Lycée CHATEAUBRIAND
Colas Bardavid

Chapitre 31

Polynômes II

$$\mathsf{L}_i := \frac{\displaystyle\prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (X - \alpha_j)}{\displaystyle\prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (\alpha_i - \alpha_j)}$$

Expression du i-ième polynôme de Lagrange

Dans ce chapitre, on poursuit l'étude des polynômes. En particulier, on va commencer l'étude arithmétique des polynômes et ébaucher une comparaison entre $\mathbb{Z}$ et $\mathbb{K}[X]$.

Lycée CHATEAUBRIAND
MPSI 3

Colas Bardavid

31
Polynômes II

plan de cours et principaux résultats

I. Division euclidienne et divisibilité

38.13 ★★★
38.14 ★★★

1) Inversibles

a) inversibles de $\mathbb{K}[X]$

Proposition 31.1

- *Les inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.*
- *Autrement dit, les inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0.*

b) polynômes associés

2) Division euclidienne

a) en pratique *via* des exemples
b) le résultat

Théorème 31.2

Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors,

$$\exists!(Q,R) \in \mathbb{K}[X]^2 : \begin{cases} A = BQ + R \\ \deg R < \deg B. \end{cases}$$

c) raffinements

3) Divisibilité

a) définition
b) propriétés

II. Relations coefficients-racines

38.23 ★★

1) Les fonctions symétriques

2) Les relations coefficients-racines

3) Cas importants

Proposition 31.3

On a

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.$$

III. Racines multiples

38.18 38.22 38.58

1) Multiplicité d'une racine

a) un rappel

b) définition et vocabulaire

c) une caractérisation

Proposition 31.4 Ⓣ

On a

$$\mathrm{m}_\alpha(P) = m \iff \exists Q \in \mathbb{K}[X] : \begin{cases} P = (X-\alpha)^m Q \\ Q(\alpha) \neq 0. \end{cases}$$

d) propriétés

2) Majoration du nombre de racines comptées avec multiplicités

a) un lemme de factorisation simultanée

b) le résultat

Proposition 31.5 Ⓣ

1) *Un polynôme de degré $n \geqslant 0$ possède au plus n racines comptées avec multiplicités.*
2) *Soit $P \in \mathbb{K}_n[X]$.*
   Si P possède au moins $n+1$ racines comptées avec multiplicités, alors $P = 0$.

3) Caractérisation par les dérivées supérieures

Proposition 31.6

Soit $P \in \mathbb{K}[X]$, soit $\alpha \in \mathbb{K}$ et soit $m \in \mathbb{N}^*$. Alors,

$$\alpha \text{ est racine de } P \text{ avec multiplicité } m \iff \begin{cases} P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0. \end{cases}$$

IV. PGCD et PPCM entre polynômes

38.2 38.28

1) Premières définitions

a) PGCD

b) relation de Bézout

2) Algorithme d'Euclide (étendu)

a) l'algorithme d'Euclide en pratique

b) théorème de Bézout

Théorème 31.7

Soient $A, B \in \mathbb{K}[X]$ et soit D un PGCD *de A et B. Alors, il existe $U, V \in \mathbb{K}[X]$ tels que*

$$AU + BV = D.$$

c) le PGCD ne dépend pas du corps de base

3) Propriétés des PGCD

a) relation fondamentale

Proposition 31.8

Soient $A, B \in \mathbb{K}[X]$ et soit D un PGCD de A et B.

1) *Alors, pour tout $P \in \mathbb{K}[X]$,*

$$\Big(P \mid A \quad et \quad P \mid B\Big) \iff P \mid D.$$

2) *Autrement dit, on a :* $\mathrm{Div}_{\mathbb{K}[X]}(A) \cap \mathrm{Div}_{\mathbb{K}[X]}(B) = \mathrm{Div}_{\mathbb{K}[X]}(D)$.

b) deux PGCD sont associés

c) le PGCD unitaire

4) Arithmétique des polynômes

a) polynômes premiers entre eux

b) lemme de Gauss

5) PGCD d'un nombre fini de polynômes

6) PPCM

V. Polynômes irréductibles

38.34
38.37
38.47

1) Polynômes irréductibles

a) définition

b) exemples

c) premières propriétés

2) Polynômes scindés

a) définition

b) exemples

3) Factorisation dans $\mathbb{C}[X]$

a) théorème de d'Alembert-Gauss

b) irréductible de $\mathbb{C}[X]$

c) décomposition en irréductibles dans $\mathbb{C}[X]$: idée

d) l'énoncé

4) Factorisation dans $\mathbb{R}[X]$

a) racines complexes de polynômes réels

Lemme 31.9

Soit $P \in \mathbb{R}[X]$ et soit $\alpha \in \mathbb{C}$. Alors,

1) $P(\alpha) = 0 \implies P(\overline{\alpha}) = 0$.

2) $\mathrm{m}_\alpha(P) = \mathrm{m}_{\overline{\alpha}}(P)$.

b) un lemme de factorisation réelle

Lemme 31.10

Soit $P \in \mathbb{R}[X]$ non nul, et soient $Q, R \in \mathbb{C}[X]$. Alors,

$$\left.\begin{array}{l} P = QR \\ Q \in \mathbb{R}[X] \end{array}\right\} \implies R \in \mathbb{R}[X].$$

c) irréductibles de $\mathbb{R}[X]$

Théorème 31.11

Les irréductibles de $\mathbb{R}[X]$ sont

- *les polynômes de degré 1*
- *les polynômes $aX^2 + bX + c$ tels que $a \neq 0$ et $a^2 - 4ac < 0$.*

d) décomposition en irréductibles dans $\mathbb{R}[X]$

ch 34
Polynômes II

- $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$

(Mieux : $\mathbb{K}$ peut être un corps qcq)

- $n \in \mathbb{N}$

Idée : On va tracer un parallèle entre $\mathbb{Z}$ et $\mathbb{K}[X]$

Selon cette comparaison : l'objet $\mathbb{K}[X]$ est ⊕ simple que $\mathbb{Z}$

I Division euclidienne et divisibilité

1) Inversibles

a) inversibles de $\mathbb{K}[X]$

On dit que $P \in \mathbb{K}[X]$ est inversible (dans $\mathbb{K}[X]$)
$\overset{\Delta}{\Leftrightarrow}$ $\exists Q \in \mathbb{K}[X] : PQ = 1$

Prop ⊤ P inversible $\iff$ P est constant et $\neq 0$
$\iff \deg(P) = 0$

Dl ($\Leftarrow$) Osq $\deg(P) = 0$ et on écrit $P = \lambda$ avec $\lambda \in \mathbb{K}^*$. On a $P \times \frac{1}{\lambda} = 1$

($\Rightarrow$) Osq P inv. Fixons donc $Q \in \mathbb{K}[X]$ tq

$PQ = 1$

- Déjà : on a $P \neq 0$, sinon on aurait $0 = 1$
- On passe à $\deg(\cdot)$ la relat° $(*)$: on obtient $\deg(P) + \deg(Q) = \deg(1) = 0$
- Ĉ $\deg(P), \deg(Q) \in \mathbb{N}$, on a nécessairement $\deg(P) = \deg(Q) = 0$ ∎

b) Polynômes associés.

