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

Dans cette leçon, K désignera un corps commutatif.

I - RACINES D'UN POLYNOME.

1) Arithmétique des polynômes. [GOZ]

Déf 1 : Soit K un corps, k un sous-corps de K et $P \in k[X]$. Une *racine* de P dans K est un élément α de K tel que $P(\alpha)=0$.

Prop 2 : Le polynôme $X-a$ divise P dans $k[X]$ si et seulement si a est racine de P dans k.

Déf 3 : La *multiplicité* de α comme racine de P est le plus grand entier $n \in \mathbb{N}$ tel que $(X-\alpha)^n$ divise P dans $K[X]$. On dit que α est une *racine simple* si α est de multiplicité 1.

Prop 4 : La somme des multiplicités des racines de P dans K est inférieure ou égale au degré de P. Il y a égalité si et seulement si P est dans $K[X]$ produit de polynômes du premier degré. On dit alors que P est *scindé* sur K.

Rq 5 : Un polynôme qui admet un nombre de racines strictement supérieur à son degré est nul.

App 6 : Unicité pour les polynômes interpolateurs de Lagrange.

Prop 7 : [RDO] Si K est de caractéristique nulle, alors $a \in K$ est racine de P de multiplicité $n \geq 1$ $\iff \begin{cases} \forall k \leq n-1, & P^{(k)}(a)=0 \\ P^{(n)}(a) \neq 0 \end{cases}$

C-ex 8 : $(X-1)^p$ dans $\mathbb{F}_p[X]$

Déf 9 : On dit que $P \in k[X]$ est *irréductible* dans $k[X]$ si P est non inversible et $\forall R, Q \in k[X]$,
$$P = QR \Rightarrow Q \in (k[X])^\times \text{ ou } R \in (k[X])^\times$$

Ex 10 : Tout polynôme de degré 1 est irréductible.

Prop 11 : [GOZ] Soit $P \in k[X]$ tel que $\deg P \geq 2$. Si P est irréductible dans $k[X]$, alors il n'admet pas de racines dans k.

C-ex 12 : La réciproque est fausse : $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$, mais est réductible dans $\mathbb{Q}[X]$. Elle est cependant vraie pour les polynômes de degré 2 ou 3.

2) Adjonction de racines. [GOZ]

Déf 13 : Soit k un corps, K une extension de K et $\alpha \in K$. On est dans une et une seule des situations suivantes :
- ou bien il existe $P \in k[X] \setminus \{0\}$ tel que $P(\alpha)=0$. On dit alors que α est un *élément algébrique* sur k.
- ou bien le morphisme d'évaluation en α des éléments de $k[X]$ est injectif. On dit alors que α est un *élément transcendant* sur k.

Ex 14 :
- i est algébrique sur $\mathbb{R}$; $\sqrt{2}$ est algébrique sur $\mathbb{Q}$.
- e et π sont transcendants sur $\mathbb{Q}$. (ADMIS)

Déf 15 : On dit que K est une *extension algébrique* de k si tous les éléments de K sont algébriques sur k.

Déf 16 : Soit $P \in K[X]$ irréductible dans $K[X]$. On dit que le corps L est un *corps de rupture* de P sur K si et seulement si il existe $\alpha \in L$ tel que $P(\alpha)=0$ et $L = K(\alpha)$.

Th 17 : (i) Le corps $K[X]/(P)$ est un corps de rupture de P sur K.
(ii) Ce corps est unique à isomorphisme près.

Ex 18 : $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, $\mathbb{F}_4 = \mathbb{F}_2/X^2+X+1$

Cor 19 : Soit $P \in K[X]$, $\deg P \geq 1$. Il existe une extension algébrique simple L de K dans laquelle P possède au moins une racine.

Prop 20 : Soit $P \in K[X]$ de degré n. P irréductible dans $K[X] \iff P$ n'a pas de racine dans toute extension L/K telle que $[L:K] \leq \frac{n}{2}$.

