Polynômes

Extrait du programme officiel :

L'objectif de ce chapitre est d'étudier les propriétés de base de ces objets formels et de les exploiter pour la résolution de problèmes portant sur les équations algébriques et les fonctions numériques.

L'arithmétique de $\mathbb{K}[X]$ est développée selon le plan déjà utilisé pour l'arithmétique de $\mathbb{Z}$, ce qui autorise un exposé allégé. D'autre part, le programme se limite au cas où le corps de base $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Anneau des polynômes à une indéterminée	
Anneau $\mathbb{K}[X]$.	La construction de $\mathbb{K}[X]$ n'est pas exigible. Notations $\sum_{i=0}^{d} a_i X^i$, $\sum_{i=0}^{+\infty} a_i X^i$.
Degré, coefficient dominant, polynôme unitaire.	Le degré du polynôme nul est $-\infty$. Ensemble $\mathbb{K}_n[X]$ des polynômes de degré au plus n.
Degré d'une somme, d'un produit.	Le produit de deux polynômes non nuls est non nul.
Composition.	⇆ I : représentation informatique d'un polynôme ; somme, produit.
b) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{K}[X]$, diviseurs, multiples.	Caractérisation des couples de polynômes associés.
Théorème de la division euclidienne.	⇆ I : algorithme de la division euclidienne.
c) Fonctions polynomiales et racines	
Fonction polynomiale associée à un polynôme.	
Racine (ou zéro) d'un polynôme, caractérisation en termes de divisibilité.	
Le nombre de racines d'un polynôme non nul est majoré par son degré.	Détermination d'un polynôme par la fonction polynomiale associée.
Multiplicité d'une racine.	Si $P(\lambda) \neq 0$, λ est racine de P de multiplicité 0.
Polynôme scindé. Relations entre coefficients et racines.	Aucune connaissance spécifique sur le calcul des fonctions symétriques des racines n'est exigible.
d) Dérivation	
Dérivée formelle d'un polynôme.	Pour $\mathbb{K} = \mathbb{R}$, lien avec la dérivée de la fonction polynomiale associée.

CONTENUS	CAPACITÉS & COMMENTAIRES
Opérations sur les polynômes dérivés : combinaison linéaire, produit. Formule de Leibniz.	
Formule de Taylor polynomiale.	
Caractérisation de la multiplicité d'une racine par les polynômes dérivés successifs.	

e) Arithmétique dans $\mathbb{K}[X]$

PGCD de deux polynômes dont l'un au moins est non nul.	Tout diviseur commun à A et B de degré maximal est appelé un PGCD de A et B.
Algorithme d'Euclide.	L'ensemble des diviseurs communs à A et B est égal à l'ensemble des diviseurs d'un de leurs PGCD. Tous les PGCD de A et B sont associés ; un seul est unitaire. On le note $A \wedge B$.
Relation de Bézout.	L'algorithme d'Euclide fournit une relation de Bézout. $\leftrightarrows$ I : algorithme d'Euclide étendu. L'étude des idéaux de $\mathbb{K}[X]$ est hors programme.
PPCM.	Notation $A \vee B$. Lien avec le PGCD.
Couple de polynômes premiers entre eux. Théorème de Bézout. Lemme de Gauss.	
PGCD d'un nombre fini de polynômes, relation de Bézout. Polynômes premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	

f) Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème de d'Alembert-Gauss.	La démonstration est hors programme.
Polynômes irréductibles de $\mathbb{C}[X]$. Théorème de décomposition en facteurs irréductibles dans $\mathbb{C}[X]$.	Caractérisation de la divisibilité dans $\mathbb{C}[X]$ à l'aide des racines et des multiplicités. Factorisation de $X^n - 1$ dans $\mathbb{C}[X]$.
Polynômes irréductibles de $\mathbb{R}[X]$. Théorème de décomposition en facteurs irréductibles dans $\mathbb{R}[X]$.	

g) Formule d'interpolation de Lagrange

Si $x_1, \dots, x_n$ sont des éléments distincts de $\mathbb{K}$ et $y_1, \dots, y_n$ des éléments de $\mathbb{K}$, il existe un et un seul $P \in \mathbb{K}_{n-1}[X]$ tel que pour tout i : $P(x_i) = y_i$.	Expression de P. Description des polynômes Q tels que pour tout i : $Q(x_i) = y_i$.

Table des matières

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$ (voire éventuellement $\mathbb{Q}$. 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 $n \in \mathbb{N}^*$ convient.)

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** et on note

$$\mathbb{K}^{(\mathbb{N})} = \left\{(a_n)_n \ ; \ \exists\, d \in \mathbb{N}, \quad \forall\, n > d, \quad a_n = 0\right\}$$

l'ensemble des suites presque nulles.

On note alors, pour tout $k \in \mathbb{N}$, X^k la suite presque nulle

$$\left(\delta_{n,k}\right)_{n\in\mathbb{N}} = (0, \ldots, 0, \underbrace{1}_{k^{\text{e}}}, 0, 0, \ldots)$$

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

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

Définition : Polynôme

Étant donné une suite presque nulle $(a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$ d'éléments de $\mathbb{K}$, on appelle **polynôme à une indéterminée** associé à $(a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$

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

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

R1 – L'indéterminée n'est pas un nombre ! Elle n'a pas de valeur. Elle représente la suite presque nulle $(0, 1, 0, 0, \ldots)$.

R2 – Par définition, $P = \sum a_k X^k = Q = \sum b_k X^k \iff \forall\, k, \quad a_k = b_k$ (égalité de deux suites). Les cœfficients d'un polynôme formel sont uniques.

Définition

(i) Le **polynôme nul** est le polynôme dont tous les cœfficients sont nuls, noté $0_{\mathbb{K}[X]}$ ou plus simplement 0.

(ii) On appelle monôme tout polynôme de la forme aX^k avec $k \in \mathbb{N}$ et $a \neq 0$.

(iii) On appelle **polynôme constant** tout polynôme $P = a$ où $a \in \mathbb{K}$.

(iv) 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 $\mathrm{cd}\, P$.
Si $\mathrm{cd}\, P = 1$, P est dit **unitaire** ou **normalisé**.
On pose $\deg 0 = -\infty$.

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

Remarque

On définit aussi la **valuation** de P comme étant le degré minimum dans P.

2 L'anneau des polynômes

Définition : Lois $+$, $\times$ et $\cdot$

Soient $P = \sum_{k\geqslant 0} a_k X^k$, $Q = \sum_{k\geqslant 0} b_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

On définit les lois $+$, $\times$ et $\cdot$ par

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

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

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

Remarques

R 1 – Pour le produit, si $p = \deg P$ et $q = \deg Q$, $0 \leqslant m \leqslant p+q$ et $a_k b_{m-k} = 0$ si $k > p$ ou $k < m - q$, donc $c_m = \sum_{k=m-q}^{p} a_k b_{m-k} = \sum_{\ell=m-p}^{q} a_{m-\ell} b_\ell$. On a même plus précisément $c_m = \sum_{k=\max(0,m-q)}^{\min(p,m)} a_k b_{m-k}$.

