C16 - Polynômes

Introduction

Sur $K = (\mathbb{Z}/_{2\mathbb{Z}}, +, \times)$ un corp,
Il existe 4 fonctions polynomiales

Conclusion :
Sur K il existe une infinité d'écritures et 4 fonctions polynômes.
Donc le monde des écritures est plus vaste que celui des fonctions.
Dans ce chapitre on étudiera les écritures de fonctions polynomiales, qu'on appelle polynômes.

Malheureusement, on verra pour $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$ On peut établir une correspondance bijective entre les polynômes et fonctions polynomiales, ce qui ne montre pas tout l'intérêt de ces objets abstraits.
Cependant les polynômes (sur des corps finis) sont fondamentaux en maths et servent aussi beaucoup (en pratique) cryptographie.

Pour bien différencier les polynômes des fonctions polynômes on utilisera la lettre X ou (Y, ...) dans leurs écritures

- Par exemple :
  $\mathcal{P} = X^{42} - 24X - \pi$

Définition formelle des écritures

Comment définir formellement ces "écritures"? :
A l'aide des coefficients.
Une idée serait de "coder" :

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

Par le $(n+1)$-uplet :

$$(a_0, a_1, a_2, \ldots, a_n) \in \mathbb{K}^{n+1}$$

Inconvénient (Pour la somme)

$$(a_1, \ldots, a_n)$$

$$(b_1, \ldots, b_p)$$

(ne sont pas de la même taille)

On complète le plus court uplet avec des 0 par avoir la même taille.

Construction des polynômes

On choisit une représentation plus adéquate :
On va représenter un polynôme par une suite infinie et ses coefs :
$\mathcal{P} = (-\pi, 24, -42, 0, \ldots, 1, 0, \ldots)$ (le 1 a la 43^{eme} place)

On veut donc un polynôme comme un élément de $\mathbb{K}^{\mathbb{N}}$
Cependant, avec les écritures qu'on connait, on obtiens pas toutes les suites de $\mathbb{K}^{\mathbb{N}}$, mais seulement celles qui sont nulles APDCR (A partir d'un certain rang) ou, ce qui revient au même, celles qui n'ont qu'un nombre fini de termes non nuls. On note provisoirement $\mathbb{K}^{(\mathbb{N})}$ cet ensemble.

L'addition sera alors faite :

$$(a_n) + (b_n) = (a_n + b_n)$$

Pour que ce soit plus pratique on notera :

$$(a_n) = \sum_{n=0}^{+\infty} a_n X^n$$

ce qui donne :

$$\sum_{n=0}^{+\infty} a_n X^n + \sum_{n=0}^{+\infty} b_n X^n = \sum_{n=0}^{+\infty} (a_n + b_n) X^n$$

et aussi :

$$\lambda \left(\sum_{n=0}^{+\infty} a_n X^n \right) = \sum_{n=0}^{+\infty} a_n X^n = \sum_{n=0}^{+\infty} (\lambda a_n) X^n$$

On obitens une structure :

$$(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$$

avec $\cdot$ mult par un scalaire
qui sera un $\mathbb{K}$-espace vectoriel

Multiplication de polynômes

Coté polynômes

$$\left(\sum_{p=0}^{+\infty} a_n X^n \right) \left(\sum_{q=0}^{+\infty} b_n X^n \right)$$

$$= (a_0 + a_1 X + \dots)(b_0 + b_1 X + \dots)$$

$$= \sum_{p=0}^{+\infty} a_n X^n$$

Coté suite :

On nomme ca la convolution

$$(a_n)_n * (b_n)_n = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_n = \left(\sum_{k=0}^{n} a_{n-k} b_k \right)_n = \left(\sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_q b_q \right)$$

On obtiens aussi un anneau commutatif :

$$(\mathbb{K}^{(\mathbb{N})}, +, *)$$

Notation : Anneau des polynômes

$$(\mathbb{K}[X], +, \times)$$

L'anneau des polynômes à coef dans $\mathbb{K}$

$(\mathbb{K}[X], +, \cdot, \times)$ est la $\mathbb{K}$ algèbre des polynômes à coefficient dans $\mathbb{K}$

Remarque

Polynomes	Suites
0	$(0, 0, \ldots)$
1	$(1, 0, \ldots)$
X	$(0, 1, 0, \ldots)$
X^k	$(0, 0, \ldots, 0, 1, 0, \ldots) = (S_{n,k})_{n\in\mathbb{N}}$

L'écriture est cohérente
car X^n est bien la puissance n^{ieme} de X par le produit qu'on vient de définir.
Plus généralement :

$$X^k X^l \approx (S_{n,k})_{n\in\mathbb{N}} * (S_{n,l})_{n\in\mathbb{N}} = \left(\sum_{i=0}^{n} \delta_{i,k}\delta_{n-i,l}\right)_n$$

$$= \left(\sum_{i=0}^{n} \delta_{i,k}\delta_{i,n-l}\right)_n = (\delta_{n,k+l})_n = X^{k+l}$$

I. Anneau $\mathbb{K}[X]$

Définition

Soit $u \in \mathbb{K}^{\mathbb{N}}$,
On dit que u est presque nulle si :

$$\{n \in \mathbb{N} | u_n \neq 0\}$$

est fini
On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites presque nulles.

Rappel

Grace a l'addition de $\mathbb{K}$ on a : $(\mathbb{K}^{\mathbb{N}}, +)$ un groupe abélien

Proposition

$\mathbb{K}^{(\mathbb{N})}$ est un sous groupe de $\mathbb{K}^{\mathbb{N}}$

Démonstration :
Par la caractérisation des sous groupes :

1. $$0_{\mathbb{K}^{\mathbb{N}}} \in \mathbb{K}^{(\mathbb{N})}$$
   (car $\varnothing$ et fini)
2. Stabilité par addition :
   Soient $u, v \in \mathbb{K}^{(\mathbb{N})}$
   Alors :
   $$\{n \in \mathbb{N} | u_n + v_n \neq 0\} \subset \{n \in \mathbb{N} | u_n \neq 0\} \cup \{n \in \mathbb{N} | v_n \neq 0\}$$
   Donc cet ensemble est fini (car une réunion d'ensembles finis est fini et une partie d'un ensemble fini est finie) Donc $u + v \in \mathbb{K}^{(\mathbb{N})}$
3. Stabilité par l'opposé
   Soit $u \in \mathbb{K}^{(\mathbb{N})}$
   Alors $\{n \in \mathbb{N} \mid -u_n \neq 0\} = \{n \in \mathbb{N} | u_n \neq 0\}$ est fini donc $-u \in \mathbb{K}^{(\mathbb{N})}$

Définition

On définit la multiplication externe

$$\begin{cases}\mathbb{K}\times\mathbb{K}^{(\mathbb{N})}\longrightarrow\mathbb{K}^{(\mathbb{N})}\\(\lambda,u)\longmapsto\lambda u\end{cases}$$

Proposition

On a les "4 props d'un espace vectoriel" déjà vues :

$$\begin{aligned}&(1):\forall u\in\mathbb{K}^{(\mathbb{N})},1\cdot u=u\\&(2):\forall\lambda,\mu\in\mathbb{K},\forall u\in\mathbb{K}^{(\mathbb{N})},(\lambda\cdot\mu)u=\lambda(\mu u)\\&(3):\forall\lambda,\mu\in\mathbb{K},\forall u\in\mathbb{K}^{(\mathbb{N})},(\lambda+\mu)u=\lambda u+\mu u\\&(4):\forall\lambda\in\mathbb{K},\forall u,v\in\mathbb{K}^{\mathbb{N}},\lambda(u+v)=\lambda u+\lambda v\end{aligned}$$

démo : en exo, très facile

Définition

Pour $u,v\in\mathbb{K}^{(\mathbb{N})}$, on définit $u*v$ (convolution de u et v) par

$$u*v=\left(\sum_{k=0}^{n}u_kv_{n-k}\right)_n=\left(\sum_{k=0}^{n}u_{n-k}v_k\right)_n=\left(\sum_{\substack{0\leq p,q\leq n\\ \overline{p+q=n}}}u_pv_q\right)_n$$

exo : vérifier les deux égalités

Propriété

$$\forall u,v\in\mathbb{K}^{(\mathbb{N})},u*v\in\mathbb{K}^{(\mathbb{N})}$$

démo : exo

Théorème

$(\mathbb{K}^{(\mathbb{N})},+,*)$ est un anneau commutatif

(On a aussi $(\mathbb{K}^{(\mathbb{N})},+,\cdot,*)$ est une $\mathbb{K}$-algèbre commutative.)

Démonstration :
-> Automatique : $(\mathbb{K}^{(\mathbb{N})},+)$ est un groupe abélien car $(\mathbb{K},+)$ l'est

-> Démontré : $\mathbb{K}^{(\mathbb{N})} \underset{s.g.}{\subset} \mathbb{K}^{\mathbb{N}}$

Reste a montrer :

- Les propretés de $*$ ($\times$)
- Les distributivités

La commutativité de $*$ est immediate par changement d'indices, pour les autres propriétés, les faire en exo.

On trouve comme neutre de $*$:

$$1 = (\delta_{n,0})_n = (1, 0, 0, \ldots)$$

Définition

On pose $X = (\delta_{n,q})_{n\in\mathbb{N}}$ est on l'appelle l'indéterminée par la loi $*$.

Lemme

Pour tout $k \in \mathbb{N}$,
X^k au sens de la loi $*$
s'écrit :

$$X^k = (\delta_{n,k})_{n\in\mathbb{N}} = (0, 0, \ldots, 0, 1, 0, \ldots)$$

1 a l'indice k

Démonstration : Par recurrence sur k.
Pour $k \in \mathbb{N}$, on pose :

$$\mathcal{A}_k : X^k = (\delta_{n,k})_{n\in\mathbb{N}}$$

- Initialisation

  $$X^0 = 1 = (\delta_{n,0})_{n\in\mathbb{N}}$$

  Car on est dans un anneau

- Hérédité
  Soit $k \in \mathbb{N}$ tq A_k,
  Alors

$$X^{k+1} = XX^k$$

Par hypothèse de recurrence et par def de la convolution :

$$XX^k(\delta_{n,k})_n * (\delta_{n,1})_n = \left(\sum_{l=0}^{n} \delta_{n-l,1}\delta_{l,k}\right)_n$$

Or,
$\delta_{l,k}$ est nul pour tout l si $n < k$

$$\text{Si } n < k, 0 = \delta_{n,k+1}$$
$$\text{Si } n \geq k, \delta_{n-k,1} = \delta_{n,k+1}$$

Ainsi $X^{k+1} = \delta_{n,k+1}$ ie A_{n+1} est vérifié

Propriétés

En notant $X = (0, 1, 0, \ldots)$
Tout polynôme $\mathcal{P}$ s'écrit de manière unique :

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n$$

Avec $(a_n)_n \in \mathbb{K}^{(\mathbb{N})}$ qui représente $\mathcal{P}$

Démonstration :
Avec notre construction :

$$\mathcal{P} = (a_n) \in \mathbb{K}^{(\mathbb{N})}$$

Il existe $N \in \mathbb{N}$ tq $\forall n > N, a_n = 0$
Alors $\mathcal{P} = (a_0, a_1, \ldots, a_N, 0, \ldots)$

Par opération de $\mathbb{K}^{\mathbb{N}}$:

$$\mathcal{P} = a_0(1,0,\ldots) + a_1(0,1,0\ldots) + \cdots + a_N(0,0,\ldots,1,0,\ldots)$$

1 a l'indice N

$$\mathcal{P} = \sum_{n=0}^{N} a_n X^n = \sum_{n=0}^{\infty} a_n X^n$$

Avec la convention qu'on ne somme que les termes non nuls (somme finie)

Définition

On écrit alors plus les polynômes que sous la forme précédente : CL des X^n.
À partir de cet instant, on oublie les notations avec les suites. On obtient un anneau commutatif (même algèbre !) qu'on appelle anneau des polynômes à une indéterminée (X) sur $\mathbb{K}$ et qu'on note $(\mathbb{K}[X], +, \times)$ (on oublie aussi la notation $*$)

Important : avec ces notations les calculs se font "comme d'habitude".

