

Introduction

Dans toute la suite \mathbb{K} est \mathbb{R} ou \mathbb{C}

On connaît les fonctions polynômes définies, par exemple, par :

$$\forall x \in \mathbb{R}, f(x) = x^3 + 2x^2 - 7,$$

en particulier les trinômes du second degré : $ax^2 + bx + c$

Mais si A est une matrice carrée, on peut aussi calculer $f(A) = A^3 + 2A^2 - 7I$

Le but est de généraliser et donc d'introduire des polynômes formels : un polynôme formel s'écrit avec X au lieu de x

On distinguera alors

- le polynôme $P = X^3 + 2X^2 - 7$
- d'avec la fonction polynomiale f définie par

$$\forall x \in \mathbb{R}, f(x) = x^3 + 2x^2 - 7$$

Mais pas la peine de se prendre la tête avec cela maintenant. Tout s'éclairera en son temps. Et la lumière jaillira au dessus de nos têtes baissées pour illuminer nos fronts plissés par la douleur lancinante due au travail exténuant de nos pauvres neurones dévitalisés.

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

1.1 Définitions élémentaires

Introduction On construit les polynômes formels à partir d'une indéterminée (notée classiquement X) est de ses puissances notées $X^0 = 1, X^1 = X, X^2, X^3, \dots$

Définition 1 : Polynôme

On appelle polynôme à coefficients dans \mathbb{K} toute combinaison linéaire des puissances de X qui s'écrit sous la forme

$$P = \sum_{k=0}^n a_k X^k \quad \text{avec} \quad \forall k \in [[0, n]], a_k \in \mathbb{K}$$

Définition 2 : suite presque nulle

On dit qu'une suite $(a_n)_{n \in \mathbb{N}}$ est presque nulle si tous ses termes, sauf éventuellement un nombre fini, sont nuls

Ce qui équivaut à dire que cette suite est nulle à partir d'un certain rang

Propriété 1

Tout polynôme s'écrit de façon unique sous la forme

$$P = \sum_{k=0}^{+\infty} a_k X^k$$

où $(a_k)_{k \in \mathbb{N}}$ est une suite presque nulle de \mathbb{K}

Propriété 2 : Égalité

Deux polynômes $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ sont égaux

si et seulement si $(a_k)_{k \in \mathbb{N}} = (b_k)_{k \in \mathbb{N}}$

$\iff \forall k \in \mathbb{N}, a_k = b_k$

Définition 3 : Notation

L'ensemble des polynôme à une indéterminée X et à coefficients dans \mathbb{K} est noté $\mathbb{K}[X]$

On a trivialement $\mathbb{R}[X] \subset \mathbb{C}[X]$

Exemple : $1 + X + i.X^2 \in \mathbb{C}[X]$

Le polynôme nul se note faute de mieux 0

Définition 4 : Monôme

On appelle monôme tout polynôme de la forme $a_n X^n$

1.2 Degré

Définition 5 : Degré

- Si P est le polynôme nul, par convention $d^\circ P = -\infty$
- Si $P = \sum_{k=0}^{+\infty} a_k X^k \neq 0$

$$d^\circ P = n \iff a_n \neq 0 \text{ et } \forall k > n, a_k = 0$$

On a alors $P = \sum_{k=0}^n a_k X^k$ avec $n = d^\circ P$
- Conséquence :

$$d^\circ P \leq n \iff \forall k > n, a_k = 0$$

Définition 6 : coefficient dominant

- Soit $P = \sum_{k=0}^n a_k X^k \neq 0$ un polynôme de degré n
 Alors a_n est appelé le coefficient dominant de P
 $a_n X^n$ est appelé le terme dominant de P
 Si $a_n = 1$, alors P est appelé un polynôme unitaire

Exemple : $P = -3X^4 + 7X - 4$ P est de degré 4
 son coefficient dominant est -3
 Son terme dominant est $-3X^4$ (= son terme de plus haut degré)
 P n'est pas unitaire
 Par contre $\frac{-1}{3}P = X^4 - \frac{7}{3}X + \frac{4}{3}$ est unitaire (on dit que c'est le polynôme unitaire associé à P)

Définition 7 : $\mathbb{K}_n[X]$

$\mathbb{K}_n[X]$ est l'ensemble des polynômes de degré inférieur ou égal à n

1.3 Espace vectoriel

Définition 8 : Combinaison linéaire

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$, $Q = \sum_{k=0}^{+\infty} b_k X^k$, $q(\lambda, \mu) \in \mathbb{K}^2$
 On définit alors $\lambda.P + \mu.Q = \sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) X^k$

Propriété 3 : degré de la somme

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

- $d^\circ(P + Q) \leq \max(d^\circ(P), d^\circ(Q))$
- Si $d^\circ(P) \neq d^\circ(Q)$
 alors $d^\circ(P + Q) = \max(d^\circ(P), d^\circ(Q))$
- En particulier :

$$(d^\circ P \leq n) \text{ et } (d^\circ Q \leq n) \Rightarrow d^\circ(\lambda P + \mu Q) \leq n$$

Exemple :