Déf 21 : Soit E une extension de K, $P \in K[X]$, $\deg P = n \in \mathbb{N}^*$. On dit que E est un corps de décomposition de P sur K si :
(i) $\exists a \in E, \exists (\alpha_1, \dots, \alpha_n) \in E^n$ tels que $P = a(X-\alpha_1)\dots(X-\alpha_n)$
(ii) $E = K(\alpha_1, \dots, \alpha_n)$

Prop 22 : Soit $P \in K[X]$, $\deg P \geq 1$.
(i) Il existe un corps de décomposition L de P sur K avec $[L:K] \leq n!$.
(ii) Celui-ci est unique à isomorphisme près. On le note $D_K(P)$.

Ex 23 : $\mathbb{Q}(\sqrt{2}) = D_{\mathbb{Q}}(X^2-2)$, $\mathbb{C} = D_{\mathbb{R}}(X^2+1)$

App 24 : Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.

(i) Il existe un corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.

(ii) Ce corps est unique à isomorphisme près.

Déf 25. Les conditions suivantes sont équivalentes :

(1) Tout polynôme de degré supérieur ou égal à 1 de $K[X]$ est scindé sur K.

(2) Tout polynôme de degré supérieur ou égal à 1 de $K[X]$ admet au moins une racine dans K.

(3) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

(4) Toute extension algébrique de K est identique à K.

On dit alors que K est algébriquement clos.

Ex 26 : • $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

• Les corps finis ne sont pas algébriquement clos.

Th 27 : Théorème de D'Alembert-Gauß.

Le corps $\mathbb{C}$ est algébriquement clos.

Cor 28 : Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 ou les polynômes de degré 2 n'ayant pas de racine réelle.

App : Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.

3) Groupe de Galois.

Déf 29 : Soit $P \in K[X]$ unitaire, $\deg P \geq 2$ et $L := D_K(P)$.

On appelle groupe de Galois du polynôme P sur K le groupe de Galois de L sur K. (i.e. $Aut_K(L)$)

Ex 30 : • Le groupe de Galois de X^2+1 sur $\mathbb{R}$ est $Gal(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \sigma\}$ (où σ désigne le morphisme conjugaison)

• Soit $d \in \mathbb{N}^*$ sans facteur carré, alors le groupe de Galois de X^2-d sur $\mathbb{Q}$ est $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt{d})}, \sigma\}$,

où $\forall x,y \in \mathbb{Q}$, $\sigma(x+y\sqrt{d}) = x - y\sqrt{d}$.

Prop 31 : Soit L et M deux extensions de K.

Pour tout K-morphisme $g : L \to M$, $\forall P \in K[X]$, $\forall \alpha \in L$, $g(P(\alpha)) = P(g(\alpha))$.

Donc α racine de $P \Leftrightarrow g(\alpha)$ racine de P.

Prop 32 : Soit R l'ensemble des racines de $P \in K[X]$ dans $D_K(P)$, et $G = Gal(D_K(P)/K)$.

Alors G est isomorphe à un sous-groupe de $\mathfrak{S}(R)$.

Th 33 : Soit $P \in K[X]$, de degré supérieur ou égal à 2, séparable sur K. Alors P irréductible dans $K[X] \Leftrightarrow G$ agit transitivement sur R.

II - FONCTIONS SYMETRIQUES ELEMENTAIRES. [GOZ]

1) Polynômes symétriques.

Dans cette partie, A désignera un anneau commutatif unitaire.

Déf 34 : Soit $P \in A[X_1, \dots, X_n]$

On dit que P est un polynôme symétrique si
$\forall \sigma \in \mathfrak{S}_n$, $P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

On notera $Sym(A[X_1, \dots, X_n])$ leur ensemble.

Prop/Déf 35 : Dans $A[X_1, \dots, X_n]$, les n polynômes Σ_p (pour $1 \leq p \leq n$) définis par : $\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$

sont appelés polynômes symétriques élémentaires.

Déf 36 : Soit un monôme $aX_1^{\alpha_1} \dots X_n^{\alpha_n}$, où $a \in A^*$ et les $\alpha_i \in \mathbb{N}$.

On appelle poids de ce monôme, l'entier $\sum_{i=1}^n i\alpha_i$.

Soit $P \in A[X_1, \dots, X_n] \setminus \{0\}$. On appelle poids de P le maximum des poids des monômes non nuls dont il est la somme.

Rq 37 : Soit $P \in A[X_1, \dots, X_n]$ symétrique.

