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 $(a_0, a_1, \dots, a_d, 0, 0, \dots)$ 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 $(0, \dots, 0, \underbrace{1}_{k^e}, 0, 0, \dots)$.

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

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

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 $\mathbb{K}[X]$.

- 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.

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

2 Opérations sur les polynômes

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

  $$c_m = \sum_{m=k+\ell} a_k b_\ell = \sum_{k=0}^{m} a_k b_{m-k} = \sum_{\ell=0}^{m} a_{m-\ell} b_\ell.$$
- $P \circ Q = P(Q) = \sum_{k \geqslant 0} a_k Q^k$.

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

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

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.)

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

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

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.

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 $\tilde{P}' = \widetilde{P'}$.*

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 $\tilde{P}(a) = 0$.

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

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 $\tilde{P}$.

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 $P = (X-a)^m Q$ 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.

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

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.

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 $y_1, \ldots, y_n \in \mathbb{K}$ 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 $x_1, \ldots, x_p \in \mathbb{K}$ deux à deux distincts et $m_1, \ldots, m_p \in \mathbb{N}^*$ tels que

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

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

Propriété : Caractérisation avec les racines

Soit P un polynôme non constant admettant exactement p racines d'ordres respectifs $m_1, \ldots, m_p$ dans $\mathbb{K}$.

P est scindé si et seulement si $m_1 + \cdots + m_p = \deg P$.

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.

5 Relations cœfficients-racines

Définition : Fonctions symétriques élémentaires

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

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

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

$$\sigma_2 = \sum_{1 \leqslant i_1 < i_2 \leqslant n} x_{i_1}x_{i_2} \qquad \left(\frac{n(n-1)}{2} \text{ termes}\right)$$

$$= x_1x_2 + x_1x_3 + \cdots + x_1x_n + \cdots + x_{n-1}x_n.$$

$$\vdots$$

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k}. \qquad \left(\binom{n}{k} \text{ termes}\right)$$

$$\vdots$$

$$\sigma_n = x_1x_2\cdots x_n. \qquad (1 \text{ terme})$$

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

Ainsi,

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

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,

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

On cherche donc le polynôme $L_i = u^{-1}\Big(0, \ldots, \underbrace{1}_{i^e}, \ldots, 0\Big)$ 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 $x_0, \ldots, x_n$ deux à deux distincts, on appelle i^e polynôme de Lagrange associé à $(x_0, \ldots, x_n)$ 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 $x_0, \ldots, x_n \in \mathbb{K}$ deux à deux distincts et $y_0, \ldots, y_n \in \mathbb{K}$, 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 $((x_0, y_0), \ldots, (x_n, y_n))$ sont les polynômes $P + \left(\prod_{i=0}^{n} (X - x_i)\right) Q$ où $Q \in \mathbb{K}[X]$ et $P = \sum_{i=0}^{n} y_i L_i$.

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$\}$.

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 $\deg R < \deg B$.

Théorème

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

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 $A \wedge B$.

Propriété : Relation de Bézout

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

Propriété : Caractérisation

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

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

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

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.

Théorème : de Bézout

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

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

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 $A_1 \wedge B_1 = 1$.*

Théorème : Lemme de Gauß

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

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.

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 $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.

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

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 $A_1 \cdots A_n | B$.*

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 $P = UV \Longrightarrow U$ ou V inversible.

Les autres polynômes sont dits **réductibles**.

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

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.

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

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

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.

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).

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.

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, $\alpha_1,\dots,\alpha_n$ pôles de F d'ordre $m_1,\dots,m_n$: $F=\dfrac{A}{\prod_{k=1}^{n}(X-\alpha_k)^{m_k}}$ 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

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

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

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

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.

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

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

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