Remarque

Si on avait défini les polynômes sous forme d'écritures

$$\sum_{n=0}^{\infty} a_n X^n$$

avec (a_n) presque nulle on aurait dû démontrer toutes les propriétés de groupe, anneaux (espace vectoriel, algèbre) à la main.
Pour s’entraîner a la manipulation de ces écritures on va prouver les propriétés de la multiplicité des polynômes dans ce nouveau

cadre (Non nécessaire du point de vue purement logique (Le but ici est de s'entraîner)) :

Commutativité :

Soient $\mathcal{P}, \mathcal{Q} \in \mathbb{K}[X]$
Il s'écrirait

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n$$

$$\mathcal{Q} = \sum_{n=0}^{\infty} b_n X^n$$

avec $(a_n), (b_n) \in \mathbb{K}^{(\mathbb{N})}$
Alors

$$\mathcal{P}\mathcal{Q} = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_{n-k} b_k \right) X^n = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j} \right) X^n$$

avec le changement d'indice : $j = n - k$ et $k = n - j$

$$\mathcal{P}\mathcal{Q} = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} b_{n-j} a_j \right) X^n = \mathcal{Q}\mathcal{P}$$

Associativité :

Soient

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n$$

et

$$\mathcal{Q} = \sum_{n=0}^{\infty} b_n X^n$$

et

$$\mathcal{R} = \sum_{n=0}^{\infty} c_n X^n$$

des polynômes

Alors :

$$(\mathcal{P}\mathcal{Q})\mathcal{R} = \left(\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_{n-k}b_k\right)X^n\right)\left(\sum_{n=0}^{\infty} c_n X^n\right)$$

Pour $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} a_{n-k}b_k = \sum_{\substack{0\leq p,q\leq n \\ p+q=n}} a_p b_q$$

Excalidraw 1.

Alors :

$$(\mathcal{P}\mathcal{Q})R = \left(\sum_{n=0}^{\infty}\left(\sum_{\substack{0\leq p,q\leq n \\ p+q=n}} a_q b_q\right)X^n\right)\left(\sum_{n=0}^{\infty} c_n X^n\right)$$

Détails sur les calculs de sommes (aparté / Précisions faites par moi) :

Par définition de la convolution :

$$(\mathcal{P}\mathcal{Q})\mathcal{R} = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\left(\sum_{\substack{0\leq p,q\leq k \\ p+q=k}} a_p b_q\right)c_{n-k}\right)X^n$$

Par le changement d'indice : $r = n - k$

$$\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\left(\sum_{\substack{0\leq p,q\leq k\\ p+q=k}} a_p b_q\right) c_r\right) X^n$$

Changement d'écriture des sommes : (et parce-que c_r n'est pas dépendant des indices p et q) :

$$\sum_{n=0}^{\infty}\left(\sum_{\substack{0\leq k,r\leq n\\ r+k=n}}\left(\sum_{\substack{0\leq p,q\leq k\\ p+q=k}} a_p b_q c_r\right)\right) X^n$$

Ainsi :

$$\sum_{n=0}^{\infty}\left(\sum_{\substack{0\leq p,q,r\leq n\\ p+q+r=n}} a_p b_q c_r\right) X^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{\substack{0\leq l,r\leq n\\ l+r=n}}\left(\left(\sum_{\substack{0\leq p,q\leq l\\ p+q=l}} a_p b_q\right) c_r\right)\right) X^n = \sum_{n=0}^{\infty}\left(\sum_{\substack{0\leq p,q,r\leq n\\ p+q+r=n}} a_p b_q c_r\right) X^n$$

De même

$$\mathcal{P}(\mathcal{Q}\mathcal{R}) = \sum_{\substack{0\leq p,q,r\leq n\\ p+q+r=n}} a_p b_q c_r$$

Ainsi,

$$(\mathcal{P}\mathcal{Q})\mathcal{R} = \mathcal{P}(\mathcal{Q}\mathcal{R})$$

Retenir les formules :

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty}\left(\sum_{\substack{0\le p,q\le n\\ p+q=n}} a_p b_q\right) X^n$$

et

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right)\left(\sum_{n=0}^{\infty} c_n X^n\right) = \sum_{\substack{0\le p,q,r\le n\\ p+q+r=n}} a_p b_q c_r$$

Imaginer les suivantes (Destinés au meks chaud)

Soient $k \in \mathbb{N}^*$ et pour tout $i \in [\![1, k]\!]$, $(a_{i,n})_n \in \mathbb{K}^{(\mathbb{N})}$

Alors :

$$\prod_{i=1}^{k}\left(\sum_{n=0}^{\infty} a_{i,n} X^n\right) = \sum_{n=0}^{\infty}\left(\sum_{p\in I_{k,n}} \prod_{i=1}^{k} a_i p_i\right) X^n$$

où

$$I_{k,n} = \left\{(p_i)_{i=1}^{k} \in [\![0, n]\!]^k \middle| \sum_{i=1}^{k} p_i = n\right\}$$

Element neutre :

$$1 = \sum_{n=0}^{\infty} \delta_{n,0} X^n$$

Pour

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n$$

$$1 \times \mathcal{P} = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \delta_{n-k,0} a_k\right) X^n = \sum_{n=0}^{\infty} a_n X^n = \mathcal{P}$$

et $\mathcal{P} \times 1 = \mathcal{P}$
par commutativité de $\times$

Distributivité a gauche

Par commutativité de $\times$, la distributivité à gauche suffit :
Soient

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n$$

et

$$\mathcal{Q} = \sum_{n=0}^{\infty} b_n X^n$$

et

$$\mathcal{R} = \sum_{n=0}^{\infty} c_n X^n$$

Alors :

$$\mathcal{P}(\mathcal{Q} + \mathcal{R}) = \left(\sum_{n=0}^{\infty} a_n X^n\right) \left(\sum_{n=0}^{\infty} (b_n + c_n) X^n\right)$$

Par définition de X :

$$= \sum_{n=0}^{n} \left(\sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_p (b_q + c_q)\right) X^n$$

Par distributivité dans $\mathbb{K}$ et par linéarité de X

$$= \sum_{n=0}^{\infty} \left(\sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_p b_q + \sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_p c_q \right) X^n$$

Par distributivité mixte a droite et a gauche :

$$= \sum_{n=0}^{\infty} \left(\left(\sum_{p,q} a_q b_q \right) X^n + \left(\sum_{p,q} a_p c_q \right) X^n \right)$$

Par commutativité et associativité de + :

$$= \left(\sum_{n=0}^{\infty} \left(\sum_{p,q} a_p b_q \right) X^n \right) + \left(\sum_{n=0}^{\infty} \left(\sum_{p,q} a_p c_q \right) X^n \right) = \mathcal{PQ} + \mathcal{PR}$$

Propriété

L'application :

$$\phi : \begin{cases} \mathbb{K} \to \mathbb{K}[X] \\ \lambda \mapsto \lambda 1_{\mathbb{K}[X]} \end{cases}$$

est un morphisme d'anneau injectif

Démonstration :

Pour $\lambda, \mu \in \mathbb{K}$,

$$\phi(\lambda + \mu) = (\lambda + \mu) 1_{\mathbb{K}[X]} = \lambda 1_{\mathbb{K}[X]} + \mu 1_{\mathbb{K}[X]}$$

Par distributivité mixte a droite.

De plus

$$\phi(1_{\mathbb{K}}) = 1_{\mathbb{K}} 1_{\mathbb{K}[X]} = 1_{\mathbb{K}[X]}$$

et pour $\lambda, \mu \in \mathbb{K}$,

$$\phi(\lambda\mu) = (\lambda\mu) 1_{\mathbb{K}[X]} = (\lambda\mu) X^0$$

et

$$\phi(\lambda)\phi(\mu) = (\lambda 1_{\mathbb{K}[X]})(\mu 1_{\mathbb{K}[X]}) = (\lambda X^0)(\mu X^0) = (\lambda\mu)X^0$$

(inj ϕ en exo)

Alors on identifie $\mathbb{K}$ à son image $\phi(\mathbb{K})$ (qui lui est isomorphe par la propriété précédente)
Ainsi on a :

$$\mathbb{K} \subset \mathbb{K}[X]$$

Cet abus est possible puisqu'en le faisant les deux multiplications (externe et entre les polynômes) coincident :
Si $\lambda \in \mathbb{K}$ et $\mathcal{P} \in \mathbb{K}[X]$

$$\phi(\lambda) \cdot \mathcal{P} = (\lambda 1_{\mathbb{K}[X]})\mathcal{P} = \lambda(1_{\mathbb{K}[X]}\mathcal{P}) = \lambda P$$

On peut alors calculer avec les règles usuelles de calcul très simplement
Soient

$$\mathcal{P}_1 = 1 + 2X + 3X^2 \left(= \sum_{n=0}^{\infty} a_n X^n \text{ avec } (a_n) = (1, 2, 3, 0, \ldots)\right)$$

et

$$\mathcal{P}_2 = 4X + 5X^3 \left(= \sum_{n=0}^{\infty} b_n X^n \text{ avec } (b_n) = (0, 4, 0, 5, 0, \ldots)\right)$$

On a alors :

$$\mathcal{P}_1 + \mathcal{P}_2 = 1 + 6X + 3X^2 + 5X^3$$

et

$$\mathcal{P}_1\mathcal{P}_2 = 4X + 8X^2 + 17X^3 + 10X^4 + 15X^5$$

Définition

Soit $\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{K}[X]$
Alors on appelle de degré de $\mathcal{P}$ l'entier naturel :

$$deg(\mathcal{P})(= d^{\circ}\mathcal{P}) = sup_{\overline{\mathbb{R}}}\{n \in \mathbb{N} | a_n \neq 0\}$$

et si $\mathcal{P} \neq 0$:

$$deg(\mathcal{P}) = max_{\overline{\mathbb{R}}}\{n \in \mathbb{N} | a_n \neq 0\}$$

Par convention :

$$deg(0) = -\infty$$

On a alors :

$$\mathcal{P} = \sum_{n=0}^{deg(\mathcal{P})} a_n X^n$$

Définition

Pour $n \in \mathbb{N}$,

$$\mathbb{K}_n[X] = \{\mathcal{P} \in \mathbb{K}[X] \mid deg(\mathcal{P}) \leq n\}$$

Plus précisément :

Propriété

$$\forall, \mathcal{P}, \mathcal{Q} \in \mathbb{K}[X],$$

$$deg(\mathcal{P} + \mathcal{Q}) \leq max(deg(\mathcal{P}), deg(\mathcal{Q}))$$

et

$$deg(\mathcal{P}) \neq deg(\mathcal{Q}) \Rightarrow deg(\mathcal{P} + \mathcal{Q}) = max(deg(\mathcal{P}), deg(\mathcal{Q}))$$

