

Polynômes et fractions rationnelles

Extrait du programme officiel :

CONTENUS

CAPACITÉS & COMMENTAIRES

Anneaux $\mathbb{K}[X]$

Dans ce paragraphe, \mathbb{K} est un sous-corps de \mathbb{C} .

Idéaux de $\mathbb{K}[X]$.

Définition du PGCD de $n \geq 2$ polynômes en termes d'idéaux, relation de Bézout.

Irréductibles de $\mathbb{K}[X]$. Existence et unicité de la décomposition en facteurs irréductibles unitaires.

Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Par convention, le PGCD est unitaire.

La démonstration du théorème de d'Alembert-Gauss est hors programme.

L'étude des irréductibles de $\mathbb{K}[X]$ pour un corps autre que \mathbb{R} ou \mathbb{C} n'est pas un objectif du programme.

Table des matières

8 Polynômes et fractions rationnelles	1
I L'algèbre des polynômes	2
1 Polynômes formels à une indéterminée	2
2 Opérations sur les polynômes	3
3 Dérivation formelle	4
II Fonctions polynomiales, racines	5
1 Fonctions polynomiales	5
2 Formule de Taylor	5
3 Racines	6
4 Polynômes scindés	8
5 Relations coefficients-racines	9
III Interpolation de Lagrange	10
IV Arithmétique sur $\mathbb{K}[X]$ (MPI)	12
1 L'anneau $\mathbb{K}[X]$	12
2 PGCD de deux polynômes	13
3 PGCD d'une famille finie de polynômes	15
4 Polynômes irréductibles	16
5 Irréductibles sur $\mathbb{R}[X]$	17
6 PPCM (Complément)	19
V Décomposition en éléments simples	19
1 Partie entière	19
2 Décomposition en éléments simples dans $\mathbb{C}(X)$	20
3 Décomposition en éléments simples dans $\mathbb{R}(X)$	21
4 Décomposition en éléments simples de P'/P	22

\mathbb{K} désigne un sous-corps de \mathbb{C} .

En fait tout corps convient, mais pour certaines propriétés, on a besoin qu'il soit de caractéristique nulle, c'est-à-dire tel que $n \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}} + \dots + 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ si $n \in \mathbb{N}^*$.

I L'ALGÈBRE DES POLYNÔMES

1 Polynômes formels à une indéterminée

Se donner un polynôme à coefficients dans \mathbb{K} , c'est se donner la suite $(a_0, a_1, \dots, a_d, 0, 0, \dots)$ de ses coefficients ayant un nombre fini de termes non nuls (nulle à partir d'un certain rang). On parle alors de suite **presque nulle**.

On note alors, pour tout $k \in \mathbb{N}$, X^k la suite presque nulle $(0, \dots, 0, \underbrace{1}_{k^e}, 0, 0, \dots)$.

Cela permet de transformer la notation $(a_0, a_1, \dots, a_d, 0, 0, \dots)$ en

$$P = a_0 + a_1 X + \dots + a_d X^d + 0 + 0 + \dots = \underbrace{\sum_{k=0}^{+\infty} a_k X^k}_{\text{somme finie}} = \sum_{k=0}^d a_k X^k.$$

On note parfois $P(X)$ pour P .

X est appelée **indéterminée**. L'ensemble des polynômes à une indéterminée à coefficients dans \mathbb{K} est noté $\mathbb{K}[X]$.

Remarque

- R1 – L'indéterminée n'est pas un nombre ! Elle n'a pas de valeur. Elle représente la suite presque nulle $(0, 1, 0, 0, \dots)$.
- R2 – Par définition, $P = \sum a_k X^k = Q = \sum b_k X^k \iff \forall k, a_k = b_k$ (égalité de deux suites). Les coefficients d'un polynôme formel sont uniques.

- Le **polynôme nul** est le polynôme dont tous les coefficients sont nuls, noté $0_{\mathbb{K}[X]}$ ou plus simplement 0 .
- On appelle **monôme** tout polynôme de la forme aX^k avec $k \in \mathbb{N}$ et $a \neq 0$.
- On appelle **polynôme constant** tout polynôme $P = a$ où $a \in \mathbb{K}$.
- Si $P \in \mathbb{K}[X] \setminus \{0\}$, on appelle **degré de P**, noté $\deg P$, le plus grand $k \in \mathbb{N}$ tel que $a_k \neq 0$ (qui existe bien).

$$\deg P = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$$

$a_{\deg P}$ est appelé **coefficient dominant** de P , noté $\text{cd } P$.

Si $\text{cd } P = 1$, P est dit **unitaire** ou **normalisé**.

On pose $\deg 0 = -\infty$.

- On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg P \leq n\}$ l'ensemble des polynômes de degré **au plus** n .

$$\mathbb{K}_n[X] = \left\{ a_0 + a_1 X + \dots + a_n X^n, (a_0, \dots, a_n) \in \mathbb{K}^{n+1} \right\}.$$

2 Opérations sur les polynômes

Pour $P = \sum_{k \geq 0} a_k X^k, Q = \sum_{k \geq 0} b_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on définit les lois $+, \times, \cdot, \circ$ par

- $P + Q = \sum_{k \geq 0} (a_k + b_k) X^k$
- $\lambda P = \sum_{k \geq 0} (\lambda a_k) X^k$
- $P \times Q = \sum_{k \geq 0} a_k X^k \times \sum_{\ell \geq 0} b_\ell X^\ell = \sum_{\substack{m \geq 0 \\ (m=k+\ell)}} c_m X^m$

en faisant une sommation par diagonales, c'est-à-dire avec

$$c_m = \sum_{m=k+\ell} a_k b_\ell = \sum_{k=0}^m a_k b_{m-k} = \sum_{\ell=0}^m a_{m-\ell} b_\ell.$$

- $P \circ Q = P(Q) = \sum_{k \geq 0} a_k Q^k$.

Propriété 1 : Opérations algébriques et degré

Si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, $P + Q, P \times Q$ et λP sont des polynômes et

- $\deg(P + Q) \leq \max(\deg P, \deg Q)$ avec égalité si et seulement si $\deg P \neq \deg Q$ ou $(\deg P = \deg Q$ et $\text{cd } P + \text{cd } Q \neq 0)$
- $\deg(\lambda P) = \deg P$ et $\text{cd}(\lambda P) = \lambda \text{cd } P$ **si** $\lambda \neq 0$, sinon $\lambda P = 0$.
- $\deg(PQ) = \deg P + \deg Q$ et $\text{cd}(PQ) = \text{cd } P \text{cd } Q$.
- Si Q **non constant**, alors

$$\deg(P \circ Q) = \deg P \deg Q$$

et

$$\text{cd}(P \circ Q) = \text{cd } P \times (\text{cd } Q)^{\deg P}.$$

Remarque

- R3 – En général, on a $\deg(\alpha P + \beta Q) \leq \max(\deg P, \deg Q)$.



Propriété 2 : Structure d’anneau commutatif intègre

$(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -algèbre commutative intègre d’élément unité le polynôme constant 1 et dont le groupe des inversible est $\mathbb{K}_0[X] \setminus \{0\}$ (polynômes constants non nuls.)