Déf° : Soient $P, Q \in \mathbb{K}[X]$. On dit qu'ils sont associés $\overset{\Delta}{\text{ssi}}$ $\exists \lambda \in \mathbb{K}^* : P = \lambda Q$

(exo) : P et Q associés $\Leftrightarrow P \mid Q$ et $Q \mid P$

Rq :

- Si A anneau commutatif, x, y associés $\overset{\Delta}{\text{ssi}}$:

$\exists u \in U(A) : x = uy$

- On a alors $Div_A(x) = Div(y)$

2) Division euclidienne polynomiale

Th : Soient $A, B \in \mathbb{K}[X]$ tq $B \neq 0$

Alors $\exists ! \ (Q,R) \in \mathbb{K}[X] :$ $\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$

Pf On procède par (rec) sur $\deg(A)$

On note :

$$\mathcal{P}(d) : \text{“} \forall A \in \mathbb{K}_d[X], \exists (Q,R) \in \mathbb{K}[X]^2 : \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

- Si $d \in [\![0, \deg(B)-1]\!]$:

(**Rq** : si $\deg(B) = 0$: c'est ok

On écrit $B = \lambda$ avec $\lambda \in \mathbb{K}^*$

On a $\forall A, \ A = B\left(\frac{A}{\lambda}\right) + 0$)

Osq $\deg(B) \geq 1$

$d = 0, \ d = 1, \ \ldots, d = \deg(B) - 1,$: ok

Si $A \in \mathbb{K}_{\deg(B)-1}[X]$, on écrit $A = B \times 0 + A$

- **Hérédité :**

Soit $d \geq \deg(B) - 1$. Osq $\mathcal{P}(d)$

Soit $P \in \mathbb{K}_{d+1}[X]$ qu'on écrit

$$P = a_{d+1} X^{d+1} + \widetilde{P}$$

avec $a_{d+1} \in \mathbb{K}$ et avec $\widetilde{P} \in \mathbb{K}_d[X]$

On veut "tuer" $a_{d+1} X^{d+1}$ à l'aide de B.

On écrit $B = \sum_{k=0}^{m} b_k X^k$ avec $\begin{cases} m = \deg(B) \\ \forall k,\ b_k \in \mathbb{K} \\ b_n \neq 0 \end{cases}$

On a $d+1 \geq \deg(B) = m$

On considère $X^{(d+1)-m} \cdot B$; mieux $\frac{a_{d+1}}{b_m} X^{(d+1)-m} \cdot B$

On a $\frac{a_{d+1}}{b_m} X^{(d+1)-m} B = \frac{a_{d+1}}{b_m} X^{(d+1)-m} \left(b_m X^m + \dots + b_1 X + b_0 \right)$

$= a_{d+1} X^{d+1} + C$ avec $C \in \mathbb{K}_d[X]$

On a $A - \frac{a_{d+1}}{b_m} X^{(d+1)-m} B = \underbrace{\widetilde{P}}_{\in \mathbb{K}_d[X]} - \underbrace{C}_{\in \mathbb{K}_d[X]} \in \mathbb{K}_d[X]$

ĉ $\mathcal{P}(d)$ est Vraie, on écrit

$$\widetilde{P} - C = B \cdot \widetilde{Q} + \widetilde{R} \quad \text{avec} \quad \widetilde{Q}, \widetilde{R} \in \mathbb{K}[X]$$
$$\text{et} \quad \deg(\widetilde{R}) < \deg(B)$$

On a finalement

$$A = B\left(\widetilde{Q} + \frac{a_{d+1}}{b_m} X^{(d+1)-m}\right) + \widetilde{R} \text{ : c'est une DE}$$

(existen

Exemple :

$$\begin{array}{r|l}
\textcircled{A}\ 2X^4 + 3X^3 - X^2 + X - 1 & \textcircled{B}\ X^2 + 3X + 2 \\
\hline
2X^4 + 6X^3 + 4X^2 & 2X^2 - 3X + 4 \\
\hline
-3X^3 - 5X^2 + X - 1 & \textcircled{Q} \\
-3X^3 - 9X^2 - 6X & \\
\hline
4X^2 + 7X - 1 & \\
4X^2 + 12X + 8 & \\
\hline
-5X - 9 & \\
\textcircled{R} &
\end{array}$$

CCl : $2X^4 + 3X^3 - X^2 + X - 1 = (X^2 + 3X + 2)(2X^2 + 3X + 2) + (-5X - 9)$

c) raffinements *

On dispose d'une DE dans $\mathbb{Z}[X]$

Soient $A, B \in \mathbb{Z}[X]$ tq $B \neq 0$

Si ① Si B unitaire :

$$\exists (Q,R) \in \mathbb{Z}[X]^2 : \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases} (*)$$

② Notons $b_d \in \mathbb{Z}$ le coefficient dominant de B

Si $\forall k,\ b_d \mid \text{coeff}_k(P)$, on a $(*)$

3) Divisibilité

a) def°

Def : Soient $A, B \in \mathbb{K}[X]$ On dit que A divise B (dans $\mathbb{K}[X]$) ssi $\exists C \in \mathbb{K}[X] : B = AC$

On note alors $A \mid B$

• On note $\underset{\mathbb{K}[X]}{Div}(A)$ ou $div(A)$ l'ens défini par

$$\underset{\mathbb{K}[X]}{Div}(A) := \{P \in \mathbb{K}[X] \mid P \mid A\}$$

Exemples :

- $(X-1) \mid X(X-1)(X-2)$
- $X \mid P \iff P(0) = 0$

b) propriétés

- On a $Div_{\mathbb{K}[X]}(0) = \mathbb{K}[X]$
- On a $Div_{\mathbb{K}[X]}(1) = \mathbb{K}_0[X]$
- (T) $(A \mid B \text{ et } B \mid C) \Rightarrow A \mid C$
- (T) $\left.\begin{matrix} P \mid A \\ P \mid B \end{matrix}\right\} \Rightarrow \forall (U,V) \in \mathbb{K}[X]^2,\ P \mid AU + BV$
- (T) $A \mid B \Rightarrow A \mid BC$
- **Prop :** (T)

$$\left.\begin{matrix} A \mid B \\ B \neq 0 \end{matrix}\right\} \Rightarrow \deg(A) \leq \deg(B)$$

DI Fixons $C \in \mathbb{K}[X]$ tq $B = AC$

On a $\deg(B) = \deg(A) + \deg(C)$

Or $C \neq 0$ (sinon $B = 0$) Donc $\deg(C) \in \mathbb{N}$

Donc $\deg(C) \geq 0$ ∎

Rq : On peut définir $x|y$ dans un anneau commutatif

Prop (F) : Soit A anneau commutatif intègre

$(x|y \text{ et } y|x) \Leftrightarrow \exists u \in U(A) : y = ux$

D/ $\Leftarrow$ (F) ĉ $ux = y$, on a $x|y$

Fixons w tq $uw = 1$; on a $x = wy$

et donc $y|x$

$\Rightarrow$ Osq $x|y$ et $y|x$ Fixons $k, \ell \in A$

tq $\begin{cases} y = kx \\ x = \ell y \end{cases}$

D'où $y = k\ell y$ et donc

$(1 - k\ell)\, y = 0$

rq : $0 \in Div(x) \Rightarrow x = 0$ (AF)

Osq $x, y \neq 0$

Ĉ A intègre, on a $1 - k\ell = 0$ donc $k \in U(A)$ ∎

Rq: Ainsi, "$|$" est une relation d'ordre sur $\{P \in \mathbb{K}[X] \mid P \neq 0 \text{ et } P \text{ unitaire}\}$

II Relations coefficients - racines

Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$ qu'on écrit $P = a_0 + a_1 X + \dots + a_n X^n$

avec $\forall i,\ a_i \in \mathbb{K}$ et $a_n \neq 0$

Fixons $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ tq $P = a_n \prod_{i=1}^{n} (X - \alpha_i)$

But : mq les a_i s'expriment en f° des α_i

1) Les fonctions symétriques

On pose $\sigma_1 := \sum_{i=1}^{n} \alpha_i$

$$\sigma_2 := (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_1\alpha_n) + (\alpha_2\alpha_3 + \alpha_2\alpha_4 + \dots + \alpha_2\alpha_n) + \dots$$

ie on pose $\sigma_2 := \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j$

On pose $\sigma_3 := \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots$

$$\sigma_3 := \sum_{1\le i<j<k\le n} \alpha_i\alpha_j\alpha_k$$

etc ...

$$\sigma_{n-1} := \alpha_1 \cdots \alpha_{n-1}\alpha_n + \alpha_1 \cdots \alpha_{n-1}\alpha_n + \cdots + \alpha_1\alpha_2 \cdots \alpha_n$$

$$= \sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_{n-1}}$$

Enfin, on pose $\sigma_n = \alpha_1\alpha_2\cdots\alpha_n$

Rq : On pose

On a $\sigma_k = \sum_{I\subset[\![1,n]\!],\ |I|=k} \prod_{i\in I} \alpha_i$

Ce sont les fonctions symétriques élémentaires des racines.