Alors P a même degré partiel par rapport à chacune des indéterminées $X_1, \dots, X_n$. Ce degré partiel commun est appelé degré partiel, et est noté $d_p(P)$.

Prop 38 : Soit $P \in A[X_1, \dots, X_n] \setminus \{0\}$ de poids π.

Alors le polynôme $Q(X_1, \dots, X_n) := P(\Sigma_1, \dots, \Sigma_n)$ est un polynôme symétrique de degré partiel au plus π.

Th 39 : Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique tel que $d_p(P) = k$.

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 $d_p(P)$.

Ex 40 : $X_1^2 + \dots + X_n^2 = \Sigma_1^2 - 2\Sigma_2$

Th 41 : Relations entre coefficients et racines d'un polynôme.

Soit $P \in A[X]$ et $(\alpha_1, \dots, \alpha_n) \in A^n$. Les conditions suivantes sont équivalentes :

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

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

Déf 42 : Soit A, B deux anneaux commutatifs unitaires, avec $A \subset B$.
Soit $P \in A[X]$ un polynôme unitaire qui est scindé sur B
(i.e. $\exists (\alpha_1, \dots, \alpha_n) \in B^n$ tel que $P(X) = (X-\alpha_1)\dots(X-\alpha_n)$)
Alors pour tout polynôme symétrique S de $A[X_1, \dots, X_n]$,
$S(\alpha_1, \dots, \alpha_n) \in A$.

DO] **Déf 43** : On appelle <u>polynômes symétriques homogènes</u> les polynômes définis par : $\forall k \in \mathbb{N}$, $S_k = \sum_{p=0}^{k} X_p^k$

Th 44 : <u>Formules de Newton</u>

1) $\forall k \in [\![1, n]\!]$, $S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} + \dots + (-1)^k S_0 \Sigma_k = 0$
ii) $\forall k \geq n$, $S_k - \Sigma_1 S_{k-1} + \dots + (-1)^n \Sigma_n S_{k-n} = 0$

GN] **App 45** : <u>Caractérisation des matrices nilpotentes avec la trace</u>
Soit K un sous-corps de $\mathbb{C}$ et $A \in M_n(K)$.
Si pour tout $k \geq 1$ la trace de A^k est nulle, alors A est nilpotente.

G2] **2) Aspect topologique.**

Th 46 : <u>Continuité des racines d'un polynôme.</u>
Soit $P \in \mathbb{C}[X]$. On écrit $P = (X - z_1)\dots(X - z_n)$
$$= X^n + \sum_{k=1}^{n} (-1)^k \Sigma_k(z_1, \dots, z_n) X^{n-k}$$
/1
Alors l'application $\bar{e} : \mathbb{C}^n / \mathfrak{S}_n \longrightarrow \mathbb{C}^n$
$$(z_1, \dots, z_n) \longmapsto (\Sigma_1(z_1, \dots, z_n), \dots, \Sigma_n(z_1, \dots, z_n))$$
est un homéomorphisme.
Autrement dit, les racines d'un polynôme sont continues en les coefficients.

App 47 : L'application qui à une matrice associe son polynôme caractéristique est continue.

U] **III - RESULTANT**

1) Définition et premières propriétés

Déf 49 : Soit $P, Q \in K[X]$ de degrés respectifs $p, q \in \mathbb{N}^*$.
Posons $\varphi : K_{q-1}[X] \times K_{p-1}[X] \to K_{p+q-1}[X]$
$$(U, V) \longmapsto UP + VQ$$
La matrice de φ dans les bases $((X^{q-1}, 0), \dots, (1, 0), (0, X^{p-1}), \dots, (0, 1))$ et $(X^{p+q-1}, \dots, 1)$ est appelée la <u>matrice de Sylvester</u> de P et Q.
Son déterminant est appelé le <u>résultant</u> de P et Q, noté $\mathrm{Res}(P, Q)$.

Prop 50 : Les assertions suivantes sont équivalentes :
(i) P et Q ont un diviseur commun non constant dans $K[X]$.
(ii) $\mathrm{res}(P, Q) = 0$
(iii) $\exists U \in K_{q-1}[X], \exists V \in K_{p-1}[X]$ tels que $UP = VQ$.