Démonstration :
Soit $\mathcal{P}, \mathcal{Q} \in \mathbb{K}[X]$,
S'écrivant :

$$\mathcal{P} = \sum_{n=0}^{\infty} a_n X^n \text{ et } \mathcal{Q} = \sum_{n=0}^{\infty} b_n X^n$$

Alors

$$P + Q = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

Pour $n > max(deg(P), deg(Q))$,

$$a_n + b_n = 0 + 0 = 0$$

Donc

$$deg(P + Q) \leq max(deg(P), deg(Q))$$

Si $deg(P) \neq deg(Q)$,
quitte a échanger P et Q (+ est commutative), on peut supposer que $deg(P) > deg(Q)$
En particulier

$$deg(P) = d \in \mathbb{N}$$

e

$$a_d + b_d = a_d \neq 0$$

car ($deg(Q) < d$ et $deg(P) = d$)

Donc

$$deg(P + Q) \geq d$$

or

$$deg(P + Q) \leq d$$

par ce qui précède,

$$deg(P+Q) = d$$

Corollaire

$$\forall n \in \mathbb{N} \cup \{-\infty\}, \mathbb{K}_n[X] \underset{s.g.}{\subset} (\mathbb{K}[X], +)$$

Démonstration :
Soit $n \in \mathbb{N} \cup \{-\infty\}$,
Par la caractérisation des sous groupes :

- $\mathbb{K}_n[X] \subset \mathbb{K}[X]$ par définition de $\mathbb{K}_n[X]$
- $deg(0) = -\infty$ Donc $0 \in \mathbb{K}_n[X]$
- Par la propriété précédente : $\mathbb{K}_n[X]$ est stable pâr $+$
- $\mathbb{K}_n[X]$ est trivialement stable par passage a l'opposé :

$$\forall P \in \mathbb{K}[X], deg(-P) = deg(P)$$

Remarque

$\mathbb{K}_n[X]$ est un sous espace vectoriel de $\mathbb{K}[X]$ or il est de plus stable par multiplication externe.

ATTENTION :
$\mathbb{K}_n[X]$ n'est pas un sous anneau de $\mathbb{K}[X]$ pour $n \geq 1$
(mais l'est pour $n = -\infty$ et $n = 0$ car $\mathbb{K}_{-\infty}[X] = \{0\}$ et $\mathbb{K}_0[X] = \mathbb{K}$)

Propriété

$$\forall P, Q \in \mathbb{K}[X], deg(PQ) = deg(P) + deg(Q)$$

(Avec les conventions que $(-\infty) + n = -\infty$ pour tout $n \in \mathbb{N} \cup \{-\infty\}$)

Démonstration :

1. Si $P = 0$ ou $Q = 0$ alors :
   0 étant absorbant (on est dans un anneau)
   On a :
   $PQ = 0$ et la formule est vérifiée
2. Si $P \neq 0$ et $Q \neq 0$
   ie $deg(P), deg(Q) \in \mathbb{N}$

Alors P et Q s'écrivent :

$$P = \sum_{n=0}^{deg(P)} a_n X^n, Q = \sum_{n=0}^{deg(Q)} b_n X^n$$

Soit $n > deg(P) + deg(Q)$
Alors le coefficient du monôme de PQ de degré n est :

$$c_n = \sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_p b_q$$

Or pour tout $p, q \in \mathbb{N}$,

$$(p \leq deg(P) \text{ et } q \leq deg(Q)) \Rightarrow p + q < n$$

Donc par contraposition :

$$p + 1 \geq n \Rightarrow p > deg(P) \text{ ou } q > deg(Q) \Rightarrow a_p = 0 \text{ ou } b_q = 0$$

A fortiori, si $p + q = n$, $a_p b_q = 0$
Donc $c_n = 0$
Ainsi $deg(PQ) \leq deg(P) + deg(Q)$
Soit $n = deg(P) + deg(Q)$ alors :

$$c_n = \sum_{\substack{0 \leq p,q \leq n \\ p+q=n}} a_p b_q = a_{deg(P)} b_{deg(Q)} \neq 0$$

Car, pour $p, q \in [\![0, n]\!]$ tels que $p + q = n$

$$\begin{cases} p < deg(P) \Rightarrow q > deg(Q) \Rightarrow a_p b_q = a_p \times 0 = 0 \\ p > deg(P) \Rightarrow a_p b_q = 0 b_q = 0 \end{cases}$$

Donc

$$deg(PQ) \geq deg(P) + deg(Q)$$

et enfin

$$deg(PQ) = deg(P) + deg(Q)$$

Remarque

Si $P = 42X^{24} + 3X - 1$
et $Q = -42X^{24} - 3X^7$
alors $deg(P+Q) < max(deg(P), deg(Q))$

Définition

Soient $P, Q \in \mathbb{K}[X]$,
On note $Q \circ P$ ou $Q(P)$
Le polynôme composé de Q et P obtenu en remplaçant dans l'écriture de Q les X par P

Plus précisément :
si

$$Q = \sum_{n=0}^{\infty} b_n X^n$$

Alors

$$Q \circ P = Q(P) = \sum_{n=0}^{\infty} b_n P^n$$

(Cette somme est finie)

Remarque

Soit

$$P = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{K}[X]$$

$$P \circ X = P(X) = P$$

(Pas pour les fonctions seulement pour les polynômes)

Exemple

$Q = X^3 + X - 1$
$P = X^2$
$R = X + 1$
$S = 1$

$$Q \circ P = Q(X^2) = (X^2)^3 + X^2 - 1 = X^6 + X^2 - 1$$

$$Q \circ R = Q(X+1) = (X+1)^3 + (X+1) - 1 = X^3 + 3X^2 + 4X + 1$$

$$S \circ P = S(X^2) = 1$$

$$S \circ R = S(X+1) = 1$$

Propriété

$$\forall P, Q \in \mathbb{K}[X], deg(Q \circ P) = deg(Q)deg(P)$$

Démonstration en exo

Définition

Pour $P \in \mathbb{K}[X] \backslash \{0\}$
Le monôme de degré $deg(P)$ de P est appelé son terme dominant et son coefficient est appelé le coefficient dominant de P

Exemple

Le coef dominant de $\pi X^{42} + 3$ est π

Définition

$P \in \mathbb{K}[X]$ est dit unitaire ssi $P \neq 0$ et son coef dominant est 1

Exemple :

$X^{42} - 2X^{21}$ est unitaire

Exercice

Pour $P, Q \in \mathbb{K}[X]$ mq $PQ = 0 \Leftrightarrow (P = 0 \text{ ou } Q = 0)$

II. Divisibilité (Analogue sur $\mathbb{Z}$)

Définition

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

$$A|B \overset{def.}{\Leftrightarrow} \exists D \in \mathbb{K}[X], AD = B$$

(terminologie A divise B, B est multiple de A, etc...)

Propriété

1. $|$ est réflexive mais pas antisymétrique
2. Si

$$\forall D, A, B \in \mathbb{K}[X], \forall \lambda, \mu \in \mathbb{K}, (D|A \text{ et } D|B) \Rightarrow D|\lambda A + \mu B$$

3. $$\forall A, B, C, D \in \mathbb{K}[X], (A|B \text{ et } C|D) \Rightarrow AC|BD$$

En particulier si $n \in \mathbb{N}^*$ et $A|B$ alors $A^n|B^n$

4. On dit que $A, B \in \mathbb{K}[X]$ sont associés ssi

$$(A|B \text{ et } B|A)$$

Alors pour tout $A, B \in \mathbb{K}[X]$, A et B sont associés ssi'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$

Demonstration du 1., 2., 3. pareil que dans $\mathbb{Z}$.
Démonstration de la 4. :

- $\Leftarrow$ est facile.
  Soit $\lambda \in \mathbb{K}^*$ tq $A = \lambda B$
  Comme $\lambda B = A$ Donc $B|A$
  Puis $\frac{1}{\lambda}A = B$ Donc $A|B$
- $\Rightarrow$:
  Supposons que $A|B$ et $B|A$ avec $A \neq 0 \neq B$
  Comme $A|B$, il existe $D \in \mathbb{K}[X]$ tel que $AD = B$
  Donc $deg(A) + deg(D) = deg(B)$
  Comme $B \neq 0$, $D \neq 0$ Donc $deg(D) \in \mathbb{N}$ et $deg(A) \leq deg(B)$
  Par symétrie des rôles, $deg(B) \leq deg(A)$ donc
  $deg(B) = deg(A)$ Comme $A \neq 0$ et $B \neq 0$,
  $deg(A) = deg(B) \in \mathbb{N}$
  et comme $deg(A) + deg(D) = deg(B) = deg(A)$ dans $\mathbb{N}$
  Alors $deg(D) = 0$
  ie $D = \mu \in \mathbb{K}^*$
  et $A = \frac{1}{\mu}B$ avec $\frac{1}{\mu} \in \mathbb{K}^*$ Si $A = 0$ ou $B = 0$,
  Quitte a échanger A et B, $A = 0$ et comme $A|B$, $B = 0$ et
  $0 = 1.0$ avec $1 \in \mathbb{K}^*$ Dans tous les cas, $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$

Remarque

Unification des deux résultats dans A qui est $\mathbb{Z}$ ou $\mathbb{K}[X]$:
Deux éléments A et B sont associés
ssi
il existe $D \in A^\times$ tel que $A = DB$
ie A et B son égaux à la multiplication par un inversible près

Rappel

$\mathbb{Z}^{\times} = \{-1, 1\}$
et ici : $K[X]^{\times} = \mathbb{K}^{\times}$

Propriété

$$(\mathbb{K}[X])^{\times} = \mathbb{K}^{*}$$

Démonstration :
Par double inclusion :

- "$\supset$" est triviale (si $\lambda \in \mathbb{K}^{\times}$, $\lambda \times \frac{1}{\lambda} = 1$)
- "$\subset$"
  Soit $P \in (\mathbb{K}[X])^{\times}$
  Il existe $Q \in \mathbb{K}[X]$ tq $PQ = 1$
  Et alors $deg(PQ) = 0$
  ie $deg(P) + deg(Q) = 0$
  Ainsi d'abord $P, Q \neq 0$ ($deg(0) = -\infty$)
  Donc $deg(P), deg(Q) \in \mathbb{N}$
  et comme leur somme est nulle,
  alors $deg(P) = deg(Q) = 0$
  Donc en particulier $P \in \mathbb{K}^{\times}$

Exercice

Diviser $3X^3 + 2X^2 + X$ par $X - 1$
Exalibur 2

$$3X^3 + 2X^2 + X = (X-1)(3X^2 + 5X + 6) + 6$$

Théorème

$$\forall A, B \in \mathbb{K}[X], B \neq 0 \Rightarrow \exists! Q, R \in \mathbb{K}[X], \begin{cases} A = BQ + R \\ deg(R) < deg(B) \end{cases}$$

Démonstration :

Soit $A, B \in \mathbb{K}[X]$ tq $B \neq 0$

Unicité :

Soient (Q_1, R_1) et (Q_2, R_2) convenant,

On a :

$$BQ_1 + R_1 = A = BQ_2 + R_2$$

Donc :

$$B(Q_1 - Q_2) = R_2 - R_1$$

On a alors :

$$deg(B) + deg(Q_1 - Q_2) = deg(R_2 - R_1) \leq max(deg(R_1), deg(R_2)) < deg$$

Donc

$$deg(Q_1 - Q_2) = -\infty$$

ie $Q_1 = Q_2$

Puis en reportant dans $B(Q_1 - Q_2) = R_2 - R_1$,

$$R_1 = R_2$$

Existence

Elle est évidente si $deg(B) = 0$

$$B = \lambda \in \mathbb{K}^{\times}, \text{ donc } A = \lambda \left(\frac{1}{\lambda} A\right) + 0$$