$P = 2X^3 - 4X + 7$ $Q = 9X^2 + 12X - 5$ $R = -2X^3 + 8X^2 + 1$
 $P + Q = 2X^3 + 9X^2 + 8X + 2$ $P + R = 8X^2 - 4X + 8$

- $d^\circ P \neq d^\circ Q$ donc $P + Q$ est du degré le plus élevé :

$$d^\circ(P + Q) = \max(d^\circ(P), d^\circ(Q)) = \max(2, 3) = 3$$
- $d^\circ P = d^\circ R = 3$ donc $P + R$ est de degré au plus 3, mais on ne peut rien dire de plus :

$$d^\circ(P + R) = 2 \text{ mais } d^\circ(P - R) = 3$$

Propriété 4 : espaces vectoriels

$\mathbb{K}[X]$ est un espace vectoriel
 Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est un sev de $\mathbb{K}[X]$

Provient de $(d^\circ P \leq n) \text{ et } (d^\circ Q \leq n) \Rightarrow d^\circ(\lambda P + \mu Q) \leq n$

Propriété 5 : dimension, bases canoniques

- $(1, X, X^2, X^3, \dots)$ est la base canonique (infinie) de $\mathbb{K}[X]$
- $(1, X, X^2, X^3, \dots, X^n)$ est la base canonique de $\mathbb{K}_n[X]$
- $\dim \mathbb{K}_n[X] = n + 1$

1.4 Produit

Exemple

$$P(X) = a_0 + a_1X + a_2X^2$$

$$Q(X) = b_0 + b_1X + b_2X^2 + b_3X^3$$

$$\begin{aligned} PQ &= (a_0 + a_1X + a_2X^2)(b_0 + b_1X + b_2X^2 + b_3X^3) \\ &= a_0b_0 + a_0b_1X + a_0b_2X^2 + a_0b_3X^3 \\ &\quad + a_1b_0X + a_1b_1X^2 + a_1b_2X^3 + a_1b_3X^4 \\ &\quad + a_2b_0X^2 + a_2b_1X^3 + a_2b_2X^4 + a_2b_3X^5 \end{aligned}$$

Terme en X^2 : $c_2 = a_0b_2 + a_1b_1 + a_2b_0 = \sum_{i=0}^2 a_i b_{2-i}$

Terme en X^4 : $c_4 = a_1b_3 + a_2b_2$

Mais comme $b_4 = 0$ (car $d^\circ Q = 3$) et $a_3 = a_4 = 0$ (car $d^\circ P = 3$)

on peut ajouter les termes manquant :

$$c_4 = a_0b_4 + (a_1b_3 + a_2b_2) + a_3b_1 + a_4b_0 = \sum_{i=0}^4 a_i b_{4-i}$$

Ce qui donne une formule qui marche à tous les coups et qu'on peut généraliser :

$$c_k = a_0b_k + a_1b_{k-1} + \dots + a_i b_{k-i} + \dots + a_k b_0 = \sum_{i=0}^k a_i b_{k-i}$$

Cela permet de définir le produit de deux polynômes :

Définition 9 : Produit

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$, $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbb{K}[X]$

On définit le polynôme $PQ = \sum_{k=0}^{+\infty} c_k X^k$ avec $c_k = \sum_{i=0}^k a_i b_{k-i}$

En particulier, si $P = X^k$ et $Q = X^\ell$, alors $X^k X^\ell = PQ = X^{k+\ell}$
Ce qui justifie a posteriori la notation sous forme de puissance : (X^n)

Exemple

Calculer $P.Q$ avec $P(X) = X^n + X^{n-1} + \dots + X + 1$
et $Q(X) = nX^n + (n-1)X^{n-1} + \dots + X$

Posons $R = P.Q$

$$P(X) = \sum_{k=0}^n X^k = \sum_{k=0}^{+\infty} a_k X^k \quad \text{avec} \quad a_k = \begin{cases} 1 & \text{si } 0 \leq k \leq n \\ 0 & \text{sinon} \end{cases}$$

$$Q(X) = \sum_{k=0}^n kX^k = \sum_{k=0}^{+\infty} b_k X^k \quad \text{avec} \quad b_k = \begin{cases} k & \text{si } 0 \leq k \leq n \\ 0 & \text{sinon} \end{cases}$$

Alors $R = \sum_{k=0}^{+\infty} c_k X^k$ avec $c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k a_{k-i} b_i$

Remarquons qu'il sera plus facile d'utiliser la deuxième formule.