Remarque

R4 – L’isomorphisme d’algèbres trivial $\mathbb{K} \rightarrow \mathbb{K}_0[X]$ permet de confondre \mathbb{K} et $\mathbb{K}_0[X]$, c’est-à-dire les constantes λ et les polynômes constants $P = \lambda$.

3 Dérivation formelle

Définition 1 : Polynôme dérivé

Si $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$, on appelle **polynôme dérivé de P** , noté P' , le polynôme défini par

$$P' = \sum_{k=1}^n k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$$

$$= a_1 + 2a_2X + \dots + n a_n X^{n-1}.$$

et $0' = 0$.

Plus généralement, on note $P^{(0)} = P, P^{(1)} = P', P^{(2)} = P'' = (P')'$ et pour tout $k \in \mathbb{N}^*, P^{(k)} = (P^{(k-1)})'$.

Remarque

R5 – Il n’est pas question ici de dérivabilité : la dérivation est une simple opération algébrique sur les polynômes.

Propriété 3 : de la dérivation

Soient $P, Q \in \mathbb{K}[X], \alpha, \beta \in \mathbb{K}$.

- (i) $\deg P' = \deg P - 1$ si P non constant, $-\infty$ sinon.
Plus généralement, $\deg P^{(n)} = \deg P - n$ si $\deg P \geq n, -\infty$ sinon.
En général, $\deg P^{(n)} \leq \deg P - n$.

(ii) **Linéarité** : $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$.

(iii) **Formule de Leibniz**

$(PQ)' = P'Q + PQ'$ et plus généralement, $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$.

(iv) $(P \circ Q)' = Q' \times P' \circ Q$.

Remarque

R6 – $P^{(n)} = 0$ si $n \geq \deg P + 1$ et si $d = \deg P, P^{(d)} = d! \text{cd } P$.

R7 – $\deg P = \min \{ n \in \mathbb{N} \mid P^{(n)} = 0 \} - 1$ si $P \neq 0$.

R8 – Si $n \in \mathbb{N}$,

$$(X-a)^k)^{(n)} = \begin{cases} 0 & \text{si } n \geq k+1 \\ k! & \text{si } n = k \\ k(k-1) \dots (k-n+1)(X-a)^{k-n} = \frac{k!}{(k-n)!} (X-a)^{k-n} & \text{sinon.} \end{cases}$$

$$\mathbf{R9} - \text{Si } P = \sum_{k=0}^d a_k X^k, \text{ alors pour tout } n \in \mathbb{N}, P^{(n)} = \begin{cases} 0 & \text{si } n \geq d+1 \\ d! a_d & \text{si } n = d \\ \sum_{k=n}^d k(k-1)\dots(k-n+1) a_k X^{k-n} & \text{sinon.} \end{cases}$$

II FONCTIONS POLYNOMIALES, RACINES

1 Fonctions polynomiales

Définition 2 : Fonction polynôme associée

$$\text{Si } P = \sum_{k \geq 0} a_k X^k \in \mathbb{K}[X], \text{ on note } \tilde{P} : \begin{cases} \mathbb{K} & \rightarrow \mathbb{K} \\ x & \rightarrow \tilde{P}(x) = \sum_{k \geq 0} a_k x^k \end{cases} \text{ appelée fonction polynôme associée à } P.$$

Remarque

- R10** – Mathématiquement, P et \tilde{P} sont des objets fondamentalement différents. Cependant, sous certaines conditions, on peut les identifier (cf plus loin). Ainsi, on fait souvent l’abus de notation $P(x)$ pour $\tilde{P}(x)$.
- R11** – On peut en fait définir un polynôme pour autre chose qu’un élément de \mathbb{K} : il suffit de pouvoir élever à une puissance k et faire des combinaisons linéaires (matrices, fonctions, polynômes, etc.) : la structure de \mathbb{K} -algèbre est adaptée.
- R12** – Si $P, Q \in \mathbb{K}[X]$, $P \circ Q = \tilde{P}(Q)$ (on applique la fonction polynôme à un polynôme au lieu d’un élément de \mathbb{K} .)

Propriété 4 : Fonction polynôme et opérations

- Si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$
- (i) $\widetilde{P+Q} = \tilde{P} + \tilde{Q}$.
 - (ii) $\widetilde{P \times Q} = \tilde{P} \times \tilde{Q}$.
 - (iii) $\widetilde{\lambda P} = \lambda \tilde{P}$.
 - (iv) $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.
 - (v) Sur \mathbb{R} , \tilde{P} est dérivable et $\tilde{P}' = \tilde{P}'$.

Remarque

- R13** – L’application $P \mapsto \tilde{P}$ est un morphisme de \mathbb{K} -algèbres de $\mathbb{K}[X]$ vers l’algèbre des fonctions de \mathbb{K} dans \mathbb{K} .

2 Formule de Taylor

Théorème 1 : Formule de Taylor

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$P(X) = \sum_{n=0}^{+\infty} \frac{\tilde{P}^{(n)}(a)}{n!} (X - a)^n$$

la somme étant finie, c’est-à-dire

$$P(X + a) = \sum_{n=0}^{+\infty} \frac{\tilde{P}^{(n)}(a)}{n!} X^n.$$



Corollaire 1 : Formule de Mac Laurin

$$P = \sum_{n=0}^{+\infty} \frac{\tilde{P}^{(n)}(0)}{n!} X^n \text{ c'est-à-dire les coefficients de } P \text{ sont les } a_n = \frac{\tilde{P}^{(n)}(0)}{n!}.$$

3 Racines

Définition 3 : Racine

$a \in \mathbb{K}$ est un **zéro** ou une **racine** de $P \in \mathbb{K}[X]$ lorsque $\tilde{P}(a) = 0$.

Remarque

R 14 – Cela dépend du corps \mathbb{K} .

R 15 – Un polynôme réel de degré impair a toujours une racine réelle (conséquence du théorème des valeurs intermédiaires.)

Propriété 5 : Racine et division

Soit $P \in \mathbb{K}[X]$.

(i) a est racine de P si et seulement si $(X - a) | P$.

(ii) x_1, \dots, x_n sont racines deux à deux distinctes de P si et seulement si $(X - x_1) \cdots (X - x_n) | P$.

Remarque

R 16 – Si $P | Q$, toute racine de P est racine de Q . La réciproque est fautive en général.

Corollaire 2 : Nombre de racines

Soit $P \in \mathbb{K}[X]$.

(i) Si $P \neq 0$, P admet au plus $\deg P$ racines.

(ii) Si P admet strictement plus de $\deg P$ racines, $P = 0$.

(iii) Si P admet une infinité de racines, $P = 0$.

Corollaire 3 : Identification polynôme et fonction polynôme

Si \mathbb{K} est infini et $\tilde{P} = \tilde{Q}$, alors $P = Q$. On peut alors confondre P et \tilde{P} .

Démonstration

Si $\tilde{P} = \tilde{Q}$ et \mathbb{K} infini, alors $P - Q$ a une infinité de racines, donc est nul. ■

Remarque

R 17 – Si $\mathbb{K} = \{x_1, \dots, x_n\}$ fini (par exemple $\mathbb{Z}/p\mathbb{Z}$ avec p premier), $P = \prod_{k=1}^n (X - x_k) \neq 0$ (il est unitaire) et pourtant $\tilde{P} \equiv 0$ (pas plus de racines que le degré!).

