7

Polynômes et fractions rationnelles

$\mathbb{K}$ 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 $(a_0, a_1, \ldots, a_d, 0, 0, \ldots) \in \mathbb{K}^{(\mathbb{N})}$ 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 $(0, \ldots, 0, \underbrace{1}_{(k+1)^e}, 0, 0, \ldots)$.

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'indéterminée n'est pas un nombre ! Elle n'a pas de valeur. Elle représente la suite presque nulle $(0, 1, 0, 0, \ldots)$.
- L'ensemble des polynômes à une indéterminée à cœfficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.
- 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.
- 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.
$$\mathbb{K}_n[X] = \left\{a_0 + a_1 X + \cdots + a_n X^n,\ (a_0, \ldots, a_n) \in \mathbb{K}^{n+1}\right\} = \operatorname{Vect}\left(1, X, \ldots, X^n\right).$$

2 Opérations sur les polynômes

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

- $P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$
- $\lambda P = \sum_{k=0}^{+\infty} (\lambda a_k) X^k$
- $P \times Q = \sum_{k=0}^{+\infty} a_k X^k \times \sum_{\ell=0}^{+\infty} b_\ell X^\ell = \sum_{\substack{m=0 \\ (m=k+\ell)}}^{+\infty} c_m X^m$
en faisant une sommation par diagonales, c'est-à-dire avec
$$c_m = \sum_{m=k+\ell} a_k b_\ell = \sum_{k=0}^{m} a_k b_{m-k} = \sum_{\ell=0}^{m} a_{m-\ell} b_\ell.$$
- $P \circ Q = P(Q) = \sum_{k=0}^{+\infty} a_k Q^k$.

Propriété 1 : Opérations algébriques et degré

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

- $\deg(P + Q) \leqslant \max(\deg P, \deg Q)$ *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

R 1 – En général, on a $\deg(\alpha P+\beta Q)\leqslant \max(\deg P, \deg Q)$.

Propriété 2 : Structure d'algèbre commutative 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 inversibles est $\mathbb{K}_0[X]\setminus\{0\}$ (polynômes constants non nuls.)

Remarque

R 2 – 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 1 : Polynôme dérivé

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

$$\begin{aligned}P'&=\sum_{k=1}^{n}ka_kX^{k-1}=\sum_{k=0}^{n-1}(k+1)a_{k+1}X^k\\&=a_1+2a_2X+\cdots+na_nX^{n-1}.\end{aligned}$$

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

R 3 – Il n'est pas question ici de dérivabilité : la dérivation est une simple opération algébrique sur les polynômes.

Propriété 3 : de la dérivation

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

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

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

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

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

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

Remarque

R 4 – $P^{(n)}=0$ si $n\geqslant \deg P+1$ et si $d=\deg P$, $P^{(d)}=d!\operatorname{cd}P$.

R 5 – $\deg P=\min\left\{n\in\mathbb{N}\mid P^{(n)}=0\right\}-1$ si $P\neq 0$.

R 6 – 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 7 – Si $P=\sum_{k=0}^{d}a_kX^k$, alors pour tout $n\in\mathbb{N}$, $P^{(n)}=\begin{cases}0 & \text{si } n\geqslant d+1\\ d!a_d & \text{si } n=d\\ \sum_{k=n}^{d}k(k-1)\cdots(k-n+1)a_kX^{k-n} & \text{sinon.}\end{cases}$

II Fonctions polynomiales, racines

1 Fonctions polynomiales

Définition 2 : Fonction polynôme associée

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

Remarque

R 8 – 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 9 – 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 10 – 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 $\mathbb{K}$.)

Propriété 4 : Fonction polynôme et opérations

Si $P, Q \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$

(i) $\widetilde{P+Q} = \tilde{P} + \tilde{Q}$.

(ii) $\widetilde{P \times Q} = \tilde{P} \times \tilde{Q}$.

(iii) $\widetilde{\lambda P} = \lambda \tilde{P}$.

(iv) $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

(v) *Sur* $\mathbb{R}$, $\tilde{P}$ *est dérivable et* $\tilde{P}' = \widetilde{P'}$.

Remarque

R 11 – L'application $P \mapsto \tilde{P}$ est un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ vers l'algèbre des fonctions de $\mathbb{K}$ dans $\mathbb{K}$.

