CHAPITRE VIII

Polynômes

$\mathbb{K}$ 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 $n_{\mathbb{K}} = n \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ si $n \in \mathbb{N}^*$.

I L'ALGÈBRE DES POLYNÔMES

1 Polynômes formels à une indéterminée

Se donner un polynôme à cœfficents dans $\mathbb{K}$, c'est se donner la suite $(a_0, a_1, \ldots, a_d, 0, 0, \ldots)$ de ses cœfficients 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 $(0, \ldots, 0, \underbrace{1}_{k^e}, 0, 0, \ldots)$.

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

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

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

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

Remarques

R 1 – L'indéterminée n'est pas un nombre ! Elle n'a pas de valeur. Elle représente la suite presque nulle $(0, 1, 0, 0, \ldots)$.

R 2 – 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 cœfficients d'un polynôme formel sont uniques.

- Le **polynôme nul** est le polynôme dont tous les cœfficients 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 **cœfficient dominant** de P, noté $\operatorname{cd} P$.
  Si $\operatorname{cd} P = 1$, P est dit **unitaire** ou **normalisé**.
  On pose $\deg 0 = -\infty$.
- On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg P \leqslant n\}$ l'ensemble des polynômes de degré **au plus** n.

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

2 Opérations sur les polynômes

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

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

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

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

- $P \circ Q = P(Q) = \sum\limits_{k \geqslant 0} a_k Q^k$.

Propriété : 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

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

Remarque

En général, on a $\deg(\alpha P + \beta Q) \leqslant \max(\deg P, \deg Q)$.

Propriété : 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

L'isomorphisme d'algèbres trivial $\mathbb{K} \to \mathbb{K}_0[X]$ 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 : Polynôme dérivé

Si $P = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$, on appelle **polynôme dérivé de** P, noté P', le polynôme défini par

$$\begin{aligned} P' &= \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k \\ &= a_1 + 2a_2 X + \dots + n a_n X^{n-1}. \end{aligned}$$

et $0' = 0$.

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

Remarque

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

Propriétés

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* $\deg P \geqslant n$, *$-\infty$ sinon.*
En général, $\deg P^{(n)} \leqslant \deg P - n$.

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

(iii) ***Formule de Leibniz***

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

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

Remarques

R 1 – $P^{(n)} = 0$ si $n \geqslant \deg P + 1$ et si $d = \deg P$, $P^{(d)} = d! \operatorname{cd} P$.

R 2 – $\deg P = \min\left\{n \in \mathbb{N} \mid P^{(n)} = 0\right\} - 1$ si $P \neq 0$.

R 3 – Si $n \in \mathbb{N}$,

$$\left((X-a)^k\right)^{(n)} = \begin{cases} 0 & \text{si } n \geqslant k+1 \\ k! & \text{si } n = k \\ k(k-1)\cdots(k-n+1)(X-a)^{k-n} = \dfrac{k!}{(k-n)!}(X-a)^{k-n} & \text{sinon.} \end{cases}$$

R 4 – Si $P = \sum_{k=0}^{d} a_k X^k$, alors pour tout $n \in \mathbb{N}$, $P^{(n)} \begin{cases} 0 & \text{si } n \geqslant d+1 \\ d!a_d & \text{si } n = d \\ \sum_{k=n}^{d} k(k-1)\cdots(k-n+1)a_k X^{k-n} & \text{sinon.} \end{cases}$

II FONCTIONS POLYNOMIALES, RACINES

1 Fonctions polynomiales

Définition : Fonction polynôme associée

Si $P = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$, on note $\tilde{P} : \left| \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \tilde{P}(x) = \sum_{k\geqslant 0} a_k x^k \end{array}\right.$ appelée **fonction polynomiale associée à** P.

Remarques

R 1 – 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 $\tilde{P}(x)$.

R 2 – 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.

R 3 – Si $P, Q \in \mathbb{K}[X]$, $P \circ Q = \tilde{P}(Q)$ (on applique la fonction polynomiale à un polynôme au lieu d'un élément de $\mathbb{K}$.)

Propriétés : 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 $\tilde{P}' = \widetilde{P'}$.

Remarque

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 : Formule de Taylor

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. $P(X) = \sum_{n\geqslant 0} \dfrac{\tilde{P}^{(n)}(a)}{n!}(X-a)^n$ *c'est-à-dire* $P(X+a) = \sum_{n\geqslant 0} \dfrac{\tilde{P}^{(n)}(a)}{n!}X^n$.