Ex : Voici les f° symétriques élém de a, b, c, d

- $\sigma_1 = a+b+c+d$
- $\sigma_2 = ab + ac + ad + bc + bd + cd$
- $\sigma_3 = abc + abd + acd + bcd$
- $\sigma_4 = abcd$

2) Les relat° coeff - racines.

Prop : On a $\frac{a_{n-1}}{a_n} = -\sigma_1$ ie $\frac{a_{n-k}}{a_n} = (-1)^k \sigma_k$

$$\frac{a_{n-2}}{a_n} = \sigma_2$$
$$\vdots$$
$$\frac{a_0}{a_n} = (-1)^n \sigma_n$$

DI • On développe le produit $(X-\alpha_1)\dots(X-\alpha_n)$ et on constate que les termes en X^{n-1} sont :

$$-\alpha_1 X^{n-1} - \alpha_2 X^{n-1} - \dots - \alpha_n X^{n-1} = -\sigma_1 X^{n-1}$$

• De même pour les autres termes ∎

Rq : On écrit $I_k(n) := P_k(\llbracket 1, n \rrbracket)$

On a $I_k(n) =$ " $I_{k-1}(n-1) \cup \{n\}$ " $\sqcup I_k(n-1)$

On utilise cette relation pour faire DI par (rec) sur n ■

3) Cas importants

Prop (T) :

$$\begin{cases} \alpha_1 + \dots + \alpha_n = -\dfrac{a_{n-1}}{a_n} \\ \alpha_1 \alpha_2 \dots \alpha_n = (-1)^n \dfrac{a_0}{a_n} \end{cases}$$

4) F° Symétrique

Déf informelle : Une fonction $f(\alpha_1, \dots, \alpha_n)$ des racines est dite symétrique

$\overset{\Delta}{\text{ssi}}$ $\forall \sigma \in \mathfrak{S}_n$, $f(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) = f(\alpha_1, \dots, \alpha_n)$

Ex :

(*) $a^2 + b^2 + c^2 + d^2$

(*) $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d}$

(*) $\left(\frac{a}{b} + \frac{b}{a}\right) + \left(\frac{c}{d} + \frac{d}{c}\right) + \left(\frac{a}{c} + \frac{c}{a}\right) + \left(\frac{b}{c} + \frac{c}{b}\right) + \left(\frac{d}{b} + \frac{b}{d}\right) + \left(\frac{d}{a} + \frac{a}{d}\right)$

Prop (HP)

- Toute f° symétrique f est f° des σ_i
- Soit f symétrique ; alors $\exists g : f = g(\sigma_1, \sigma_2, \dots, \sigma_n)$

D/ non ∎

Ex : ⊛ $a^2+b^2+c^2+d^2 = (a+b+c+d)^2 - 2(ab+bc+\dots)$

$= \sigma_1^2 - 2\sigma_2$

⊛ $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} = (abc + abd + acd + bcd) \times \frac{1}{abcd}$

$= \frac{\sigma_3}{\sigma_4}$

⊛ Notons $f = \left(\frac{a}{b} + \frac{b}{a}\right) + \dots$

On a $(abcd) f = \left(a^2bcd + ab^2cd\right) + \dots$ = (AF)

III !! Racines multiples

1) Multiplicité d'une racine

a) rappel

Prop ① : α racine de $P \iff P(\alpha) = 0 \iff (x-\alpha) \mid P$

D1/ cf ch polynômes I

D2/ avec la DE

$\Leftarrow$ (AC)++ ok

$\Rightarrow$ Osq $P(\alpha) = 0$ On fait la DE de P par $(x-\alpha)$: on écrit

$$P = (x-\alpha) \cdot Q + R$$

avec $Q, R \in \mathbb{K}[X]$ et avec $\deg(R) < \deg(x-\alpha) = 1$

Fixons donc $\lambda \in \mathbb{K}$ tq $P = (x-\alpha)Q + \lambda$ (*)

En evaluant (*) en α, on obtient $P(\alpha) = \lambda$

Ĉ $P(\alpha) = 0$, on a $\lambda = 0$ et $P = (x-\alpha)Q$;

On a $(x-\alpha) \mid P$ ■

b) def° et vocabulaire

Def° : Soit $P \in \mathbb{K}[X]$ non nul.

Soit $\alpha \in \mathbb{K}$

On appelle **multiplicité de α en tant que racine de P**, et on note **$m_\alpha(P)$**, l'entier naturel défini par :

$$m_\alpha(P) := \max \left\{ k \in \mathbb{N} \mid (X-\alpha)^k \mid P \right\}$$

D/ • L'ens $\left\{ k \in \mathbb{N} \mid (X-\alpha)^k \mid P \right\} \neq \emptyset$ car contient 0

• Il est majoré car $\oplus$ $(X-\alpha)^k \mid P \Rightarrow$ $P \neq 0$

$k = \deg\left((X-\alpha)^k\right) \leq \deg(P)$ ▨

Convention : si $\alpha \in \mathbb{K}$, on pose

$$m_\alpha\left(0_{\mathbb{K}[X]}\right) = +\infty$$

Rq : il y a un gd parallelisme entre les $m_\alpha(\cdot)$ et les $v_p(\cdot)$ de $\mathbb{Z}$

Fait ⓣ

1) α racine de $P \iff m_\alpha(P) \geq 1$

2) α n'est pas racine de $P \iff m_\alpha(P) = 0$

Vocabulaire ⓣ

- α est racine simple de P ssi $m_\alpha(P) = 1$
- ——— double ——— $= 2$
- α est racine multiple de P ssi $m_\alpha(P) \geq 2$

Ex : Posons $P := X(X-1)^2(X-2)$

On a $m_0(P) = 1$
$m_1(P) = 2$
$m_2(P) = 1$

$\forall \alpha \in \mathbb{R} \setminus \{0,1,2\}$, $m_\alpha(P) = 0$

c) Une caractérisation

Prop : Soit $P \in \mathbb{K}[X]$, soit $m \in \mathbb{N}$.
Alors $m = m_\alpha(P) \iff \exists Q \in \mathbb{K}[X]$:

$$\begin{cases} P = (X-\alpha)^m \cdot Q \\ Q(\alpha) \neq 0 \end{cases}$$

D/ $\Rightarrow$ (T) On a $(X-\alpha)^m \mid P$

Fixons Q tq $P = (X-\alpha)^m Q$

On a $\underline{Q(\alpha) \neq 0}$. En effet, si $Q(\alpha)=0$,

On écrit $Q = (X-\alpha)R$; on a alors

$P = (X-\alpha)^{m+1} R$ (abs) avec m maximal

$\Leftarrow$ (T) Fixons Q tq $P = (X-\alpha)^m Q$

et $Q(\alpha) \neq 0$

Soit $k \in \mathbb{N}$ tq

$$(X-\alpha)^k \mid P$$

ORPA et osq $k > m$: on a $(X-\alpha)^k = (X-\alpha)^m X$

$$(X-\alpha)^{\underbrace{(k-m)}_{\geq 1}}$$

$\in \mathbb{K}[X]$

ĉ $(X-\alpha)^m (X-\alpha)^{k-m} \mid P = (X-\alpha)^m Q$

On a $(X-\alpha)^{k-m} \mid Q$; ĉ $k-m \geq 1$, on a

$Q(\alpha) = 0$: (Abs) ∎

d) Propriétés

Prop ⓣ : 1) $m_\alpha(PQ) = m_\alpha(P) + m_\alpha(Q)$

2) $m_\alpha(P+Q) \geq \min\left(m_\alpha(P); m_\alpha(Q)\right)$

D/ 1) On note $m_P := m_\alpha(P)$

$m_Q := m_\alpha(Q)$

et on écrit $P = (X-\alpha)^{m_P} \cdot R$

$Q = (X-\alpha)^{m_Q} \cdot S$

avec $R, S \in \mathbb{K}[X]$ tq $R(\alpha) \neq 0$ et $S(\alpha) \neq 0$

On a $PQ = (X-\alpha)^{m_P+m_Q} \underbrace{(RS)}_{T :=}$

et $T(\alpha) = \underbrace{R(\alpha)}_{\neq 0} \underbrace{\cdot S(\alpha)}_{\neq 0} \neq 0$