2 Formule de Taylor

Théorème 1 : Formule de Taylor

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

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

la somme étant finie, c'est-à-dire

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

Corollaire 1 : Formule de Mac Laurin

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

3 Racines

Définition 3 : Racine

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

Remarque

R 12 – Cela dépend du corps $\mathbb{K}$.

R 13 – Un polynôme réel de degré impair a toujours une racine réelle (conséquence du théorème des valeurs intermédiaires.)

Propriété 5 : Racine et division

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

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

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

Remarque

R 14 – Si $P|Q$, toute racine de P est racine de Q. La réciproque est fausse en général.

Corollaire 2 : Nombre de racines

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

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

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

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

Corollaire 3 : Identification polynôme et fonction polynôme

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

Remarque

R 15 – Si $\mathbb{K} = \{x_1, \dots, x_n\}$ fini (par exemple $\mathbb{Z}/p\mathbb{Z}$ avec p premier), $P = \prod_{k=1}^{n}(X-x_k) \neq 0$ (il est unitaire) et pourtant $\tilde{P} \equiv 0$ (pas plus de racines que le degré !).

Exercice 1

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

Définition 4 : Multiplicité

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

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

Ainsi, a est racine d'ordre m si et seulement si $(X-a)^m|P$ et $(X-a)^{m+1}\nmid P$ 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.

Remarque

R 16 – Si $(X-a)^n|P$ alors a est racine de P d'ordre **au moins** n.

R 17 – L'ordre est toujours au plus égal au degré du polynôme.

Propriété 6

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

Propriété 7 : Caractérisation de l'ordre

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

Exercice 2 : CCINP 85

Corollaire 4 : Multiplicité des racines de P vs P'

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

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

Exercice 3

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

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

4 Polynômes scindés

Définition 5 : Polynôme scindé

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

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

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

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

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

$x^2+1=(x-i)(x+i)$

Remarque

R 18 – ⚠ Scindé sur $\mathbb{C}$ $\not\Leftarrow$ 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 $\mathbb{Q}$.

$=(X-\sqrt{2})(X+\sqrt{2})$

Propriété 8 : Caractérisation avec les racines

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

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

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

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

Corollaire 5 : Version alternative équivalente

Tout polynôme à cœfficients complexes non constant est scindé.

Corollaire 6 : Divisibilité et racines

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

Remarque

R 19 – C'est donc toujours vrai dans $\mathbb{C}$.

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

5 Relations cœfficients-racines

Définition 6 : Fonctions symétriques élémentaires

Soient $n\in\mathbb{N}^*$, $x_1,\dots,x_n\in\mathbb{K}$.
On appelle **fonctions symétriques élémentaires** de $x_1,\dots,x_n$ les nombres

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

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

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

$$\vdots$$

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

$$\vdots$$

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

Exemple

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

Remarque

R 20 – On peut montrer que toute fonction polynomiale en $x_1,\dots,x_n$ symétrique en $x_1,\dots,x_n$ s'exprime comme un polynôme en $\sigma_1,\dots,\sigma_n$.

Exemple

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

Propriété 9 : 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,

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

Remarque

R 21 – 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 22 – Si $n = 2$, on retrouve que les racines complexes de $aX^2 + bX + c$ ont une somme égale à $-b/a$ et un produit égal à c/a.

Voir exercice du TD : 14, 20

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 7 : 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 10 : 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 11

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

Exercice 4 : CCINP 87, 90

IV Arithmétique sur $\mathbb{K}[X]$ (MPI)

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

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

Propriété 12 : Description des polynômes associés

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

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

Théorème 3 : Division euclidienne polynomiale

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

Remarque : Algorithme

R 23 – 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.

Théorème 4 : $\mathbb{K}[X]$ est principal

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

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

2 PGCD de deux polynômes

Définition 8 : PGCD

Soient $A, B \in \mathbb{K}[X]$ non tous les deux nuls. L'idéal $A\mathbb{K}[X] + B\mathbb{K}[X]$ étant principal et non réduit à $\{0\}$, on a un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ appelé PGCD de A et B noté $D = A \wedge B$.

Si $A = B = 0_{\mathbb{K}[X]}$, on pose $0 \wedge 0 = 0$.