Corollaire : Formule de Mac Laurin

$P = \sum_{n\geqslant 0} \dfrac{\tilde{P}^{(n)}(0)}{n!}X^n$ *c'est-à-dire les cœfficients de P sont les* $a_n = \dfrac{\tilde{P}^{(n)}(0)}{n!}$.

3 Racines

Définition : Racine

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

Remarques

R 1 – Cela dépend du corps $\mathbb{K}$.

R 2 – Un polynôme réel de degré impair a toujours une racine réelle (conséquence du théorème des valeurs intermédiaires.)

Propriétés : 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

Si $P|Q$, toute racine de P est racine de Q. La réciproque est fausse en général.

Corollaire : 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 : 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

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 !).

Définition : 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

$$m = \max\left\{k \in \mathbb{N}\ ;\ (X-a)^k \middle| P\right\}$$

Ainsi, a est racine d'ordre m si et seulement si $(X-a)^m \big| P$ et $(X-a)^{m+1} \not\big| P$ 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 $m \geqslant 1$, 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 $m \geqslant 2$, a est racine multiple de P.

Remarques

R 1 – Si $(X-a)^n \Big| P$ alors a est racine de P d'ordre **au moins** n.

R 2 – L'ordre est toujours au plus égal au degré du polynôme.

Propriété

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

Propriété : 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 $\forall\, k\in[\![0,m-1]\!]$, $\tilde{P}^{(k)}(a)=0$ et $\tilde{P}^{(m)}(a)\neq 0$.

Exercice : 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 $\left(1, X-a, (X-a)^2, \cdots, (X-a)^n\right)$.
   (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 $\forall k\in[\![0,r-1]\!]$, $P^{(k)}(a)=0$.
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

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

Exemple

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

Exercice

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

4 Polynômes scindés

Définition : 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 $\deg P\geqslant 1$, $\lambda=\operatorname{cd}P$, $x_1,\dots,x_p$ sont les racines de P deux à deux distinctes de multiplicités respectives $m_1,\dots,m_p$.

Remarque

⚠ Scindé sur $\mathbb{C}$ $\not\Longleftrightarrow$ 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 : 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 $m_1+\dots+m_p=\deg P$.

Théorème : Théorème de d'Alembert-Gauß(Thm. fondam. de l'alg.)

Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.
On dit que le corps $\mathbb{C}$ est ***algébriquement clos****.*

Corollaire

Tout polynôme à cœfficients complexes non constant est scindé.

Corollaire

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

C'est donc toujours vrai dans $\mathbb{C}$.

5 Relations cœfficients-racines

Définition : 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

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{n} x_i = x_1+x_2+\dots+x_n. && (n \text{ termes})\\
\sigma_2 &= \sum_{1\leqslant i_1<i_2\leqslant n} x_{i_1}x_{i_2} && (\frac{n(n-1)}{2} \text{ termes})\\
&= x_1x_2+x_1x_3+\dots+x_1x_n+\dots+x_{n-1}x_n.\\
&\vdots\\
\sigma_k &= \sum_{1\leqslant i_1<i_2<\dots<i_k\leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k}. && (\binom{n}{k} \text{ termes})\\
&\vdots\\
\sigma_n &= x_1x_2\cdots x_n. && (1 \text{ terme})
\end{aligned}$$

Exemple

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

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

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

Propriété : Relations cœfficients-racines

*Soient $n \in \mathbb{N}^*$, $a_0, \cdots, a_n \in \mathbb{K}$ tel que $a_n \neq 0$, $P = a_0 + \cdots + a_n X^n$, **scindé** sur $\mathbb{K}$, $x_1, \ldots, x_n$ 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 $x_1, \ldots, x_n$,*

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

Ainsi,

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

Remarques

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

R 2 – 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.