R 2 – On reconnaît l'addition $u + v$ de deux suites (terme à terme) et le produit externe $\lambda \cdot u$.

Quid de la multiplication ? La formule repose sur la sommation par diagonales et donc sur le fait que $X^p \times X^q = X^{p+q}$. Mais est-ce bien le cas ?

Soient $P = X^p$ et $Q = X^q$. Alors pour tout k, $a_k = \delta_{p,k}$ et $b_k = \delta_{q,k}$.

Par définition, $P \times Q = \sum_{m \geqslant 0} c_m X^m$ où $c_m = \sum_{k+\ell=m} a_k b_\ell = \sum_{k+\ell=m} \delta_{p,k}\delta_{q,\ell}$.

Or $\delta_{p,k}\delta_{q,\ell} = 0$ si $k \neq p$ et $\ell \neq q$. Donc $c_m = 0$ si $m \neq p+q$ et $c_{p+q} = 1 \times 1 = 1$. Donc $X^p \times X^q = X^{p+q}$. Ouf.

En particulier, pour tout k, $X^k = (X)^k = \underbrace{X \times \cdots \times X}_{k \text{ fois}}$. Ouf.

R 3 – On peut donc écrire des algorithmes de calculs de somme, de produits de polynômes, par exemple stockés sous forme de liste. Essayez !

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* $\operatorname{cd}(PQ) = \operatorname{cd} P \operatorname{cd} Q$.

Remarque

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

Démonstration

C'est immédiat si $P = 0$ ou $Q = 0$.

On suppose donc que $P \neq 0$ et $Q \neq 0$.

On peut donc écrire $P = a_0 + \cdots + a_p X^p$ et $Q = b_0 + \cdots + b_q X^q$ avec $a_p \neq 0$ et $b_q \neq 0$.

- Si $k > \deg P = p$ et $k > \deg Q = q$, alors $a_k + b_k = 0$. Donc $P+Q$ est bien un polynôme et $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$.
  - ⋆ Si $\deg P = p \neq \deg Q = p$, par exemple $p > q$, alors par définition
  $$P + Q = (a_0 + b_0) + \cdots + (a_q + b_q)X^q + a_{q+1}X^{q+1} + \cdots + a_p X^p$$
  avec $a_p = \operatorname{cd} P \neq 0$ donc $\deg(P+Q) = \deg P$ et $\operatorname{cd}(P+Q) = \operatorname{cd} P$.
  - ⋆ Si $\deg P = \deg Q = p$, $P + Q = (a_0 + b_0) + \cdots + (a_p + b_p)X^p$ donc
    - soit $a_p + bp = \operatorname{cd} P + \operatorname{cd} Q \neq 0$ et alors $\deg(P+Q) = \deg P = \deg Q$ et $\operatorname{cd}(P+Q) = \operatorname{cd} P + \operatorname{cd} Q$,
    - soit $a_p + bp = \operatorname{cd} P + \operatorname{cd} Q = 0$ et alors $\deg(P+Q) < \deg P = \deg Q$.
- $\lambda P = \lambda a_0 + \cdots + (\lambda a_p)X^p$ donc si $\lambda \neq 0$, $\lambda a_p = \lambda \operatorname{cd} P \neq 0$, donc $\deg(\lambda P) = \deg P$ et $\operatorname{cd}(\lambda P) = \lambda \operatorname{cd} P$.
- Si $m > \deg P + \deg Q = p + q$, $c_m = \sum_{k+\ell=m} a_k b_\ell$ avec $k + \ell = m > p + q$ donc on n'a pas $k \leqslant p$ et $\ell \leqslant q$, donc $a_k = 0$ ou $b_\ell = 0$, donc $c_m = 0$.
  Donc PQ est un polynôme de degré au plus $p + q = \deg P + \deg Q$. Or si $m = p+q$, $k + \ell = p + q$ avec $k \leqslant p$ et $\ell \leqslant q$ équivaut à $k = p$ et $\ell = q$, donc $c_{p+q} = a_p b_q = \operatorname{cd} P \operatorname{cd} Q \neq 0$.
  Donc $\deg(PQ) = \deg P + \deg Q$ et $\operatorname{cd}(PQ) = \operatorname{cd} P \operatorname{cd} Q$. □

Remarque

Pour le produit, on a envie d'écrire

$$PQ = \left(a_0 + \cdots + a_p X^p\right)\left(b_0 + \cdots + b_q X^q\right) = \underbrace{a_0 b_0 + \cdots +}_{\text{pas de terme en } X^{p+q}} a_p b_q X^{p+q}$$

Mais a-t-on le droit ? On sait déjà que $X^p \times X^q = X^{p+q}$, il manque de l'associativité, de la distributivité...

Propriété : Structure d'anneau commutatif intègre

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif 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.)

Démonstration

- Les associativités, les commutativités, la distributivité sont de simples vérifications en utilisant la définition de somme et produit de polynômes.
  Par exemple, si $P = \sum a_k X^k$, $Q = \sum b_k X^k$ et $R = \sum c_k X^k$, alors $P(Q+R) = \sum d_m X^m$ où $d_m = \sum_{k+\ell=m} a_k(b_\ell + c_\ell) = \sum_{k+\ell=m} a_k b_\ell + \sum_{k+\ell=m} a_k c_\ell$ avec les propriétés habituelles de $+$ et $\times$ sur $\mathbb{K}$, donc $P(Q+R) = PQ + PR$.

- L'élément neutre pour $+$ est le polynôme nul, celui pour $\times$ est le polynôme constant 1 (par distributivité,

  $$\left(a_0 + \cdots + a_n X^n\right) \times 1 = a_0(X^0 \times X^0) + \cdots + a_n(X^n \times X^0) = a_0 + \cdots + a_n X^n$$

  d'après la remarque faite précédemment.)

- L'opposé d'un polynôme P est le polynôme $-P = -1 \cdot P$ (On vérifie que $P + (-P) = -P + P = 0_{\mathbb{K}[X]}$.)

- 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.

□

Remarques

R1 – On peut donc manipuler les polynômes « comme des sommes d'éléments de $\mathbb{K}$ ».

R2 – L'isomorphisme d'anneau 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 Composition

Définition : Composée

Soit $P = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$.

On définit le **polynôme composé** $P \circ Q = P(Q) = \sum_{k\geqslant 0} a_k Q^k \in \mathbb{K}[X]$.

On parle aussi de **substitution**.

Remarques

R1 – Ne pas dire « On pose $X = Q$ », cela n'a aucun sens !

R2 – Cela correspond à la notion de composée de fonction habituelle.

R3 – Le loi $\circ$ sur $\mathbb{K}[X]$ n'est pas commutative. Par exemple,

$$X^2 \circ (X+1) = (X+1)^2 \neq X^2 + 1 = (X+1) \circ (X^2).$$

R4 – Elle admet un élément neutre : $P = X$ (qui correspond à l'identité).