2) Discriminant.

Déf 51 : On suppose $\deg P \geq 2$. Le <u>discriminant</u> de P, noté $\mathrm{disc}(P)$, est défini par : $\mathrm{disc}(P) = \dfrac{(-1)^{\frac{p(p-1)}{2}}}{a_p} \mathrm{res}(P, P')$.

Ex 52 : $\mathrm{disc}(aX^2 + bX + c) = b^2 - 4ac$; $\mathrm{disc}(X^3 + pX + q) = -4p^3 - 27q^2$ [GOZ] [TAU]

Prop 53 : Soit $P \in K[X]$ tel que $\deg P \geq 2$.
Si K est de caractéristique nulle et P est scindé sur K, alors P n'a que des racines simples si et seulement si $\mathrm{disc}(P) \neq 0$.

Prop 54 : Soit $P \in K[X]$ scindé sur K, $\deg P \geq 2$ et $\alpha_1, \dots, \alpha_p$ les racines de P comptées avec multiplicité.
Alors $\mathrm{disc}(P) = a_p^{2p-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$

IV - LOCALISATION ET RECHERCHE DE RACINES.

Prop 55 : Soit $P = X^d + a_1 X^{d-1} + \dots + a_d \in \mathbb{C}[X]$ [MGN]
Alors pour toute racine λ de P, $|\lambda| \leq 1 + \max_{1 \leq k \leq n} |a_k|$

Th 56 : <u>Théorème de Gauss-Lucas.</u> [GOZ]
Soit $P \in \mathbb{C}[X]$ non constant.
Toute racine de P' appartient à l'enveloppe convexe des racines de P.

Th 57 : <u>Localisation des racines</u>
Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$ à racines simples.
Soit $t \in \mathbb{R}$ tel que $P(t) \neq 0$. [DIE]
Alors il existe une forme quadratique $Q(P)$ telle que $\mathrm{rg}(Q) = n$ et la signature de $Q(P)$, notée $(p+r, q+r)$, vérifie : DEV
- p est le nombre de racines réelles strictement supérieures à t.
- q est le nombre de racines réelles strictement inférieures à t
- $2r$ est le nombre de racines imaginaires.

Th 58 : <u>Méthode de Newton pour les polynômes à racines réelles.</u>
Soit $r \in \mathbb{N}^*$ et $\xi_1 < \dots < \xi_r$ dans $\mathbb{R}$. Soit $(m_i)_{1 \leq i \leq r} \in \mathbb{N}^r$ et $P = \prod_{i=1}^{r} (X - \xi_i)^{m_i}$. Soit $x_0 \in \mathbb{R}$, $x_0 > \xi_r$. On définit par récurrence $\forall n \in \mathbb{N}$, $x_{n+1} = x_n - \dfrac{P(x_n)}{P'(x_n)}$. La suite $(x_n)_{n \in \mathbb{N}}$ est bien définie, strictement décroissante et converge ξ_r.

Références.

[GOZ] Théorie de Galois, Ivan Gozard.
[RDO] Cours de mathématiques spéciales, E. Ramis, C. Deschamps, J. Odoux.
[FGN] Oraux X-ENS Algèbre 2, S. Francinou, H. , S. Nicolas.
[H2G2] Histoires hédonistes de groupes et de géométries 1, P. Caldero, J. Germoni
[TAU] Algèbre, Patrice Tauvel.
[MGN] Algèbre Concrète, Maurice Mignotte.
[DIE] Calcul infinitésimal, Jean Dieudonné.

Continuité des racines d'un polynôme

Fabien Kütle et Vadim Ognov

Référence : Caldero-Germoni, Histoires hédonistes de groupes et géométrie, p.79-80

Soit $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$ on note $e_k(z)$ l'évaluation en z du k-ième polynôme symétrique élémentaire. On définit alors l'application

$$e : \begin{cases} \mathbb{C}^n \longrightarrow \mathbb{C}^n \\ z \longmapsto (e_k(z))_{1\leqslant k\leqslant n} \end{cases}.$$

En particulier, on a pour tout $z \in \mathbb{C}^n$,

$$P_{e(z)}(X) := \prod_{i=1}^{n}(X - z_i) = X^n + \sum_{i=1}^{n}(-1)^k e_k(z)X^{n-k}.$$

On munit $\mathbb{C}^n$ de la norme euclidienne usuelle.