III INTERPOLATION DE LAGRANGE

- **Problématique** : Étant donné $n \in \mathbb{N}$, $n+1$ scalaires $x_0, \ldots, x_n \in \mathbb{K}$ deux à deux distincts, et $y_0, \ldots, y_n \in \mathbb{K}$ 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

  $$\forall\, k \in [\![0, n]\!], \quad P(x_k) = y_k.$$

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

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

  L'application $u : \left|\begin{array}{ccc} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}^{n+1} \\ P & \longmapsto & (P(x_k))_{k \in [\![0,n]\!]} \end{array}\right.$ 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 $x_0, \ldots, x_n$, 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 $x_0, \ldots, x_n$.
  L'unique solution au problème est donc, par linéarité,

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

  On cherche donc le polynôme $L_i = u^{-1}\Big(0, \ldots, \underbrace{1}_{i^{\text{e}}}, \ldots, 0\Big)$ 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 : 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 : 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 $P = \sum_{i=0}^{n} y_i \cdot Li$.

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

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 : CCINP 87

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

1. Montrer que si $b_0, b_1, \cdots, b_n$ sont $n+1$ réels quelconques, alors il existe un unique polynôme P vérifiant $\deg P \leqslant n$ et $\forall i \in \{0, \cdots, n\}$ $P(a_i) = b_i$.
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 : 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 $\Phi : \begin{array}{ccc} \mathbb{K}_2[X] & \longrightarrow & \mathbb{K}^3 \\ P & \longmapsto & \big(P(a_1), P(a_2), P(a_3)\big) \end{array}$ est un isomorphisme d'espaces vectoriels.
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 $\mathbb{K}[X]$

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

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

Démonstration

- La structure d'anneau commutatif a été vue en classe de MPSI.
  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 $P=\lambda\neq 0$, $P^{-1}=\lambda^{-1}=\dfrac{1}{\lambda}$.
- Si $PQ=0$ alors $\deg(PQ)=\deg P+\deg Q=-\infty$ donc $\deg P=-\infty$ ou $\deg Q=-\infty$, d'où l'intégrité. □

Corollaire

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 : 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

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.

Exemple

Poser une division quelconque.

Démonstration

- **Existence** : Soit $d=\deg B$, $B=b_0+\cdots+b_dX^d$ avec $b_d\neq 0$. Si $d=0$, le couple $(A/b_0,0)$ convient. Sinon, on raisonne par récurrence forte sur $n=\deg A$, $A=a_0+\cdots+a_nX^n$.
  - ⋆ Si $n<d$, $(0,A)$ convient.
  - ⋆ Si le résultat est vrai pour tout polynôme de degré au plus $n-1$, alors on écrit $A=\dfrac{a_n}{b_d}X^{n-d}B+A_1$ avec $\deg A_1\leqslant n-1$.
    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 $\left(Q_1+\dfrac{a_n}{b_d}X^{n-d},R\right)$ 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

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

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 $R = P - P_0 Q \in I$ et $\deg R < \min E$ donc $R = 0$ et $P = P_0 Q \in (P_0)$. □

Remarque

Les idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$ sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés.

Donc dans le cas d'un idéal non nul, quitte à choisir un générateur positif (dans $\mathbb{Z}$) ou unitaire (dans $\mathbb{K}[X]$) on a de plus unicité de celui-ci.

2 PGCD de deux polynômes

Définition : PGCD

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

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

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

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 : 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 : Caractérisation

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

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

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

Démonstration

($\Longrightarrow$) Si $D = A \wedge B$ alors D est unitaire et $AK[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ donc $A, B \in D\mathbb{K}[X]$ 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 $AU + BV = A \wedge B$, $C | A \wedge B$.

($\Longleftarrow$) 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. □

Remarques

R 1 – Les diviseurs de D sont alors exactement les diviseurs communs à A et à B.

R 2 – Les racines des pgcd sont exactement les racines communes de A et B, de multiplicité le minimum des multiplicités.

Exercice

Soit $A = X^5 - X^4 + 2X^3 + 1$ et $B = X^4 - X^3 + 3X^2 - 2X + 2$.

1. À l'aide de l'algorithme d'Euclide, déterminer $D = A \wedge B$.
2. En déduire $(U, V) \in \mathbb{R}[X]^2$ tel que $AU + BV = D$.

Définition : Nombre entiers 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

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

Théorème : de Bézout

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

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

Démonstration

($\Longrightarrow$) Connu

($\Longleftarrow$) 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

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

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

Démonstration

□

Théorème : 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 : 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

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

Démonstration

- $(\Longrightarrow)$: Pas de facteur $(X-a)$ commun.
- $(\Longleftarrow)$: 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 : pgcd de n polynômes

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

Remarques

R 1 – Comme pour deux polynômes, il s'agit du plus grand diviseur commun unitaire au sens de la division (et aussi du degré).