R5 – Elle est distributive sur $+$ à droite mais pas à gauche : $(P+Q) \circ R = P \circ R + Q \circ R$ mais $X^2 \circ (1+1) = 4 \neq 1 = X^2 \circ 1 + X^2 \circ 1$.

Propriété : Degré d'une composée

Soient $P, Q \in \mathbb{K}[X]$, avec Q ***non constant****. Alors* $\deg(P(Q)) = \deg P \deg Q$.

Remarque

Si Q est constant, $P(Q)$ l'est aussi.

Démonstration

Si $P = a_0 + \cdots + a_p X^p$ et $Q = b_0 + \cdots + b_q X^q$ avec $b_q \neq 0$ et $a_p \neq 0$, alors $P(Q) = b_0 + b_1 Q + \cdots + a_p Q^p$.
Donc $\deg(P(Q)) \leqslant \max(\deg Q, \ldots, \deg Q^p) = p \deg Q = \deg P \times \deg Q$.
Or le seul terme de degré $\deg P \times \deg Q$ dans $P(Q)$ est dans $a_p \left(b_0 + \cdots + b_q X^q\right)^p$ (car $\deg Q > 0$) et vaut $a_p b_q^p X^{p+q}$ avec $a_p b_q^q \neq 0$.
Donc $\deg(P(Q)) = \deg P \deg Q$ et $\mathrm{cd}(P(Q)) = \mathrm{cd}\, P \times (\mathrm{cd}\, Q)^{\deg P}$. □

Exemple

Les polynômes $P \in \mathbb{K}[X]$ tels que $P\left(X^2\right) = \left(X^2+1\right) P$ sont les $a(X^2-1)$ avec $a \in \mathbb{K}$.

4 Dérivation formelle

Définition : Polynôme dérivé

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

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

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,* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

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

Remarques

R1 – $P^{(n)} = 0$ si $n \geqslant \deg P + 1$ et si $d = \deg P$, $P^{(d)} = d! \operatorname{cd} P$.

R2 – $\deg P = \min\left\{n \in \mathbb{N} \mid P^{(n)} = 0\right\} - 1$ si $P \neq 0$.

R3 – Si $n \in \mathbb{N}$, $\left((X-a)^k\right)^{(n)} = \begin{cases} 0 & \text{si } n \geqslant k+1 \\ k! & \text{si } n = k \\ k(k-1)\cdots(k-n+1)(X-a)^{k-n} = \dfrac{k!}{(k-n)!}(X-a)^{k-n} & \text{sinon.} \end{cases}$

R4 – Si $P = \sum_{k=0}^{d} a_k X^k$, alors pour tout $n \in \mathbb{N}$, $P^{(n)} \begin{cases} 0 & \text{si } n \geqslant d+1 \\ d! a_d & \text{si } n = d \\ \sum_{k=n}^{d} k(k-1)\cdots(k-n+1) a_k X^{k-n} & \text{sinon.} \end{cases}$

Démonstration

(i) Facile puis récurrence.

(ii) Il suffit de l'écrire.

(iii)

$$(PQ)' = \left(\sum_{k\in\mathbb{N}} a_k X^k \sum_{\ell\in\mathbb{N}} b_\ell X^\ell\right)' = \left(\sum_{k,\ell\in\mathbb{N}} a_k b_\ell X^{k+\ell}\right)' = \sum_{(k,\ell)\neq\{(0,0)\}} (k+\ell) a_k b_\ell X^{k+\ell-1}$$
$$= \sum_{k\in\mathbb{N}^*} k a_k X^{k-1} \sum_{\ell\in\mathbb{N}} b_\ell X^\ell + \sum_{k\in\mathbb{N}} a_k X^k \sum_{\ell\in\mathbb{N}^*} \ell b_\ell X^{\ell-1} = P'Q + PQ'.$$

Pour la formule de Leibniz : comme pour les fonctions.

(iv) $(P\circ Q)' = \sum_{k\in\mathbb{N}} a_k \left(Q^k\right)'$. Il suffit de démontrer, par récurrence (facile), que $(Q^n)' = nQ'Q^{n-1}$.

□

II DIVISIBILITÉ ET DIVISION EUCLIDIENNE

1 Division euclidienne

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

deg joue dans $\mathbb{K}[X]$ le même rôle que $|\cdot|$ dans $\mathbb{Z}$.

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

$X^4 + 2X^3 - X + 6 = \left(X^3 - 6X^2 + X + 4\right)(X+8) + 47X^2 - 13X - 26$, en posant la division.

Démonstration

- **Existence** : Soit $d = \deg B$, $B = b_0 + \cdots + b_d X^d$ avec $b_d \neq 0$. Si $d = 0$, le couple $(A/b_0, 0)$ convient. Sinon, on raisonne par récurrence forte sur $n = \deg A$, $A = a_0 + \cdots + a_n X^n$.
  - ⋆ 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 $\deg A_1 \leqslant n-1$.

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 $\left(Q_1 + \frac{a_n}{b_d} X^{n-d}, R\right)$ 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 $R_1 = R_2$. □

Remarque

On peut donc écrire un algorithme de division euclidienne de polynômes, stockés par exemple sous forme de liste. C'est très facile en récursif vu la récurrence constructive. Essayez !

2 Diviseurs, multiples

Définition : Diviseurs, multiples

Si $A, B \in \mathbb{K}[X]$, on dit que B **divise** A ou que A **est un multiple de** B, et on note $B|A$ lorsque l'on a $Q \in \mathbb{K}[X]$ tel que $A = BQ$.
L'ensemble des multiples de B est noté $B\mathbb{K}[X]$.
Si $A|B$ et $B|A$, A et B sont dit **associés**.

Remarques

R1 – Si $B \neq 0$, $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.

R2 – Tout B divise 0 et $0|A$ si et seulement si $A = 0$.

R3 – Si $B|A$ et $A \neq 0$, alors $\deg B \leqslant \deg A$.

R4 – Si $B|A$ et $\lambda, \mu \neq 0$, alors $\lambda B | \mu A$: on peut en particulier toujours se ramener à des polynômes unitaires. On notera, si $P \neq 0$, $\mathcal{N}(P) = \frac{P}{\mathrm{cd}\, P}$ le normalisé de P, si $P = 0$, on peut poser $\mathcal{N}(P) = 0$. $\mathcal{N}(P)$ est l'analogue de $|k|$ dans $\mathbb{Z}$.

Propriétés

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

(i) La relation | est transitive et réflexive sur $\mathbb{K}[X]$.

(ii) A et B sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$ si et seulement si $\mathcal{N}(A) = \mathcal{N}(B)$.

(iii) $B|A \Longrightarrow B|AC$

(iv) $B|A$ et $B|C \Longrightarrow B|(PA + QC)$

(v) $B|A$ et $D|C \Longrightarrow BD|AC$

(vi) $B|A \Longrightarrow \forall\, n \in \mathbb{N},\ B^n \big| A^n$

Remarques

R1 – $|$ est une relation d'ordre partiel sur l'ensemble des polynômes unitaires.