Exercice 1

Si $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} , $P(X+a) = \sum_{n \geq 0} \frac{a^n}{n!} P^{(n)}(X)$. En effet, il suffit d'écrire $\tilde{P}(x+a) = \tilde{P}(a+x) = \sum_{n \geq 0} \frac{\tilde{P}^{(n)}(x)}{n!} a^n = \left(\sum_{n \geq 0} \frac{a^n}{n!} P^{(n)} \right)(x)$
 (on applique Taylor au point x , évalué en $a \dots$) d'où l'égalité des polynômes sur le corps infini.

Définition 4 : Multiplicité

Soient $P \in \mathbb{K}[X]$ tel que $P \neq 0$, $a \in \mathbb{K}$.
 On appelle **ordre de multiplicité** de a en tant que racine de P l'entier

$$m = \max \{ k \in \mathbb{N} ; (X-a)^k \mid P \}$$

Ainsi, a est racine d'ordre m si et seulement si $(X-a)^m \mid P$ et $(X-a)^{m+1} \nmid P$ si et seulement si on a $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ et $Q(a) \neq 0$.

- Si $m = 0$, a n'est pas racine de P .
- Si $m \geq 1$, a est racine de P .
- Si $m = 1$, a est racine simple de P .
- Si $m = 2$, a est racine double de P .
- Si $m = 3$, a est racine triple de P .
- Si $m \geq 2$, a est racine multiple de P .

Remarque

- R 18 – Si $(X-a)^n \mid P$ alors a est racine de P d'ordre **au moins** n .
- R 19 – L'ordre est toujours au plus égal au degré du polynôme.

Propriété 6

x_1, \dots, x_n deux à deux distincts sont racines d'ordre au moins m_1, \dots, m_n respectivement si et seulement si $(X-x_1)^{m_1} \dots (X-x_n)^{m_n} \mid P$.

Propriété 7 : Caractérisation de l'ordre

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}$.
 a est racine d'ordre m de P si et seulement si $\forall k \in \llbracket 0, m-1 \rrbracket$, $\tilde{P}^{(k)}(a) = 0$ et $\tilde{P}^{(m)}(a) \neq 0$.

Exercice 2 : CCINP 85

1. Soient $n \in \mathbb{N}^*$, $P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$.
 - (a) Donner sans démonstration, en utilisant la formule de Taylor, la décomposition de $P(X)$ dans la base $(1, X-a, (X-a)^2, \dots, (X-a)^n)$.
 - (b) Soit $r \in \mathbb{N}^*$. En déduire que :
 a est une racine de P d'ordre de multiplicité r si et seulement si $P^{(r)}(a) \neq 0$ et $\forall k \in \llbracket 0, r-1 \rrbracket$, $P^{(k)}(a) = 0$.
2. Déterminer deux réels a et b pour que 1 soit racine double du polynôme $P = X^5 + aX^2 + bX$ et factoriser alors ce polynôme dans $\mathbb{R}[X]$.

Corollaire 4 : Multiplicité des racines de P vs P'

Si a est racine d'ordre $m \geq 2$ de P , a racine d'ordre $m-1$ de P' . La réciproque est fautive si on ne suppose pas a racine de P .



Exemple

E1 – $P = X(X - 2)$ et $P' = 2X - 2 : 1$ est racine simple de P' , mais n'est pas racine double de P .

Exercice 3

Montrer que $(X - 1)^3 \mid nX^{n+2} - (n + 2)X^{n+1} + (n + 2)X - n$.



Voir exercice du TD : 10, 11, 15, 18

4 Polynômes scindés

Définition 5 : Polynôme scindé

$P \in \mathbb{K}[X]$ est dit **scindé** sur \mathbb{K} s'il peut s'écrire comme produit de polynômes de degré 1 de $\mathbb{K}[X]$, c'est-à-dire si on a $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}^*$ et $y_1, \dots, y_n \in \mathbb{K}$ tels que

$$P = \lambda(X - y_1) \cdots (X - y_n),$$

c'est-à-dire si on a $\lambda \in \mathbb{K}^*$, $p \in \mathbb{N}^*$ et $x_1, \dots, x_p \in \mathbb{K}$ deux à deux distincts et $m_1, \dots, m_p \in \mathbb{N}^*$ tels que

$$P = \lambda(X - x_1)^{m_1} \cdots (X - x_p)^{m_p}.$$

Alors $\deg P \geq 1$, $\lambda = \text{cd } P$, x_1, \dots, x_p sont les racines de P deux à deux distinctes de multiplicités respectives m_1, \dots, m_p .

Remarque

R20 – Scindé sur $\mathbb{C} \Leftrightarrow$ scindé sur \mathbb{R} .

$P = X^2 - 1$ est scindé sur \mathbb{C} mais pas sur \mathbb{R} .

$P = X^2 - 2$ est scindé sur \mathbb{R}, \mathbb{C} mais pas sur \mathbb{Q} .

Propriété 8 : Caractérisation avec les racines

Soit P un polynôme non constant admettant exactement p racines d'ordres respectifs m_1, \dots, m_p dans \mathbb{K} . P est scindé si et seulement si

$$m_1 + \cdots + m_p = \deg P.$$

Théorème 2 : Théorème de d'Alembert-Gauß (Théorème fondamental de l'algèbre)

Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.

On dit que le corps \mathbb{C} est **algébriquement clos**.

Corollaire 5 : Version alternative équivalente

Tout polynôme à coefficients complexes non constant est scindé.

Corollaire 6 : Divisibilité et racines

Si P est scindé, alors $P|Q$ si et seulement si toutes les racines de P sont racines de Q avec des multiplicités au moins égales à celles pour P .

Remarque

R 21 – C'est donc toujours vrai dans \mathbb{C} .



Voir exercice du TD : 12, 13, 16, 17

5 Relations coefficients-racines

Définition 6 : Fonctions symétriques élémentaires

Soient $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in \mathbb{K}$.

On appelle **fonctions symétriques élémentaires** de x_1, \dots, x_n les nombres

$$\sigma_1 = \sum_{i=1}^n x_i = x_1 + x_2 + \dots + x_n. \quad (n \text{ termes})$$

$$\begin{aligned} \sigma_2 &= \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \quad \left(\frac{n(n-1)}{2} \text{ termes} \right) \\ &= x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + \dots + x_{n-1} x_n. \end{aligned}$$

⋮

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}. \quad \left(\binom{n}{k} \text{ termes} \right)$$

⋮

$$\sigma_n = x_1 x_2 \dots x_n. \quad (1 \text{ terme})$$

Exemple

E 2 – Si $n = 3$, les fonctions symétriques élémentaires en x, y, z sont $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + xz$ et $\sigma_3 = xyz$.

Remarque

R 22 – On peut montrer que toute fonction polynomiale en x_1, \dots, x_n symétrique en x_1, \dots, x_n s'exprime comme un polynôme en $\sigma_1, \dots, \sigma_n$.

Exemple

E 3 – $S_1 = x_1 + \dots + x_n = \sigma_1$ et $S_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$.