D'après c) On a $m_\alpha(PQ) = m_P + m_Q$ ■ 1)

2) cf la même démo pour $v_p(\cdot)$: ok ■

2) Majoration de # racines avec multiplicité

a) un lemme de factorisation simultanée

Lemme : Soit $P \in \mathbb{K}[X]$ non nul.
Soient $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ 2 à 2 distincts

On note (1) $m_i := m_{\alpha_i}(P) \in \mathbb{N}$

Alors : $\exists\, Q \in \mathbb{K}[X]$: $P = (X-\alpha_1)^{m_1} \cdots (X-\alpha_r)^{m_r} Q$

D/ (rec) sur r

$r = 1$ ok

Hérédité : Soit $r \geq 1$ Osq HR_r

On écrit $P = \prod_{i=1}^{r} (X-\alpha_i)^{m_i} \cdot Q$

But : écrire $Q = (X-\alpha_{r+1})^{m_{r+1}} \cdot R$

On a $m_{\alpha_{r+1}}(P) = \sum_{i=1}^{r} m_{\alpha_{r+1}}\left((X-\alpha_i)^{m_i}\right) + m_{\alpha_{r+1}}(Q)$

Or, $\forall i \in [\![1, r]\!]$, $m_{\alpha_{r+1}}\left((X-\alpha_i)^{m_i}\right) = 0$

car si $i \in [\![1, r]\!]$, $(\alpha_{r+1} - \alpha_i)^{m_i} \neq 0$

car les α_k sont 2 à 2 distincts.

Bilan : $m_{\alpha_{r+1}}(P) = m_{\alpha_{r+1}}(Q) = m_{r+1}$ notation

On écrit $Q = (X - \alpha_{r+1})^{m_{r+1}} \cdot R$ avec $R \in \mathbb{K}[X]$

On a bien ce qu'on voulait ∎

Concrètement :

Si $m_1(P) = 2$ et $n_0(P) = 3$ et $m_4(P) = 2$

On peut écrire $P = X^3(X-1)^2(X-4)^2 Q$

avec $Q \in \mathbb{R}[X]$

rq* : Si $P \in \mathbb{Z}[X]$, on a $Q \in \mathbb{Z}[X]$

b) Le résultat

Prop : 1) Un polynôme de degré $n \geq 1$ possède au plus n racines comptées avec multiplicités

2) **Ie :** Soient $\alpha_1, \dots, \alpha_r$ des racines de P 2 à 2 $\neq$ tes

Alors, on a $\sum_{i=1}^{r} m_{\alpha_i}(P) \leq n$

3) Si $P \in \mathbb{K}_n[X]$ possède au moins $(n+1)$ racines comptées avec multiplicités, alors $P = 0$.

D1 2)⊕ On écrit $P = \prod_{i=1}^{r} (X-\alpha_i)^{m_{\alpha_i}(P)} \cdot Q$

et on passe à deg(·) :

on a $\deg(P) = \sum_{i=1}^{r} \deg\left((X-\alpha_i)^{m_{\alpha_i}(P)}\right) + \deg(Q)$

$m_{\alpha_i}(P)$

Ĉ $P \neq 0$, on a $Q \neq 0$ et donc $\deg(Q) \geq 0$

■ 2)

4), 3) ok ■

3)!! Caractérisat° par les dérivées supérieures

Prop : Soit $P \in \mathbb{K}[X]$, soit $\alpha \in \mathbb{K}$, soit $m \in \mathbb{N}$

Alors : 1) α est racine de P avec multiplicité m

$$\iff \begin{cases} P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0 \end{cases}$$

2) $P(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$

$$\Rightarrow \quad m_\alpha(P) \geq m .$$

D/ 1)

Lemme : Soit α racine de P.
Alors $m_\alpha(P') = m_\alpha(P) - 1$

D/ On écrit $P = (X-\alpha)^m \cdot Q$ avec $\begin{cases} m := m_\alpha(P) \\ Q \in \mathbb{K}[X] \\ Q(\alpha) \neq 0 \end{cases}$

Rq : On a $m \geq 1$

On a $P' = m(X-\alpha)^{m-1} \cdot Q + (X-\alpha)^m Q'$

$= (X-\alpha)^{m-1} \underbrace{\left[mQ + (X-\alpha)Q' \right]}_{R}$

On a $R(\alpha) = \underbrace{m}_{\geq 1} \underbrace{Q(\alpha)}_{\neq 0} \neq 0$

On a DALC : $m_\alpha(P') = m - 1$ ■

puis (rec) sur m ou sur $\deg(P)$: (AF)

D/2 💡 On utilise FT polynomiale

1) (⇒) Osq $m_\alpha(P) = m$ on écrit

$P = (X-\alpha)^m Q$ avec $Q(\alpha) \neq 0$

On écrit $Q = \sum_{k=0}^{d} a_k (X-\alpha)^k$

où $d := \deg(Q)$ et avec $\forall k,\ a_k \in \mathbb{K}$

Rappel : $\left(1, (X-\alpha), (X-\alpha)^2, \dots, (X-\alpha)^d\right)$

base de $\mathbb{K}_d[X]$

2) Algo d'Euclide étendu

a) En pratique

C'est le même

Posons $A := X^4 + X^3 + 1$ et $B := X^2 + X + 1$

Calculons un PGCD de A et B ainsi qu'une relat° de Bezout

(AF)

A	B	R	Q	U	V
$X^4 + X^3 + 1$	$X^2 + X + 1$	$X + 2$	$X^2 - 1$		
$X^2 + X + 1$	$X + 2$	3	$X - 1$		
$X + 2$	3	0	$\frac{X+2}{3}$		

Ainsi :

- 3 est un PGCD de $X^4 + X^3 + 1$ et de $X^2 + X + 1$
- On a $(X^4 + X^3 + 1)(1 - X) + (X^2 + X + 1)(X^3 - X^2 - X + 2)$

$= 3$

b) Théorème de Bézout

Thm : Soient $A, B \in \mathbb{K}[X]$

Soit D un PGCD de A et B

Alors : $\exists (U,V) \in \mathbb{K}[X]^2 : AU + BV = D$

Lemme : Deux PGCD sont associés

D/ ② Soient $D_1, D_2 \in \mathbb{K}[X]$ des PGCD de A et B. Mq $\exists \lambda \in \mathbb{K}^* : D_1 = \lambda D_2$

- Si $A = B = 0$, ok
- Osq $A \neq 0$.
- Notons c_1 le coeff. dominant de D_1.

(rq : $D_1 \neq 0$ car $A \neq 0$ et $D_1 | A$)

C_2 ——————————— D_2.