R 2 – La définition s'étend à $0 \wedge \cdots \wedge 0 = 0$.

Propriété

(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 $A_1U_1 + \cdots A_nU_n = \bigwedge_{k=1}^{n} A_k$.*

Définition : 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 $\forall\, i \neq j,\quad A_i \wedge A_j = 1$.

Propriété

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

Théorème : 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 $A_1U_1+\cdots+A_nU_n = 1$.

Propriété

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

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 : 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 $P = UV \Longrightarrow U \text{ ou } V$ inversible.

Les autres polynômes sont dits **réductibles**.

Remarques

R 1 – Si P est irréductible dans $\mathbb{K}$ et $\deg P \geqslant 2$, P n'a pas de racine dans $\mathbb{K}$. La réciproque est fausse.

R 2 – P est réductible dans $\mathbb{K}[X]$ ss'il admet un diviseur Q tel que $0 < \deg Q < \deg P$.

Propriété

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) $P|A_1 \cdots A_n \Longleftrightarrow \exists i$ 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 $\Longleftarrow$ 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 : 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 $\lambda = \mathrm{cd}\, A$, $P_1, \dots, P_k$ 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 cœfficient 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 $1 \leqslant i \leqslant k$, $\alpha_i = \max\left\{m \mid P_i^m|A\right\}$.

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 $n \geqslant 1$, 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 cœfficient 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

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

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

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

Démonstration

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

Réciproquement les polynômes de degré 1 sont bien irréductibles. $\square$

5 Irréductibles sur $\mathbb{R}[X]$

Propriété

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

Démonstration

Pour tout $k \in \mathbb{N}$, $P^{(k)}\left(\overline{\alpha}\right) = \overline{P^{(k)}(\alpha)}$ car les cœfficients sont réels.

Il suffit alors d'application la caractérisation de l'ordre des racines avec les dérivées. $\square$

Propriété : 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 $\deg P \geqslant 2$, P a une racine complexe par théorème de d'Alembert-GauSS, qui ne peut être réelle sinon P sera réductible. Mais alors $\overline{\alpha}$ est également racine, distincte de α, donc $(X-\alpha)\left(X-\overline{\alpha}\right) = X^2 - 2(\mathfrak{Re}\,\alpha)X + |\alpha|^2$ divise P dans $\mathbb{R}[X]$ et comme P est irréductible dans $\mathbb{R}[X]$, $P = \lambda\left(X^2 - 2(\mathfrak{Re}\,\alpha)X + |\alpha|^2\right) \in \mathbb{R}[X]$. $\square$

Remarques

R 1 – La décomposition en irréductibles dans $\mathbb{C}$ redonne le fait que tout polynôme à cœfficient complexe est constant ou scindé. Elle est de la forme

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

R 2 – Les décompositions en irréductibles dans $\mathbb{R}[X]$ sont donc de la forme

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

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

R 3 – Pour décomposer en irréductibles dans $\mathbb{R}[X]$, on peut décomposer dans $\mathbb{C}[X]$ puis rassembler les $X-\alpha$ et $X-\overline{\alpha}$ si $\alpha \in \mathbb{C}\setminus\mathbb{R}$.

Exemples

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

E 2 – Décomposition en irréductibles de $X^4 + 1$.

Propriété

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

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

6 PPCM (Complément)

Définition : 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

(i) Il s'agit du plus petit multiple unitaire commun à A et à B au sens de la division.

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

(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

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 $G_1 = G$. □

Remarques

R 1 – La partie entière est le quotient de la division euclidienne du numérateur par la dénominateur.

R 2 – C'est l'analogue de la partie entière sur $\mathbb{Q}$.

R 3 – Si $\deg F < 0$, alors sa partie entière est nulle.

R 4 – Si $F \in \mathbb{K}[X]$, sa partie entière est F elle-même.

R 5 – $\mathbb{K}[X]$ et $\mathbb{K}^-(X)$ sont supplémentaires dans $\mathbb{K}(X)$.

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

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

Soit $F \in \mathbb{C}(X)$, $F = \dfrac{A}{B}$ sous forme irréductible, $\alpha_1, \ldots, \alpha_n$ pôles de F d'ordre $m_1, \ldots, m_n$: $F = \dfrac{A}{\prod_{k=1}^{n} (X - \alpha_k)^{m_k}}$ et $Q \in \mathbb{C}[X]$ la partie entière de F.