- 1er cas : si $0 \leq k \leq n$
 $0 \leq i \leq k \Rightarrow 0 \leq k-i \leq k \leq n \Rightarrow a_{k-i} = 1$ et $b_i = i$
$$c_k = \sum_{i=0}^k a_{k-i} b_i = \sum_{i=0}^k i = \frac{k(k+1)}{2}$$

- 2ème cas : si $n+1 \leq k \leq 2n$
Dans ce cas, certains termes de la somme sont nuls et donc vont disparaître :
Pour $i > n$, $b_i = 0$ Donc

$$c_k = \sum_{i=0}^k a_{k-i}b_i = \sum_{i=0}^n a_{k-i}b_i + \sum_{i=n+1}^k a_{k-i}b_i = \sum_{i=0}^n a_{k-i}b_i$$

De même $a_{k-i} = 0$ pour $k-i > n \iff i < k-n$ Donc :

$$\begin{aligned} c_k &= \sum_{i=0}^{n-k-1} a_{k-i}b_i + \sum_{i=n-k}^n a_{k-i}b_i \\ &= 0 + \sum_{i=k-n}^n a_{k-i}b_i \end{aligned}$$

Maintenant, puisque $0 \leq i \leq n$, $a_{k-i} = 1$
et comme $0 \leq k-i \leq n$, $b_i = i$

$$c_k = \sum_{i=k-n}^n a_{k-i}b_i = \sum_{i=k-n}^n i \quad (\text{somme suite arithmétique})$$

« (=nombre de termes \times moyenne des extrêmes) »

$$= (n - (k - n) + 1) \frac{n + (k - n)}{2} = \frac{(2n - k + 1)k}{2}$$

- 3ème cas : si $2n < k$: $c_k = 0$

Propriété 6 : Degré du produit

|| Soient P, Q deux polynômes :
|| $d^\circ PQ = d^\circ P + d^\circ Q$ (avec la convention $-\infty + n = -\infty$)

Propriété 7 : degré d'une puissance

|| Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$
|| $d^\circ(P^n) = n \cdot d^\circ P$

Propriété 8 : Intégrité

|| $\forall P, Q \in \mathbb{K}[X], PQ = 0 \implies P = 0$ ou $Q = 0$

Propriété 9 Règle de calcul

|| $\forall P, Q, R \in \mathbb{K}[X], \forall a \in \mathbb{K},$
|| $PQ = QP$
|| $P(QR) = (PQ)R$
|| $a(PQ) = (aP)Q = P(aQ)$
|| $P(Q+R) = PQ + PR$ (et $(Q+R)P = QP + RP$
|| car le produit est commutatif)

|| $P.1 = P$
|| $P.0 = 0$

1.5 composition

Exemple

$$P = X^2 - 2X + 7 \quad Q = 2X - 3$$

$$\begin{aligned} P \circ Q &= Q^2 - 2Q + 7 \\ &= (2X - 3)^2 - 2(2X - 3) + 7 \\ &= (4X^2 - 12X + 9) - 4X + 6 + 7 \\ &= 4X^2 - 16X + 22 \end{aligned}$$

$$Q \circ P = 2P - 3 = 2X^2 - 4X + 11$$

On remarque que : $P \circ Q \neq Q \circ P$

Définition 10 : Composée de polynômes

|| Soient P et Q deux polynômes tels que : $P = \sum_{k=0}^{+\infty} a_k X^k$

|| Alors $P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k$

ATTENTION : en règle générale $P \circ Q \neq Q \circ P$

En particulier,

$$\begin{array}{r}
 X^4 + X^3 + X + 1 \quad | \quad 2X^2 - X + 1 \\
 -X^4 + \frac{1}{2}X^3 - \frac{1}{2}X^2 \quad | \quad \downarrow \quad \frac{1}{2}X^2 + \frac{3}{4}X \\
 \hline
 \frac{3}{2}X^3 - \frac{1}{2}X^2 + X \\
 -\frac{3}{2}X^3 + \frac{3}{4}X^2 - \frac{3}{4}X \quad | \quad \downarrow \\
 \hline
 \frac{1}{4}X^2 + \frac{1}{4}X + 1
 \end{array}$$

Et encore :

$$\begin{array}{r}
 X^4 + X^3 + X + 1 \quad | \quad 2X^2 - X + 1 \\
 -X^4 + \frac{1}{2}X^3 - \frac{1}{2}X^2 \quad | \quad \downarrow \quad \frac{1}{2}X^2 + \frac{3}{4}X + \frac{1}{8} \\
 \hline
 \frac{3}{2}X^3 - \frac{1}{2}X^2 + X \\
 -\frac{3}{2}X^3 + \frac{3}{4}X^2 - \frac{3}{4}X \quad | \quad \downarrow \\
 \hline
 \frac{1}{4}X^2 + \frac{1}{4}X + 1 \\
 -\frac{1}{4}X^2 + \frac{1}{8}X - \frac{1}{8} \\
 \hline
 \frac{3}{8}X + \frac{7}{8}
 \end{array}$$

On obtient donc

- Un quotient $Q = \frac{1}{2}X^2 + \frac{3}{4}X + \frac{1}{8}$
- un reste $R = \frac{3}{8}X + \frac{7}{8}$

tels que $A = BQ + R$ et $d^\circ R < d^\circ B$

Comment détecter une erreur ?