- e est continue car les e_k sont des polynômes.
- e est surjective. Si $w \in \mathbb{C}^n$, on considère le polynôme $P(X) = X^n + \sum_{k=1}^{n}(-1)^k w_k X^{n-k}$. Par le théorème de D'Alembert-Gauss, P admet n racines notées $\lambda_1, \ldots, \lambda_n$. Donc $(\lambda_1, \ldots, \lambda_n)$ appartient à $e^{-1}(w)$.
- Pour tout $w \in \mathbb{C}^n$, $\mathfrak{S}_n$ agit sur $e^{-1}(w)$ selon $\sigma \bullet (z_1, \ldots, z_n) = (z_{\sigma(1)}, \ldots, z_{\sigma(n)})$. En effet, comme les e_k sont symétriques, si $z \in e^{-1}(w)$ alors pour tout $\sigma \in \mathfrak{S}_n$, $e(\sigma \bullet z) = e(z) = w$. De plus, si z et z' appartiennent à $e^{-1}(w)$ alors $P_{e(z)} = P_{e(z')}$ donc $\{z_i\} = \{z'_i\}$. Donc l'action est transitive.

On peut dès lors définir l'application suivante

$$\overline{e} : \begin{cases} \mathbb{C}^n/\mathfrak{S}_n & \longrightarrow \mathbb{C}^n \\ \pi(z) & \longmapsto e(z) \end{cases}.$$

Comme $\mathbb{C}^n/\mathfrak{S}_n$ est muni de la topologie quotient, la propriété universelle et la continuité de e assure que $\overline{e}$ est une bijection continue.

Théorème 1

L'application $\overline{e} : \mathbb{C}^n/\mathfrak{S}_n \to \mathbb{C}^n$ est un homéomorphisme.

On a besoin du lemme suivant.

Lemme 1

L'application $\delta : \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{R}_+$ telle que

$$\forall z, z' \in \mathbb{C}^n \qquad \delta(z, z') = \min_{\sigma \in \mathfrak{S}_n} \|z - \sigma \bullet z'\|_2$$

passe au quotient sous l'action de $\mathfrak{S}_n$ et induit une distance sur $\mathbb{C}^n/\mathfrak{S}_n$. Cette distance métrise la topologie quotient.

▸ δ est symétrique et on a, pour tous $z, z', z'' \in \mathbb{C}^n$ et pour tout $\sigma \in \mathfrak{S}_n$

$$\begin{aligned} & \|z - \sigma \bullet z'\|_2 \leqslant \|z - \tau \bullet z''\|_2 + \|z'' - \tau \bullet z''\|_2 + \|z'' - \sigma \bullet z\|_2 \qquad \forall \tau \\ \text{donc} \quad & \|z - \sigma \bullet z'\|_2 \leqslant \min_{\tau} \left(\|z - \tau \bullet z''\|_2 + \|z'' - \tau \bullet z''\|_2 + \|z'' - \sigma \bullet z\|_2 \right) \\ & \|z - \sigma \bullet z'\|_2 \leqslant \min_{\tau} \|z - \tau \bullet z''\|_2 + \|z'' - \sigma \bullet z\|_2 \qquad \text{pour } \tau = \mathrm{Id}. \end{aligned}$$

Donc

$$\delta(z, z') \leqslant \delta(z, z'') + \delta(z'', z').$$

De plus, pour tout $\tau \in \mathfrak{S}_n$, pour tout $z, z' \in \mathbb{C}^n$,

$$\delta(z, \tau \bullet z') = \delta(z, z')$$

Donc δ passe au quotient en une application $d : \big(\pi(z), \pi(z')\big) \mapsto \min_{\omega \in \pi(z')} \|z - \omega\|_2$. Alors $d\big(\pi(z), \pi(z')\big) = 0$ si et seulement $\pi(z) = \pi(z')$ dans $\mathbb{C}^n/\mathfrak{S}_n$.

Donc d est une distance.