On suppose alors $deg(B) \geq 1$

On raisonne par récurrence forte sur $n = deg(A)$

Si $n < deg(B)$, $A = B \times 0 + A$ convient

en particulier cela couvre le cas $A = 0$

On suppose maintenant le cas ou $A \neq 0$

ie $n \in \mathbb{N}$
On pose pour $n \in \mathbb{N}$,

$$\mathcal{A}_n :'' \forall A \in \mathbb{K}[X], (deg(A) = n \Rightarrow)''$$

- Initialisation :
  $\mathcal{A}_0$ et $\mathcal{A}_{deg(B)}$ sont vraies par la remarque préliminaire
- Hérédité
  Soit A de degré n
  On écrit :

  $$A = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

  et

  $$B = b_p X^p + b_{p-1} X^{p-1} + \cdots + b_0$$

  avec $a_n \neq 0$ et $b_p \neq 0$ et $n \geq p$ Alors on pose
  $A_1 = A - \frac{a_n}{b_p} X^{n-p} B$
  On a : $deg(A_1) < deg(A)$
  Donc par (H.R.F.) ou la fait que $A_1 = 0$,
  Il existe $Q_1, R_1 \in \mathbb{K}[X]$ tel que $A_1 = BQ_1 + R_1$, et
  $deg(R_1) < deg(B)$ Alors

  $$A = B\left(\frac{a_n}{b_p} X^{n-p} + Q_1\right) + R_1$$

  Ainsi $\mathcal{A}_{n+1}$ est prouvé par récurrence forte : $\forall n \in \mathbb{N}, \mathcal{A}_n$

Exercice

Faire la division euclidienne de :

$$X^4 + 2X^3 - 4X^2 + 6X - 1$$

par

$$X^2 + X + 1$$

et trouver

$$Q = X^2 + X - 6$$

$$R = 11X + 5$$

Exercice

Soient $n \in \mathbb{N}$ et $a \in \mathbb{R}$,
Déterminer le reste de la division euclidienne de :

$$A = (\sin(a)X + \cos(a))^n$$

par

$$B = X^2 + 1$$

III. Fonctions polynomiales et racines

Définition

Pour

$$P = \sum_{n=0}^{d} a_n X^n \text{ avec } a_d \neq 0$$

Un polynôme non nul, on définit sa fonction polynôme (ou polynomiale) associé $\tilde{P}$ par

$$\tilde{P} : \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto \sum_{n=0}^{d} a_n x^n \end{cases}$$

Pour $P = 0_{\mathbb{K}[X]}$
On pose :

$$\tilde{P} : \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto 0 \end{cases}$$

Exemple

Si $P = X^2 - 1 \in \mathbb{R}[X]$

$$\tilde{P} : \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto x^2 - 1 \end{cases}$$

Définition

On appelle racine ou zéro de $P \in \mathbb{K}[X]$ tout $\alpha \in \mathbb{K}$: tel que $\tilde{P}(\alpha) = 0$

Exemple

Les racines (ou zéros) de $X^2 - 1 \in \mathbb{R}[X]$ sont -1 et 1
L'unique racine de $X^3 - 1 \in \mathbb{R}[X]$ est 1
Mais $X^3 - 1 \in \mathbb{C}[X]$ a trois racines $1, j$ et j^2

Cependant par abus de langage on parlera parfois des "racines complexes" ou "réelles" de $X^3 - 1$

Ainsi $P \to \tilde{P}$ est une application de $\mathbb{K}[X]$ vers l'ensemble des fonctions polynômes

Proposition

$$\forall P, Q \in \mathbb{K}[X], \forall \lambda, \mu \in \mathbb{K}, \begin{cases} \lambda P \widetilde{+ \mu} Q = \lambda \widetilde{P} + \mu \widetilde{Q} \\ \widetilde{PQ} = \tilde{P}\tilde{Q} \\ \widetilde{Q \circ P} = \tilde{Q} \circ \tilde{P} \end{cases}$$

Problème de formatage
Au dessus de
$\lambda P + \mu Q$
PQ
$Q \circ P$

à gauche de l'égalité
on a un "grand" tilde au dessus

Propriété

$$\begin{cases} \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}} \\ P \mapsto \tilde{P} \end{cases}$$

est un morphisme d'anneaux dont l'image est le sous anneau des fonctions polynomiales
(c'est aussi un morphisme d'anneaux injectif)

!!

Démonstration :
Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$,

$$\tilde{\lambda} : \begin{cases} \mathbb{K} \to \mathbb{K} \\ x \mapsto \lambda \end{cases}$$

par déf de $\sim$

Pour $x \in \mathbb{K}$,
En notant :

$$P = \sum_{n=0}^{\infty} a_n X^n \text{ et } Q = \sum_{n=0}^{\infty} b_n X^n$$

$$(\lambda P \tilde{+} \mu Q)(x) = \left(\lambda \sum_{n=0}^{\infty} a_n X^n \tilde{+} \mu \sum_{n=0}^{\infty} b_n X^n \right)(x)$$

$$= \left(\sum_{n=0}^{\infty} (\lambda a_n + \mu b_n) X^n \right)(x)$$

$$= \sum_{n=0}^{\infty} (\lambda a_n + \mu b_n) x^n = \lambda \sum_{n=0}^{\infty} a_n x^n + \mu \sum_{n=0}^{\infty} b_n x^n = (\lambda \tilde{P} + \mu \tilde{Q})(x)$$

Donc :

$$\lambda P \tilde{+} \mu Q = \lambda \tilde{P} + \mu \tilde{Q}$$

Les 2 autres sont a faire en exo.

Corrollaire

Car $P \mapsto \tilde{P}$ préservent $+$ et $\times$ et envoie $1_{\mathbb{K}[X]}$ sur $(x \mapsto 1) = 1_{\mathbb{K}^{\mathbb{K}}}$

Remarque importante

$P \neq \tilde{P}$ (deux objets de natures différentes)
Mais si $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$

$$P(\lambda) = P \circ \lambda = \sum_{n=0}^{\infty} a_n \lambda^n = \tilde{P}(\lambda)$$

On peut donc écrire $P(\lambda)$ qui veut tuer $\tilde{P}(\lambda)$ mais attention, P n'est pas une application

Définition

$P(\lambda) \in \mathbb{K}$ s'appelle l'évaluation de P en λ (et non P appliqué à lambda)

Propriété

Soient, $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$
Alors,
λ est racine de P ssi $(X - \lambda) | P$

Remarque

Le degré du reste < le degré du diviseur

Démonstration :
On fait la division euclidienne de P par $X - \lambda (\neq 0)$:

$$P = (X - \lambda)Q + \mu, \text{ avec } \mu \in \mathbb{K}$$

et on évalue ses membres en λ ce qui donne :

$$P(\lambda) = (\lambda - \lambda)Q(\lambda) + \mu$$

ie

$$P(\lambda) = \mu$$

Ainsi λ est racine de P
ssi $P(\lambda) = 0$
ssi $\mu = 0$

Si $\mu = 0, P = (X - \lambda)Q$
Donc
$(X - \lambda)|P$

Réciproquement si $(X - \lambda)|P$
Alors P s'écrit $P = (X - \lambda)D$

Corollaire

Tout $P \in \mathbb{K}[X]\backslash\{0\}$
a au plus $deg(P)$ racines

Démonstration :
Soient $\alpha_1, \ldots, \alpha_k$ racines deux a deux distincts de P alors
$P = (X - \alpha_1)P_1$ avec $P_1 \in \mathbb{K}[X]\backslash\{0\}$
Puis

$$P_1 = (X - \alpha_2)P_2$$

Or

$$P_2 \in \mathbb{K}[X]\backslash\{0\}$$

Par récurrence rapide,

$$P = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_k) P_k$$

avec $P_k \neq 0$

Donc $deg(P) = k + deg(P_k) \geq k$

Corollaire

$$\phi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}} \\ P \mapsto \tilde{P} \end{cases}$$

C'est un morphisme injectif
Car $\mathbb{K}$ est infini.

Démonstration :
Soient $P, Q \in \mathbb{K}[X]$ tq $\tilde{P} = \tilde{Q}$
On a alors $P \tilde{-} Q = 0_{\mathbb{K}^{\mathbb{K}}}$
Donc $P - Q$ a une infinité de racines
Donc $P - Q = 0$ ie $P = Q$

Remarque

Attention ce résultat est faux par le corp fini (comme déjà vu avec $\mathbb{Z}/_2\mathbb{Z}[X]$ en introduction)

Remarque

Si on autorise les corps à être non commutatifs, il n'y a pas de division euclidienne et le résultat est aussi faux : $X^2 + 1$ a une infinité de racines dans $\mathbb{H}$ (corp des quaternions)

Définition

Soient $p \in \mathbb{K}[X] \backslash \{0\}$ et $\lambda \in \mathbb{K}$
On appelle multiplicité de λ dans P l'entier naturel :

$$m_\lambda = max\{k \in \mathbb{N} \mid (X-\lambda)^k | P\}$$

$$\Leftrightarrow P = (X-\lambda)^{m_\lambda} Q$$

Avec $Q(\lambda) \neq 0$

Caractérisation

$$P(\lambda) = P'(\lambda) \cdots = P^{(m_\lambda - 1)}(\lambda) = 0$$

et

$$P^{(m_\lambda)}(\lambda) \neq 0$$

Remarque

Elle vaut 0 si 0 n'est pas racine de P

Définition

Une racine de P de multiplicité :

1 est appelé racine simple

2 est appelé racine double

etc...

Exemple

$P \in \mathbb{C}[X]$ de degré 2
possède

- Soit une racine double
- Soit deux racines simples

Définition

Soit $P \in \mathbb{K}[X] \backslash \{0\}$
On dit que P est scindé s'il est constant ou s'écrit comme
polynômes de degré 1.