On peut remplacer par exemple X par une valeur et à n'importe quelle étape du calcul on doit avoir $A = BQ_k + R_k$ où Q_k et R_k sont le quotient et le reste intermédiaires

Exemple : après deux étapes, on a :

$$\begin{array}{r}
 X^4 + X^3 + X + 1 \quad | \quad 2X^2 - X + 1 \\
 \frac{1}{4}X^2 + \frac{1}{4}X + 1 \quad | \quad \frac{1}{2}X^2 + \frac{3}{4}X
 \end{array}$$

On remplace X par 1

$$\begin{array}{r}
 4 \quad | \quad 2 \\
 \frac{6}{4} \quad | \quad \frac{5}{4}
 \end{array}
 \quad \text{et on a bien} \quad (BQ_2 + R_2)(1) = 2 \times \frac{5}{4} + \frac{6}{4} = \frac{16}{4} = 4 = A(1)$$

Ca marche !

Il ne reste plus qu'à formuler la propriété et la démontrer :

Propriété 11 : Théorème

Soient A et B deux polynômes tels que $B \neq 0$

Alors il existe un unique couple de polynômes (Q, R) tels que :

$$A = B.Q + R \quad \text{et} \quad d^\circ R < d^\circ B$$

Q est appelé le quotient et R le reste de la division euclidienne de A par B .

Exemples d'applications

a) Soient $A = X^7 - 5X^3 + 7$ et $B = X - 2$
 Quel est le reste de la division euclidienne de A par B ?

Il existe Q, R tel que $A = BQ + R$

avec $d^\circ R < 1 \Rightarrow d^\circ R \leq 0 \Rightarrow R = \text{constante}$

$$A = BQ + R \Rightarrow A = (X - 2)Q + R$$

On évalue cette expression en 0 ? : $A(0) = 7 = -2Q(0) + R$ pas intéressant

$$\text{En } 2? \Rightarrow A(2) = 0.Q(2) + R$$

$$\Rightarrow R = A(2) = 128 - 40 + 7 = 95$$

b) $A = X^7 - 5X^3 + 7, \quad B = X^2 - X = X(X - 1)$ Reste R ?
 $d^\circ R < d^\circ B \Rightarrow d^\circ R \leq 1 \Rightarrow R = aX + b$ avec $a, b \in \mathbb{R}$

$$A(X) = (X^2 - X)Q(X) + aX + b$$

$$\text{en } 0 : A(0) = 0.Q(0) + a.0 + b \Rightarrow 7 = b$$

$$\text{en } 1 : A(1) = 0.Q(1) + a.1 + b \Rightarrow A(1) = 3 = a + b = a + 7 \Rightarrow a = -4$$

$$\text{D'où } R = -4X + 7$$

$$c) \begin{cases} A = X^7 - 5X^3 + 7, & B = X^2 + 4 & \text{Reste ?} \\ d^\circ R < d^\circ B = 2 & \Rightarrow & R = aX + b \text{ avec } a, b \in \mathbb{R} \end{cases}$$

$$A = (X^2 + 4)Q + aX + b$$

$$\text{Racines de } B? \quad x^2 + 4 = 0 \iff x = 2i \text{ ou } x = -2i$$

$$\text{En } 2i : \quad A(X) = (X^2 + 4)Q(X) + aX + b \Rightarrow A(2i) = a \cdot 2i + b$$

$$\begin{aligned} \text{avec } A(2i) &= (2i)^7 - 5(2i)^3 + 7 = 2^7 i^7 - 5 \cdot 2^3 i^3 + 7 \\ &= -128i + 40i + 7 = -88i + 7 \end{aligned}$$

$$\text{Donc } -88i + 7 = 2ai + b \quad \text{avec } (a, b) \in \mathbb{R}^2 \quad (\text{sinon l'identification est interdite})$$

$$\Rightarrow a = -44, b = 7 \Rightarrow R = -44X + 7$$

Définition 11 : divisibilité

| A est divisible par B si et seulement si il existe Q tel que A = BQ

3 fonctions polynomiales et racines

Définition 12 : fonction polynôme

A tout polynôme $P = \sum_{k=0}^n a_k X^k$ de $\mathbb{K}[X]$ on associe une fonction

$$\tilde{P} : \mathbb{K} \rightarrow \mathbb{K} \quad \text{telle que } \forall x \in \mathbb{K}, \tilde{P}(x) = \sum_{k=0}^n a_k x^k$$

\tilde{P} est appelée la fonction polynomiale associée à P

Propriété 12

$$\begin{cases} (aP + bQ) = a\tilde{P} + b\tilde{Q} & (\tilde{P}Q) = \tilde{P}\tilde{Q} \\ (P \circ Q) = \tilde{P} \circ \tilde{Q} & (\tilde{P})' = (\tilde{P})' \end{cases}$$

Définition 13 : Racine d'un polynôme

| a ∈ K est racine du polynôme P si et seulement si $\tilde{P}(a) = 0$

Vocabulaire : Attention à bien distinguer « racine » et « solution »

On parle des racines d'un **polynôme** et des solutions d'une **équation**.
De façon plus précise, on dira

$$\begin{cases} a \text{ est } \mathbf{racine} \text{ du polynôme } P \\ \iff a \text{ est } \mathbf{solution} \text{ de l'équation } P(x) = 0 \end{cases}$$