R2 – Pour les polynômes associés, le ± 1 de $\mathbb{Z}$ devient $\lambda \in \mathbb{K}^*$ (inversibles).

Démonstration

(ii) Le sens indirect est immédiat.
Si A et B sont associés, on a $P, Q \in \mathbb{K}[X]$ tels que $A = BQ = APQ$. Donc soit $A = 0$, soit $PQ = 1$ par intégrité, donc soit $A = 0$, soit P et Q sont des polynômes constants non nuls. □

III 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

R1 – 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 $\tilde{P}(x)$.

R2 – 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.)

R3 – 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 $\tilde{P}' = \widetilde{P'}$.

Démonstration

Vérifications immédiates vu la définition des opérations sur $\mathbb{K}[X]$. □

Remarque

L'application $P \mapsto \tilde{P}$ est un morphisme d'anneau de $\mathbb{K}[X]$ vers l'anneau des fonctions de $\mathbb{K}$ dans $\mathbb{K}$ (voir la propriété suivante, avec $\tilde{1} \equiv 1$.

2 Formule de Taylor

Théorème : Formule de Taylor

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

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

c'est-à-dire

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

Corollaire : Formule de Mac Laurin

$$P = \sum_{n \geqslant 0} \frac{\tilde{P}^{(n)}(0)}{n!}X^n$$

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

Démonstration

On vérifie directement la formule de Mac Laurin (avec $\tilde{P}^{(n)}(0) = n!a_n$.)

Ensuite, on pose $Q = P(X+a)$. Alors, en tant que polynôme composé, par récurrence, pour tout $n \geqslant 0$, $Q^{(n)} = P^{(n)}(X+a)$, donc $\tilde{Q}^{(n)}(0) = \tilde{P}^{(n)}(a)$.

La formule de Mac Laurin donne alors le résultat. □

3 Racines

a Définition

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

R1 – Cela dépend du corps $\mathbb{K}$.

Exemple

X^2-1 et X^2-2 dans $\mathbb{R}$ et $\mathbb{C}$.

R2 – Un polynôme réel de degré impair a toujours une racine réelle (conséquence du théorème des valeurs intermédiaires.)

b Propriétés

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 $(X-x_1)\cdots(X-x_n)|P$.

Démonstration

Formule de Taylor : $P(X) = \sum_{n\geqslant 0} \frac{\tilde{P}^{(n)}(a)}{n!}(X-a)^n$. Donc si a est racine de P, $P(X) = \sum_{n\geqslant 1} \frac{\tilde{P}^{(n)}(a)}{n!}(X-a)^n$ est divisible par $(X-a)$ et si P est divisible par $X-a$, on a bien $\tilde{P}(a)=0$.

Ou : division euclidienne de P par $(X-a)$: $P=(X-a)Q+\lambda$. a est racine de P si et seulement si $\lambda=0$.

Puis récurrence, si c'est vrai pour $n-1$, alors $P=(X-x_1)\cdots(X-x_{n-1})Q$ dont l'évaluation en x_n est nulle donc $Q(x_n)=0$ car ils sont deux à deux distincts, donc on peut factoriser Q par $X-x_n$ ce qui établit la récurrence. □

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, $P=0$.

Démonstration

Tout cela vient de la factorisation par $(X-x_1)\cdots(X-x_n)$. □

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. □

Remarques

R1 – 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 !).

R2 – L'application $P\mapsto\tilde{P}$ est un isomorphisme d'anneau de $\mathbb{K}[X]$ vers l'anneau des fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$.

Exercice

Si $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, $P(X+a)=\sum_{n\geqslant 0}\frac{a^n}{n!}P^{(n)}(X)$.

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

C Multiplicité

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 $(X-a)^{m+1}\not|P$ si et seulement si on a $Q\in\mathbb{K}[X]$ tel que $P=(X-a)^mQ$ 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

R1 – Si $(X-a)^n \mid P$ alors a est racine de P d'ordre **au moins** n.

R2 – L'ordre est toujours au plus égal au degré du polynôme.

Exemple

$P = (X-1)^3\left(X^2+1\right)\left(X-\sqrt{2}\right)$.

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

Démonstration

Un sens est évident. L'autre peut se faire laborieusement par récurrence mais ce sera immédiat avec l'arithmétique des polynômes. □

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 $\tilde{P}^{(m)}(a) \neq 0$.

Démonstration

- $(\Longleftarrow)$: La formule de Taylor donne directement $P = \sum_{n \geqslant m} \frac{\tilde{P}^{(n)}(a)}{n!}(X-a)^n = (X-a)^m Q$ avec $\tilde{P}^{(m)}(a) \neq 0$ donc $Q(a) \neq 0$.
- $(\Longrightarrow)$:
  - ⋆ **Première méthode** : Si $P = (X-a)^m Q$ avec $Q(a) \neq 0$, pour tout $n \leqslant m$, par la formule de Leibniz, $P^{(n)} = \sum_{k=0}^{n} \binom{n}{k} \frac{m!}{(m-k)!}(X-a)^{m-k} Q^{(n-k)}$.
    - Si $n < m$, on obtient $\tilde{P}^{(n)}(a) = 0$.
    - Si $n = m$, on obtient $\tilde{P}^{(m)}(a) = m!\,Q(a) \neq 0$.
  - ⋆ **Seconde méthode** : Avec la formule de Taylor,

$$P = \left(\sum_{n \geqslant m} \frac{\tilde{P}^{(n)}(a)}{n!}(X-a)^{n-m}\right)(X-a)^m + \underbrace{\sum_{n=0}^{m-1} \frac{\tilde{P}^{(n)}(a)}{n!}(X-a)^n}_{=R}$$

  avec $\deg R < m$. D'autre part, $P = (X-a)^m Q + 0$ avec $Q(a) \neq 0$. Par unicité du reste et du quotient de la division euclidienne, $R = 0$ donc $R(X+a) = 0$ donne $\forall\, k \in [\![0, m-1]\!]$, $\tilde{P}^{(k)}(a) = 0$, et $Q(a) \neq 0$ donne $\tilde{P}^{(m)}(a) \neq 0$. □

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.

Démonstration

$P = X(X-2)$ et $P' = 2X-2$. □

Exercice

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

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

Démonstration

On a Q tel que $P = (X - x_1)^{m_1}\cdots(X - x_p)^{m_p} Q$. Alors P est scindé si et seulement si $\deg Q = 0$ (sinon Q aurait au moins une racine). □

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**.*

Démonstration : (Hors programme)

Soit $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$ tel que $\deg P \geqslant 1$, avec $a_n \neq 0$.

Soit $f = |\tilde{P}| : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{R}^+ \\ z & \longmapsto & |a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0| \end{array} \right.$.

Idée : Montrer que f atteint un minimum sur $\mathbb{C}$ et qu'il est nul.

Première étape : f minoré par $f(0)$ pour z grand.

