Polynômes

$\mathbb{K}[X]$ est un anneau euclidien, donc principal ; tout polynôme de $\mathbb{K}[X]$ se décompose en produit d'irréductibles normalisés et de $\lambda \in \mathbb{K}^*$

Prop Si $P \in \mathbb{K}[X]$ $\deg P = 1$, P est irréductible
$\deg P \in \{2,3\}$ P est irréductible $\Leftrightarrow$ P sans racine

D/ $\Rightarrow$ si P est irréductible de degré ≥ 2, il est sans racine

(sinon $P = (X-a)Q$) $\Leftarrow$ Si P se factorise de façon non triviale

$P = \underset{\deg \geq 1}{Q} \underset{\deg \geq 1}{R}$ $\left| \begin{array}{l} \deg P = 2 \ \deg Q = \deg R = 1 \\ \deg P = 3 : \deg Q = 1 \text{ ou } \deg R = 1 \end{array} \right.$

Contrex : $(X^2+1)^2$ dans $\mathbb{R}[X]$

Prop : si $\mathbb{K} \subset \mathbb{L}$ (extension de corps) et $(A,B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$

$A \wedge B$ est le même dans $\mathbb{L}[X]$ et dans $\mathbb{K}[X]$

D/ L'algorithme d'Euclide reste dans $\mathbb{K}[X]$

I Polynômes complexes

D'Alembert Gauss les polynômes irréductibles sont de degré 1

Si $P = \lambda \prod_{1}^{n} (X - z_i)^{\alpha_i}$, $Q = \mu \prod_{i=1}^{n} (z - z_i)^{\beta_i}$ $\alpha_i \geq 0$, $\beta_i \geq 0$

$P \wedge Q = \prod_{i=1}^{n} (X - z_i)^{\min(\alpha_i, \beta_i)}$

Ex $X^m - 1 \wedge X^n - 1 = X^{m \wedge n} - 1$

D/ $X^m - 1$ est dissocié de racines $\mathbb{U}_m$
$X^n - 1$

avec ce qui précède $X^m - 1 \wedge X^n - 1 = \prod_{\xi \in \mathbb{U}_n \cap \mathbb{U}_m} (X - \xi)$

si $\xi^m = 1$ et $\xi^n = 1$ on trouve $um + vn = d$, $u, v \in \mathbb{Z}$

$$\xi^d = \xi \dots = 1$$

donc $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_d$

__Localisation des racines__ : $P = X^n + a_{n-1} X^{n-1} + \dots + a_0$

Si $\underset{=0}{P(z)}$, alors $|z| \leq 1 + \max_{0 \leq k \leq n} (|a_k|)$

Ex Soit $n \geq 1$, $P_k \in \mathbb{C}_n[X]$ $P_k(X) = X^n + \dots$

On suppose que $P_k \xrightarrow{CVS} P \in \mathbb{C}_n[X]$

Soit $\overline{D}(a, r)$ un disque ouvert de $\mathbb{C}$ contenant ℓ racines de P avec multiplicité

Mq $\exists K \in \mathbb{N}$ $\forall k \geq K$ $D(a, r)$ contient ℓ racines de P_k avec multiplicité.

S/ En effet, les coef de P_k forment des suites convergentes

On fixe $a_0, \dots, a_n \in \mathbb{C}$ 2 à 2 $\neq$ $L_j = \dfrac{\prod_{i \neq j} (X - a_i)}{\prod_{i \neq j} (a_i - a_j)}$

16L1

$P_k(X) = \sum_{j=0}^{n} P_k(a_j) L_j(X)$ d'où (*)

On a Mq : (*) montre que $M = 1 + \max_{0 \le l \le n} |a_{k,l}|$ convient $k \in \mathbb{N}$

(ii) On écrit $P_k(X) = \prod_{i=1}^{n} (X - z_{k,i})$

BW : Soit $\varphi_{\mathbb{N}} \nearrow \mathbb{N}$ tq $\forall i$, $z_{\varphi(k),i} \longrightarrow z_i$ avec les relations coefficients racines $\prod_{i=1}^{n} (X - z_{\varphi(k),i}) \xrightarrow[\text{coeff}]{} \prod_{i=1}^{n} (X - z_i)$ coeff par coeff

donc $\prod_{i=1}^{n} (X - z_i) = P$

(iii) Par l'abs. $A = \{ k \in \mathbb{N} \,/\, P_k$ possède moins de $l-1$ racines de $D(a,r)$ est infini distinctes

On extrait avec P à valeurs dans A | $P(X) = \prod_{i=1}^{l-1} (X - z_{\varphi(n),i})$

$\prod_{l}^{n} (X - z_{\varphi(n),i})$

$| z_{\varphi(n),i} \longrightarrow z_i$ à la limite $\prod_{l}^{n} (X - z_i)$ hors du disque ouvert

P, or $z_i \notin D(a,r)$ $i = 0 \dots n$

$z_i \notin D(a,r)$ $i \geq l$ car $\mathbb{C} \setminus D(a,r)$ est fermé, Abs

DM $\to$ Gauss Lucas, Grace...