Exemple

$$42 \text{ et } 2(X-1)(X-3)^3$$

Sont scindés
Mais

$$X^2 + X + 1 \in \mathbb{R}[X]$$

n'est pas scindé et 0 n'est pas scindé

Ecriture d'un polynôme scindé P

$$P = a_d \prod_{i=1}^{d} (X - \lambda_i)$$

où $\lambda_1, \ldots, \lambda_d$ sont les racines décrites avec multiplication donc éventuellement égales

Autre Ecriture :
On regroupe les racines multiples ce qui donne

$$P = a_d \prod_{j=1}^{k} (X - \mu_j)^{m_j}$$

avec :
a_d : coefficient dominant
Pour tout j,
m_j est la multiplicité de μ_j dans P.
Ou
$\mu_1, \ldots, \mu_k$ sont les racines décrites
Sans multiplicité donc deux a deux distinctes

Exemple

s'écrit

$$P = 2(X-1)(X+3)(X+3)(X+3) = 2\prod_{i=1}^{4}(X-\lambda_i)$$

avec
$\lambda_1 = 1$ et $\lambda_2 = \lambda_3 = \lambda_4 = -3$

et aussi

$$P = 2(X-1)(X+3)^3 = 2\prod_{j=1}^{2}(X-\mu_j)^{m_j}$$

avec :
$\mu_1 = 1$
$\mu_2 = -3$
et
$m_1 = 1$
$m_2 = 3$

Propriété : Formules de Viète

Soit $P = \sum_{n=0}^{d} a_n X^n$ de degré d avec $a_d \neq 0$
qu'on suppose scindé de racines $\lambda_1, \dots, \lambda_d$ décrites avec multiplicité
Alors pour tout $p \in [\![1, d]\!]$

$$\sigma_p = \sum_{1 \leq i_1 \leq i_2 \leq \dots < i_p \leq d} \lambda_{i_1}\lambda_{i_2}\dots\lambda_{i_p} = (-1)^p \frac{a_{d-p}}{a_d}$$

Par ♡ :

$$\sigma_d = \sum_{i=1}^{d} \lambda_i = -\frac{a_{d-1}}{a_d}$$

et

$$\sigma_d = \prod_{j=1}^{d} \lambda_j = (-1)^d \frac{a}{a_d}$$

Cas particulier déjà connu

$$P = aX^2 + bX + c \in \mathbb{C}[X]$$

On sait que P a deux racines si on les compte avec multiplicité, λ_1 et λ_2 (éventuellement égales). Et

$$\begin{cases} \sigma_1 = \lambda_1 + \lambda_2 = -\frac{b}{a} \\ \sigma_2 = \lambda_1\lambda_2 = \frac{c}{a} \end{cases}$$

Remarque

$$\sigma_p = \sum_{1 \leq i_1 \leq i_2 \leq \cdots < i_p \leq d} \quad \prod_{j=1}^{p} \lambda_{i_j}$$

Et même mieux

$$\sigma_p = \sum_{A \in \mathcal{P}_p([1,d])} \prod_{i \in A} \lambda_i$$

Démonstration (Non formelle):

$$\frac{1}{a_d} P = (X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_d)$$

$$= X^d - (\lambda_1 + \lambda_2 + \cdots + \lambda_d)X^{d-1} +$$

$$+(\lambda_1\lambda_2 + \lambda_1\lambda_3 + \cdots + \lambda_1\lambda_d + \lambda_2\lambda_3 + \cdots + \lambda_{d-1}\lambda_d)X^{d-2}$$

$$\dots + (-1)^p \left(\sum_{1 \leq i_1 < i_2 \dots < i_p \leq d} \lambda_{i_1} \lambda_{i_2} \dots \lambda_{i_p} \right) X^{d-p}$$

$$\dots + (-1)^d \prod_{j=1}^{d} \lambda_j$$

En identifiant les coefficients (car deux polynômes sont égaux (l'écriture $P = \sum_{n=0}^{\infty} a_n X^n$) est unique)

Pour tout $p \in [\![1, q]\!]$, !!!!!!!!!!!!!!!!!!!!! Pas sur demander a qqn

$$\frac{a_{d-p}}{a_d} = (-1)^p \sum_{1 \leq i_1 < i_2 \dots < i_p \leq d} \lambda_{i_1} \lambda_{i_2} \dots \lambda_{i_p}$$

et

$$\frac{1}{(-1)^p} = (-1)^p$$

Donc,

$$\sigma_p = (-1)^p \frac{a_{d-p}}{a_d}$$

Exercice

$$X^4 + X^2 + 1$$

est scindé sur $\mathbb{R}$ / sur $\mathbb{C}$
idem pour :
$X^2 - 2X + 1$
$X^2 - 1$
$X^2 + X + 1$
$X^3 - 1$

IV. Dérivation

Définition

Alors le polynôme dérivé de P est :

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

Propriété

Si $\mathbb{K} = \mathbb{R}$, $\tilde{P}' = (\tilde{P})'$

Propriété

Soient $P \in \mathbb{K}[X] \backslash \{0\}$ et $d = deg(P)$
On a :

$$P^d \in \mathbb{K}^*$$

$$P^{(d+1)} = 0$$

Démonstration : En exo, facile

Propriété

Opération sur les dérivés (masculin)
Soient $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$
On a :

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q'$$

$$(PQ)' = P'Q + PQ'$$

$$\forall n \in \mathbb{N}, (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(n-k)} Q^{(k)}$$

(Formule de Leibniz)

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

Remarque

Si $\mathbb{K} = \mathbb{R}$ on a des preuves très simples. Par exemple :

$$(\tilde{PQ})' = \tilde{PQ}' = (\tilde{P}\tilde{Q})' = \tilde{P}'\tilde{Q} + \tilde{P}\tilde{Q}' = P'Q \tilde{+} PQ'$$

Donc $(PQ)' = P'Q + PQ'$

Démonstrations :

Dans le cas général :
Cas des CL Immédiat

- Produit :

$$PQ = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} a_{n-k} b_k \right) X^n$$

Donc,

$$P'Q + PQ' =$$

$$\left(\sum_{n=0}^{\infty}(n+1)a_{n+1}X^n\right)\left(\sum_{n=0}^{\infty}b_nX^n\right) + \left(\sum_{n=0}^{\infty}a_nX^n\right)\left(\sum_{n=0}^{\infty}(n+1)b_{n+1}X^n\right)$$

$$= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k}\right)X^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k} + \sum_{k=-1}^{n-1}a_{k+1}(n-k)b_{n-k}\right)X^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{k=-1}^{n-1}(k+1)a_{k+i}b_{n-k} + \sum_{k=-1}^{n}(n-k)a_{k+1}b_{n-k}\right)X^n$$

car $(-1+1)a_{-1+1}b_{n+1} = 0$ et $(n-n)a_{n+1}b_0 = 0$

$$= \sum_{n=0}^{\infty}(n+1)\left(\sum_{k=-1}^{n} a_{k+1}b_{n-k}\right)X^n$$

$$= \sum_{n=0}^{\infty}(n+1)\left(\sum_{k=0}^{n+1} a_k b_{(n+1)-k}\right)X^n = \left(\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)X^n\right) = (PQ)'$$

- Composition :

$$(Q \circ P)' = \left(\sum_{n=0}^{\infty} b_n P^n\right)' \stackrel{C.L.}{=} \sum_{n=0}^{\infty} b_n (P^n)'$$

$$\stackrel{\text{lemme}}{=} \left(\sum_{n=1}^{\infty} n b_n P^{n-1}\right)P' = (Q' \circ P)P'$$

- Formule de Leibniz a faire en copiant la démonstration du binôme

Lemme : pour montrer la composition

$$(P^n)' = \begin{cases} nP^{n-1}P' \text{ si } n \geq 1 \\ 0 \text{ si } n = 0 \end{cases}$$

Par récurrence pour $n \geq 1$ ($n = 0$ à part)
On pose pour $n \in \mathbb{N}^*$,

$$\mathcal{A}_n :'' \ (P^n)' = nP^{n-1}P' \ ''$$

Initialisation

$(P^1)' = P' = 1 \times P^0 \times P'$ Donc $\mathcal{A}_1$

Hérédité

Soit $n \in \mathbb{N}$, tq $\mathcal{A}_n$
On a alors :

$$(P^{n+1})' = (P \times P^n)' = P' \times P^n + P \times (nP^{n-1}P') = (n+1)P^nP'$$

Donc $\mathcal{A}_{n+1}$

Définition

Pour $P \in \mathbb{K}[X]$,
un polynôme primitive de P est un $Q \in \mathbb{K}[X]$ tq $Q' = P$

Propriété

Les primitives de $P = \sum_{n=0}^{\infty} a_n X^n$
sont les

$$\sum_{n=0}^{\infty} \frac{a_n}{n+1} X^{n+1} + C,\ C \in \mathbb{K}$$

ie les :

$$\sum_{n=0}^{\infty} \frac{a_{n-1}}{n} X^n + C,\ C \in \mathbb{K}$$

Démonstration
Exo facile ($Q = \sum_{n=0}^{\infty} b_n X^n$ dériver et identifier)

Théorème : Formule de Taylor polynomiale au point $a \in \mathbb{K}$

Soient $P \in \mathbb{K}[X] \backslash \{0\}$ et $a \in \mathbb{K}$
Alors

$$P = \sum_{k=0}^{deg(P)} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Démonstration :
Par récurrence
On pose pour $d \in \mathbb{N}$,

$$\mathcal{B}_d :'' \text{ Pour tout } P \in \mathbb{K}[X] \text{ de degré } d, P = \sum_{k=0}^{deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k \text{ ''}$$

Initialisation

Soit $P \in \mathbb{K}[X]$ de degré 0, ie $P = \lambda \in \mathbb{K}^*$
Alors

$$\sum_{k=0}^{deg(P)} \frac{P^{(k)}(a)}{0!}(X-a)^0 = \lambda = P$$

Ainsi $\mathcal{B}_0$ est vraie

Hérédité

Soit $d \in \mathbb{N}$ tq $\mathcal{B}_n$,
Soit $P \in \mathbb{K}[X]$ tq $deg(P) = d+1$
Alors $deg(P') = d$ donc on peut lui appliquer l'hypothèse de récurrence et

$$P' = \sum_{k=0}^{d} \frac{P^{(k+1)}(a)}{k!}(X-a)^k$$

En primitivant,

$$P = \sum_{k=0}^{d} \frac{p^{(k+1)}(a)}{k!} \times \frac{1}{k+1}(X-a)^{k+1} + C$$

Ou $C \in \mathbb{R}$

Donc

$$C = P(a) = \frac{P^{(0)}(a)}{0!}(x-a)^0$$

et

$$P=\sum_{k=0}^{d+1}\frac{P^{(k)}(a)}{k!}(x-a)^k$$

Ainsi
$\mathcal{B}_{d+1}$ est vérifiée

Par récurrence le résultat est prouvé

Corollaire fondamental

Soient $P\in\mathbb{K}[X]\backslash\{0\}$, $\lambda\in\mathbb{K}$ et $n\in\mathbb{N}$,
Alors λ est "racine" de P de multiplicité m ssi

$$P(\lambda)=P'(\lambda)=\cdots=P^{(n-1)}=0$$

et

$$P^{(n)}(\lambda)\neq 0$$

Démonstration :
Par la FTP de p en λ,

$$P=\sum_{k=0}^{deg(P)}\frac{p^{(k)}(\lambda)}{k!}(X-\lambda)^k$$

Si on suppose

$$\begin{cases}P(\lambda)=P'(\lambda)=\cdots=P^{(n-1)}(\lambda)=0\\ P^{(n)}(\lambda)\neq 0\end{cases}$$

Alors

$$P=\sum_{k=n}^{deg(P)}\frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k$$

$$= (X-\lambda)^n \sum_{k=n}^{deg(P)} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-n}$$

Par le changement d'indice :

$$\left[\left[\begin{matrix} k = n + g \\ g = k - n \end{matrix}\right.\right.$$

On a :

$$P = (X-\lambda)^n \sum_{j=0}^{deg(P)-1} \frac{P^{(n+g)}(\lambda)}{(n-g)!}(X-\lambda)^{g}$$

avec

$$Q(\lambda) = \frac{P^{(n)}(\lambda)}{n!} \neq 0$$

Donc λ est de multiplicité n dans P

Réciproquement :

Supposons que λ soit de multiplicité n dans P

Alors P s'écrit

$$P = (X-\lambda)^n Q$$

avec $Q(\lambda) \neq 0$

On a alors pour $n \leq n-1$

$$P^{(n)} = \sum_{k=0}^{n} \binom{n}{k} \frac{n!}{(n-k)!}(X-\lambda)^{n-k} Q^{(n-k)}$$