▸ On munit $\mathbb{C}^n/\mathfrak{S}_n$ de la distance d. Alors la projection canonique π est continue. On montre également que π est ouverte et fermée.

- Si X est un fermé de $\mathbb{C}^n$ et $\big(\pi(x_n)\big)_{n \in \mathbb{N}}$ une suite de $\pi(X)$ qui converge vers $\pi(z)$ alors il existe $z' \in \pi(z)$ tel que x_n converge vers z'. Donc z' appartient à X donc $\pi(z) = \pi(z')$ appartient à $\pi(X)$.
- Si U est un ouvert de $\mathbb{C}^n$ et $\pi(z)$ appartient à $\pi(U)$ alors il existe z' dans U telle que $z' \in \pi(z)$. Soit $r > 0$ tel que $B(z', r) \subset U$, on a $B_d\big(\pi(z'), r\big) \subset \pi(U)$.

Ainsi, la topologie induite par d est la topologie quotient.

On peut désormais montrer le théorème.

Démonstration : ▸ Soit $M > 0$ et $B := B_d(0, M)$. Pour tout fermé $X \subset \overline{B}$, $\pi^{-1}(X)$ est un fermé borné de $\mathbb{C}^n$ donc un compact. Alors $\overline{e}(X) = e \circ \pi^{-1}(X)$ est un compact donc un fermé de $\mathbb{C}^n$. Donc $\overline{e}$ est une bijection continue et fermé sur $\overline{B}$ donc $\overline{e}_{|\overline{B}}$ est un homéomorphisme.

▸ Soit U un ouvert de $\mathbb{C}^n/\mathfrak{S}_n$ et $x \in U$. Il existe $r > 0$ et $M > 0$ tels que $B_d(x, r) \subset U$ et $\overline{B_d(x, r)} \subset B_d(0, M)$. Comme $\overline{e}_{|B}$ est ouverte, $\overline{e}(x)$ est un point intérieur de $\overline{e}\big(B_d(x, r)\big)$. Donc x est un point intérieur de $\overline{e}(U)$.

Remarque : Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$ et $\varepsilon > 0$ qui sépare les (λ_i) pour la distance d. Alors il existe $\delta > 0$ tel que

$$b \in B(a, \delta) \quad \Rightarrow \quad Q(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \text{ admet exactement } m_i \text{ racines dans } B(\lambda_i, \epsilon).$$

Localisation de racines

Fabien Kütle et Vadim Ognov

Référence : Dieudonné, Calcul infinitésimal, p.64-65

Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$ à racines simples. Soit $t \in \mathbb{R}$ tel que $P(t) \neq 0$. On va montrer le théorème suivant.

Théorème 1

Il existe une forme quadratique $\mathcal{Q}(P)$ telle que $\operatorname{rg} \mathcal{Q} = n$ et la signature de $\mathcal{Q}(P)$, notée $(p+r, q+r)$, vérifie

- *p est le nombre de racines réelles strictement supérieures à t ;*
- *q est le nombre de racines réelles strictement inférieures à t ;*
- *$2r$ est le nombre de racines imaginaires.*

Démonstration : Pour tout $P \in \mathbb{R}[X]$, on note $P^\bullet$ le polynôme $P^\bullet(X) = (X-t)P'(X)$.
On définit alors un polynôme symétrique

$$\mathcal{S}(P)(X,Y) = \frac{P(X)P^\bullet(Y) - P(Y)P^\bullet(X)}{X-Y} = \sum_{i,j=0}^{n-1} a_{ij} X^i Y^j$$

On a $a_{ij} = a_{ji}$ pour tout i, j donc l'application $\mathcal{Q}(P)$ définie par

$$\forall u = (u_0, \ldots, u_{n-1}) \in \mathbb{R}^n \qquad \mathcal{Q}(P)(u) = \sum_{i,j=0}^{n-1} a_{ij} u_i u_j$$

est une forme quadratique.