II Polynômes réels

Irréductibles de $\mathbb{R}[X]$ | $X - a$ $a \in \mathbb{R}$

$X^2 - aX + b$ | $a^2 - 4b < 0$

D/ Si $X-z \mid P$ réel il vient $X-\bar{z} \mid P$ par conjugaison

si $z \notin \mathbb{R}$ $(X-z)(X-\bar{z}) \mid P$

$$X^2 - 2\mathrm{Re}(z) + |z|^2 \mid P$$

Ex I: $\left\{ \underset{P \geq 0}{P \in \mathbb{R}[X]} \right\} \underset{\supset \text{clair}}{=} \left\{ A^2+B^2 \mid (A,B) \in \mathbb{R}[X]^2 \right\} = \mathcal{S}$

Obs $\mathcal{S}$ est donc un ensemble stable par multiplication

$$P(X) = \lambda \prod_{1}^{m} (X-a_i)^{\alpha_i} \prod_{m+1}^{n} (X^2+b_iX+c_i)_{\text{irréd}}$$

$\lambda > 0$ $\quad P(x) \xrightarrow[+\infty]{} +\infty \mid X^2+b_iX+c_i = \left(X+\frac{b_i}{2}\right)^2 - c_i - \frac{b_i^2}{4} \in \mathcal{S}$

En a_i $P(x) \underset{a_i}{\sim} \mu (x-a_i)^{\alpha_i}$ donc α_i est pair

$$\text{donc } (X-a_i)^{\alpha_i} = \left((X-a_i)^{\alpha_i/2}\right)^2$$

par stabilité par produit on a l'inclusion réciproque.

Polynômes scindés

① Soit $P \in \mathbb{R}[X]$, scindé $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$

i) Si P est scindé P' aussi idem $P + \lambda P'$, $\lambda \in \mathbb{R}$.
dissocié P' aussi

ii) P dissocié $\forall k \; a_k^2 + a_{k+1}^2 > 0$

iii) P scindé $a_k a_{k+2} \leq a_{k+1}^2$

iv) $P_k = X^n + a_{n-1}X^{n-1} + \dots + a_0$ scindé $P_k \xrightarrow{CVS} P$

alors P est scindé

i) Rolle : si $a_1 < \dots < a_n$ sont les zéros de P de multiplicités $\alpha_1 \dots \alpha_n$; a_i racine de P' de mult $\alpha_i - 1$ $i = 1 \dots n$

Rolle donne $a_1 < b_1 < a_2 < \dots < b_{n-1} < a_n$ b_i zéros

de P'. Total $\alpha_1 + \dots + \alpha_{n-1} \geq n + n - 1 = n-1$

RMI) décroissance des nbre de racines multiples ($si > 0$)

Ex : $L_n(x) = \dfrac{1}{2^n n!} \dfrac{d^n}{dx^n}\left((x^2-1)^n\right)$ est scindé à racines

dans $]-1,1[$

$P + \alpha P'$: on regarde $e^{\alpha t} P(t) = f(t)$. Si a est racine

d'ordre r, $f(a+h) = \lambda h^r + O(h^{r+1})$

$f'(a+h) = r\lambda h^{r-1} + O(h^r)$

$Q(t) = \beta P(t) + P'(t)$: $Q(a+h)e^a e^h = r h^{r-1} + O(h^r)$

Fin : $\alpha = 0$ OK

$\alpha \neq 0$, $\beta = \frac{1}{\alpha}$, de m̂ que dans la 1ère partie, Q possède

$n-1$ racines réelles

Peace on you :)