- Ocsd $D := C_2 D_1 - C_1 D_2$

On a une chute de degré **échec** ∎

D/ lemme

- Grâce à l'algo d'Euclide, fixons $\Delta, U, V \in \mathbb{K}[X]$ tq
  1) $AU+BV = \Delta$
  2) Δ est un PGCD de A et B

- Soit D un PGCD de A et B
- On a $D \mid A$ et $D \mid B$, donc $D \mid AU+BV$ ie $D \mid \Delta$
- Fixons donc $C \in \mathbb{K}[X]$ tq $\Delta = CD$
  On a alors $\deg(A) = \deg(C) + \deg(D)$
  On a $\deg D = \deg \Delta$.
  Donc C est un polynôme cst de degré 0.
  Ainsi, on peut l'écrire $C = \lambda$ avec $\lambda \in \mathbb{K}^*$.
- Bilan : D est associé à Δ
- Ĉ la relation d'association est une relᵒ d'équivalence : on conclut ▨

D/ thm

- Déjà, grâce à Euclide, on se donne U, V, Δ tq $\begin{cases} AU+BV = \Delta \\ \Delta \text{ PGCD} \end{cases}$

• Soit D PGCD ; on l'écrit $D = \lambda\Delta$ avec $\lambda \in \mathbb{K}^*$ et on conclut ▨.

c)* ! Le PGCD ne dépend pas du corps de base

Rq : On a le fait pour $\mathbb{R} \subset \mathbb{C}$, mais ceci marche pour $\mathbb{K} \subset \mathbb{L}$ corps qcq.

Rq ! : Posons $P := X^2+1 \in \mathbb{R}[X]$

Fait : $\mathrm{Div}_{\mathbb{R}[X]}(X^2+1) = \text{"}\{1, X^2+1\}\text{"}$

$= \{\lambda ; \lambda \in \mathbb{K}^*\}$

$\cup \{\mu(X^2+1) ; \mu \in \mathbb{K}^*\}$

Mais $X-i,\ X+i \in \mathrm{Div}_{\mathbb{C}[X]}(X^2+1)$

($\mathrm{Div}_{\mathbb{C}[X]}(X^2+1) = \text{"}\{1, X^2+1, X \pm i, \}\text{"}$)

Ainsi : À priori ; si $A, B \in \mathbb{R}[X]$, on a

$\mathrm{Div}_{\mathbb{R}[X]}(A) \cap \mathrm{Div}_{\mathbb{R}[X]}(B)$ qui va être $\neq^t$

de $\mathrm{Div}_{\mathbb{C}[X]}(A) \cap \mathrm{Div}_{\mathbb{C}[X]}(B)$.

Déf : Soient $A, B \in \mathbb{K}[X]$.

Le PGCD de A et B, noté $A \wedge B$ est l'unique polynôme unitaire D qui est un PGCD de A et de B.

DI : Si D_1, D_2 sont des PGCD unitaires de A et de B, alors ils sont associés, ils sont égaux ■

(AC)

Rq : Plus précisément, on peut le noter $A \wedge^{[\mathbb{K}]} B$

Proposition Soient $A, B \in \mathbb{R}[X]$

$$A \wedge^{[\mathbb{R}]} B = A \wedge^{[\mathbb{C}]} B$$

D⁺ / Classiq. Le PGCD se calcule avec des divisions euclidiennes.

Mais si : $A, B \in \mathbb{R}[X]$ (avec $B \neq 0$)

La DE de A par B dans $\mathbb{C}[X]$ est la même que celle dans $\mathbb{R}[X]$.

$A, B \in \mathbb{R}[X]$ ⟵ $\exists!\,(Q,R) \in \mathbb{R}[X]^2 : (\dots)$

$A, B \in \mathbb{C}[X] \supset \mathbb{R}[X]$ (DE) ⟶ $\exists!\,(Q,R) \in \mathbb{C}[X]^2 : (\dots)$

Ce sont le $\overline{m}$ par unicité de la DE dans $\mathbb{C}[X]$.

■

D/ On note $D_{\mathbb{R}} := A \wedge^{[\mathbb{R}]} B$

$D_{\mathbb{C}} := A \wedge^{[\mathbb{C}]} B$

On se donne $(\dots)$ AU_B $AU_{\mathbb{R}} + BV_{\mathbb{R}} = D_{\mathbb{R}}$

$AU_{\mathbb{C}} + BV_{\mathbb{C}} = D_{\mathbb{C}}$

- On a $D_{\mathbb{R}} \mid A$ dans $\mathbb{R}[X]$; donc
  à fortiori
  $D_{\mathbb{R}} \mid A$ dans $\mathbb{C}[X]$;

  via $\overline{m}$, $D_{\mathbb{R}} \mid B$ dans $\mathbb{C}[X]$

  Donc $D_{\mathbb{R}} \mid AU_{\mathbb{C}} + BV_{\mathbb{C}} = D_{\mathbb{C}}$

- On a $D_{\mathbb{C}} \mid A$ et $D_{\mathbb{C}} \mid B$

  Donc $D_{\mathbb{C}} \mid \underbrace{AU_{\mathbb{R}}}_{\text{"}\mathbb{C}[X]\text{"}} + \underbrace{RV_{\mathbb{R}}}_{\in \mathbb{C}[X]} = D_{\mathbb{R}}$

- Ccl : $D_{\mathbb{R}}$ et $D_{\mathbb{C}}$ sont associés dans $\mathbb{C}$, ĉ ils sont unitaires, ils sont égaux. ■

Rq (T) : Unicité de la DE dans $\mathbb{K}[X]$

Soient (Q_1, R_1), (Q_2, R_2) tq

$A = BQ_1 + R_1$ et $A = BQ_2 + R_2$

avec $\deg(R_1), \deg(R_2) < \deg(B)$

Mq $Q_1 = Q_2$ et $R_1 = R_2$

On a $B(Q_2 - Q_1) = R_1 - R_2$

Donc $\deg(B) + \deg(Q_2 - Q_1) = \deg(R_1 - R_2)$

Donc (⋆) : $\deg(Q_2 - Q_1) = \underbrace{\deg(R_1 - R_2)}_{<\deg(B)} - \deg(B)$

< 0

Donc $Q_2 = Q_1$; de là : $R_1 = R_2$ ∎

3) Propriétés des PGCD

a) Relat° fale

Prop : Soient $A, B \in \mathbb{K}[X]$

Sort D un PGCD de A et B

1) Alors (T) $P|A$ et $P|B \iff P|D$

2) ie $Div(A) \cap Div(B) = Div(D)$

D/ " Avec Bézout " (AF) * ■

b) Arithmétique des polynômes

a) polynômes premiers entre eux

Déf (T) : A et B sont premiers entre eux $\overset{\Delta}{ss}$ $A \wedge B = 1$

b) Lemme de Gauss

Prop (T) :

$$\left.\begin{array}{l} A|BC \\ A \wedge B = 1 \end{array}\right\} \Rightarrow A|C$$

D/ ok ■

c) Autres conséquences

Prop $\left.\begin{array}{l} A \mid P \\ B \mid P \\ A \wedge B = 1 \end{array}\right\} \Rightarrow \quad AB \mid P$

D/ [Simon] □

Prop : $\left.\begin{array}{l} A \wedge B = 1 \\ B \wedge P = 1 \end{array}\right\} \Rightarrow AB \wedge P = 1$

D/ $1 = AU + PV \quad ; \quad 1 = BW + PT$

Donc $1 = (AU + PV)(BW + PT) =$

$AB\,UW + P(\text{qqch})$ □

Corollaire

$$A \wedge B \Rightarrow \forall k, \ell, \quad A^k \wedge B^\ell = 1$$

d) Exemples

Soient $\lambda, \mu \in \mathbb{K}$ tq $\lambda \neq \mu$

Alors $\underline{R^x}$

$$\boxed{(X-\lambda) \wedge (X-\mu) = 1}$$

DL : $(X-\mu) - (X-\lambda) = \lambda - \mu$

: Donc $\frac{1}{\lambda-\mu}(X-\mu) + \frac{(-1)}{\lambda-\mu}(X-\lambda) = 1$

• Ainsi : on a une relat° de Bézout "égale à 1" entre $(X-\lambda)$ et $(X-\mu)$: ils sont premiers entre eux. ■

• Ainsi : (R^x) $\boxed{\forall k, p \in \mathbb{N}, (X-\lambda)^k \wedge (X-\mu)^p = 1}$

5) PGCD d'un nb fini de polynômes

Def° (T) : On dit que $\underline{D}$ est un PGCD de $P_1, \dots, P_N$ ssi $\forall i$, $D | P_i$ et D est de degré maximal

Lemme : $\left[\left[\left(\left(P_1 \wedge P_2\right) \wedge P_3\right) \wedge P_4\right) \cdots\right] \wedge P_N$

est un PGCD

Prop : 1) Tout les PGCD sont associés entre eux.