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

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

Démonstration

Admis. □

Remarque

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

Propriété : Partie polaire relative à un pôle simple

Si α pôle simple de $F = \dfrac{A}{B}$ sous forme irréductible, $\dfrac{\lambda}{X-\alpha}$ avec $\lambda \in \mathbb{C}$ la partie polaire associée à α. Alors $F = \dfrac{A}{(X-\alpha)B_1}$ 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 $B_1(\alpha) = B'(\alpha)$.

□

Exemples : Le « cache »

E 1 – $F = \dfrac{1}{(X-1)(X+2)} = \dfrac{1/3}{X-1} + \dfrac{-1/3}{X+2}$.

E 2 – *Très classique* : $F = \dfrac{1}{X^n - 1} = \displaystyle\sum_{k=0}^{n-1} \frac{\lambda_k}{X-\omega_k}$ avec, en utilisant la deuxième formule, $\omega_k = \mathrm{e}^{\frac{2ik\pi}{n}}$ et $\lambda_k = \dfrac{1}{n\omega_k^{n-1}} = \dfrac{\omega_k}{n}$.

Propriété : Partie polaire relative à un pôle d'ordre $\geqslant 2$

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

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

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

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

Remarque

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

Exemple

$F = \dfrac{2X+1}{X^3 - 2X^2 + X} = \dfrac{2X+1}{(X-1)^2 X} = 0 + \dfrac{a}{X-1} + \dfrac{3}{(X-1)^2} + \dfrac{b}{X}$.

Évaluation en 2 : $\dfrac{5}{2} = a + 3 + \dfrac{b}{2}$ et limite de $xF(x)$ en $+\infty$: $0 = a + b$ d'où $a = -1$ et $b = 1$.

Remarque

Exploiter la parité !

Exemple

$F = \dfrac{X}{(X^2-1)^2} = \dfrac{a}{(X-1)^2} + \dfrac{b}{X-1} + \dfrac{c}{(X+1)^2} + \dfrac{d}{X+1} = \dfrac{1/4}{(X-1)^2} - \dfrac{1/4}{(X+1)^2}$ car $F(X) = -F(-X)$ donc par unicité, $b = d$ et $c = -a$ avec $a = \dfrac{1}{4}$ par le « cache », et $xF(x) \xrightarrow[x\to+\infty]{} 0 = b + d = 2b$ donc $b = d = 0$.

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

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

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

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

$$F = \underbrace{Q}_{\text{partie entière}} + \sum_{k=1}^{p} \underbrace{\left(\sum_{j=1}^{m_k} \overbrace{\frac{\lambda_{k,j}}{(X-x_k)^j}}^{\substack{\text{élément simple}\\ \text{de 1}^{\text{e}}\text{ espèce}}}\right)}_{\text{partie polaire associée à } x_k} + \sum_{i=1}^{r} \underbrace{\left(\sum_{\ell=1}^{n_i} \overbrace{\frac{\mu_{i,\ell}X+\nu_{i,\ell}}{\left(X^2+p_iX+q_i\right)^{\ell}}}^{\substack{\text{élément simple}\\ \text{de 2}^{\text{e}}\text{ espèce}}}\right)}_{\text{partie polaire associée à } X^2+p_iX+q_i}.$$

Démonstration

Admis. □

Remarques

R 1 – 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 $\mathbb{R}^-(X)$.

R 2 – Les méthode vues dans $\mathbb{C}$ s'appliquent pour les pôles réels. Pour les μ et ν, 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 $F = \overline{F}$ et l'unicité des cœfficients donne des relations entre ceux-ci (comme avec la parité).

Exemples

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

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

4 Décomposition en éléments simples de P'/P

Propriété : 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 $\dfrac{P'}{P}$ est donnée par* $\dfrac{P'}{P} = \sum_{k=1}^{p}\dfrac{m_k}{X-x_k}$.

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

Démonstration

Il suffit d'écrire P' directement. $\square$

Remarque

En considérant les multiplicités, on voit facilement que $\dfrac{P'}{P}$ n'a que des pôles simples.

Exemple

$\displaystyle\sum_{\omega\in\mathbb{U}_n} \frac{1}{2-\omega} = \frac{n2^{n-1}}{2^n-1}$ avec $P = X^n - 1$.