Propriété 9 : Relations coefficients-racines

Soient $n \in \mathbb{N}^*$, $a_0, \dots, a_n \in \mathbb{K}$ tel que $a_n \neq 0$, $P = a_0 + \dots + a_n X^n$, **scindé** sur \mathbb{K} , x_1, \dots, x_n ses racines **comptées avec leur multiplicité**, donc $P = a_n(X - x_1) \cdots (X - x_n)$. En notant σ_k les fonctions symétriques élémentaires en x_1, \dots, x_n ,

- $\sigma_1 = -\frac{a_{n-1}}{a_n}$. (somme)
- \vdots
- $\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$.
- \vdots
- $\sigma_n = (-1)^n \frac{a_0}{a_n}$. (produit)

Ainsi,

$$P = a_n \left(X^n - \underbrace{\sigma_1}_{\text{somme}} X^{n-1} + \sigma_2 X^{n-2} + \dots + (-1)^n \underbrace{\sigma_n}_{\text{produit}} \right).$$

Remarque

R23 – En particulier, si P est unitaire, $P = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \dots + (-1)^n \sigma_n$.

R24 – Si $n = 2$, on retrouve que les racines complexes de $aX^2 + bX + c$ ont une somme égale à $-b/a$ et un produit égal à c/a .



Voir exercice du TD : 14, 20



INTERPOLATION DE LAGRANGE

- **Problématique** : Étant donné $n \in \mathbb{N}$, $n + 1$ scalaires $x_0, \dots, x_n \in \mathbb{K}$ deux à deux distincts, et $y_0, \dots, y_n \in \mathbb{K}$ fixés (par exemple pour tout k , $y_k = f(x_k)$ où f est une fonction connue ou non).

On cherche des polynômes $P \in \mathbb{K}[X]$ tels que

$$\forall k \in \llbracket 0, n \rrbracket, P(x_k) = y_k.$$

C'est un problème d'**interpolation**.

- **Principe** : C'est un problème linéaire.

L'application $u : \begin{cases} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}^{n+1} \\ P & \longmapsto & (P(x_k))_{k \in \llbracket 0, n \rrbracket} \end{cases}$ est une application linéaire injective entre deux espaces de dimension $n + 1$.

En effet, son noyau est réduit aux polynômes de degré au plus n admettent les $n + 1$ racines distinctes x_0, \dots, x_n , c'est-à-dire au polynôme nul.

Il s'agit donc d'un isomorphisme.

On peut aussi remarquer que sa matrice dans les bases canoniques est la matrice de Vandermonde associée à x_0, \dots, x_n .

L'unique solution au problème est donc, par linéarité,

$$u^{-1}(y_0, \dots, y_n) = \sum_{i=0}^n y_i \cdot u^{-1}\left(0, \dots, \underbrace{1}_{i^{\text{e}}}, \dots, 0\right).$$

On cherche donc le polynôme $L_i = u^{-1}\left(0, \dots, \underbrace{1}_{i^{\text{e}}}, \dots, 0\right)$ tel que $L_i(x_i) = 1$ et $L_i(x_j) = 0$ si $j \neq i$, c'est-à-dire $L_i(x_j) = \delta_{i,j}$.

Alors les x_j pour $j \neq i$ sont racines de L_i . Donc $L_i = \prod_{j \neq i} (X - x_j) Q$.

Comme $\deg L_i = 1$, alors Q est constant : $Q = \lambda$ et $L_i(x_i) = 1 = \prod_{j \neq i} (x_i - x_j)$.

Définition 7 : Polynômes de Lagrange

Si $n \in \mathbb{N}^*$ et x_0, \dots, x_n deux à deux distincts, on appelle i^{e} polynôme de Lagrange associé à (x_0, \dots, x_n) le polynôme

$$L_i = \frac{\prod_{j \neq i} (X - x_j)}{\prod_{j \neq i} (x_i - x_j)}.$$

Propriété 10 : Polynôme d'interpolation de Lagrange

Étant donné $x_0, \dots, x_n \in \mathbb{K}$ deux à deux distincts et $y_0, \dots, y_n \in \mathbb{K}$, il existe un unique polynôme P de degré au plus n tel que $\forall i, P(x_i) = y_i$.

Il s'agit de $P = \sum_{i=0}^n y_i \cdot L_i$.

Comme le problème est linéaire (en fait affine), on peut le résoudre sur $\mathbb{K}[X]$ en passant par solution particulière et solution du problème homogène associé.

Propriété 11

Les polynômes d'interpolation associés aux points $((x_0, y_0), \dots, (x_n, y_n))$ sont les polynômes $P + \left(\prod_{i=0}^n (X - x_i) \right) Q$ où $Q \in \mathbb{K}[X]$ et $P = \sum_{i=0}^n y_i L_i$.

Démonstration

Ils conviennent et si A convient, x_0, \dots, x_n sont racines de $A - P$ qui s'écrit donc $\left(\prod_{i=0}^n (X - x_i) \right) Q$. ■

Exercice 4 : CCINP 87

Soient a_0, a_1, \dots, a_n $n + 1$ réels deux à deux distincts.

1. Montrer que si b_0, b_1, \dots, b_n sont $n + 1$ réels quelconques, alors il existe un unique polynôme P vérifiant $\deg P \leq n$ et $\forall i \in \{0, \dots, n\} P(a_i) = b_i$.
2. Soit $k \in \{0, \dots, n\}$.

Expliciter ce polynôme P , que l'on notera L_k , lorsque $\forall i \in \{0, \dots, n\} b_i = \begin{cases} 0 & \text{si } i \neq k \\ 1 & \text{si } i = k \end{cases}$

3. Prouver que $\forall p \in \{0, \dots, n\}, \sum_{k=0}^n a_k^p L_k = X^p$.

Exercice 5 : CCINP 90

\mathbb{K} désigne le corps des réels ou celui des complexes.
Soient a_1, a_2, a_3 trois scalaires distincts donnés de \mathbb{K} .

1. Montrer que $\Phi: \mathbb{K}_2[X] \rightarrow \mathbb{K}^3$ est un isomorphisme d'espaces vectoriels.
$$P \mapsto (P(a_1), P(a_2), P(a_3))$$
2. On note (e_1, e_2, e_3) la base canonique de \mathbb{K}^3 et on pose

$$\forall k \in \{1, 2, 3\}, L_k = \Phi^{-1}(e_k).$$

- (a) Justifier que (L_1, L_2, L_3) est une base de $\mathbb{K}_2[X]$.
- (b) Exprimer les polynômes L_1, L_2 et L_3 en fonction de a_1, a_2 et a_3 .



3. Soit $P \in \mathbb{K}_2[X]$. Déterminer les coordonnées de P dans la base (L_1, L_2, L_3) .
4. Application : On se place dans \mathbb{R}^2 muni d'un repère orthonormé et on considère les trois points $A(0, 1), B(1, 3), C(2, 1)$.
Déterminer une fonction polynomiale de degré 2 dont la courbe passe par les points A, B et C .

IV ARITHMÉTIQUE SUR $\mathbb{K}[X]$ (MPI)

Dans cette partie, \mathbb{K} désigne un sous-corps de \mathbb{C} , comme, \mathbb{Q}, \mathbb{R} ou \mathbb{C} .