2) Si D est un PGCD de $P_1, \dots, P_N$: alors,
$\exists\ U_1, \dots, U_N \in \mathbb{K}[X] : U_1 P_1 + \dots + U_N P_N = D$

3) On note $P_1 \wedge P_2 \wedge \dots \wedge P_N$ l'unique PGCD unitaire

D/ ok ∎

Rq : (idée) Tout se passe parfaitement

Prop : 1) $(PA) \wedge (PB) = P(A \wedge B)$

2) $(AP_1) \wedge (AP_2) \wedge \dots \wedge (AP_N) = A(P_1 \wedge \dots \wedge P_N)$

D/ (exo) ∎

Rq : $\forall i,\ Q \mid P_i \iff Q \mid P_1 \wedge \dots \wedge P_N$

- Ie $\bigcap_{i=1}^{N} \mathrm{Div}(P_i) = \mathrm{Div}\left(\underbrace{P_1 \wedge \dots \wedge P_N}_{\bigwedge_{i=1}^{N} P_i}\right)$

Def° (!!)

1) On dit que les P_i sont premiers entre eux dans leurs ensemble $\overset{\Delta}{\underset{ssi}{}}$ $P_1 \wedge \dots \wedge P_N = 1$

2) On dit qu'ils sont 2 à 2 premiers entre eux

$\overset{\Delta}{\underset{ssi}{}}$ $\forall i \neq j$, $P_i \wedge P_j = 1$

Rq : 2) $\Rightarrow$ 1)

6) PPCM

Pareil que pour $\mathbb{Z}$

Prop : $(A \wedge B) \times \underbrace{(A \vee B)}_{\text{PPCM unitaire}}$ et ~~$=$~~ $A \times B$ sont associés

V) Polynômes irréductibles

1) Polynômes irréductibles

a) Définition

Déf : Soit $P \in \mathbb{K}[X]$ non nul et non inversible

ie de degré ≥ 1

On dit que P est irréductible (dans $\mathbb{K}[X]$)

$\overset{\Delta}{\text{ssi}}$ " P n'est pas factorisable dans $\mathbb{K}[X]$ de façon non triviale ".

ie $\overset{\Delta}{\text{ssi}}$ $\forall Q, R \in \mathbb{K}[X]$, $P = QR \Rightarrow$ (Q inversible ou R inversible)

ie $\overset{\Delta}{\text{ssi}}$ $\forall Q, R \in \mathbb{K}[X]$, $P = QR \Rightarrow$ (Q cste ou R cste)

b) Exemples

Rq : Soit $P \in \mathbb{K}[X]$ de degré ≥ 1.

Alors : "P réductible" ie P non irréductible $\Leftrightarrow$

$$\exists\, Q, R \in \mathbb{K}[X] : \begin{cases} P = QR \\ \deg Q \geq 1 \\ \deg R \geq 1 \end{cases}$$

Fait 1 : X^2+1 est irréductible dans $\mathbb{R}[X]$

D/ ORPA, osq X^2+1 n'est pas irréductible

et on fixe $Q, R \in \mathbb{R}[X]$ tq $X^2+1 = Q \times R$

avec $\begin{cases} \deg(Q) \geq 1 \\ \deg(R) \geq 1 \end{cases}$

- Ĉ $\deg(Q) + \deg(R) = 2$, on a $\deg(P) = \deg(R) = 1$
- Or

Lemme (R^*) :

$$\left.\begin{array}{l} P \in \mathbb{K}[X] \\ \deg(P) = 1 \end{array}\right\} \Rightarrow P \text{ possède une racine dans } \mathbb{K}$$

D/ (T) $P = aX+b$ $(a, b \in \mathbb{K})$

$\alpha := -\frac{b}{a} \in \mathbb{K}$ racine de P ∎

- Fixons donc $\alpha \in \mathbb{R}$ une racine de Q.
- Donc α racine de X^2+1
- Donc $\boxed{\alpha^2 = -1}$ (Abs) car $\forall t \in \mathbb{R}, t^2 \geq 0$

∎

Fait 2 : X^2+1 n'est pas irréductible dans $\mathbb{C}[X]$

D/ On a $X^2+1 = (X-i)(X+i)$ ∎

c) Premières propriétés

Fait : P (irr) $\Rightarrow \forall \lambda \in \mathbb{K}^*, \lambda P$ (irr)

D/ ok ∎

Fait : $\deg(P) = 1 \Rightarrow P$ (i)

D/ (T) $P = QR \longrightarrow \deg Q + \deg R = 1$

$\deg Q = 0$ ou $\deg R = 0$ ∎

Corollaire :

Les $(X-\lambda)$ pour $\lambda \in \mathbb{K}$ forment une famille de polynômes (irr) 2 à 2 premiers entre eux

Fait : Soit $P \in \mathbb{K}[X]$ de degré 2. Alors :

P (irr) (dans $\mathbb{K}[X]$) $\Longleftrightarrow$ P n'a pas de racine dans $\mathbb{K}$

D/ (AF) ∎

Rq : $\deg P \geq 2$, P possède une racine dans $\mathbb{K}$ $\Big\} \Rightarrow P$ n'est pas (irr)

Corollaire : Soient $a, b \in \mathbb{R}$. On pose

$$P := X^2 + aX + b$$

Alors $a^2 - 4b < 0 \Rightarrow P$ (irr) dans $\mathbb{R}[X]$

D/ (ok) ∎

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

2) Polynômes scindés

a) défo

Déf : Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$

On dit que P est scindé dans $\mathbb{K}$ $\overset{\Delta}{\text{ssi}}$

$$\exists\, \lambda \in \mathbb{K}^*,\ \exists\, \alpha_1, \dots, \alpha_n \in \mathbb{K} : \quad P = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

Rq : ie $\overset{\Delta}{\text{ssi}}$ " toutes ses racines dans $\mathbb{K}$ "

Ex :
- $X(X-1)(X-2)$ est scindé dans $\mathbb{R}$
- $X^2 + X + 1$ ne l'est pas

- Mais, ĉ $X^2+X+1 = (X-j)(X-\bar{j})$
  il est scindé dans $\mathbb{C}$
- $X(X-1)^2(X-2)$ est scindé dans $\mathbb{R}$
- Mieux : $X(X-1)(X-2)$ est scindé à racines simples

3) Factorisation dans $\mathbb{C}[X]$

a) thm de d'Alembert-Gauss

Thm !! Tout polynôme $P \in \mathbb{C}[X]$ de degré ≥ 1 possède une racine dans $\mathbb{C}$

Rq : On dit que $\mathbb{C}$ est algebriquement clos

D/ non ∎

b) irréductibles de $\mathbb{C}[X]$

Prop : Les irréductibles unitaires de $\mathbb{C}$ sont les $(X-\lambda)$ où $\lambda \in \mathbb{C}$

D/ ⊛ $\deg P \geq 2 \longrightarrow$ on fixe $\alpha \in \mathbb{C}$ tq $P(\alpha)=0$