On a

$$f(z) = |a_n||z|^n \left|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right| \geqslant |a_n||z|^n \left|1 - \frac{|a_{n-1}|}{|a_n||z|} + \cdots + \frac{|a_0|}{|a_n||z|^n}\right|$$

donc $f(z) \xrightarrow[|z|\to+\infty]{} +\infty$ et on a $r > 0$ tel que $|z| > r \Longrightarrow f(z) \geqslant f(0)$.

Deuxième étape : f atteint sa borne inférieure sur $D_r = \{z \in \mathbb{C}, |z| \leqslant r\}$.

f est minorée (par 0) donc admet une borne inférieure m sur D_r.

Par caractérisation séquentielle, on a une suite $(z_n)_n \in D_r^{\mathbb{N}}$ telle que $f(z_n) \to m$.

La suite $(z_n)_n$ étant bornée, par théorème de Bolzano-Weierstraß, on a une extractrice φ telle que $z_{\varphi(n)} \to z_\infty \in \mathbb{C}$ (en fait, on a même $z_\infty \in D_r$).

Alors $f\left(z_{\varphi(n)}\right) = \left|a_n z_{\varphi(n)}^n + a_{n-1} z_{\varphi(n)}^{n-1} + \cdots + a_0\right| \to \left|a_n z_\infty^n + a_{n-1} z_\infty^{n-1} + \cdots + a_0\right| = f(z_\infty)$.

Or, par extraction, $f\left(z_{\varphi(n)}\right) \to m$, donc, par unicité de la limite, $m = f(z_\infty)$.

Troisième étape : f admet un minimum sur $\mathbb{C}$

On a alors $\forall z \in D_r,\ \ f(z) \geqslant m$ et $\forall z \notin D_r,\ \ f(z) \geqslant f(0) \geqslant m$.

Donc $m = f(z_\infty)$ est le minimum de f sur $\mathbb{C}$.

Quatrième étape : $m = 0$ par l'absurde

Si $m \neq 0$, on pose $Q = P(z_\infty + X) = b_n X^n + \cdots + B_1 X + b_0$, avec $b_0 = \tilde{P}(z_\infty) \neq 0$ et $b_n \neq 0$.

Soit k le plus petit indice strictement positif tel que $b_k \neq 0$ et ω une racine k-ème de $-\dfrac{b_0}{b_k}$.

Si $t \in \mathbb{R}$, on calcule

$$f(z_\infty + \omega t) = \left|\tilde{Q}(\omega t)\right| = \left|b_n \omega^n t^n + \cdots + b_k \omega^k t^k + b_0\right| = \left|b_n \omega^n t^n + \cdots - b_0 t^k + b_0\right| = |b_0|\left|t^k \varepsilon(t) - t^k + 1\right|$$

avec $\varepsilon(t) \xrightarrow[t\to 0]{} 0$.

On peut donc choisir t assez petit pour que $0 < t < 1$ et $|\varepsilon(t)| < 1$ et on obtient

$$f(z_\infty + \omega t) \leqslant |b_0|\left(\left|1 - t^k\right| + t^k |\varepsilon(t)|\right) < |b_0|\left(1 - t^k + t^k\right) = |b_0| = m$$

ce qui est contradictoire.

C'est donc que $m = \left|\tilde{P}(z_\infty)\right|$=0 et donc z_∞ est racine de P.

□

Corollaire

Tout polynôme à cœfficients complexes non constant est scindé.

Démonstration

Soient $x_1,\dots,x_p$ les racines complexes de P (il y en a !) de multiplicités $m_1,\dots,m_p$.

Alors $P=\prod_{k=1}^{p}(X-x_k)^{m_k}Q$ où Q n'a pas de racine. Donc, d'après le théorème de d'Alembert-Gauß, Q est constant et P 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

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

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

$S_1=x_1+\cdots+x_n=\sigma_1$.

$S_2=x_1^2+\cdots+x_n^2=\sigma_1^2-2\sigma_2$.

$S_3=x_1^3+\cdots+x_n^3=$? C'est plus compliqué.

Par exemple, si $n=3$,

$$(x+y+z)^3=(x+y+z)(x+y+z)(x+y+z)=x^3+y^3+z^3+3(x^2y+x^2z+y^2z+xy^2+xz^2+yz^2)+6xyz$$

Ce qui permet alors d'écrire $S_3=\sigma_1^3-6\sigma_3-3(\sigma_1\sigma_2-3\sigma_3)=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$.

Plus simple ? $S_1S_2=S_3+\sum_{i_1\neq i_2}x_{i_1}x_{i_2}^2=S_3+\sigma_1\sigma_2-3\sigma_3$ donc $S_3=\sigma_1(\sigma_1^2-2\sigma_2)-\sigma_1\sigma_2+3\sigma_3$ ce qui redonne le résultat dans le cas général.

Propriété : Relations cœfficients-racines

*Soient $n\in\mathbb{N}^*$, $a_0,\cdots,a_n\in\mathbb{K}$ tel que $a_n\neq 0$, $P=a_0+\cdots+a_nX^n$, **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)*
- $\sigma_2=\dfrac{a_{n-2}}{a_n}$.
- $\vdots$
- $\sigma_k=(-1)^k\dfrac{a_{n-k}}{a_n}$.
- $\vdots$
- $\sigma_n=(-1)^n\dfrac{a_0}{a_n}$. *(produit)*

Ainsi, $P=a_n\big(X^n-\underbrace{\sigma_1}_{\text{somme}}X^{n-1}+\sigma_2X^{n-2}+\cdots+(-1)^n\underbrace{\sigma_n}_{\text{produit}}\big)$.

Démonstration

$P=a_0+\cdots+a_nX^n=a_n(X-x_1)\cdots(X-x_n)$.
Le cœffcient en X^{n-k} : k termes où on prend $-x_i$ et $n-k$ termes où on prend X.
On obtient $a_{n-k}=a_n\sum_{i_1<\cdots<i_k}(-x_{i_1})\cdots(-x_{i_k})=(-1)^ka_n\sigma_k$. □

Remarques

R1 – En particulier, si P est unitaire, $P=X^n-\sigma_1X^{n-1}+\sigma_2X^{n-2}+\cdots+(-1)^n\sigma_n$.

R2 – 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.

Exemple

Si $x_1,\ldots,x_4$ sont les racines complexes de $P=1+X^2+X^3+X^4$, alors $S=x_1^2+x_2^2+x_3^2+x_4^2=-1$ (donc il y a des racines non réelles !)

IV ARITHMÉTIQUE

1 Polynômes irréductibles

a Généralités

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 $P = UV \Longrightarrow U$ ou V inversible.
Les autres polynômes sont dits **réductibles**.

Remarque

C'est l'équivalent des nombres premiers et de leur opposé.

Exemples

E1 – Un polynôme de degré 1 est toujours irréductible.

E2 – X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

E3 – X^2-2 est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

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 $\lambda = \operatorname{cd} A$, $P_1, \dots, P_k$ sont les diviseurs irréductibles unitaires de A.