1 L'anneau $\mathbb{K}[X]$

Théorème 3 : Structure de $\mathbb{K}[X]$

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif et intègre.
Son groupe des inversibles est $U_{\mathbb{K}[X]} = \mathbb{K}_0[X] \setminus \{0\}$, ensemble des polynômes constants non nuls.
 $(\mathbb{K}[X], +, \times, \cdot)$ a une structure de \mathbb{K} -algèbre.

Démonstration

- La structure d'anneau commutatif a été vue en classe de MP21.
L'élément neutre pour $+$ est le polynôme nul, celui pour \times est le polynôme constant 1
- Si P est inversible pour \times , alors on a Q tel que $PQ = 1$ et alors $\deg P + \deg Q = 0$ donc $\deg P = \deg Q = 0$. La réciproque est bien sûr vraie, avec, pour $P = \lambda \neq 0$, $P^{-1} = \lambda^{-1} = \frac{1}{\lambda}$.
- Si $PQ = 0$ alors $\deg(PQ) = \deg P + \deg Q = -\infty$ donc $\deg P = -\infty$ ou $\deg Q = -\infty$, d'où l'intégrité. ■

Corollaire 7 : Description des polynômes associés

Si $P, Q \in \mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.

Théorème 4 : Division euclidienne polynomiale

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tel que $A = BQ + R$ et $\deg R < \deg B$.

Remarque : Algorithme

R 25 – C'est celui que l'on utilise en posant la division. On s'intéresse au terme de plus haut degré dans A que l'on compense en multipliant B par un monôme, et on recommence en soustrayant.

Démonstration

- Existence** : Soit $d = \deg B$, $B = b_0 + \dots + b_d X^d$ avec $b_d \neq 0$. Si $d = 0$, le couple $(A/b_0, 0)$ convient. Sinon, on raisonne par récurrence forte sur $n = \deg A$, $A = a_0 + \dots + a_n X^n$.
 - Si $n < d$, $(0, A)$ convient.
 - Si le résultat est vrai pour tout polynôme de degré au plus $n-1$, alors on écrit $A = \frac{a_n}{b_d} X^{n-d} B + A_1$ avec $\deg A_1 \leq n-1$.
Par hypothèse de récurrence, on a $(Q_1, R) \in \mathbb{K}[X]$ tels que $A = BQ_1 + R$ et $\deg R < \deg B$.
Alors $\left(Q_1 + \frac{a_n}{b_d} X^{n-d}, R\right)$ convient.

- **Unicité** : Si (Q_1, R_1) et (Q_2, R_2) conviennent, alors $B(Q_1 - Q_2) = R_2 - R_1$. Vu les degrés, on en tire $Q_1 = Q_2$, puis $R_1 = R_2$. ■

Théorème 5 : $\mathbb{K}[X]$ est principal

L'anneau $\mathbb{K}[X]$ est principal.

En particulier, tout idéal de $\mathbb{K}[X]$ s'écrit sous la forme $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$. Si l'idéal est non nul, on peut choisir P de manière unique en le supposant unitaire.

Démonstration

C'est un anneau intègre. Montrons que ses idéaux sont tous principaux.

Soit I un idéal de $\mathbb{K}[X]$.

- Si $I = \{0\}$ alors $I = 0\mathbb{K}[X] = (0)$.
- Sinon, l'ensemble $E = \{\deg P, P \in I, P \neq 0\}$ est une partie non vide de \mathbb{N} donc admet un minimum. Soit $P_0 \in I$ réalisant ce minimum. On montre que $I = (P_0)$.
 - ★ On a déjà $P_0 \in I$ donc par définition d'un idéal, $(P_0) = P_0\mathbb{K}[X] \subset I$.
 - ★ Si, réciproquement, $P \in I$, effectuons la division euclidienne par P_0 : on a $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = P_0Q + R$ et $\deg R < \deg P_0$.
Alors $R = P - P_0Q \in I$ et $\deg R < \min E$ donc $R = 0$ et $P = P_0Q \in (P_0)$.

2 PGCD de deux polynômes

Définition 8 : PGCD

Soient $A, B \in \mathbb{K}[X]$ non tous les deux nuls.

$$I = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV, U, V \in \mathbb{K}[X]\}$$

est un idéal non réduit à zéro de $\mathbb{K}[X]$.

Son unique générateur unitaire est appelé pgcd de A et B , noté $A \wedge B$.

Remarque

R26 – La définition s'étend au cas où $A = B = 0$ en posant $A \wedge B = 0$ car $(0) + (0) = (0)$ même si alors, on ne peut plus dire que $A \wedge B$ est unitaire.

Propriété 12 : Relation de Bézout

Si $A, B \in \mathbb{K}[X]$, on peut trouver $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$.

Démonstration

$$A \wedge B \in A \wedge B\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X].$$

Propriété 13 : Caractérisation du PGCD

Soit $(A, B) \neq (0, 0)$.

$$D = A \wedge B \iff \begin{cases} D \text{ est unitaire} \\ D|A \text{ et } D|B \\ \forall C \in \mathbb{K}[X], (C|A \text{ et } C|B) \implies C|D \end{cases}$$

Il s'agit donc du plus grand diviseur unitaire au sens de la division.



Démonstration

(\Rightarrow) Si $D = A \wedge B$ alors D est unitaire et $AK[X] + BK[X] = DK[X]$ donc $A, B \in DK[X]$ soit $D|A$ et $D|B$.
 Et si $C|A$ et $C|B$, alors, comme on a $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B, C|A \wedge B$.
 (\Leftarrow) Si D est un diviseur commun unitaire plus grand que tous les autres au sens de la division, alors D divise $AU + BV = A \wedge B$, et comme $A \wedge B$ est un diviseur commun, il divise D .
 D et $A \wedge B$ étant associés et unitaires, ils sont égaux. ■

Remarque

R 27 – Les diviseurs de D sont alors exactement les diviseurs communs à A et à B .
R 28 – Les racines des pgcd sont exactement les racines communes de A et B , de multiplicité le minimum des multiplicités.

Définition 9 : Polynômes premiers entre eux

$A, B \in \mathbb{K}[X]$ sont dits **premiers entre eux** lorsque $A \wedge B = 1$, c'est-à-dire lorsque les seuls diviseurs communs sont les polynômes constants non nuls.

Remarque

R 29 – Lorsque c'est le cas, ils n'ont pas de racine commune dans \mathbb{K} . La réciproque est fausse.

Théorème 6 : de Bézout

Soit $A, B \in \mathbb{K}[X]$.

$$A \wedge B = 1 \iff \exists U, V \in \mathbb{K}[X], AU + BV = 1$$

Démonstration

(\Rightarrow) Connu
 (\Leftarrow) S'il existe $U, V \in \mathbb{K}[X]$ tel que $AU + BV = 1$, alors $1 \in (A \wedge B)$ donc $(A \wedge B) = \mathbb{K}[X] = (1)$. ■

Corollaire 8

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

(i) $A \wedge BC = 1 \iff A \wedge B = A \wedge C = 1$

(ii) Si $D = A \wedge B$, on a $A_1, B_1 \in \mathbb{K}[X]$ tels que $A = DA_1, B = DB_1$ et $A_1 \wedge B_1 = 1$.

Remarque

R 30 – (i) s'étend à un produit quelconque (fini) de polynômes.