$0\mathbb{K}[X]$

Remarque

R 24 – 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 13 : 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 14 : Caractérisation du PGCD

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

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

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

Les diviseurs communs de A et B sont exactement les diviseurs de $A \wedge B$.

Remarque

R 25 – Les diviseurs de D sont alors exactement les diviseurs communs à A et à B.

R 26 – Les racines des pgcd sont exactement les racines communes de A et B, de multiplicité le minimum des multiplicités.

On a toujours l'algo d'Euclide avec la propriété $A \wedge B = (A - BQ) \wedge B$ avec Q qcq. Par unicité de la D.E., si $P \in \mathbb{R}[X]$, l'algo. d'Euclide dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ est le même. Donc le pgcd ne dépend pas du corps.

Définition 9 : Polynômes premiers entre eux

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

Remarque

R 27 – Lorsque c'est le cas, ils n'ont pas de racine commune dans $\mathbb{K}$. La réciproque est fausse.

$A = X^2+1$ et $B = (X^2+1)^2$ n'ont pas de racine commune dans $\mathbb{R}$.

et $A \wedge B = X^2+1 \neq 1$.

Théorème 5 : de Bézout

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

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

Corollaire 7

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

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

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

Remarque

R 28 – (i) s'étend à un produit quelconque (fini) de polynômes.

Théorème 6 : Lemme de Gauß

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

Propriété 15 : 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

R 29 – C'est toujours vrai si $\mathbb{K} = \mathbb{C}$.

Voir exercice du TD : 21, 22

3 PGCD d'une famille finie de polynômes

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

Définition 10 : pgcd de n polynômes

Soient $(A_1, \ldots, A_n) \in (\mathbb{K}[X])^n \setminus \{(0, \ldots, 0)\}$.

On appelle PGCD de $A_1, \ldots, A_n$ noté $\bigwedge_{j=1}^{n} A_j$ l'unique polynôme unitaire tel que

$$A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = \left(\bigwedge_{j=1}^{n} A_j\right)\mathbb{K}[X]$$

Remarque

R 30 – Comme pour deux polynômes, il s'agit du plus grand diviseur commun unitaire au sens de la division (et aussi du degré).

R 31 – La définition s'étend à $0 \wedge \cdots \wedge 0 = 0$.

Propriété 16

(*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 11 : Polynômes premiers entre eux dans leur ensemble

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

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

Propriété 17

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

Théorème 7 : 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 18 : Diviseurs deux à deux premiers entre eux

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

Remarque : Application

R 32 – Si $x_1, \dots, x_n$ sont racines de P d'ordre au moins $m_1, \dots, m_n$ alors $(X - x_1)^{m_1} \cdots (X - x_n)^{m_n} | P$ car les $(X - x_i)^{m_i}$ sont premiers entre eux deux à deux (scindés sans racine commune).

4 Polynômes irréductibles

Définition 12 : Polynôme irréductible

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

Les autres polynômes sont dits **réductibles**.

Sinon $P = (X - \alpha)Q$ avec $\deg Q \geqslant 1$

Remarque

R 33 – 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.

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

$= (X^2+1)\times(X^2+1)$

R 34 – P est réductible dans $\mathbb{K}[X]$ ss'il admet un diviseur Q tel que $0 < \deg Q < \deg P$.

Équivalent des nb premiers dans $\mathbb{Z}$.

Propriété 19 : des polynômes irréductibles

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

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

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

Théorème 8 : 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.

Remarque

R 35 – On dit que l'anneau $\mathbb{K}[X]$ est factoriel.

Propriété 20 : Irréductibles de $\mathbb{C}[X]$

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

5 Irréductibles sur $\mathbb{R}[X]$

Csq du thm de d'Al. Gauß : tout polynôme complexe non ctt a une racine complexe.

Propriété 21 : Racine complexe de polynôme réel

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 22 : 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).

Remarque

R 36 – 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 37 – Les décompositions en irréductibles dans $\mathbb{R}[X]$ sont donc de la forme

$$P = \lambda(X - x_1)^{m_1} \cdots (X - x_n)^{m_n} \left(X^2 + a_1 X + b_1\right)^{\ell_1} \cdots \left(X^2 + a_k X + b_k\right)^{\ell_k}$$

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

R 38 – 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 $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

Exemple

E 4 – Décomposition en irréductibles de $X^n - 1$.