Donc

$$P^{(n)}(\lambda) = 0$$

et aussi

$$P^{(n)}=\sum_{k=0}^{n}\frac{n!}{(n-k)!}(X-\lambda)^{n-k}Q^{(n-k)}$$

Donc :

$$P^{(n)}(\lambda)=n!Q(\lambda)\neq 0$$

Remarque

Pour $n=0$, λ n'est pas racine de P

Exemple

$P=X^3-3X+2$, $P'=3X^2-3$ et $P''=6X$
Or

$$\begin{cases}P(1)=P'(1)=0\\ P''(1)=6\neq 0\end{cases}$$

Donc 1 est racine double de P

et aussi :

$$\begin{cases}P(-2)=0\\ P'(-2)=9\neq 0\end{cases}$$

Donc 2 est racine simple de p

V Arithmétique dans $\mathbb{K}[X]$

1. PGCD

Définition

Pour $A,B\in\mathbb{K}[X]$,
un PGCD de A et B est un $D\in\mathbb{K}[X]$ tel que :

$$\begin{cases} D|A \text{ et } D|B \\ \forall C \in \mathbb{K}[X], ((C|A \text{ et } C|B) \Rightarrow C|D) \end{cases}$$

Théorème : Existence et unicité du PGCD

Soient $A, b \in \mathbb{K}[X]$,
Si $A = B = 0$
0 est PGCD de A et B et c'est le seul
On note $A \wedge B = 0$

Existence :

Si $A \neq 0$ ou $B \neq 0$, l'ensemble des diviseurs communs unitaires de A et B possède un plus grand élément au sens de la restriction de ma relation $|$ à l'ensemble des polynômes unitaires.
Ce maximum est un $PGCD$, on l'appelle le PGCD de A et B et on le note $A \wedge B$

Unicité

De plus tout PGCD de A et B est assuré à A et B et réciproquement, ie
Les PGCD de A et B sont les $\lambda A \wedge B$ pour $\lambda \in \mathbb{K}^*$

Démonstration :
Cas $A = B = 0$ en exo
Cas ou $A \neq 0$ et $B \neq 0$,

Unicité

Soient D_1 et D_2 deux PGCD DE A et B
Comme D_1 est diviseur commun et D_2 et PGCD de A et B, alors $D_1|D_2$
Par symétrie des rôles, $D_2|D_1$ donc D_1 et D_2 sont associées ie $\exists \lambda \in \mathbb{K}^*, D_2 = \lambda D_1$

Existence

L'existence provient de l'Algorithme d'Euclide appliqué à A et B lorsque $B \neq 0$ de B à A sinon en normalisant le PGCD à la fin pour avoir un polynôme unitaire.
De plus si on applique l'algorithme d'Euclide étendu, on prouve en même temps :

Propriété : Relation de Bézout

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

Remarque

Le cas $A = B = 0$ est trivial

Remarque

Implicitement l'enoncé du Théorème, on a dit que la restricition de la relation de divisibilité à l'ensemble des polynômes unitaires est une relation d'ordre. (Comme $|$ est déjà réflexive et transitive, il n'y a qu'a vérifier l'anisymétrie, ce qui est direct)

Lemme de l'Algorithme d'Euclide

Pour, $A, B \in \mathbb{K}[X]$ tq $B \neq 0$ et $A = BQ + R$ la division euclidienne de A par B, $A \wedge B = B \wedge R$

et l'aglorithme d'Euclide étendu sont identique au cas de $\mathbb{Z}$

Propriété

Pour $(A, B) \in (\mathbb{K}[X])^2 \backslash \{(0, 0)\}$,
$A \wedge B$ est aussi le diviseur commun unitaires de A et B de degré maximal

2. Polynômes premiers entre eux

Définition

$A, B \in \mathbb{K}[X]$ sont premiers entre eux ssi $A \wedge B = 1$ ce qui équivaut à ce que les seuls diviseurs commun soient les $\lambda \in \mathbb{K}^*$

Théorème de Bézout

$$\forall A, B \in \mathbb{K}[X], A \wedge B = 1 \Leftrightarrow (\exists u, v \in \mathbb{K}[\mathbb{X}], AU + BV = 1)$$

Démonstration :

$\Rightarrow$ par la relation de bézout

$\Leftarrow$ si $D|A$ et $D|B$, $D|A$ et $D|AU + BV = 1$ etc

Théorème de Gauss

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

$$\left.\begin{array}{l} A|BC \\ A \wedge B = 1 \end{array}\right\} \Rightarrow A|C$$

Théorème de divisibilité par produit

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

$$\left.\begin{array}{l} A|C \\ B|C \\ A \wedge B = 1 \end{array}\right\} \Rightarrow AB|C$$

3. PGCD de plus de 2 polynômes

Définition

Pour $A_1, A_2, \ldots, A_n \in \mathbb{K}[X]$, un PGCD est un $D \in \mathbb{K}[X]$ tq

$$\begin{cases} \forall i & nbsp; \in [\![1, n]\!], C|A_i \\ \forall C \in \mathbb{K}[X], ((\forall i \in [\![1, n]\!], C|A_i) \Rightarrow C|D) \end{cases}$$

Théorème

Si $A_1 = \cdots = A_n = 0$ alors le seul PGCD est 0.
Sinon, l'ensemble des diviseurs communs unitaires des A_i possède un élément maximum pour la relation $|$ restreint a l'ensemble des polynomes unitaires, qu'on note $A_1 \wedge \cdots \wedge A_n$ et les PGCD des A_i sont les $\lambda A_1 \wedge \cdots \wedge A_n, \lambda \in \mathbb{K}^*$ et $A_1 \wedge \ldots A_n$ est aussi le diviseur commun unitaire des A_i de degré max.

Remarque

$A_1 \wedge \cdots \wedge A_n$ est appelé le PGCD des A_i

Propriété : Relation de Bézout

$$\forall_{A_1, \ldots, A_n} \in \mathbb{K}[X], \exists U_1, \ldots, U_n \in \mathbb{K}[X], \sum_{i=1}^{n} A_i U_i = \bigwedge_{i=1}^{n} A_i$$

Tout cela se prouve comme dans $\mathbb{Z}$ en fait la loi $\wedge$ est commutative et associative ce qui permet de calculer le PGCD et éventuellement de trouver des coefs de Bézout de proche en proche comme dans le cas de $\mathbb{Z}$

$$A \wedge B \wedge C = (A \wedge B) \wedge C$$

et on peut trouver U, V tel que

$$AU - BV = A \wedge B$$

puis W, Y tel que

$$(A \wedge B)W + CY = A \wedge B \wedge C$$

et ainsi

$$A(UW) + B(VW) + CY = A \wedge B \wedge C$$

4. PPCM

Définition

Pour $A, B \in \mathbb{K}[X]$, un PPCM de A et de B est un $M \in \mathbb{K}[X]$ tel que

$$\begin{cases} A|M \text{ et } B|M \\ \forall N \in \mathbb{K}[X], ((A|N \text{ et } B|N) \Rightarrow M|N) \end{cases}$$

Théorème

Soient $A, B \in \mathbb{K}[X]$,
Si $A = 0$ ou $B = 0$ le seul multiple commun des 0 donc 0 est PPCM que l'on appelle le PPCM de A et B noté $A \vee B$

Si $A \neq 0$ et $B \neq 0$, il existe un unique PPCM unitaire qu'on appele le PPCM de A et B qu'on note $A \vee B$ et les PPCM de A et B sont les $\lambda A \vee B$ pour $\lambda \in \mathbb{K}^*$.

De plus

$$AB = a_{d_a} b_{d_b} (A \wedge b)(A \vee B)$$

ou a_{d_a} et b_{d_b} sont les coefs dominants de A et B

Démonstration : Comme dans $\mathbb{Z}$ et en exo

VI Polynômes irreducible sur $\mathbb{R}[X]$ ou $\mathbb{C}[X]$

Définition

$P \in \mathbb{K}[X]$ est dit irréductible ssi

$$\begin{cases} deg(P) \geq 1 \\ \forall Q, R \in \mathbb{K}[X], P = QR \Rightarrow \begin{cases} deg(Q) = 0 \\ oudeg(R) = 0 \end{cases} \end{cases}$$

Propriété

Tout polynôme de degré 1 est irréductible

Démonstration immédiate

Théorème d'Alembert - Gauss ou Théorème fondamental de l'algèbre

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

Corollaire 1

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé

Démonstration :
Si $P \in \mathbb{C}^*$ il est "déjà" scindé.
Si $d = deg(P) \geq 1$, il admet une racine λ_1 donc il s'écrit
$P = (X - \lambda_1)P_1$ et ainsi de suite...
Par récurrence rapide $P = (X - \lambda_1) \ldots (X - \lambda_d)a_d$

Corollaire 2

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

Démonstration en exo : simple

Corollaire 3

Pour $P, Q \in \mathbb{C}[X]$,
$P|Q$ ssi
Toute racine de P est aussi racine de Q avec une multiplicité des Q au moins égale a la multiplicité dans P

Démonstration en exo

Exemple

$$X^n - 1 = \prod_{k=0}^{n-1}(X - e^{\frac{i2k\pi}{n}})$$

(points dur le cercle trigo)
$(X - e^{\frac{i2k\pi}{n}})$ irréductible

Reformulation des résultats précédents

Théorème

Tout $P \in \mathbb{C}[X] \backslash \{0\}$ s'écrit comme produit de puissances de facteur irréductibles et cette écriture est unique à l'ordre près et à la multiplication par des élément de $\mathbb{K}^*$ près.
Plus précisément, il s'écrit :

$$P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$$

avec $\lambda \in \mathbb{K}^*$ et pour tout $i \in [\![1, k]\!]$,
P_i est irréductible unitaire avec $\alpha_i \in \mathbb{N}^*$
de manière unique à l'ordre des $P_1^{\alpha_1}, \dots, P_k^{\alpha k}$ près

Cette formation est générique car elle n'utilise pas le fait que les irréductibles de $\mathbb{C}[X]$ donc de degré 1 --> elle est valable à l'identique par $\mathbb{R}[X]$.

Irréductibilité dans $\mathbb{R}[X]$

Théorème

Les irréductibles de $\mathbb{R}[X]$ sont :

- Les polynômes de degré 1
- Les polynômes de degré 2 sans racines (réelles) ie de discriminant strictement négatif.

Démonstration :

- Ceux de degré 1 sont irréductibles (déjà vu)

Un polynôme de degré 2 est de discriminant strictement négatif ne peut pas s'écrire $P = QR$ avec $deg(Q) \geq 1$ et $deg(R) \geq 1$
car sinon on aurait $deg(Q) = deg(P) = 1$
Donc Q aurait une racine dans P aussi.
CONTRADICTION!