Démonstration

■

Théorème 7 : Lemme de Gauß

Soient $A, B, C \in \mathbb{K}[X]$.
Si $A|BC$ et $A \wedge B = 1$, alors $A|C$.

Démonstration

On a $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$ et $A|BC$ donc $C = ACU + BCV$ est divisible par A . ■

Propriété 14 : Cas des polynômes scindés

Si A ou B est **scindé**,
 $A \wedge B = 1 \iff A$ et B n'ont pas de racine commune.

Remarque

R31 – C'est toujours vrai si $\mathbb{K} = \mathbb{C}$.



Voir exercice du TD : 21, 22

Démonstration

- (\implies) : Pas de facteur $(X - a)$ commun.
- (\impliedby) : Si A et B n'ont pas de racine commune, un diviseur de A et de B , nécessairement constant ou scindé n'a pas de racine, donc est constant. ■

3 PGCD d'une famille finie de polynômes

Soit $n \in \mathbb{N} \setminus \{0, 1\}$.

Définition 10 : pgcd de n polynômes

Soient $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n \setminus \{(0, \dots, 0)\}$. On note $D = A_1 \wedge A_2 \wedge \dots \wedge A_n = \bigwedge_{k=1}^n A_k$ l'unique polynôme unitaire tel que $A_1\mathbb{K}[X] + \dots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.

Remarque

- R32 – Comme pour deux polynômes, il s'agit du plus grand diviseur commun unitaire au sens de la division (et aussi du degré).
- R33 – La définition s'étend à $0 \wedge \dots \wedge 0 = 0$.

Propriété 15

- (i) **Associativité** : $A \wedge B \wedge C = (A \wedge B) \wedge C = A \wedge (B \wedge C)$.
- (ii) Les diviseurs communs à A_1, \dots, A_n sont exactement les diviseurs de $\bigwedge_{k=1}^n A_k$.
- (iii) **Relation de Bézout** : On a $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que $A_1U_1 + \dots + A_nU_n = \bigwedge_{k=1}^n A_k$.



Définition 11 : Polynômes premiers entre eux dans leur ensemble

A_1, \dots, A_n sont dits **premiers entre eux dans leur ensemble** lorsque $\bigwedge_{k=1}^n A_k = 1$, c'est-à-dire que le seul diviseur unitaire commun à tous les A_k est 1.

A_1, \dots, A_n sont dits **premiers entre eux deux à deux** lorsque $\forall i \neq j, A_i \wedge A_j = 1$.

Propriété 16

Premiers entre eux deux à deux \implies premiers entre eux dans leur ensemble, mais la réciproque est fautive pour plus de deux polynômes.

Théorème 8 : de Bézout

A_1, \dots, A_n sont premiers entre eux dans leur ensemble si et seulement si on a U_1, \dots, U_n tels que $A_1 U_1 + \dots + A_n U_n = 1$.

Propriété 17 : Diviseurs deux à deux premiers entre eux

Si A_1, \dots, A_n sont premiers entre eux **deux à deux** et divisent B , alors $A_1 \cdots A_n | B$.

Remarque : Application

R 34 – Si x_1, \dots, x_n sont racines de P d'ordre au moins m_1, \dots, m_n alors $(X - x_1)^{m_1} \cdots (X - x_n)^{m_n} | P$ car les $(X - x_i)^{m_i}$ sont premiers entre eux deux à deux (scindés sans racine commune).

4 Polynômes irréductibles

Définition 12 : Polynôme irréductible

On appelle **polynôme irréductible** tout polynôme $P \in \mathbb{K}[X]$ **non constant** dont les seuls diviseurs sont les λ et λP pour $\lambda \in \mathbb{K}^*$, c'est-à-dire tels que $P = UV \implies U$ ou V inversible.

Les autres polynômes sont dits **réductibles**.

Remarque

R 35 – Si P est irréductible dans \mathbb{K} et $\deg P \geq 2$, P n'a pas de racine dans \mathbb{K} . La réciproque est fautive.

R 36 – P est réductible dans $\mathbb{K}[X]$ ss'il admet un diviseur Q tel que $0 < \deg Q < \deg P$.

Propriété 18 : des polynômes irréductibles

Soit P un polynôme irréductible, et $A, A_1, \dots, A_n \in \mathbb{K}[X]$.

(i) Soit $P | A$, soit $P \wedge A = 1$.

(ii) $P | A_1 \cdots A_n \iff \exists i$ tel que $P | A_i$.

Démonstration

(i) $P \wedge A$ divise P qui est irréductible (et A), donc vaut soit 1, soit P (à normalisation près).

(ii) Le sens \Leftarrow ne pose pas de problème.

Pour l'autre sens, par contraposée, si P ne divise aucun des A_i , il est premier avec chacun (par (i)), donc il est premier avec le produit, donc il ne le divise pas. ■

Théorème 9 : Décomposition en produit d'irréductibles

Tout $A \in \mathbb{K}[X] \setminus \{0\}$ s'écrit de manière unique à l'ordre des facteurs près sous la forme

$$A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, P_1, \dots, P_k irréductibles deux à deux distincts unitaires, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.
Alors $\lambda = \text{cd } A$, P_1, \dots, P_k sont les diviseurs irréductibles unitaires de A .

Démonstration

Unicité Si A se décompose ainsi sous cette forme $\lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$, avec P_1, \dots, P_k irréductibles deux à deux distincts unitaires, alors

- λ est le coefficient dominant de A .
- Si P est un diviseur unitaire irréductible de A , alors $P | P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ donc P divise l'un des P_i par irréductibilité, et alors, nécessairement, $P = P_i$.
Réciproquement, chaque P_i divise A .
Ainsi, P_1, \dots, P_k sont exactement les diviseurs irréductibles unitaires de A , k en est leur nombre.
- Enfin, $P_1^{\alpha_1} | A$ et $P_1^{\alpha_1+1} \nmid A$, sinon on aurait $P_1 | P_2^{\alpha_2} \cdots P_k^{\alpha_k}$.
En raisonnant de même pour chaque diviseur irréductible unitaire, on obtient pour $1 \leq i \leq k$,
 $\alpha_i = \max \{m \mid P_i^m | A\}$.

Tout cela nous donne l'**unicité de la décomposition (à l'ordre des facteurs près) sous réserve de son existence**.

Existence Par récurrence sur $n = \deg A$.

- Si $n = 0$, il n'y a rien à faire.
- Si, pour un $n \geq 1$, c'est vrai jusqu'au degré $n-1$, soit A est irréductible et il n'y a rien à faire d'autre que de factoriser le coefficient dominant, soit ce n'est pas le cas, et on écrit $A = UV$ avec $\deg U < n$ et $\deg V < n$, on applique deux fois l'hypothèse de récurrence et celle-ci s'établit. ■

Remarque

R37 – On dit que l'anneau $\mathbb{K}[X]$ est factoriel.

Propriété 19 : Irréductibles de $\mathbb{C}[X]$

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

Démonstration

Si P est irréductible et $\deg P \geq 2$, il est non constant et ne peut pas avoir de racine car \mathbb{C} est algébriquement clos (théorème de d'Alembert-Gauß).