E 5 – Décomposition en irréductibles de $X^4 + 1$.

Propriété 23 : Expression du PGCD en produit d'irréductibles

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

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

Voir exercice du TD : 19

6 PPCM (Complément)

Définition 13 : PPCM

Soit $A, B \in \mathbb{K}[X] \setminus \{0\}$,
$A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal engendré par un unique polynôme unitaire $A \vee B$ appelé PPCM de A et B : $A\mathbb{K}[X] \cap B\mathbb{K}[X] = A \vee B\,\mathbb{K}[X]$.
On pose $A \vee 0 = 0$

Propriété 24 : du PPCM

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

(ii) *Si $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ 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 1 : Partie entière

Soit $F \in \mathbb{K}(X)$.
On note $\mathbb{K}^-(X) = \{F \in \mathbb{K}(X) \mid \deg F < 0\}$.
Il existe un unique couple $(Q, G) \in \mathbb{K}[X] \times \mathbb{K}^-(X)$ tel que $F = Q + G$. Q est appelé **partie entière** de F.

Remarque

R 39 – La partie entière est le quotient de la division euclidienne du numérateur par le dénominateur.

R 40 – C'est l'analogue de la partie entière sur $\mathbb{Q}$.

R 41 – Si $\deg F < 0$, alors sa partie entière est nulle.

R 42 – Si $F \in \mathbb{K}[X]$, sa partie entière est F elle-même.

R 43 – $\mathbb{K}[X]$ et $\mathbb{K}^-(X)$ sont supplémentaires dans $\mathbb{K}(X)$. $= \mathbb{K}[X] \oplus \mathbb{K}^-(X)$

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

Théorème 9 : 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 $m_1, \dots, m_n$:

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

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

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

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

Remarque

R 44 – Les $\left(\dfrac{1}{(X-a)^n}\right)_{(a,n) \in \mathbb{C} \times \mathbb{N}^*}$ est une base de $\mathbb{C}^-(X)$.

Pour $\mathbb{C}(X)$
$(X^n)_{n \in \mathbb{N}} \oplus \left(\dfrac{1}{(X-a)^n}\right)_{a \in \mathbb{C}, n \in \mathbb{N}^*}$

Propriété 25 : 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

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

Exemple : Le « cache »

E 6 – $F = \dfrac{1}{(X-1)(X+2)}$

Exemple : *Très classique*

E 7 – $F = \dfrac{1}{X^n - 1}$

Propriété 26 : 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,

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

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

Alors $\lambda_m = [\widetilde{(X-\alpha)^m F}](\alpha) = \dfrac{A(\alpha)}{B_1(\alpha)}$ 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.

Méthode 1

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

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

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

Exemple

E 8 – $F = \dfrac{2X+1}{X^3 - 2X^2 + X}$

Exemple

E 9 – $F = \dfrac{X}{(X^2-1)^2}$

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

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

Théorème 10 : 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 réels tels que

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

Méthode 2

Les méthodes 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).

Remarque

R 45 – Les $\frac{1}{(X-a)^n}$ pour $a\in\mathbb{R}$ et $n\in\mathbb{N}^*$ et les $\frac{1}{(X^2+pX+q)^n}$ et $\frac{X}{(X^2+pX+q)^n}$ pour $p,q\in\mathbb{R}$ tels que $p^2<4q$ et $n\in\mathbb{N}^*$ forment une base de $\mathbb{R}^-(X)$.

Exemple

E 10 – $F=\dfrac{X^3-1}{X^3+X}$

E 11 – $F=\dfrac{X^3}{(X-1)^3(X+2)}$

E 12 – $F=\dfrac{2X^2}{(X^2+1)^3}$

4 Décomposition en éléments simples de P'/P

Propriété 27 : Décomposition en éléments simples de P'/P

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

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

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

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

Remarque

R 46 – En considérant les ordres, on voit facilement que $\frac{P'}{P}$ n'a que des pôles simples.

Exemple

E 13 – $\displaystyle\sum_{\omega\in\mathbb{U}_n}\frac{1}{2-\omega}=?$

Voir exercice du TD : 28