Propriété 13 : Caractérisation des racines

$$\begin{cases} a \in \mathbb{K} \text{ est racine du polynôme } P \\ \text{si et seulement si } P \text{ est divisible par } X - a \\ \text{C'est-à-dire il existe } Q \in \mathbb{K}[X] \text{ tel que } P = (X - a)Q \end{cases}$$

Définition 14 : Multiplicité d'une racine

$$\begin{cases} a \text{ est racine de multiplicité } m \in \mathbb{N}^* \text{ de } P \text{ ssi} \\ \text{il existe } Q \in \mathbb{K}[X] \text{ tel que} \\ P = (X - a)^m Q \quad \text{avec } Q(a) \neq 0 \end{cases}$$

Définition 15 : Conventions

- Si a n'est pas racine de P ($\iff P(a) \neq 0$), on dit que a est racine de multiplicité 0
- Une racine de multiplicité 1 est dite racine simple.
- On définit de même les racines doubles, triples, etc.

Exemples

- $P(X) = (X - 2)^3(X^3 + X^2 + X + 1) = (X - 2)^3Q$
2 est racine de multiplicité 3 de P car $Q(2) = 8 + 4 + 2 + 1 \neq 0$
- $P(X) = (X - i)^2(X + i)^2(X - 3)(X + 4)^3$
i et -i sont racines doubles, 3 est racine simple et -4 est racine triple de P

Propriété 14 : multiplicité

$$\begin{cases} a \text{ est racine de multiplicité } \mathbf{au moins} \ m \in \mathbb{N}^* \text{ de } P \\ \text{ssi il existe } Q \in \mathbb{K}[X] \text{ tel que} \\ P = (X - a)^m Q \end{cases}$$

Remarque : il n'a donc pas de condition sur Q dans ce cas.

Propriété 15 : racines et divisibilité

$\alpha_1, \dots, \alpha_p$ sont des racines distinctes de P de multiplicités respectives m_1, \dots, m_p si et seulement si il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = \left(\prod_{k=1}^p (X - \alpha_k)^{m_k} \right) \cdot Q \quad \text{et} \quad \forall k \in \llbracket 1, p \rrbracket, Q(\alpha_k) \neq 0$$
Propriété 16 (Conséquence) : Degré et racines

• Si $\alpha_1, \dots, \alpha_p$ sont des racines de P de multiplicités respectives m_1, \dots, m_p

Alors $d^\circ P \geq \sum_{k=1}^p m_k$

• En particulier un polynôme de degré n possède au plus n racines distinctes

Propriété 17 (Conséquence) : polynôme nul et racines

• Un polynôme P de degré au plus n est nul si et seulement si il possède au moins $n + 1$ racines distinctes

• Un polynôme est nul si et seulement si il possède une infinité de racines distinctes

• Deux polynômes P et Q de degré au plus n sont égaux si et seulement si ils coïncident pour $n + 1$ valeurs c'est-à-dire qu'il existe $n + 1$ valeurs distinctes x_1, \dots, x_n, x_{n+1} telles que

$$\forall i \in \llbracket 1, n + 1 \rrbracket, P(x_i) = Q(x_i)$$

• Deux polynômes P et Q sont égaux si et seulement si ils coïncident pour une infinité de valeurs c'est-à-dire qu'il existe une infinité d'éléments $x_i \in \mathbb{K}$ tels que $\forall i, P(x_i) = Q(x_i)$

Exemple : Soit P un polynôme tel que $\forall n \in \mathbb{N}, P(n) = 0$
 P admet alors une infinité de racines. Donc P est le polynôme nul.

Remarquer que cela ne vaut pas pour des fonctions classiques : par exemple $f : x \mapsto \sin(\pi x)$ qui s'annule pour tout $n \in \mathbb{Z}$ et qui pourtant n'est pas la fonction nulle.

Définition 16 : Polynôme scindé

• P polynôme de degré n est scindé si et seulement si il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ tel que

$$P = a_n(X - \alpha_1) \cdots (X - \alpha_n) = a_n \prod_{k=1}^n (X - \alpha_k),$$

les α_k n'étant pas nécessairement distincts

• On peut dire de façon équivalente :
 P est scindé s'il admet p racines distinctes $\alpha_1, \dots, \alpha_p$ de multiplicités m_1, \dots, m_p telles que

$$d^\circ P = m_1 + \cdots + m_p$$

Dans ce cas : $P = a_n \prod_{k=1}^p (X - \alpha_k)^{m_k}$

Définition 17 : Polynôme simplement scindé

Un polynôme P est dit simplement scindé s'il est scindé et que toutes ses racines sont simples

Autrement dit, un polynôme de degré n est simplement scindé si et seulement si il admet n racines distinctes

4 Polynômes irréductibles et décomposition

4.1 Polynômes irréductibles

Propriété 18 : Théorème de d'Alembert-Gauss

|| Soit P un polynôme de degré ≥ 1 de $\mathbb{C}[X]$
 || Alors P admet au moins une racine dans \mathbb{C} .

Polynôme irréductible : Un polynôme P est irréductible s'il ne peut pas se décomposer comme un produit non trivial de deux polynômes

Par exemple : $P = 2X - 3$ peut s'écrire $P = QR$ avec $Q = 2$ et $R = X - 3/2$. Mais dans ce cas, la décomposition est « triviale » : on peut toujours mettre un polynôme constant en facteur. C'est donc sans intérêt.