Ex : $(a_k, a_{k+1}) \neq (0,0)$ si P est dimocié

supposons $a_k = a_{k+1} = 0$ $\quad P^{(k)}(x) = k!\, a_k + (k+1)!\, a_{k+1} x$

$+ \frac{(k+2)!}{2} a_{k+2} x^2 + \dots$

0 est de mult 2 or P est dimo
donc $P^{(k)}$ aussi clairemde

Ex : $a_k a_{k+2} \leq a_{k+1}^2$: On regarde P'/P

$$\frac{P'}{P} = \sum_{i=1}^{m} \frac{1}{X - a_i}$$

alors $\left(\frac{P'}{P}\right)' = -\sum_{i=1}^{m} \frac{1}{(X-a_i)^2}$

$\hookrightarrow \frac{P''P - P'^2}{P^2} \leq 0$ sur $\mathbb{R} \setminus I_{gm}$

donc $P''P - P'^2 \leq 0$ en 0 $\quad P''(0)P(0) \leq P'^2(0)$

On remplace P par $P^{(k)}$ qui demeure scindé

$$P^{(k+2)}(0)\, P^{(k)}(0) \leq P^{(k+1)}(0)^2$$

$$(k+2)!\, a_{k+2}\, k!\, a_k \leq (k+1)!^2\, a_{k+1}^2$$

$$a_{k+2} a_k \leq \frac{k+1}{k+2} a_{k+1}^2 \leq a_{k+1}^2$$

$X^2 \pm X \pm 1$ $\Delta = 1 \pm 4$

Ex Soit $z \in \mathbb{C} \setminus \mathbb{R}$ $\forall k \in \mathbb{N}$ $|P_k(z)| = \prod_{j=1}^{n} |z - a_j| \geq |\operatorname{Im} z|^n$

$k \to +\infty$ $|P(z)| \geq |\operatorname{Im}(z)|^n$

pas de racines complexes

Ex : Trouver les $P \in \mathbb{R}[X]$. $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \{-1, 0, 1\}$

qui sont scindés sur $\mathbb{R}$

S/ On se ramène si $P(0) = \pm 1$. Soient $x_1 \dots x_n$ les racines de P

On a $\prod_{k=1}^{m} x_k = 1$ donc $\prod_{k=1}^{m} x_k^2 = 1$

IAG $\sum x_k^2 \geq n$

mais $\sum_{k=1}^{m} x_k^2 = \left(\sum_{k=1}^{m} x_k\right)^2 - 2\sum_{k \neq l} x_k x_l$

$= (-a_{m-1})^2 - 2a_{m-2} \geq n \to 3 \geq n$

absurde ?

III Polynômes à coeff rationnels

Rappel : P de deg 2 ou 3 P irréductible $\iff$ P sans racine

Ex Recherche de racines $P(X) = a_n X^n + \dots + a_1 X + a_0$ $a_i \in \mathbb{Z}$, $a_n \neq 0$

trouver les racines rationnelles de P

S/ On part de $P(p/q) = 0$, $p \wedge q = 1$, il vient

$p^n a_n + a_{n-1} q^{n-1} p + \dots + a_0 q^n = 0$

Gauss : $p \mid p^n a_n + \dots + a_0 q^n \to p \mid a_0 q^n \xrightarrow{\text{Gauss}} p \mid a_0$

de même $q \mid a_n$

Classique

Ex Soit $P \in \mathbb{Q}[X]$ irréductible et a une racine CMPLX de P Mq a est simple

S/ On a $P' \neq 0$, $\deg P' < \deg P$ (de $\mathbb{Z}/p\mathbb{Z}$ $(X^p - a)' = 0$)

donc $P \wedge P' = 1$ (car P irréd donc soit P' associé à P ou $P' \wedge P = 1$)

Algorithme d'Euclide, il existe $U, V \in \mathbb{Q}[X]$

$UP + VP' = 1$, $\underline{U(a)P(a)} + V(a)P'(a) = 1 \mid P'(a) \neq 0$

ASTUCE

X **Ex**: Soit $P \in \mathbb{Q}[X]$ avec $\deg P = 5$

Si P possède une racine double dans $\mathbb{C}$, il possède une racine rationnelle

S/ Avec ce qui précède P est irréductible

1er cas $\deg P \leq 3$: $P = QR$ OK

On se ramène à $\deg Q = 2$, $\deg R = 3$, Q et R sans racine dans $\mathbb{Q}$. Alors Q et R sont irréductibles

Soit a une racine double de P. Q et R irr, a est racine double ni de Q ni de R : $Q(a) = R(a) = 0$ ABS car $Q \wedge R = 1$