Réciproquement les polynômes de degré 1 sont bien irréductibles. ■

5 Irréductibles sur $\mathbb{R}[X]$

Propriété 20 : Racine complexe de polynôme réel

Soit $P \in \mathbb{R}[X]$, alors si $\alpha \in \mathbb{C}$ est racine de P , $\bar{\alpha}$ l'est aussi, de même ordre.



Démonstration

Pour tout $k \in \mathbb{N}$, $P^{(k)}(\bar{\alpha}) = \overline{P^{(k)}(\alpha)}$ car les coefficients sont réels.
Il suffit alors d'appliquer la caractérisation de l'ordre des racines avec les dérivées. ■

Propriété 21 : Irréductibles de $\mathbb{R}[X]$

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle (à discriminant strictement négatif).

Démonstration

Si P est de degré 1, il est irréductible.

Si P est de degré 2 sans racine réelle et si $P = UV$, alors ni U ni V ne peut être de degré 1 sinon P aurait une racine réelle. Donc P est irréductible.

Réciproquement, si P est irréductible et $\deg P \geq 2$, P a une racine complexe par théorème de d'Alembert-Gauß, qui ne peut être réelle sinon P sera réductible. Mais alors $\bar{\alpha}$ est également racine, distincte de α , donc $(X - \alpha)(X - \bar{\alpha}) = X^2 - 2(\Re \alpha)X + |\alpha|^2$ divise P dans $\mathbb{R}[X]$ et comme P est irréductible dans $\mathbb{R}[X]$, $P = \lambda(X^2 - 2(\Re \alpha)X + |\alpha|^2) \in \mathbb{R}[X]$. ■

Remarque

R38 – La décomposition en irréductibles dans \mathbb{C} redonne le fait que tout polynôme à coefficient complexe est constant ou scindé. Elle est de la forme

$$P = \lambda(X - x_1)^{m_1} \cdots (X - x_n)^{m_n}.$$

R39 – Les décompositions en irréductibles dans $\mathbb{R}[X]$ sont donc de la forme

$$P = \lambda(X - x_1)^{m_1} \cdots (X - x_n)^{m_n} (X^2 + a_1X + b_1)^{\ell_1} \cdots (X^2 + a_kX + b_k)^{\ell_k}$$

avec pour tout i , $\Delta_k = a_k^2 - 4b_k < 0$.

R40 – Pour décomposer en irréductibles dans $\mathbb{R}[X]$, on peut décomposer dans $\mathbb{C}[X]$ puis rassembler les $X - \alpha$ et $X - \bar{\alpha}$ si $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

Exemple

E4 – Décomposition en irréductibles de $X^n - 1$.

E5 – Décomposition en irréductibles de $X^4 + 1$.

Propriété 22 : Expression du PGCD en produit d'irréductibles

Si $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \cdots P_k^{\beta_k}$ décompositions en irréductibles (avec exposants éventuellement nuls), alors

$$A \wedge B = P_1^{\min(\alpha_1, \beta_1)} \cdots P_k^{\min(\alpha_k, \beta_k)}.$$



Voir exercice du TD : 19

6 PPCM (Complément)

Définition 13 : PPCM

Le PPCM de deux polynômes A, B non nuls est l'unique générateur unitaire $A \vee B$ de l'idéal $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ des multiples communs à A et à B .

On a donc $A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$.

On peut poser $0 \vee 0 = 0$.

Propriété 23 : du PPCM

- (i) Il s'agit du plus petit multiple unitaire commun à A et à B au sens de la division.
- (ii) Si $A = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \dots P_k^{\beta_k}$ décompositions en irréductibles (avec exposant éventuellement nuls), alors $A \vee B = P_1^{\max(\alpha_1, \beta_1)} \dots P_k^{\max(\alpha_k, \beta_k)}$.
- (iii) On a toujours que AB et $(A \wedge B)(A \vee B)$ sont associés (donc égaux à normalisation près).

V DÉCOMPOSITION EN ÉLÉMENTS SIMPLES

1 Partie entière

Définition – Propriété 1 : Partie entière

Soit $F \in \mathbb{K}(X)$.

On note $\mathbb{K}^-(X) = \{F \in \mathbb{K}(X) \mid \deg F < 0\}$.

Il existe un unique couple $(Q, G) \in \mathbb{K}[X] \times \mathbb{K}^-(X)$ tel que $F = Q + G$. Q est appelé **partie entière** de F .

Démonstration

L'existence provient de la division euclidienne.

Si (Q, G) et (Q_1, G_1) conviennent, $Q_1 - Q = G - G_1 \in \mathbb{K}[X] \cap \mathbb{K}^-(X) = \{0\}$ donc $Q_1 = Q$ puis $G_1 = G$. ■

Remarque

R41 – La partie entière est le quotient de la division euclidienne du numérateur par le dénominateur.

R42 – C'est l'analogue de la partie entière sur \mathbb{Q} .

R43 – Si $\deg F < 0$, alors sa partie entière est nulle.

R44 – Si $F \in \mathbb{K}[X]$, sa partie entière est F elle-même.

R45 – $\mathbb{K}[X]$ et $\mathbb{K}^-(X)$ sont supplémentaires dans $\mathbb{K}(X)$.



2 Décomposition en éléments simples dans $\mathbb{C}(X)$

Théorème 10 : Décomposition en éléments simples dans $\mathbb{C}(X)$

Soit $F \in \mathbb{C}(X)$, $F = \frac{A}{B}$ sous forme irréductible, $\alpha_1, \dots, \alpha_n$ pôles de F d'ordre m_1, \dots, m_n :

$$F = \frac{A}{\prod_{k=1}^n (X - \alpha_k)^{m_k}}$$

et $Q \in \mathbb{C}[X]$ la partie entière de F .

Alors il existe une unique famille $(\lambda_{k,j})_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m_k}}$ de nombres complexes telle que

$$F = \underbrace{Q}_{\text{partie entière}} + \underbrace{\frac{\lambda_{1,1}}{X - \alpha_1} + \dots + \frac{\lambda_{1,m_1}}{(X - \alpha_1)^{m_1}}}_{\text{partie polaire associée à } \alpha_1} + \dots + \underbrace{\frac{\lambda_{n,1}}{X - \alpha_n} + \dots + \frac{\lambda_{n,m_n}}{(X - \alpha_n)^{m_n}}}_{\text{partie polaire associée à } \alpha_n}$$

Démonstration

Admis.

Remarque

R46 – Les $\frac{1}{(X - a)^n}$ pour $a \in \mathbb{C}$ et $n \in \mathbb{N}^*$ forment une base de $\mathbb{C}^-(X)$.

Propriété 24 : Partie polaire relative à un pôle simple

Si α pôle simple de $F = \frac{A}{B}$ sous forme irréductible, $\frac{\lambda}{X - \alpha}$ avec $\lambda \in \mathbb{C}$ la partie polaire associée à α . Alors

$F = \frac{A}{(X - \alpha)B_1}$ avec $B_1(\alpha) \neq 0$ et

$$\lambda = [\widetilde{(X - \alpha)F}](\alpha) = \frac{A(\alpha)}{B_1(\alpha)} = \frac{A(\alpha)}{B'(\alpha)}.$$

Démonstration

- $F = \frac{\lambda}{X - \alpha} + G$ avec G n'admettant pas α comme pôle. Alors $(X - \alpha)F = \lambda + (X - \alpha)G$ puis on évalue en α .
- $B = (X - \alpha)B_1$ donc $B' = B_1 + (X - \alpha)B_1'$ donc $B_1(\alpha) = B'(\alpha)$.