Par contre pour $P = X^2 + 1 = (X - i)(X + i)$ la décomposition en produit (dans $\mathbb{C}[X]$) est non triviale.

Définition 18 : Polynômes irréductibles

Soit $P \in \mathbb{K}[X]$ un polynôme non constant,
 P est irréductible dans $\mathbb{K}[X]$
 $\iff \forall (A, B) \in \mathbb{K}[X], (P = AB) \implies (A \text{ est constant ou } B \text{ est constant})$
 $\iff \forall (A, B) \in \mathbb{K}[X], (P = AB) \implies (A \in \mathbb{K} \text{ ou } B \in \mathbb{K})$

Définition 19 : Polynômes réductibles

Soit $P \in \mathbb{K}[X]$, P est réductible dans $\mathbb{K}[X]$ ssi
 $\exists (A, B) \in \mathbb{K}[X]^2, P = AB$ et $d^\circ A \geq 1$ et $d^\circ B \geq 1$

Exemple : $P = X^2 + 4$ est irréductible dans $\mathbb{R}[X]$ mais réductible dans $\mathbb{C}[X]$

4.2 Décomposition dans $\mathbb{C}[X]$

Propriété 19 : Polynômes irréductibles de $\mathbb{C}[X]$

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont ses polynômes de degré 1 (de la forme $P = aX + b$)
- Les polynômes irréductibles **unitaires** de $\mathbb{C}[X]$ sont de la forme $X - \alpha$ avec $\alpha \in \mathbb{R}$

Propriété 20 : Décomposition d'un polynôme dans $\mathbb{C}[X]$

Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$.
 Alors il existe n nombre complexes (non nécessairement deux à deux distincts) z_1, \dots, z_n tels que :

$$P = a_n(X - z_1)(X - z_2) \dots (X - z_n)$$

 De plus cette décomposition est unique à l'ordre des facteurs près.
 Un complexe a est une racine de multiplicité k ssi il apparaît exactement k fois dans la décomposition.

Cette décomposition peut aussi s'écrire :

Propriété 21 : Décomposition d'un polynôme dans $\mathbb{C}[X]$

$$P(X) = a_n(X - z_1)^{m_1}(X - z_2)^{m_2} \dots (X - z_k)^{m_k} = a_n \prod_{i=1}^k (X - z_i)^{m_i}$$

 où z_1, \dots, z_k sont k racines **distinctes** de P
 et m_1, \dots, m_k sont leurs ordres de multiplicité respectifs.
 On a donc : $m_1 + \dots + m_k = n$.

Conséquence :

Propriété 22 : Polynômes scindés de $\mathbb{C}[X]$

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

Propriété 23 : Somme et produit des racines

Soit $P = \sum_{k=0}^n a_k X^k$ un polynôme de degré n dans $\mathbb{C}[X]$
 Soient $\alpha_1, \dots, \alpha_n$ ses n racines (distinctes ou non) dans \mathbb{C}
 Alors $s = \alpha_1 + \alpha_2 + \dots + \alpha_n = \frac{-a_{n-1}}{a_n}$
 et $p = \alpha_1 \alpha_2 \dots \alpha_n = (-1)^n \frac{a_0}{a_n}$
 En particulier $P(0) = a_0 \implies p = \alpha_1 \dots \alpha_n = (-1)^n \frac{P(0)}{a_n}$

En effet, par développement :

$$\begin{aligned} P &= a_n(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n) \\ &= a_n(X^n - (\alpha_1 + \alpha_2 + \dots + \alpha_n)X^{n-1} + \dots + (-1)^n \alpha_1 \alpha_2 \dots \alpha_n) \\ &= a_n X^n - a_n(\alpha_1 + \alpha_2 + \dots + \alpha_n)X^{n-1} + \dots + a_n(-1)^n \alpha_1 \alpha_2 \dots \alpha_n \end{aligned}$$

$\implies a_{n-1} = -a_n(\alpha_1 + \alpha_2 + \dots + \alpha_n)$ et $a_0 = a_n(-1)^n(\alpha_1 \alpha_2 \dots \alpha_n)$

4.3 Décomposition dans $\mathbb{R}[X]$

Exemple : $P = X^4 + X^2 + 1$

Trouver la factorisation dans \mathbb{C} , puis la factorisation dans \mathbb{R}

Décomposons dans $\mathbb{C}[X]$

Attention :

Ne surtout pas écrire $X^4 + X^2 + 1 = 0$ ce qui serait absurde.