IV Irréductibilité de $\mathbb{Z}[X]$

Ex : Soient $a_1, \dots, a_m \in \mathbb{Z}$ 2 à 2 $\neq$; soit $P = 1 + \prod_{i=1}^{m} (X - a_i)^2$

M Q : P est irréductible

S/ Par l'absurde $P(X) = Q(X) R(X)$, $Q, R \in \mathbb{Z}[X]$
$\deg Q \geq 1$ $\deg R \geq 1$

il vient $Q(a_i) R(a_i) = 1$ $i = 1 \dots m$ $\deg Q \geq 1$, $\deg R \geq 1$

$Q(a_i) = R(a_i) = \varepsilon_i \in \{-1, 1\}$ $i = 1 \dots m$

UTILISATION DE $\mathbb{R}$!

$P = QR$ est valable dans $\mathbb{R}[x]$ ($\mathbb{C}$ si racines complexes)
> 0 sur $\mathbb{R}$

donc Q et R ne s'annulent pas donc sont de signe constant
par ex $Q > 0$ $R > 0$, $\varepsilon_i = 1$ $\forall i$

Par ex $\deg Q \leq n$: il vient $Q(a_i) - 1 = 0$, $i = 1 \dots n$

$$Q(X) - 1 = \lambda \prod_{i=1}^{m} (X - a_i)$$

$\lambda = 1$ (coef dom de P)

$$Q = 1 + \prod_{i=1}^{n} (X - a_i)$$

Idem avec R : $R = Q$, $P = Q^2$, ...

Ex. Soit $P = X^n + a_{n-1} X^{n-1} + \dots + a_0$; on suppose qu'il existe un nbre premier p tq $\begin{cases} p / a_i & i = 0 \dots n-1 \\ p^2 \nmid a_0 \end{cases}$

Alors P est irréductible dans $\mathbb{Z}[X]$

$S/$ ABS $P = QR$, $Q, R \in \mathbb{Z}[X]$ $Q(X) = X^r + b_{r-1}X^{r-1} + \dots$

$R(X) = X^s + b_{s-1}X^{s-1} + \dots$

On pose dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$X^n = (X^r + \overline{b_{r-1}}X^{r-1} + \dots)(X^s + \overline{c_{s-1}}X^{s-1} + \dots)$$

or par unicité de décomposition de X^n en irréductibles

les seuls facteurs unitaires de X^n sont les X^ℓ

donc $\overline{b_{r-1}} = \dots = \overline{b_0} = 0 = \overline{c_{s-1}} = \dots = \overline{c_0}$

or $a_0 = c_0 b_0$ absurde

donc $p^2 / \underbrace{c_0 b_0}_{= a_0}$

$\int_{-\infty}^{+\infty} f(t)\,dt$

Ex Mq $\left|\begin{array}{l} X^4+1 \text{ est irréductible dans } \mathbb{Q}[X] \\ \forall p \text{ premier, } X^4+1 \text{ est réductible dans } \mathbb{Z}/p\mathbb{Z} \end{array}\right.$

$S/$ Dans $\mathbb{R}[X]$; $X^4+1 = (X^2+1)^2 - 2X^2$ $\notin \mathbb{Q}[X]$ = unicité

$= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X - 1)$

$p=2$ $X^4+1 = (X^2+1)^2$

$p \geq 3$ Si $\overline{2} = a^2$ $\left(\left(\frac{2}{p}\right) = 1\right)$ il vient $X^4 + \overline{1} = (X^2+1)^2 - a^2X^2$

$= (X^2 - aX + 1)(X^2 + aX + 1)$

Sinon 2 n'est pas un carré mod p

$P(X) = (X^2 - \overline{1})^2 + \overline{2}X^2$

si -2 est un carré modulo p : $-\bar{2} = b^2$. $P(X) = (X - \bar{1})^2 - b^2$
ETC

Enfin si $\bar{2}$ ni $-\bar{2}$ ne sont pas des carrés mod p

$$\left.\begin{array}{l} 2^{\frac{p-1}{2}} = -1\,[p] \\ (-2)^{\frac{p-1}{2}} = -1\,[p] \end{array}\right) (-4)^{\frac{p-1}{2}} = 1\,[p] \quad : \; -\bar{4} = c^2$$

$$-\bar{1} = \left(\frac{c}{2}\right)^2 = d^2$$

on multiplie 2 fois par le sym de 2.

alors $X^4 + \bar{1} = X^4 - (-\bar{1}) = X^4 - d^2 = (X^2 - d)(X^2 + d)$ ...

~~Compléments sur les~~