Montrons que les autres polynômes ne sont pas irréductibles :

- Ceux de degré inférieur ou égal a 0 ne le sont pas par déf de l'irréductibilité.
- Ceux de degré 2 avec racines (réelles) s'écrivent :

  $$P = a(X - \alpha)(X - \beta)$$

  Donc ne sont pas irréductibles
- Soit $P \in \mathbb{R}[X]$ tq $d = deg(P) \geq 3$
  Montrons qu'il n'est pas irréductible
  P s'écrit $\sum_{n=0}^{d} a_n X^n$ avec $d \geq 3$ et $a_d \neq 0$ on considère :

  $$Q = \sum_{n=0}^{d} a_n X^n \in \mathbb{C}[X]$$

  Par le théorème d'Alembert-Gauss Q admet une racine $\lambda \in \mathbb{C}$.
  On distingue 2 cas :
  - Si $\lambda \in \mathbb{R}$ alors $P(\lambda) = \sum_{n=0}^{d} a_n \lambda^n = Q(\lambda) = Q$
    Donc P s'écrit : $P = (X - \lambda)P_1$ avec $deg(P_1) = d - 1 \geq 1$
    Donc P n'est pas irréductible
  - Si $\lambda \in \mathbb{C} \backslash \mathbb{R}$,
    Montrons que $\overline{\lambda}$ est racine de Q
    On a :

$$\sum_{n=0}^{d} a_n \lambda^n = 0$$

Donc

$$\sum_{n=0}^{d} \overline{a_n} (\overline{\lambda})^n = \overline{\sum_{n=0}^{d} a_n \lambda^n} = \overline{0} = 0$$

Or les a_n sont réels car $P \in \mathbb{R}[X]$, donc

$$\sum_{n=0}^{d} a_n (\overline{\lambda})^n = 0$$

ie

$$Q(\overline{\lambda}) = 0$$

Comme $\lambda \notin \mathbb{R}$, $\lambda \neq \overline{\lambda}$
On a lors :

$$Q = (X - \lambda)(X - \overline{\lambda})Q_1$$

avec $Q_1 \in \mathbb{C}[X]$
Or $D_1 = (X - \lambda)(X - \overline{\lambda}) = X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$
Donc les coefs de D_1 sont réels.

On appelle $D \in \mathbb{R}[X]$ le polynôme ayant les même coefficients que D_1 On fait la division euclidienne dans $\mathbb{R}[X]$ de P par D

$$P = D \times S + T$$

Avec $deg(T) < deg(E)$
En appelant $S_1 \in \mathbb{C}[X]$ qui a les même coeficients que S et $T_1 \in \mathbb{C}[X]$ qui à les même coefficients que T on a :

$$Q = D_1 S_1 + T_1$$

Avec $deg(T_1) < deg(D_1)$
Qui est la dicision euclidienne de Q par D_1. Or

$$Q = D_1 \times Q_1 + 0$$

est aussi la division euclidienne de Q par D_1
Par unicité de la division euclidienne $T_1 = 0$
Donc,

$$P = D \times S$$

avec $deg(D) = 2$ et $deg(S) \geq 1$ Donc P n'est pas irréductible

Lemme

Soient $A, B \in \mathbb{R}[X]$,
et $A_1, B_1 \in \mathbb{C}[X]$ ayanyt les mêmes coefficients réels que A et B
Alors

$$A_1|_{\mathbb{C}[X]}B_1 \Rightarrow A|_{\mathbb{R}[X]}B$$

Remarque

En général on confond par abus A et A_1 et B et B_1 ce qui donne la formulation :

$$A|_{\mathbb{C}[X]}B \Rightarrow A|_{\mathbb{R}[X]}B$$

Théorème

Tout polynôme $P \in \mathbb{K}[X] \backslash \{0\}$ s'écrit :

$$P = a_d \prod_{i=1}^{k} P_i^{\alpha_i}$$

où

$a_d \in \mathbb{K}^*$ (coef dominant de P)
et
$\forall i \in [\![1, k]\!], P_i$ unitaire irréductible et $\alpha_i \in \mathbb{N}^*$

et cette écriture est unique à l'ordre des facteurs près

Démonstration
Se prouve comme dans $\mathbb{N}$ (par récurrence forte sur le degré)
Unicité comme pour $\mathbb{N}$ en plus compliqué

Exemple

Décomposer en facteur irréductible sur $\mathbb{R}[X]$ et $\mathbb{C}[X]$:

$$X^2 - 2X + 1 = (X - 1)^2$$

dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

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

dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

$X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$ car de degré 2 sans racines (réelles)

$$X^2 + X + 1 = (X - j)(X - \overline{j})$$

sur $\mathbb{C}[X]$

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

Par Bernoulli
Décomposition en facteurs irréductibles dans $\mathbb{R}[X]$
et

$$X^3 - 1 = (X-1)(X-j)(X-\overline{j})$$

DFI dans $\mathbb{C}[X]$
Soit $Q = X^2 + X + 1$

$$X^4 + X^2 + 1 = Q(X^2) = (X^2 - j)(X^2 - \overline{j}^2)$$

$$= (X - \overline{j})(X + \overline{j})(X - j)(X + j) = (X - j)(X - \overline{j})(X + j)(X + \overline{j})$$

$$= (X^2 + X + 1)(X^2 - X + 1)$$

VII. Interpolation de Lagrange

Soit $n \in \mathbb{N}$
Exalc 3,
On a $n+1$ contraintes.
Pour que le problème soit bien dimensionnée, on cherche P avec $n+1$ coefficients ie $P \in \mathbb{K}_n[X]$.
Cherchons a résoudre des cas simples par exemple les y_i tous nuls sauf $y_j = 1$
On cherche $L_j \in \mathbb{K}_n[X]$
tq

$$\forall i \neq j, \tilde{L_j}(x_i) = 0$$

$$\tilde{L_j}(x_j) = 1$$

Une solution est :

$$L_j = \left(\prod_{i\neq j}(X - x_i)\right)\left(\prod_{i\neq j}(x_j - x_i)\right)$$

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

(avec un léger abus sur la notation qui sera justifié des la section

suivante)
On voit alors que

$$P = \sum_{j=0}^{n+1} y_j L_j = \sum_{j=0}^{n+1} y_j \prod_{i \neq j} \frac{X - x_i}{x_j - x_i}$$

Convient
Pour tout k quelconque :

$$\tilde{P}(x_k) = \sum_{j=0}^{n} y_j \prod_{i \neq j} \frac{x_k - x_i}{x_j - x_i} = y_k \prod_{i \neq k} \frac{x_k - x_i}{x_k - x_i} = y_k$$

Question 1 : Y en a t-il d'autres ?

Soit $Q \in \mathbb{K}_n[X]$ une autre solution au problème d'interpolation précédent, alors $Q - P$ s'annule en tout x_i, $i \in [\![0, n]\!]$ et $deg(Q - P) \leq n$
Un polynôme non nul de degré $d \leq n$ a au plus d racines, donc au plus n.
Ainsi $Q - P = 0$ et $Q = P$
Ainsi P est la seule solution de P de degré inférieur à n

Question 2 : Y en a t-il d'autres ?

Analyse

Soit $Q \in \mathbb{K}[X]$ tq

$$\forall i \in [\![0, n]\!], \tilde{Q}(x_i) = y_i$$

Alors $Q - P_0$ s'annule en tout x_i
Donc

$$\prod_{i=0}^{n} (X - x_i) | Q - P_0$$

Donc

$$Q = P_0 + r\prod_{i=0}^{n}(X - x_i)$$

Avec $R \in \mathbb{K}[X]$

Synthèse

Il est clair qu'un tel polynôme convient, donc l'ensemble des solutions du problème sans la condition de degré est

$$P_0 + \left(\prod_{i=0}^{n}(X - x_i)\right)\mathbb{K}[X]$$

Conclusion

Cela nous donne le théorème suivant :

Théorème

Soient $x_0, \ldots, x_n \mathbb{K}$ 2 a 2 disjoints et $y_0, \ldots, y_n \in \mathbb{K}$ quelconques. Alors l'ensemble des polynômes P vérifiant le système de contraintes : $\forall i \in [\![0, n]\!], \tilde{P}(x_i) = y_i$ est :

$$\sum_{j=0}^{n} y_i \prod_{i\neq j} \frac{X - x_i}{x_j - x_i} + \left(\prod_{i=0}^{n}(X - x_i)\right)\mathbb{K}[\mathbb{X}]$$

Notation :

Polynomial d'interpolation de Lagrange :
Les L_j sont les interpolations de Lagrange

Fonctions rationnelles

Question :

Comment définir les fonctions $\frac{P}{Q}$ avec $P, Q \in \mathbb{K}[X]$ et $Q \neq 0$
Comment traduire $\frac{P_1}{Q_1} = \frac{P_2}{Q_2}$ sans fractions : Réponse :
$P_1Q_2 = P_2Q_1$

Soit $\mathcal{E} = \mathbb{K}[X] \times (\mathbb{K} \backslash \{0\})$,

Définition

On définit la relation $\sim$ par :

$$(P_1, Q_1) \sim (P_2, Q_2) \Leftrightarrow P_1Q_2 = P_2Q_1$$

Montrer que $\sim$ est une relation d'équivalence sur $\mathcal{E}$.

Notation

On note $\mathcal{E}/_\sim$ l'ensemble des classes d'équivalences de $\sim$

Définition de l'addition

$$\overline{(P_1, Q_1)} + \overline{(P_2, Q_2)} = \overline{(P_1, Q_2 + P_2, Q_1, Q_1Q_2)}$$

Définition du produit

$$\overline{(P_1, Q_1)} \times \overline{(P_2, Q_2)} = \overline{(P_1P_2, Q_1Q_2)}$$

On a une LCI sur $\mathcal{E}/_\sim$

Notation

$$\mathcal{E}/_\sim = \mathbb{K}(X)$$

Ses éléments sont notés $\overline{(P, Q)} = \frac{P}{Q}$

Théorème

$$(\mathcal{E}/_\sim, +, \times) \text{ est un corp.}$$

avec $0 = \overline{(0, 1)}$ et $1 = \overline{(1, 1)}$

Dont les éléments s'appellent des fractions rationelles

Théorème

$$\phi : \begin{cases} \mathbb{K}[X] \to \mathbb{K}(X) \\ P \mapsto (\overline{P, 1}) \end{cases}$$

est un morphisme d'anneau injectif

Ainsi $\phi(\mathbb{K}[X])$ est isomorphe à $\mathbb{K}[X]$ et on peut "identifier" $\mathbb{K}[X]$ à son image, ce qui se traduit pour $P \in \mathbb{K}[X]$ par $P = \frac{P}{1}$

On obtiens alors un corps : $(\mathbb{K}(X), +, \times)$ appelé corp de fonction rationnelles à une indéterminée dont les élément sont les $\frac{P}{Q}$ avec $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}(X) \backslash \{0\})$ et contient $\mathbb{K}[X]$ en notant "$\frac{P}{1} = P$"

Dans ce corp on calcule comme d'habitude

Exemple

$$\frac{(X^2-3)^2(X-1)}{(X^2-1)(X-5)^2} = \frac{(X^2-3)^2}{(X+1)(X-5)^2}$$

Forme irréductible

$$\frac{1}{X} - \frac{1}{X+1} = \frac{1}{X(X+1)}$$

Théorème

$$\mathbb{K}[X] \underset{s.a}{\subset} \mathbb{K}(X)$$

Notation

$$\overline{(P, Q)} = \frac{P}{Q}$$

On oublie la notation précédente

Remarque

Pour $Q \in \mathbb{K}[X] \backslash \{0\} \subset \mathbb{K}(X) \backslash \{0\} (= \mathbb{K}(X)^{\times})$

$$Q^{-1} = \frac{1}{Q}$$

Donc pour $P \in \mathbb{K}[X]$

$$PQ^{-1} = Q^{-1}P = \frac{P}{Q}$$

On peut voir cette barre comme une vraie division dans $\mathbb{K}(X)$

Remarque

$$\frac{PR}{QR} = \frac{P}{Q}$$

$P \in \mathbb{K}[X]$
$Q, R \in \mathbb{K}[X] \backslash \{0\}$

Définition

On appelle forme irréductible d'une fraction rationnelle $F \in \mathbb{K}(X)$ l'unique écriture : $F = \frac{P}{Q}$ où :
$P \in \mathbb{K}[X]$
$Q \in \mathbb{K}[X]$ est unitaire
$P_1 Q = 1$