On cherche des racines, donc il faut impérativement passer aux lettres minuscules (désignant donc des nombres complexes), et ne pas garder les écritures de polynômes formels

(Par contre on peut poser $Y = X^2$ où Y est aussi un polynôme, ce qui donnerait $P = Y^2 + Y + 1$) $P(x) = 0 \iff x^4 + x^2 + 1 = 0 \iff y^2 + y + 1 = 0$ avec $y^2 = x$

$$y_1 = j = e^{2i\pi/3} \quad y_2 = j^2$$

$$x^2 = y_1 = (e^{i\pi/3})^2 \iff x = x_1 = e^{i\pi/3} \text{ ou } x = x_2 = -e^{i\pi/3}$$

$$x^2 = y_2 = j^2 \iff x = x_3 = j = e^{2i\pi/3} \text{ ou } x = x_4 = -e^{2i\pi/3} \text{ Donc 4 racines :}$$

$$\begin{aligned} P &= (X^2 - j)(X^2 - j^2) \\ &= (X - x_1)(X - x_2)(X - x_3)(X - x_4) \\ &= (X - e^{i\pi/3})(X + e^{i\pi/3})(X - e^{2i\pi/3})(X + e^{2i\pi/3}) \end{aligned}$$

Mais ré-écrivons les racines sous forme exponentielle pour faire apparaître un phénomène intéressant :

$$\begin{aligned} x_1 &= e^{i\pi/3} \\ x_2 &= -e^{i\pi/3} = e^{i\pi} e^{i\pi/3} = e^{i4\pi/3} = e^{-2i\pi/3} \\ x_3 &= e^{2i\pi/3} \\ x_4 &= -e^{2i\pi/3} = e^{-i\pi/3} e^{2i\pi/3} = e^{-i\pi/3} \end{aligned}$$

Ces racines sont deux à deux conjuguées. Plus précisément :

$$x_3 = \overline{x_1} \quad \text{et} \quad x_4 = \overline{x_2}$$

Ce phénomène va nous permettre trouver la factorisation primaire dans $\mathbb{R}[X]$

$$P = (X - x_1)(X - \overline{x_1})(X - x_2)(X - \overline{x_2})$$

avec $(X - x_1)(X - \overline{x_1}) = X^2 - (x_1 + \overline{x_1})X + x_1\overline{x_1} = X^2 - 2\text{Re}(x_1) + |x_1|^2$
 et $\text{Re}(x_1) = \text{Re}(e^{2i\pi/3}) = \cos(2\pi/3) = -1/2$ et $|z_1|^2 = 1$

D'où $(X - x_1)(X - \overline{x_1}) = X^2 - X + 1$

De même $(X - x_2)(X - \overline{x_2}) = X^2 - 2\text{Re}(x_2) + |x_2|^2$ avec $\text{Re}(x_2) = \text{Re}(e^{i\pi/3}) = \cos(\pi/3) = 1/2$ et $|z_2|^2 = 1$

D'où $(X - x_2)(X - \overline{x_2}) = X^2 + X + 1$

Finalement

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

Définition 20 : Polynôme conjugué

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme de $\mathbb{C}[X]$

On appelle polynôme conjugué de P le polynôme $\overline{P} = \sum_{k=0}^{+\infty} \overline{a_k} X^k$

Exemple : $P = i.X^2 + e^{i\pi/5}X + 3 + i \implies \overline{P} = -i.X^2 + e^{-i\pi/5}X + 3 - i$

En particulier, pour $a \in \mathbb{C}$: $(X - a)^k$ et $(X - \overline{a})^k$ sont conjuguées.

Lemme : polynôme réel

Soit $P \in \mathbb{C}[X]$.
 On a alors $P \in \mathbb{R}[X] \iff \overline{P} = P$

Propriété 24

Soit $P \in \mathbb{C}[X]$, $\forall z \in \mathbb{C}$, $\overline{P(\overline{z})} = \overline{P(z)}$

Propriété 25 : Racine du polynôme conjugué

Soit $P \in \mathbb{C}[X]$
 $\alpha \in \mathbb{C}$ est racine de polynôme P de multiplicité k
 $\iff \overline{\alpha}$ est racine de \overline{P} de multiplicité k

Propriété 26

Soit $P \in \mathbb{R}[X]$ un polynôme **réel** et $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Alors

α est une racine complexe de P de multiplicité k

$\iff \bar{\alpha}$ est également racine de P de multiplicité k

Et dans ce cas, $[(X - \alpha)(X - \bar{\alpha})]^k$ est un polynôme réel diviseur de P

Propriété 27 : polynômes irréductibles de $\mathbb{R}[X]$

Les polynômes irréductibles de $\mathbb{R}[X]$ ont deux formes possibles :

- $aX - b$ avec $a \in \mathbb{R}^*$, $b \in \mathbb{R}$
- $aX^2 + bX + c$ avec $a \in \mathbb{R}^*$, $b, c \in \mathbb{R}$ et $\Delta = b^2 - 4ac < 0$

Propriété 28 : Polynômes unitaires irréductibles de $\mathbb{R}[X]$

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

- $X - b$ avec $b \in \mathbb{R}$
- $X^2 + bX + c$ avec $b, c \in \mathbb{R}$ et $\Delta = b^2 - 4c < 0$

Propriété 29 : Théorème de décomposition dans $\mathbb{R}[X]$

Un polynôme P de $\mathbb{R}[X]$ de degré n et de coefficient dominant a_n se décompose de la façon suivante :

$$P(X) = a_n \prod_{i=1}^p (X - \alpha_i) \prod_{j=1}^q (X^2 + b_j X + c_j)$$

avec

- $p + 2q = n$
- α_i, b_j, c_j sont des éléments de \mathbb{R} .
- les polynômes $X^2 + b_j X + c_j$ n'ont aucune racine dans \mathbb{R}

Cette décomposition est unique à l'ordre des facteurs près.