$(X-\alpha) \mid P \longrightarrow P$ non (irr) ∎

c) décomposition dans $\mathbb{C}[X]$

$\mathbb{Z}$	$\mathbb{C}[X]$
$n \neq 0$	$P \neq 0$
$U(\mathbb{Z}) = \{\pm 1\}$	$U(\mathbb{C}[X]) = \mathbb{K}^*$
$p \in \mathcal{P}$	$X - \alpha$
$v_p(n)$	$m_\alpha(P)$
$\lvert n \rvert$	$\deg(P)$
$n = \pm 1 \prod_{p \in \mathcal{P}} p^{v_p(n)}$	$P = \lambda \prod_{i=1}^{N} (X - \alpha_i)^{m_i}$

d) énoncé

Thm : 1) Soit $P \in \mathbb{C}[X]$ non nul. Alors P s'écrit

(R^X)
$$P = \lambda \prod_{i=1}^{N} (X - \alpha_i)^{m_i}$$

avec $\lambda \in \mathbb{K}^*$, avec $\forall i$, $\alpha_i \in \mathbb{C}$, avec $\forall i$, $m_i \in \mathbb{N}^*$

et où les α_i sont 2 à 2 distincts

2) Cette écriture est unique à l'ordre près des facteurs.

Idée de D/

existence : (rec) (Hérédité grâce à d'Alembert-Gauss)

unicité : • déjà : $\{\alpha_i ; i \in [\![1, N]\!]\} = Z_{\mathbb{C}}(P)$

• Puis : $m_{\alpha_i}(P) = \sum_{i=1}^{N} m_{\alpha_{i_0}}\left((X-\alpha_i)^{m_i}\right)$

$= \begin{cases} 0 & \text{si } i \neq i_0 \\ m_{i_0} & \text{si } i = i_0 \end{cases}$

• Enfin : $\lambda = \text{coeff}_{\text{dom}}(P)$

Rq : Ainsi : $P = \text{coeff}_{\text{dom}}(P) \prod_{\alpha \in Z_{\mathbb{C}}(P)} (X-\alpha)^{m_\alpha(P)}$

e) applicat° au calcul du PGCD

Ex : $P := X^2(X-1)^3(X-2)^2(X-5)$

$Q := (X+1)X(X-1)^2(X-5)$

On a $\text{PGCD}(P, Q) = X(X-1)^2(X-5)$

4) Factorisation dans $\mathbb{R}[X]$

a) racines complexes de polynômes réels

Lemme : Soit $P \in \mathbb{R}[X]$. Soit $\alpha \in \mathbb{C}$. Alors

1) $P(\alpha) = 0 \implies P(\overline{\alpha}) = 0$

2) $m_{\alpha}(P) = m_{\overline{\alpha}}(P)$

D/ 1) ⚓ !! Ⓣ On écrit $P = \sum_{k=0}^{n} a_k X^k$ avec $a_k \in \mathbb{R}$

$$P(\alpha) = 0 \longrightarrow \sum_{k=0}^{n} a_k \alpha^k = \overline{0}$$

$$\longrightarrow \sum_{k=0}^{n} \overline{a_k}\, \overline{\alpha}^k = 0 \quad (\overline{a_k} = a_k)$$

$$\longrightarrow P(\overline{\alpha}) = 0$$

Rq : $\{ \varphi : \mathbb{C} \longrightarrow \mathbb{C} \mid \varphi$ morphisme d'anneaux, $\forall x \in \mathbb{R}, \varphi(x) = x \}$

φ : groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$ noté $Gal(\mathbb{C}|\mathbb{R})$

$$\{ z \longmapsto \overline{z}, Id_{\mathbb{C}} \} \cong \mathbb{Z}/2\mathbb{Z} \cong (\{\pm 1\}, \times) = \mathbb{U}_2$$

2) D¹/ Ocsd $\mathcal{A} := \{k \in \mathbb{N} \mid (X-\alpha)^k \mid P\}$

$\mathcal{B} := \{\text{——} \; (X-\overline{\alpha})^k \mid P\}$

On a $\mathcal{A} = \mathcal{B}$.

mq $\mathcal{A} = \mathcal{B}$:

Soit k tq $(X-\alpha)^k \mid P$; fixons

$Q \in \mathbb{C}[X]$ tq $P = (X-\alpha)^k \cdot Q$.

On a $\overline{P} = \overline{(X-\alpha)^k \cdot Q}$

(Rq : le conjugué $\overline{R}$ de $R \in \mathbb{C}[X]$ est le polynôme dont les coeff sont les conjugués de ceux de R. On a $\overline{R+S} = \overline{R} + \overline{S}$ $\overline{RS} = \overline{R} \times \overline{S}$)

ie : $P = (X-\overline{\alpha})^k \overline{Q}$

On a $(X-\overline{\alpha})^k \mid P$ ie $k \in \mathcal{B}$.

- De même $\mathcal{B} \subset \mathcal{A}$
- Donc $\max \mathcal{A} = \max \mathcal{B}$

$m_\alpha(P)$ $m_{\overline{\alpha}}(P)$

D²/ On utilise la caractérisation par les dérivées

Si $P(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$

et $P^{(m)}(\alpha) \neq 0$

On a donc $\overline{P(\alpha)} = \dots = \overline{P^{(m-1)}(\alpha)} = \overline{0}$

$\overline{P^{(m)}(\alpha)} \neq \overline{0}$

Ie $\begin{cases} P(\overline{\alpha}) = \dots = P^{(m-1)}(\overline{\alpha}) = 0 \\ P^{(m)}(\overline{\alpha}) \neq 0 \end{cases}$ ■

Rq : Posons $P := 4X^4 - 3X^3 + 2X^2 - X + 1$

- Déterminer $Z_{\mathbb{C}}(P)$ est hyper dur.

  (si $\deg P \geq 5$, il est impossible en gal de déterminer $Z_{\mathbb{C}}(P)$)

- Ex : Resoudre $\boxed{X^5 = X+1}$

- En revanche: il est très facile de savoir si P possède des racines doubles/multiples.

Pl Soit α une racine multiple de P

Alors $P(\alpha) = P'(\alpha) = 0$

Donc $(X-\alpha) \mid P$ et $(X-\alpha) \mid P'$

Donc $(X-\alpha) \mid P \wedge P'$ donc $\deg(P \wedge P') \geq 1$

ie $\boxed{P \wedge P' \neq 1}$

- Réciproque : si $P \wedge P' \neq 1$, on a $\deg(P \wedge P') \geq 1$

D'après d'Alembert-Gauss, fixons $\alpha \in \mathbb{C}$ tq

$(P \wedge P')(\alpha) = \alpha$ ie tq $(X-\alpha) \mid P \wedge P'$

On a alors $(X-\alpha) \mid P$ et $(X-\alpha) \mid P'$

et donc $P(\alpha) = P'(\alpha) = 0$ ∎

Calcul du PGCD :

A	B	R	Q
$4X^4-3X^3+2X^2-X+1$	$16X^3-9X^2+4X-1$	$\frac{37}{64}X^2-\frac{9}{16}X+\frac{61}{64}$	$\frac{X}{4}-\frac{3}{64}$
$16X^3-9X^2+4X-1$	$37X^2-9X+61$		
etc...			

