$ d'où

$$|a_1| r^{n-1} + \cdots + |a_{n-1}| 2^k r + |a_n| \leq r^n \left(\frac{1}{2} + \cdots + \frac{1}{2^n}\right) \leq r^n \quad \rho \leq 2R$$

donc $f(r) = f(2R) \geq 0$.

• on a vu que $|a_k| \leq C_n^k \rho^k$ pour $1 \leq k \leq n$, or $C_n^k = \frac{n \cdots n-k+1}{k!} \leq n^k$

donc $|a_k|^{1/k} \leq n \cdot \rho \quad \forall k, 1 \leq k \leq n$

donc $\frac{R}{n} \leq \rho$.

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

Exercices

ne s'invente pas si on l'a pas déjà vu

1) Soit $X^p - X - 1$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$ (cf. Perrin)

Soit α tq $\alpha^2 - \alpha - 1 = 0$, $\alpha \in \overline{\mathbb{F}_p}$ (par def de $\mathbb{Z}/p\mathbb{Z}$)

$(\alpha+1)^p = \alpha^p + 1 \Rightarrow (\alpha+1)^p - (\alpha+1) - 1 = \alpha^p + 1 - \alpha - 1 - 1 = 0$

Ainsi α racine $\Rightarrow \alpha+1$ racine.

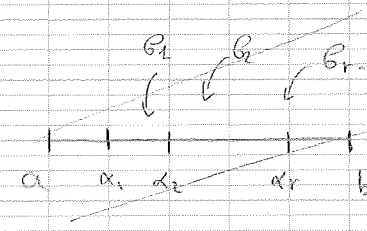
Ainsi, si on note α une racine de $X^p - X - 1$, $\alpha, \alpha+1, \dots \alpha+p-1$ sont toutes les racines de $X^p - X - 1$ (et elles sont distinctes !)

[...]

2) $P \in \mathbb{R}[X]$. $\forall x \in \mathbb{R}$, $N(x) = \#\{$ chgt de signe ds la suite $P(x), P'(x), \dots\}$

Alg $\#\{$ racines de P ds $]a,b[\} = |N(b) - N(a)| - 2k$ pour un $k \in \mathbb{N}$

(on va juste montrer $\leq$)



$|N(b) - N(a)| \geq r - 1$

$B = \{\beta_i, \exists k, P^{(k)}(\beta_i) = 0\}$. $a < \beta_1 < \dots < \beta_n < b$

$\beta_i < \gamma_i < \beta_{i+1}$

$N(b) - N(a) = \sum N(\gamma_{i+1}) - N(\gamma_i)$

[...]

3) $A, B, C \in \mathbb{Q}[X]$, $A + B + C = 0$. Premiers entre eux.

Alg $\max\{\deg A, \deg B, \deg C\} \leq$ nb de racines de ABC -1 (dans $\mathbb{C}$)

$\max\{\deg\} = \deg A = \deg B$ $\quad A = \prod (X - a_i)^{n_i}$ $\quad B = \prod (X - a_i)^{m_i}$

$C = \prod (X - c_i)^{p_i}$

$F = \frac{A}{C}$ $G = \frac{B}{C}$ $F + G + 1 = 0$

$Q = \prod (X - a_i) \prod (X - b_i) \prod (X - c_i)$

$\frac{B}{A} = - \frac{F'/F \times Q}{G'/G \times Q}$ = irred

donc $\deg A, \deg B \leq d^\circ \frac{F'}{F} Q, d^\circ \frac{G'}{G} Q$

avec $\deg Q$ = nb de r' de ABC