Propriété

Avec ces notations les fraction égales a F sont exactement les

$$\frac{PR}{QR}, R \in \mathbb{K}[X] \backslash \{0\}$$

Remarque

Avec les notation oubliés, cela dit que la classe d'équivalence de (P,Q) est $\{(PR,QR); R\in\mathbb{K}[X]\backslash\{0\}\}$
lorsque $P\wedge Q=1$

Définition

Si $F\in\mathbb{K}(X)$
et $\frac{P}{Q}$ est sa forme irréductible
Alors on appelle fonction rationnelle associé à F l'application :

$$\tilde{F}:\begin{cases}\mathbb{K}\backslash\{x\in\mathbb{K}|\tilde{Q}(x)=0\}\to\mathbb{K}\\ x\mapsto\frac{\tilde{P}(x)}{\tilde{Q}(x)}\end{cases}$$

ie :

$$\tilde{F}=\frac{\tilde{P}}{\tilde{Q}}$$

Marche sulement avec l'écriture irréductible

Exemple

$$F=\frac{(X^2-1)(X-42)}{(X+1)(X-i)}$$

Alors F est définie en -1

Car son écriture irréductible est :

$$F=\frac{(X-1)(X-42)}{(X-i)}$$

Donc :

$$\tilde{F}:\begin{cases}\mathbb{C}\backslash\{i\}\to\mathbb{C}\\ x\mapsto\frac{(X-1)(X-42)}{(X-i)}\end{cases}$$

Propriété

$$\Psi : \begin{cases} \mathbb{K}(X) \to \{\text{Fonctions rationnelles sur } \mathbb{K}\} \\ F \mapsto \tilde{F} \end{cases}$$

est injective ie

$$\forall F, G \in \mathbb{K}(X), \tilde{F} = \tilde{G} \Rightarrow F = G$$

Démonstration :
Soient $F = \frac{P}{Q}$ et $G = \frac{R}{S}$ deux éléments de $\mathbb{K}(X)$
Alors $A = \{x \in \mathbb{K} | \tilde{Q}(x) \neq 0 \text{ et } \tilde{S}(x) \neq 0\}$
est infini et pour $x \in A$
$\frac{\tilde{P}(X)}{\tilde{Q}(x)} = \frac{\tilde{R}(x)}{\tilde{S}(x)}$
Donc,

$$\tilde{P}(x)\tilde{S}(x) - \tilde{R}(x)\tilde{Q}(x) = 0$$

ie
x est racine de $PS - RQ$

Comme $PS - RQ \in \mathbb{K}[\mathbb{X}]$ a une infinité de racines, il est nul

$$PS - RQ = 0$$

Donc

$$PS = RQ$$

et comme S, R sont non nuls
Ainsi :

$$F = \frac{P}{Q} = \frac{R}{S} = G$$

Définition

Le degré de $F = \frac{P}{Q} \in \mathbb{K}(X)$
est :

$$deg(F) = deg(P) - deg(Q)$$

Cela ne dépend pas du couple (P, Q) choisit pour représenter F

Démonstration :
En effet, l'écriture irréductible de F est : $F = \frac{P_0}{Q_0}$ alors il existe un $R \in \mathbb{K}[X] \backslash \{0\}$ tel que $P = P_0 R$ et $Q = Q_0 R$
et

$$\begin{aligned} deg(P) - deg(Q) &= (deg(P_0) + deg(R)) - (deg(Q_0) + deg(R)) \\ &= deg(P_0) - deg(Q_0) \end{aligned}$$

Proposition

Soit $F = \frac{P}{Q} \in \mathbb{K}(Q)$
Faisons la division euclidienne de P par Q :

$$P = QQ_1 + R_1$$

Avec ces notations Q_1 ne dépend pas de l'écriture de F choisie

Démonstration :
Soient $(R, S) \in \mathbb{K}[X] \times (\mathbb{K}[X] \backslash \{0\})$
tel que :

$$\frac{R}{S} = F$$

soit l'écriture irréductible de F

On fait la division euclidienne de R par S :

$$R = SQ_2 + R_2$$

Avec $deg(R_2) < deg(S)$

or il existe $A \in \mathbb{K}[X] \backslash \{0\}$ tq,
$P = AR$
$Q = AS$

On obtiens alors :
$AR = ASQ_2 + AR_2$
ie

$$P = QQ_2 + AR_2$$

Avec $deg(AR_2) = deg(A) + deg(R_2) < deg(A) + deg(S) = deg(Q)$
Donc c'est une division euclidienne de P par Q.
Par unicité de la division euclidienne,
$Q_1 = Q_2$ et ($R_1 = AR_2$, ce qui ne sert pas)

Définition

Ce quotient de la division euclidienne de P par Q pour une écriture quelconque de $F \in \mathbb{K}(X)$ est appelé la partie entière de F et noté :

$$E(F)$$

Exemple

$$F = \frac{X^5 + X^4 + 2X^3 - 2X + 3}{X^4 + 3X^3 + 7X^2 + 8X + 6}$$

- Déterminer l'écriture irréductible de F :
  On note P le dénominateur Q le numérateur
  On applique l'algorithme d'Euclide

  $$(X^5 + X^4 + 2X^3 - 2X + 3) \wedge (X^4 + 3X^3 + 7X^2 + 8X + 6) = X^2 +$$

Remarque

Pour le calcul du PGCD on travaille a multiplication par un scalaire non nul près.
ATTENTION : Ne marche pas si on veut des coefficient de Bézout.

Remarque

Si $deg(F) \geq 0$, $deg(E(F)) = deg(P) - deg(Q)$
Si $deg(F) < 0$, $deg(E(F)) = 0$

Définition

Soient $F = \frac{P}{Q} \in \mathbb{K}(X)$ sous forme irréductible
Alors :

- les zéros de F (et non pas les racines de F) sont les racines de P
- Les pôles de F sont les racines de Q
- Les multiplicité des zéros sont leur multiplicités tant que racine de P.
- Les multiplicité des pôles sont leur multiplicité en tant que racine de Q.

Exemple

$$F = \frac{(X^2-3)^2(X-1)}{(X^2-1)(X-5)}$$

1 n'est pas zéro de F ("faux zéro")
On l'écrit sous forme irréductible :
Avec numérateur et dénominateur décomposé en facteurs irréductibles :

$$F = \frac{(X+\sqrt{3})^2(X-\sqrt{3})^2(X^2+X+1)}{(X+1)(X-5)^2}$$

Donc les zéros de F sont :
$-\sqrt{3}$ zéro double, $\sqrt{3}$ zéro double
et ses poles sont :
-1 pôle simple et 5 pôle double

Dans $\mathbb{C}[X]$,
Il faut alors rajouter les zéros simples j et $\overline{j}$.

Théorème : Décomposition en éléments simples

Soit

$$F = \frac{P}{(X-\lambda_1)^{\alpha_1}\dots(X-\lambda_p)^{\alpha_p}} \in \mathbb{C}[X]$$

sous forme irréductible (ou pas...)
Alors F s'écrit de manière unique sous la forme :

$$\star = F = E(F) + \frac{a_{1,1}}{X-\lambda_1} + \frac{a_{1,2}}{(X-\lambda_1)^2} + \dots + \frac{a_{1,\alpha_1}}{(X-\lambda_1)^{\alpha_1}} + \frac{a_{2,1}}{X-\lambda_2} +$$

Avec $a_{i,j} \in \mathbb{C}$

Théorème

Soit,

$$F = \frac{P}{Q} = \frac{P}{(X-\lambda_1)^{\alpha_1}\dots(X-\lambda_p)^{\alpha_p}(X^2+\mu_1X+\nu_1)^{\beta_1}\dots(X^2+\mu_qX+}$$

Sous sa forme irréductible (ou pas...)

Alors F s'écrit de manière unique :

$$F = \star + \frac{b_{1,1}X + c_{1,1}}{X^2+\mu_1X+\nu_1} + \frac{b_{1,2}X + c_{1,2}}{(X^2+\mu_1X+\nu_1)^2} + \dots + \frac{b_{1,\beta_1}X + c_{1,\beta_1}}{(X^2+\mu_1X+\nu_1)}$$

Avec $a_{i,j}$, $b_{i,j}$ et $c_{i,j}$ réels.

Exemple

Décomposition en éléments simples dans $\mathbb{R}[X]$ de :

$$F = \frac{(X^2-3)^2}{(X+1)(X-5)^2(X^2+X+1)^3}$$

$$F = 0 + \frac{\alpha}{X+1}$$

$$+\frac{\beta}{X-5} + \frac{\gamma}{(X-5)^2}$$

$$+\frac{aX+b}{X^2+X+1} + \frac{cX+d}{(X^2+X+1)^2} + \frac{eX+f}{(X^2+X+1)^3}$$

Décomposition en éléments simples dans $\mathbb{C}[X]$:

$$(1) + \frac{A}{X-j} + \frac{B}{(X-j)^2} + \frac{C}{(X-j)^3} + \frac{\overline{A}}{X-\overline{j}} + \frac{\overline{B}}{(X-\overline{j})^2} + \frac{\overline{B}}{(X-\overline{j})^3}$$

Car le numérateur et le dénominateur de F son a coefficient réels.

Méthode de Multiplication-Evaluation

Exemple

1. On multiplie par $X+1$ l'égalité fournie par le théorème.

$$\frac{(X^2-3)^2}{(X-5)^2(X^2+X+1)^3} = \alpha + (X+1)(\qquad\qquad)$$

   -1 n'est pas un pole

2. On évalue les fonctions rationnelles en -1

$$\alpha = \frac{((-1)^2-3)}{(-1-5)^2((-1)^2+(-1)+1)^3} = \frac{4}{36} = \frac{1}{9}$$

Lemme

Soit

$$\phi : \begin{cases} \mathbb{K}[X] \backslash \{0\} \to \mathbb{K}(X) \\ P \mapsto \frac{P'}{P} \end{cases}$$

Alors

$$\forall P, Q \in \mathbb{K}[X] \backslash \{0\}, \phi(PQ) = \phi(P) + \phi(Q)$$

Démonstration :
Soit $P, Q \in \mathbb{K}[X] \backslash \{0\}$
Alors,

$$\phi(PQ) = \frac{P'Q + PQ'}{PQ} = \frac{P'Q}{PQ} + \frac{PQ'}{PQ} = \frac{P'}{P} \times \frac{Q'}{Q} = \phi(P) + \phi(Q)$$

Théorème

Soient $P \in \mathbb{K}[X]$,
On considère sa DFI :

$$P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$$

ou $\lambda \in \mathbb{K}^*$
et P_i irréductible
Alors la DES de $\frac{P'}{P}$
est :

$$\frac{P'}{P} = \sum_{i=1}^{k} \alpha_i \frac{P_i'}{P_i}$$

Démonstration :
En appliquant le lemme, on obtiens :

$$\phi(\lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}) = \phi_(\lambda) + \sum_{i=1}^{k} \alpha_i \phi(P_i) = \sum_{i=1}^{k} \alpha_i \frac{P_i'}{P_i}$$

Corollaire

Soit P scindé dans $\mathbb{K}[X]$ (toujours le cas si $\mathbb{K} = \mathbb{C}$). Il s'écrit

$$P = \lambda \prod_{i=1}^{k} (X - \mu_i)^{\alpha_i}$$

Alors la DES de $\frac{P'}{P}$ est :

$$\frac{P'}{P} = \sum_{i=1}^{k} \frac{\alpha_i}{X - \mu_i}$$