Démonstration

Comme dans $\mathbb{Z}$ pour l'unicité.
L'existence se démontre par récurrence sur $n = \deg A$.
Si $n = 0$ ou $n = 1$, c'est immédiat.
Si 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. □

Corollaire

Tout polynôme non constant admet un diviseur irréductible.

Remarques

R 1 – Peut aussi se démontrer comme dans $\mathbb{Z}$ en considérant un diviseur de degré minimal.

R 2 – On peut de nouveau parler de valuation P-adique : $v_P(A) = \max\{k \ ; \ P^k | A\}$.
Si $P = X - a$, $v_{X-a}(A)$ est l'ordre de a en tant que racine de A.

b Irréductibles de $\mathbb{C}[X]$

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.
Réciproquement les polynômes de degré 1 sont bien irréductibles. □

Remarque

Ainsi, 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

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

Exemple

Décomposition en irréductible de $X^n - 1$.

c Irréductibles de $\mathbb{R}[X]$

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

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 $\mathbb{R}[X]$, $P = \lambda\left(X^2 - 2(\mathfrak{Re}\,\alpha)X + |\alpha|^2\right) \in \mathbb{R}[X]$. □

Remarques

R1 – 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, $\Delta_k = a_k^2 - 4b_k < 0$.

R2 – 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

E1 – $X^4-1 = \left(X^2-1\right)\left(X^2+1\right) = (X-1)(X+1)\left(X^2+1\right)$.
En passant par $\mathbb{C}$: $\mathbb{U}_4 = \{\pm 1, \pm \mathrm{i}\}$ donc $X^4-1 = (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i})$ redonne le résultat.

E2 – Pour X^4+1 ?
Soit on cherche les quatre racines complexes : $\dfrac{\pm 1 \pm \mathrm{i}}{\sqrt{2}}$.
Soit on cherche a, b, c, d réels tels que $X^4+1 = \left(X^2+aX+b\right)\left(X^2+cX+d\right)$.
Soit on écrit $X^4+1 = X^4 - \mathrm{i}^2$.
Soit on met sous forme canonique $X^4+1 = \left(X^2+1\right)^2 - 2X^2$.
Soit on reconnaît un **polynôme réciproque** (palindrome : les cœfficients sont symétriques), on « pose » $Y = X + \frac{1}{X}$:

$$X^4+1 = X^2\left(Y^2-2\right) = X^2(Y-\sqrt{2})(Y+\sqrt{2}) = \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right).$$

(Aura vraiment du sens avec la théorie sur les fractions rationnelles, sinon, on peut passer par les fonctions polynomiales.)

2 pgcd

Définition : pgcd

Soient $(A,B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$. On appelle **plus grand diviseur commun** à A et à B tout polynôme divisant A et B de degré maximal.

On note $A \wedge B$ le seul qui soit unitaire.

Remarques

R1 – Si $A \neq 0$ par exemple, $\{\deg P \ ; \ P|A \text{ et } P|B\} \subset \mathbb{N}$, non vide (contient $0 = \deg 1$) et majoré par $\deg A$, donc contient un plus grand élément.
Si P convient, on a facilement que pour tout $\lambda \in \mathbb{K}^*$, λP convient aussi. On peut donc supposer P unitaire. Mais quid de l'unicité ? Elle sera justifiée ci-après.

R2 – Si $B = 0$, les pgcd de A et 0 sont les λA avec $\lambda \in \mathbb{K}^*$ et $A \wedge 0 = \mathcal{N}(A) = \dfrac{A}{\mathrm{cd}\, A}$.

R3 – On peut poser $0 \wedge 0 = 0$.

Propriété

Si $A, B, Q \in \mathbb{K}[X]$, les diviseurs communs à A et B sont les diviseurs communs à $A - BQ$ et B, et en particulier, ils ont les mêmes pgcd.

Propriété : Caractérisation des pgcd

Soient $A, B, D \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$.

$$D \text{ est un pgcd de } A \text{ et } B \iff \begin{cases} D|A \text{ et } D|B \\ \forall P \in \mathbb{K}[X], \ \Big(P|A \text{ et } P|B \Longrightarrow P|D\Big) \end{cases}$$

Les pgcd sont donc des plus grand éléments pour | (qui n'est pas un ordre sur $\mathbb{K}[X]$).

Remarque

Avec la convention, $0 \wedge 0 = 0$, cela fonctionne encore.

Démonstration

- ($\Longrightarrow$) : Si D est un pgcd, on a déjà $D|A$ et $D|B$. On montre l'autre propriété par récurrence sur $\deg B$.
  - ⋆ C'est vrai si $B = 0$ ou si $\deg B = 0$.
  - ⋆ Si c'est vrai jusqu'à $\deg B - 1$, alors $A = BQ + R$ avec $\deg R < \deg B$. Si $P|A$ et $P|B$, alors $P|B$ et $P|R$, donc par hypothèse de récurrence, P divise tout pgcd de B et R, donc en particulier D.
- ($\Longleftarrow$) : Si $D|A$, $D|B$ et $\forall P \in \mathbb{K}[X]$, $\Big(P|A \text{ et } P|B \Longrightarrow P|D\Big)$, tout pgcd de A et de B divise D, donc a un degré inférieur à $\deg D$. Par maximalité, les degrés sont égaux et D est lui-même un pgcd. □

Corollaire

(i) Les diviseurs communs à A et à B sont exactement les diviseurs de n'importe lequel de leurs pgcd.

(ii) Tous les pgcd de A et B sont associés.

(iii) Il existe un unique pgcd unitaire, caractérisé par

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

$A \wedge B$ est donc le plus grand diviseur commun unitaire pour $|$ (qui est un ordre sur l'ensemble des polynômes unitaires.)

Démonstration

Conséquence immédiate. □

Remarque

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

Exemple

Si $A = X^4 + X^3$ et $B = X^2 + X + 1$, alors $A \wedge B = 1$.

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, alors

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

Démonstration

Comme dans $\mathbb{Z}$. □

Exemple

$A = X^4 + X^3$ et $B = X^3 + X^2 + X$.

3 Algorithme d'Euclide, relation de Bézout

Propriété : Algorithme d'Euclide

Soient $(A,B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$.
On effectue les divisions euclidiennes successives

$$\begin{aligned} A &= BQ_1 + R_1 \\ B &= R_1Q_2 + R_2 \\ R_1 &= R_2Q_3 + R_3 \\ &\dots \\ \forall\, k,\quad R_{k-1} &= R_kQ_{k+1} + R_{k+1} \text{ et } \deg R_{k+1} < \deg R_k \end{aligned}$$

(en notant $A = R_{-1}$ *et* $B = R_0$*.)*
Le procédé s'arrête et le dernier reste non nul est un pgcd de A *et* B*.*

Démonstration

La suite $(\deg R_k)_k$ est une suite d'entiers naturels strictement décroissante donc elle est finie et finit par atteindre 0.
De plus, on a $A \wedge B = B \wedge R = \dots = R_n \wedge 0 = \mathcal{N}(R_n)$. □

Remarque

Si $A,B \in \mathbb{R}[X]$, la division euclidienne de A par B sur $\mathbb{R}$ ou sur $\mathbb{C}$ s'écrit de la même manière par unicité (les réels sont des complexes !). Donc les pgcd dans $\mathbb{R}$ ou dans $\mathbb{C}$ sont les mêmes.
Contrairement à celles de racines, les notions de pgcd ne dépendent pas du corps de base.