Astuce : $PGCD(P, \lambda Q) = PGCD(P, Q)$

(⚠ on perd toutefois les relation de Bézout)

b) Factorisation réelle

Prop : (T)

$$\left.\begin{array}{l} P = Q \times R \\ P \in \mathbb{R}[X] \\ R \in \mathbb{R}[X] \end{array}\right\} \Rightarrow Q \in \mathbb{R}[X]$$

$P \neq 0$

D1/ $\overline{P} = \overline{Q} \times \overline{R} \longrightarrow P = \overline{Q}\,\overline{R}$

Donc $\overline{Q}R = QR$ (W Nils)

$\downarrow$

$(Q - \overline{Q})R = 0$

On a $R \neq 0$ (sinon) $\rightarrow$ $Q - \overline{Q} = 0$

$\mathbb{C}[X]$ intègre

$\downarrow$

$Q = \overline{Q} \longrightarrow Q \in \mathbb{R}[X]$

D2/ On écrit $\boxed{Q = A + iB \quad \text{avec} \quad A, B \in \mathbb{R}[X]}$

On a $P = QR = AR + iBR$

On a $iBR = 0$ car $P \in \mathbb{R}[X]$

Donc, $\forall R \neq 0$, $B = 0$, donc $Q \in \mathbb{R}[X]$ ■

D 3/ On note $A := \mathbb{R} \setminus Z_{\mathbb{R}}(?)$

Ĉ $R \neq 0$: $Z_{\mathbb{R}}(R)$ est fini ; donc A infini.

Soit $t \in \mathcal{A}$. On a $P(t) = Q(t) \cdot R(t)$

Donc $Q(t) = \dfrac{P(t)}{R(t)} \in \mathbb{R}$

ccl : $\boxed{\forall t \in \mathcal{A},\ Q(t) \in \mathbb{R}}$

On écrit $Q = A + iB$ avec (...)

On a donc : $\forall t \in \mathcal{A}$, $Q(t) = \underbrace{A(t)}_{\in \mathbb{R}} + i\underbrace{B(t)}_{\in \mathbb{R}}$

Ĉ $\forall t \in \mathbb{R}$, $B(t) = \mathrm{Im}(Q(t)) \in \mathbb{R}$

On a $\forall t \in \mathcal{A}$, $B(t) = 0$ (CRN) $\longrightarrow B = 0$ ∎

D 4/ $P = QR$ $(R \neq 0)$

On écrit $P = \widetilde{Q} \cdot R + \widetilde{T}$ avec $\widetilde{Q}, \widetilde{T} \in \mathbb{R}[X]$

$\deg(\widetilde{T}) < \deg(R)$

Unicité de la DE de P par R.

$R(Q - \widetilde{Q}) = \widetilde{T} \longrightarrow \deg(R) + \deg(Q - \widetilde{Q}) = \deg(\widetilde{T})$

$\deg(Q - \widetilde{Q}) < 0$

donc $Q - \widetilde{Q} = 0 \longrightarrow Q \in \mathbb{R}[X]$ ∎ $< \deg(R)$

c) Les irreductibles de $\mathbb{R}[X]$

Th : Les irréductibles unitaires de $\mathbb{R}[X]$ sont :

1) Les $X-\alpha$ avec $\alpha \in \mathbb{R}$

2) les X^2+aX+b avec $\begin{cases} a,b \in \mathbb{R} \\ a^2-4b<0 \end{cases}$

DI rq : Soit $P \in \mathbb{R}[X]$ unitaire, de degré $n \geq 3$, mq P_n est pas irréductible

Si deg P est impaire : alors

$$P(t) \longrightarrow +\infty \quad \text{et} \quad P(t) \longrightarrow -\infty$$
$$t \to +\infty \qquad\qquad t \to -\infty$$

$\hat{c}$ $\widetilde{P}(\cdot)$ est c^0, d'après le TVI, $\widetilde{P}(\cdot)$ s'annule, (sur $\mathbb{R}$).

Fixons $\alpha \in \mathbb{R}$ tq $P(\alpha)=0$. On a donc

$$(X-\alpha) \mid P$$

Donc P non (irr) ■

$\hat{c}$ deg $(P) \geq 1$, fixons (d'A-G) $\alpha \in \mathbb{C}$ tq

$P(\alpha)=0$. $(X-\alpha) \mid P$

$(X-\overline{\alpha}) \mid P$

- Si $\alpha \in \mathbb{R}$: ok
- Sinon, on a égalt $P(\overline{\alpha})=0$ Et donc

$$\begin{cases} (X-\alpha) \mid B \\ (X-\overline{\alpha}) \mid P \end{cases}$$

On a $\alpha \neq \overline{\alpha}$; donc $(X-\alpha) \wedge (X-\overline{\alpha}) = 1$

Donc : $(X-\alpha)(X-\overline{\alpha}) \mid P$

(R) $(X-\alpha)(X-\overline{\alpha}) = \underbrace{X^2 - 2\mathrm{Re}(\alpha) + |\alpha|^2}_{\text{(AF)} \quad \in \mathbb{R}[X]}$

Donc P non (irr) ■

(AF) $(X - e^{i\theta})(X - e^{-i\theta}) =$ (R)

Rq : ⚠ Les (irr) de $\mathbb{Q}[X]$ sont ultra difficiles à déterminer

d) décomposition en (irr) dans $\mathbb{R}[X]$

Prop : Soit $A \in \mathbb{R}[X]$ non nul.
Alors

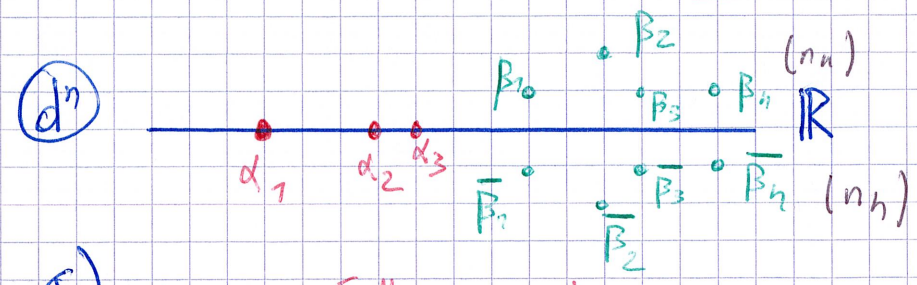
1) A s'écrit $A = \lambda \prod_{i=1}^{r} (X-\alpha_i)^{m_i} \prod_{j=1}^{s} P_j^{n_j}$

avec $\lambda \in \mathbb{R}$, avec $r, s \in \mathbb{N}$, avec $\forall i, \alpha_i \in \mathbb{R}$
avec $\forall j, P_j \in \mathbb{R}[X]$ "du type $X^2 + aX + b$ avec $a^2 - 4b < 0$"

et avec $\forall i,j$ $\begin{cases} m_i \in \mathbb{N}^* \\ n_j \in \mathbb{N}^* \end{cases}$

2) Cette écriture est unique.

D/ On bosse dans $\mathbb{C}$ et on descend dans $\mathbb{R}$



(I) racines réelles de A

Donc $\mathbb{C}[X]$:

$$A = \underbrace{\lambda \prod_{i=1}^{r} (X-\alpha_i)^{m_i}}_{\text{racines réelles}} \prod_{j=1}^{s} \underbrace{(X-\beta_j)^{n_j}(X-\overline{\beta_j})^{n_j}}_{\left(X^2 - 2\mathrm{Re}(\beta_j) + |\beta_j|^2\right)}$$

coeff dominant $\in \mathbb{R}^*$

(AF) : le "Δ" < 0

D'où l'Existence ■

Unicité :

$$A = \prod (X-\alpha_j)^{m_j} \prod P_i^{n_i} = \prod (X-\alpha_i)^{m_i} \prod (X-\beta_j)^{n_j}(X-\overline{\beta_j})^{n_j}$$

$$= \prod (X-\alpha_j)^{\mu_i} \prod Q_i^{\nu_i} = \prod (X-\alpha_i)^{\mu_i} \prod (X-b_j)^{\nu_j}(X-\overline{b_j})^{\nu_j}$$

Puis on utilise l'unicité de la décomposition de $\mathbb{C}[X]$ ■

Rq : • sinon pour π (irr), on définit $V_\pi(P)$

si : $P \in \mathbb{K}[X]$

• etc ...