5 Dérivation

Si on a une fonction polynôme

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = \sum_{k=0}^n a_k x^k$$

En dérivant on a :

$$\begin{aligned} f'(x) &= a_n \cdot n x^{n-1} + a_{n-1} (n-1) x^{n-2} + \dots + a_3 \cdot 3 x^2 + a_2 \cdot 2 x + a_1 \\ &= \sum_{j=1}^n a_j \cdot j \cdot x^{j-1} = \sum_{k=0}^{n-1} a_{k+1} (k+1) x^k \end{aligned}$$

On adapte cette formule aux polynômes :

Définition 21

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme

Alors on pose $P' = \sum_{k=0}^{+\infty} a_{k+1} (k+1) X^k$

qui est le polynôme dérivé de P

Propriété 30

- $P' = 0 \iff P$ est un polynôme constant
- Si $d^\circ P \geq 1$, $d^\circ P' = d^\circ P - 1$
- $(aP + bQ)' = a.P' + b.Q'$
- $(PQ)' = P'Q + PQ'$
- $\forall n \in \mathbb{N}^*$, $(Q^n)' = nQ^{n-1}Q'$
- $(P \circ Q)' = (P' \circ Q).Q'$

Propriété 31 : Dérivée de la fonction polynomiale

$$\| (\tilde{P}') = (\tilde{P})'$$

Propriété 32 : Égalité des dérivées

Soient P, Q deux polynômes de $\mathbb{K}[X]$

$$\| P' = Q' \iff [\exists a \in \mathbb{C}, P = Q + a]$$

Propriété 33 : Égalité de deux polynômes

Soit $a \in \mathbb{K}$ (quelconque). Alors

$$P = Q \iff [P' = Q' \text{ et } P(a) = Q(a)]$$
Définition 22 : Dérivées successives

On note $P^{(n)}$ la dérivée d'ordre n de P .
On a $P^{(0)} = P$, $P^{(1)} = P'$ et $P^{(n+1)} = (P')^{(n)} = (P^{(n)})'$

Propriété 34 : Degré et dérivées

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

- $d^\circ P \leq n \iff P^{(n+1)} = 0$
- $d^\circ P = n \iff P^{(n+1)} = 0 \text{ et } P^{(n)} \neq 0$

Exemple : $P = X^3 + X^2 + X + 1$ On a $P^{(3)} = 6 \neq 0$ et $P^{(4)} = 0$

Propriété 35 : Formule de Leibniz

Soient P et Q deux polynômes de $\mathbb{K}[X]$ et $n \in \mathbb{N}$ Alors

$$(P.Q)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$$
Propriété 36 : Formule de Taylor ($d^\circ P \leq n$)

Soit P un polynôme de degré au plus n et $a \in \mathbb{K}$, alors :

$$P = \sum_{k=0}^n P^{(k)}(a) \frac{(X-a)^k}{k!}$$
Propriété 37 : Formule de Taylor générale

Soit P un polynôme de degré quelconque et $a \in \mathbb{K}$, alors :

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

Exemple : $P = X^3 + X^2 + X + 1$

La formule de Taylor en 2 donne :

$$P(X) = \frac{P^{(3)}(3)}{3!}(X-2)^3 + \frac{P^{(2)}(2)}{2!}(X-2)^2 + \frac{P^{(1)}(2)}{1!}(X-2) + \frac{P^{(0)}(2)}{0!}$$

$$P(2) = 8 + 4 + 2 + 1 = 15$$

$$P'(X) = 3X^2 + 2X + 1 \quad P'(2) = 12 + 4 + 1 = 17$$

$$P''(X) = 6X + 2 \quad P''(2) = 14$$

$$P^{(3)}(X) = 6 \quad P^{(3)}(2) = 6$$

$$\text{D'où } P(X) = (X-2)^3 + 7(X-2)^2 + 17(X-2) + 15$$

Propriété 38 : Caractérisation des racines par les dérivées

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :

a est racine de multiplicité m

$$\iff P(a) = P'(a) = \dots = P^{(m-1)}(a) = 0 \text{ et } P^{(m)}(a) \neq 0$$

Exemple : 1 est racine de multiplicité 2 de $P = X^4 - 2X^2 + 1$

En effet $P(1) = 0$

$$P' = 4X^3 - 4X \quad P'(1) = 4 - 4 = 0$$

$$P'' = 12X^2 - 4 \quad P''(1) = 8 \neq 0$$

Propriété 39 : Conséquence

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}$. Alors

P est divisible par $(X-a)^m$

$$\iff \exists Q \in \mathbb{K}[X], P = (X-a)^m Q$$

a est racine de P de multiplicité au moins m

$$\iff P(a) = P'(a) = \dots = P^{(m-1)}(a) = 0$$