Propriété : Relation de Bézout

Si $(A,B) \neq (0,0)$*, on a* $U,V \in \mathbb{K}[X]$ *tel que* $AU + BV = A \wedge B$*.*

Démonstration

Par récurrence sur $\deg B$.
Si $B = 0$ ou B constant, c'est facile. Pour l'hérédité, c'est comme dans $\mathbb{Z}$. □

Exemple

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

Propriété : Factorisation dans un pgcd

Si $C \neq 0$, $(CA) \wedge (CB) = \mathcal{N}(C)(A \wedge B) = \dfrac{C}{\operatorname{cd} C}(A \wedge B)$.

Démonstration

On peut supposer C unitaire sans perte de généralité. Alors $C(A\wedge B)$ divise CA et CB donc leur pgcd, et est unitaire.

Et on a U et V tels que $AU+BV=A\wedge B$, donc $CAU+CBV=C(A\wedge B)$, donc $(CA)\wedge(CB)$ divise $C(A\wedge B)$ et est unitaire également. □

4 Extension à plus de deux polynômes

Exactement comme pour les entiers.

Définition : pgcd de n polynômes

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

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

5 Polynômes premiers entre eux

Définition : 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 le diviseur unitaire commun à A et B est 1.

Théorème : de Bézout

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

Démonstration

Comme dans $\mathbb{Z}$. □

Théorème : Lemme de Gauß

Si $A|BC$ *et* $A\wedge B=1$, *alors* $A|C$.

Démonstration

Comme dans $\mathbb{Z}$. □

Propriété

Si $(A,B) \in \mathbb{K}[X]^2 \setminus \{(0,0)\}$, $D = A \wedge B$, alors on peut écrire

$$\begin{cases} A = DA_1 \\ B = DB_1 \\ A_1 \wedge B_1 = 1 \end{cases}$$

Démonstration

Comme dans $\mathbb{Z}$. □

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. □

Exemple

Si $A = X^2+1$ et $B = X^3+X$, A et B n'ont pas de racine commune dans $\mathbb{R}$ et pourtant $A \wedge B = X^2+1$.

Propriété

A est premier avec $B_1, \dots, B_n$ si et seulement si A est premier avec $B_1 \cdots B_n$.

Démonstration

Comme dans $\mathbb{Z}$. □

Propriété

(i) Si P est irréductible et $A \in \mathbb{K}[X]$, soit $P|A$, soit $P \wedge A = 1$.

(ii) Si P est irréductible et $A_1, \dots, A_n \in \mathbb{K}[X]$, $P|A_1 \cdots A_n \Longrightarrow \exists i$ tel que $P|A_i$.

Démonstration

Comme dans $\mathbb{Z}$. □

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

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 : 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 $A_1\cdots A_n | B$.*

Démonstration

Comme dans $\mathbb{Z}$. □

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).

6 Multiples communs

Définition - Propriété : ppcm

Soient $A,B \in \mathbb{K}[X]\setminus\{0\}$. On appelle **plus petit commun multiple de A et B** tout multiple commun à A et à B non nul de degré minimal.

Démonstration

$E = \{\text{degrés des multiples communs à } A \text{ et à } B \text{ non nuls}\} \subset \mathbb{N}$, non vide car $\deg a + \deg B \in E$, donc admet un minimum. □

Propriété : Caractérisation

$$M \text{ est un ppcm de } A \text{ et } B \iff \begin{cases} M \neq 0 \\ A|M \text{ et } B|M \\ \forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P \Longrightarrow M|P) \end{cases}$$

Démonstration

Comme dans $\mathbb{Z}$.

Si M est un ppcm, alors $M \neq 0$ et $A|M$ et $B|M$ par définition. Si de plus, $A|P$ et $B|P$, alors par division euclidienne, $P = MQ + R$ avec $\deg R < \deg M$ et R multiple commun à A et B, donc $R = 0$ et $M|P$.

Réciproquement, si les trois propriétés sont vérifiées, M est un multiple non nul commun à A et B tel que les autres multiples communs non nuls sont divisibles par, donc de degré plus grand que celui de M. M a donc bien un degré minimal.

Ou alors : $A|M$ et $B|M$ donc un ppcm de A et B divise M, et comme A et B divisent ce ppcm, M le divise aussi, donc ils sont associés et M est aussi un ppcm. □

Corollaire

(i) Les multiples communs à A et à B sont exactement les multiples de tout ppcm de A et B : $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$.

*(ii) Il existe un unique ppcm **unitaire**, noté $A \vee B$.*

$$M = A \vee B \iff \begin{cases} M \text{ est unitaire} \\ A|M \text{ et } B|M \\ \forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P \Longrightarrow M|P) \end{cases}$$

Remarque

Il est alors cohérent de poser $A \vee 0 = 0$.

Propriété : Factorisation de ppcm

Si $A, B, C \in \mathbb{K}[X] \setminus \{0\}$,

$$(CA) \vee (CB) = \mathscr{N}(C)(A \vee B) = \frac{C}{\operatorname{cd} C}(A \vee B).$$

Démonstration

Comme dans $\mathbb{Z}$. □

Propriété

Si $A, B \in \mathbb{K}[X] \setminus \{0\}$,

- *Si $A \wedge B = 1$, $A \vee B = \mathcal{N}(AB) = \dfrac{AB}{\mathrm{cd}(AB)}$.*
- *En général, $(A \wedge B)(A \vee B) = \mathcal{N}(AB) = \dfrac{AB}{\mathrm{cd}(AB)}$.*

Démonstration

Comme dans $\mathbb{Z}$: si $A \wedge B = 1$, A et B divisent $A \wedge B$ donc AB le divise. Et AB est un multiple commun, donc est divisible par $A \wedge B$

Sinon, on écrit $A = DA_1$ et $B = DB_1$ avec $D = A \wedge B$.

Alors $(A \wedge B)(A \vee B) = D^2 \mathcal{N}(A_1 B_1) = \mathcal{N}(AB)$ car D est unitaire. □

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, alors

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

Démonstration

Comme dans $\mathbb{Z}$. □

Exemple

$A = X^4 + X^3$ et $B = X^3 + X^2 + X$.

V 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 $\forall\, k \in [\![0, n]\!]$, $\tilde{P}(x_k) = y_k$.

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

- **Principe** : L'idée est de découper le problème . On commence par chercher un polynôme L tel que $L(x_0) = 1$ et $L(x_j) = 0$ si $j \neq 0$, c'est-à-dire $L(x_j) = \delta_{j,0}$.
  Alors $x_1, \dots, x_n$ sont racines de L. Donc $L = (X - x_1) \cdots (X - x_n) Q$.
  Si on suppose de plus que $\deg L = n$, alors Q est constant : $Q = \lambda$ et $L(x_0) = 1 = \lambda (x_0 - x_1) \cdots (x_0 - x_n)$.