On considère à présent deux polynômes $P_1(X) = \sum_{i=0}^{r} b_i X^i$ et $P_2(X) = \sum_{j=0}^{s} c_j X^j$ où $r+s=n$.
Alors

$$S(P_1P_2)(X,Y) = P_2(X)P_2(Y)\mathcal{S}(P_1)(X,Y) + P_1(X)P_1(Y)\mathcal{S}(P_2)(X,Y)$$

On note $(a^1_{kl})_{0 \leqslant k,l \leqslant r-1}$, respectivement $(a^2_{kl})_{0 \leqslant k,l \leqslant s-1}$, les coefficients de $\mathcal{S}(P_1)$, respectivement $\mathcal{S}(P_2)$.
On peut alors écrire

$$\mathcal{S}(P_1P_2)(X,Y) = \sum_{k,l=0}^{r-1} a^1_{kl} \Big(\sum_{i=0}^{s} c_i X^{k+i}\Big)\Big(\sum_{j=0}^{s} c_j Y^{l+j}\Big) + \sum_{k,l=0}^{s-1} a^2_{kl} \Big(\sum_{i=0}^{r} b_i X^{k+i}\Big)\Big(\sum_{j=0}^{r} b_j Y^{l+i}\Big).$$

Si on pose pour tout $u = (u_0, \ldots, u_{n-1}) \in \mathbb{C}$ les applications linéaires v dans $\mathcal{L}(\mathbb{R}^n, \mathbb{R}^r)$ et w dans $\mathcal{L}(\mathbb{R}^n, \mathbb{R}^s)$ telles que

$$v_k(u) = \sum_{i=0}^{s} c_i u_{i+k} \qquad \forall k \in \{0, \ldots, r-1\}$$
$$w_l(u) = \sum_{j=0}^{r} b_j u_{j+l} \qquad \forall l \in \{0, \ldots, s-1\}$$

alors

$$\mathcal{Q}(P_1P_2) = \mathcal{Q}(P_1) \circ v + \mathcal{Q}(P_2) \circ w \tag{1}$$

De plus, on note que $\det(v_0, \ldots, v_{r-1}, w_0, \ldots, w_{s-1}) = \mathrm{Res}(P_2, P_1)$. Donc si P_1 et P_2 n'ont pas de racine commune alors $(v_0, \ldots, v_{r-1}, w_0, \ldots, w_{s-1})$ est libre.

On obtient par récurrence de l'équation (2) que si P se décompose sur $\mathbb{R}$ selon

$$P(X) = \prod_{i=1}^{r} (X - \lambda_i) \prod_{j=1}^{s} \left((X - \alpha_j)^2 + \beta_j^2\right)$$

alors il existe $v_1, \ldots, v_r, w_1^1, w_1^2, \ldots, w_s^1, w_s^2$ dans $\mathcal{L}(\mathbb{R}^n, \mathbb{R})$ tels que

$$\mathcal{Q}(P) = \sum_{i=1}^{r} \mathcal{Q}(X - \lambda_j) \circ v_i + \sum_{j=1}^{s} \mathcal{Q}\left((X - \alpha_j)^2 + \beta_j^2\right) \circ w_j.$$

De plus, comme P n'a pas de racine multiple dans $\mathbb{C}$ alors $(v_1, \ldots, v_r, w_1^1, \ldots, w_s^2)$ est libre.

Ainsi par la loi d'inertie de Sylvester, il suffit d'étudier les cas "$n = 1$" et "$n = 2$ et P n'a pas de racine réelle".

- Si $P = X - \lambda$ alors $\mathcal{S}(P)(X, Y) = \lambda - t$ donc $\mathcal{Q}(P)(u_0) = (\lambda - t)u_0^2$. Donc $\mathcal{Q}(P)$ est une forme quadratique de rang 1 (car t n'est pas racine de P) et de signature $(1, 0)$ si $\lambda > t$ ou $(0, 1)$ si $\lambda < t$.
- Si $P = (X - \alpha)^2 + \beta^2$ alors

$$\mathcal{Q}(P)(X, Y)(u_0, u_1) = 2(\alpha - t)u_1^2 + 4\left(\beta^2 + \alpha^2(\alpha - t)\right)u_1u_0 + 2\left(\beta^2(\alpha + t) + 2\alpha^2(\alpha - t)\right)u_0^2$$

Le déterminant de la forme polaire associée est $-4\beta^2(t + \alpha)^2$ donc $\mathcal{Q}(P)$ est une forme quadratique de signature $(1, 1)$.