Exemple : Le « cache »

$$E6 - F = \frac{1}{(X - 1)(X + 2)} = \frac{-1/3}{X - 1} + \frac{-1}{X + 2}.$$

Exemple : Très classique

$$E7 - F = \frac{1}{X^n - 1} = \sum_{k=0}^{n-1} \frac{\lambda_k}{X - \omega_k} \text{ avec } \omega_k = e^{\frac{2ik\pi}{n}} \text{ et } \lambda_k = \frac{1}{n\omega_k^{n-1}} = \frac{\omega_k}{n}.$$

$$\text{Ainsi, } F = \frac{1}{X^n - 1} = \sum_{k=0}^{n-1} \frac{\omega_k/n}{X - \omega_k}$$

Propriété 25 : Partie polaire relative à un pôle d'ordre ≥ 2

Si α pôle d'ordre $m \geq 2$ de $F = \frac{A}{B}$ sous forme irréductible,

$$F = \frac{A}{B} = \frac{A}{(X - \alpha)^m B_1} = \frac{\lambda_1}{X - \alpha} + \dots + \frac{\lambda_m}{(X - \alpha)^m} + G$$

où $B_1(\alpha) \neq 0$ et α n'est pas pôle de G .

Alors $\lambda_m = \lim_{X \rightarrow \alpha} [(X - \alpha)^m F](\alpha) = \frac{A(\alpha)}{B_1(\alpha)}$ et $F - \frac{\lambda_m}{(X - \alpha)^m}$ admet α comme pôle d'ordre au plus $m - 1$ ce qui permet de réitérer le processus.



Méthode 1

Les deux propriétés précédentes permettent de trouver les coefficients de la décomposition.

Lorsqu'il reste peu de coefficients à calculer, on peut aussi essayer d'évaluer la fraction rationnelle en des points bien choisis ou utiliser des méthodes d'analyse réelle (limite en ∞ de $x^m F(x)$...)

Penser à exploiter la parité avec l'unicité des coefficients!

Exemple

$$\text{E8 - } F = \frac{2X+1}{X^3 - 2X^2 + X} = \frac{2X+1}{(X-1)^2 X} = 0 + \frac{-1}{X-1} + \frac{3}{(X-1)^2} + \frac{1}{X}$$

$$\text{E9 - } F = \frac{X}{(X^2-1)^2} = \frac{1/4}{(X-1)^2} - \frac{1/4}{(X+1)^2}$$



Voir exercice du TD : 23, 24, 25, 26, 27



3 Décomposition en éléments simples dans $\mathbb{R}(X)$

Théorème 11 : Décomposition en éléments simples dans $\mathbb{R}(X)$

Soit $F \in \mathbb{R}(X)$, $F = \frac{A}{B}$ sous forme irréductible, avec la décomposition de B en facteur irréductibles dans $\mathbb{R} : F = \frac{A}{\prod_{k=1}^p (X - x_k)^{m_k} \prod_{i=1}^r (X^2 + p_i X + q_i)^{n_i}}$ et $Q \in \mathbb{R}[X]$ la partie entière de F .

Alors il existe d'unique familles $(\lambda_{k,j})_{\substack{1 \leq k \leq p \\ 1 \leq j \leq m_k}}$, $(\mu_{i,\ell})_{\substack{1 \leq i \leq r \\ 1 \leq \ell \leq n_i}}$ et $(v_{i,\ell})_{\substack{1 \leq i \leq r \\ 1 \leq \ell \leq n_i}}$ de nombres réels tels que

$$F = \underbrace{Q}_{\text{partie entière}} + \underbrace{\sum_{k=1}^p \left(\sum_{j=1}^{m_k} \frac{\lambda_{k,j}}{(X - x_k)^j} \right)}_{\text{partie polaire associée à } x_k} + \underbrace{\sum_{i=1}^r \left(\sum_{\ell=1}^{n_i} \frac{\mu_{i,\ell} X + v_{i,\ell}}{(X^2 + p_i X + q_i)^\ell} \right)}_{\text{partie polaire associée à } X^2 + p_i X + q_i}.$$

Démonstration

Admis.



Méthode 2

Les méthodes vues dans \mathbb{C} s'appliquent pour les pôles réels. Pour les μ et v , on peut appliquer la méthode « du cache » en α racine complexe de $X^2 + pX + q$.

On peut aussi décomposer dans \mathbb{C} et rassembler les pôles complexes non réels et leur conjugué. L'écriture $F = \bar{F}$ et l'unicité des coefficients donne des relations entre ceux-ci (comme avec la parité).

Remarque

R 47 – Les $\frac{1}{(X-a)^n}$ pour $a \in \mathbb{R}$ et $n \in \mathbb{N}^*$ et les $\frac{1}{(X^2+pX+q)^n}$ et $\frac{X}{(X^2+pX+q)^n}$ pour $p, q \in \mathbb{R}$ tels que $p^2 < 4q$ et $n \in \mathbb{N}^*$ forment une base de $\mathbb{R}^-(X)$.

Exemple

E 10 – $F = \frac{X^3 - 1}{X^3 + X} = 1 - \frac{1}{X} + \frac{X-1}{X^2+1}$ soit directement, en évaluant en i , soit en passant par \mathbb{C} .

E 11 – $F = \frac{X^3}{(X-1)^3(X+2)} = \frac{19/27}{X-1} + \frac{8/9}{(X-1)^2} + \frac{1/3}{(X-1)^3} + \frac{8/27}{X+2}$ de plusieurs façons, dont divisions euclidiennes successives du numérateur de $F - \frac{8/27}{X+2}$ par $X-1$.

E 12 – $F = \frac{2X^2}{(X^2+1)^3} = \frac{2}{(X^2+1)^2} - \frac{2}{(X^2+1)^3}$ en posant $Y = X^2$ ou avec du ± 1 .

4 Décomposition en éléments simples de P'/P

Propriété 26 : Décomposition en éléments simples de P'/P

Soit $P \in \mathbb{K}[X]$ **scindé**, $P = \lambda \prod_{k=1}^p (X - x_k)^{m_k}$. Alors la décomposition en éléments simples de $\frac{P'}{P}$ est donnée par

$$\frac{P'}{P} = \sum_{k=1}^p \frac{m_k}{X - x_k}.$$

Variante : si $P = \lambda \prod_{k=1}^n (X - y_k)$ où les y_k sont les racines **comptées avec multiplicité**, alors

$$\frac{P'}{P} = \sum_{k=1}^n \frac{1}{X - y_k}.$$

Démonstration

Il suffit d'écrire P' directement. ■

Remarque

R 48 – En considérant les ordres, on voit facilement que $\frac{P'}{P}$ n'a que des pôles simples.

Exemple

$$\text{E 13} - \sum_{\omega \in \mathbb{U}_n} \frac{1}{2 - \omega} = \frac{n2^{n-1}}{2^n - 1}.$$



Voir exercice du TD : 28