  Donc $L = \dfrac{(X - x_1) \cdots (X - x_n)}{(x_0 - x_1) \cdots (x_0 - x_n)}$.

  On peut procéder de la même manière pour $x_1, \dots, x_n$.

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

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

Avec ces polynômes, il suffit, pour avoir des valeurs $y_0, \dots, y_n$ en $x_0, \dots, x_n$, de considérer $y_0 L_0 + \cdots + y_n L_n$.

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 $\forall\, i,\ \tilde{P}(x_i) = y_i$.

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

Démonstration

L'existence provient de ce qui précède.

Si P et Q conviennent, alors P et Q sont de degré au plus n et coïncident en $n+1$ valeurs deux à deux distinctes, donc $P = Q$. □

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 racine de $A - P$ qui s'écrit donc $\left(\prod_{i=0}^{n} (X - x_i)\right) Q$. □

Exemple

Soit $B = X^3 + X^2 - 2X = X(X-1)(X+2)$.

$$L_0 = \frac{(X-1)(X-2)}{2} \qquad L_1 = \frac{X(X+2)}{3} \qquad L_{-2} = \frac{X(X-1)}{6}$$

Reste de la division euclidienne de P par B ?

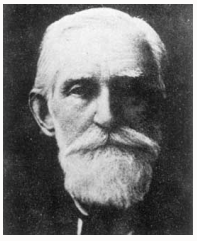
$P = BQ + R$ avec $\deg R < \deg B = 3$ et $\tilde{R}(0) = \tilde{P}(0)$, $\tilde{R}(1) = \tilde{P}(1)$ et $\tilde{R}(-2) = \tilde{P}(-2)$, donc R est le polynôme d'interpolation de Lagrange associé à $(0, \tilde{P}(0))$, $(1, \tilde{P}(1))$, $(2, \tilde{P}(2))$: $R = \tilde{P}(0)L_0 + \tilde{P}(1)L_1 + \tilde{P}(-2)L_{-2}$.

Par exemple, le reste de la division euclidienne de X^n par B est $L_1 + (-2)^n L_{-2}$.

Remarque : Phénomène de Runge

C'est séduisant pour approcher une fonction, mais peu utilisable en pratique si n devient trop grand. Les termes en X^n induisent de grandes variations qui vont perturber le comportement entre deux points d'interpolation (phénomène de Runge).

On peut montrer que pour atténuer ce phénomène, un moyen est choisir convenablement les points d'interpolation, le choix optimal étant les racines des polynômes de Tchebychev [a] $\cos\dfrac{(2k+1)\pi}{2n}$ sur $[-1,1]$, transposable à tout $[a,b]$ par transformation affine.

a. 

Pafnouti Lvovitch Tchebychev (Russie, 1821 - 1894) est un mathématicien russe. Il est connu pour ses travaux dans le domaine des probabilités et des statistiques. En théorie des nombres, Tchebychev découvre des résultats sur la répartition des nombres premiers. Les polynômes de Tchebychev sont très classiques en classe prépa.

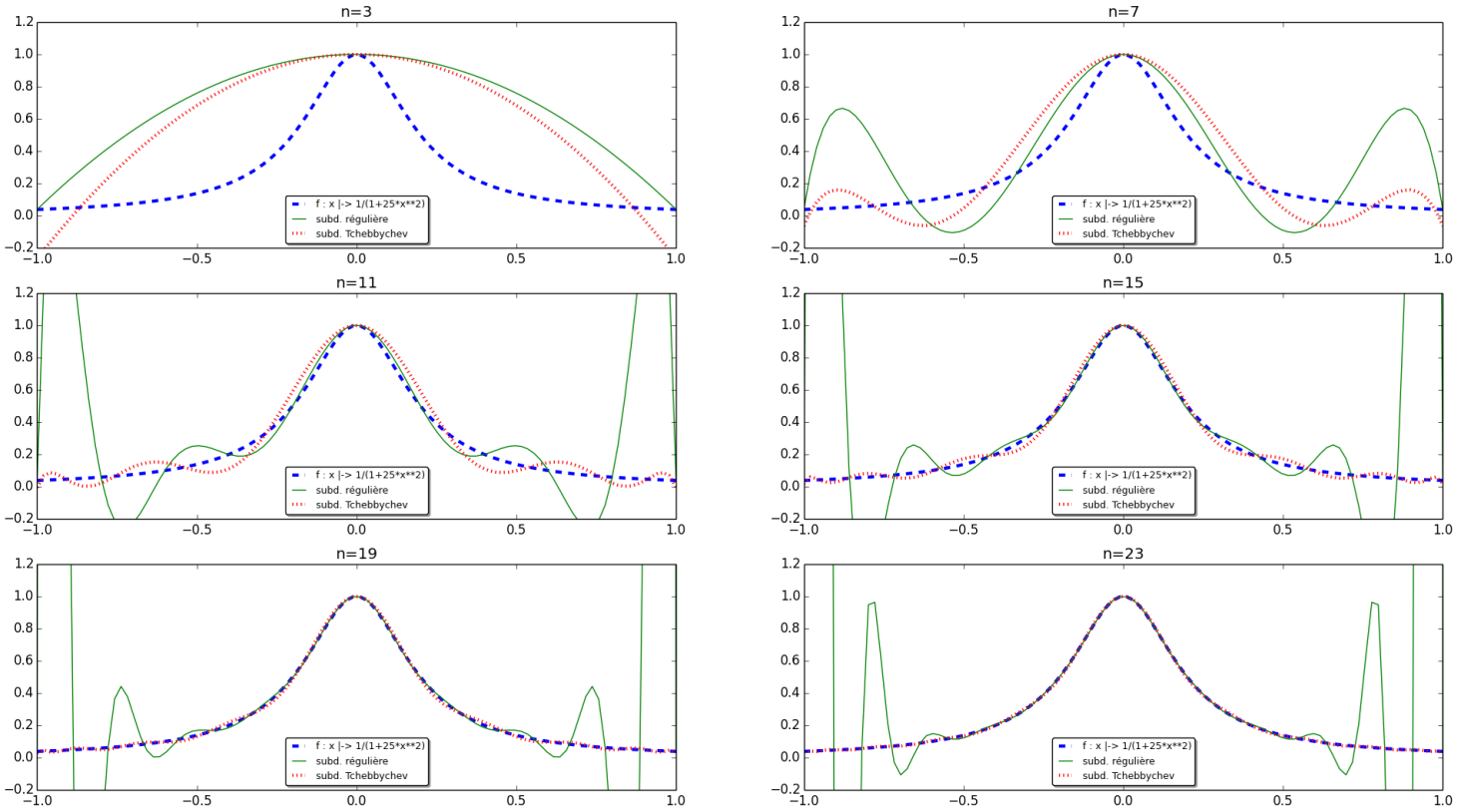


FIGURE 1 – Phénomène de Runge