

Chapitre 1

Polynômes à une indéterminée à coefficients dans \mathbb{R} ou \mathbb{C}

Dans ce chapitre \mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

1.1 L'ensemble des polynômes à une indéterminée

1.1.1 Définitions :

On appelle polynôme à une indéterminée à coefficients dans \mathbb{K} ou tout simplement polynôme, toute expression algébrique de la forme

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_2 X^2 + a_1 X + a_0$$

avec $a_i \in \mathbb{K}$ pour tout $i \in 0, \dots, n$.

- Les scalaires a_0, a_1, \dots, a_n sont appelés coefficients du polynôme P .
- X est appelé variable ou indéterminée.
- Les termes $a_k X^k$ sont appelés les monômes d'ordre k de P .
- Si $a_n = 1$ alors le polynôme est dit normalisé ou unitaire.
- Si $a_n \neq 0$ alors on appelle terme dominant de P le monôme $a_n X^n$.

Nous Notons $\mathbb{K}[X]$ L'ensemble des polynômes à une indéterminée à coefficients dans \mathbb{K} .

1.1.2 Opérations sur $\mathbb{K}[X]$:

a) Addition de deux polynômes :

Soient $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ et $Q(X) = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0$ deux polynômes de $\mathbb{K}[X]$, avec $n \in \mathbb{N}$. On définit alors le polynôme $P + Q$ par :

$$(P + Q)(X) = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \dots + (a_1 + b_1)X + (a_0 + b_0)$$

b) Multiplication de deux polynômes :

Etant donnés deux polynômes $P(X) = a_p X^p + a_{p-1} X^{p-1} + \dots + a_1 X + a_0$ et $Q(X) = b_q X^q + b_{q-1} X^{q-1} + \dots + b_1 X + b_0$, on définit le polynôme $P \cdot Q$ par :

$$(P \cdot Q)(X) = c_r X^r + c_{r-1} X^{r-1} + \dots + c_1 X + c_0$$

1.1. L'ENSEMBLE DES POLYNÔMES À UNE INDÉTERMINÉE

avec

$$r = p + q \quad \text{et} \quad c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^k a_i b_{k-i} = \sum_{j=0}^k a_{k-j} b_j, \quad k \in \{0, 1, \dots, r\}$$

1.1.3 Degré d'un polynôme :

Définition :

On appelle degré d'un polynôme P non nul, le plus grand ordre des monômes non nuls de P . On le note $\deg(P)$ ou $\partial^0 P$.

Si P est le polynôme nul, on convient que le degré de P est moins l'infini $(-\infty)$.

Exemples :

Soient $P(X) = 1 + 4X + 3X^9$ et $Q(X) = X^{12} - 2X^3 + 5X + 1$ deux polynômes de $\mathbb{K}_1[X]$, on a

- a) $\deg(P) = 9$.
- b) $\deg(Q) = 12$.

Propriétés :

Soient P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a :

- a) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.
- b) $\deg(P \cdot Q) = \deg(P) + \deg(Q)$.
- c) $\forall \alpha \in \mathbb{K}^*, \quad \deg(\alpha P) = \deg(P)$.

Preuve :

Posons

$$P = \sum_{k=0}^n a_k X^k, \quad \text{avec } a_n \neq 0,$$
$$Q = \sum_{k=0}^m b_k X^k, \quad \text{avec } b_m \neq 0.$$

a) Si $n > m$ alors

$$P + Q = \sum_{k=0}^m (a_k + b_k) X^k + \sum_{k=m+1}^n a_k X^k,$$

d'où

$$\deg(P + Q) = n.$$

De même si $m > n$, on obtient $\deg(P + Q) = m$.

Si $m = n$ alors $P + Q = \sum_{k=0}^n (a_k + b_k) X^k$.

Le monôme de plus haut degré dans l'expression de $P + Q$ est $(a_n + b_n) X^n$

1.2. DIVISION DES POLYNÔMES DANS $\mathbb{K}[X]$

→ Si $a_n = -b_n$, ce monôme est nul et l'on a alors $\deg(P + Q) < n$.
 → Si $a_n \neq -b_n$ alors $\deg(P + Q) = n$.

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

b) Le monôme dominant de $P \cdot Q$ est $c_{m+n} X^{m+n}$ avec,

$$c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} = \sum_{i=0}^n a_i b_{m+n-i} + \sum_{i=n+1}^{m+n} a_i b_{m+n-i} = a_n b_n \neq 0.$$

Car pour

$$0 \leq i \leq n \implies b_{m+n-i} = 0 \\ i \geq n+1 \implies a_i = 0$$

Donc $\deg(P \cdot Q) = \deg(P) + \deg(Q)$.

c) Claire.

1.2 Division des polynômes dans $\mathbb{K}[X]$

1.2.1 Division suivant les puissances décroissantes :

Théorème de la division euclidienne (admis) :

Soient A et B deux polynômes de $\mathbb{K}[X]$ tel que $B(0) \neq 0$. Il existe deux polynômes uniques Q et R de $\mathbb{K}[X]$ tels que :

$$A = B \cdot Q + R, \quad \text{avec } \deg(R) < \deg(B). \quad (*)$$

Le polynôme Q est appelé quotient de la division de A par B , R est le reste, B le diviseur et A le dividende.

L'opération permettant de passer du couple (A, B) , $B(0) \neq 0$, au couple (Q, R) vérifiant $(*)$ est appelée la division euclidienne de A par B .

Exemple :

Effectuer la division euclidienne de $A = 6X^4 + X^3 + X + 1$ par $B = X^2 + X + 1$.
 On a :

$6X^4 + X^3 + 0X^2 + X + 1$	$X^2 + X + 1$
$6X^4 + 6X^3 + 6X^2$	$6X^2 - 5X - 1$
$-5X^3 - 6X^2 + X + 1$	
$-5X^3 - 5X^2 - 5X$	
$-X^2 + 6X + 1$	
$-X^2 - X - 1$	
$7X + 2$	

1.2. DIVISION DES POLYNÔMES DANS $\mathbb{K}[X]$

D'où :

$$A = BQ + R, \quad \text{avec } Q = 6X^2 - 5X - 1 \text{ et } R = 7X + 2.$$

1.2.2 Racines d'un polynôme :

Définition :

Soient A et $B \in \mathbb{K}[X]$. On dit que A est divisible par B ou que B divise A si le reste de la division euclidienne de A par B est nul.

$$B \text{ divise } A \iff \exists Q \in \mathbb{K}[X] \text{ tel que : } A = BQ.$$

Exemple :

$$\text{Soient } A = X^3 - 1 \text{ et } B = X - 1. \\ \text{Alors } B \text{ divise } A : A = QB \text{ avec } Q = X^2 + X + 1.$$

Définition :

Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine de P si $P(\alpha) = 0$.

Proposition :

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

$$\alpha \text{ est une racine de } P \text{ si et seulement si } (X - \alpha) \mid P.$$

Preuve :

$$\iff \text{Si } (X - \alpha) \mid P \text{ alors } \exists Q \in \mathbb{K}[X] \text{ tel que : } P(X) = (X - \alpha)Q(X).$$

d'où

$$P(\alpha) = 0 \cdot Q(\alpha) = 0.$$

Donc α est une racine de P .

\implies Supposons α est une racine de P . D'après le théorème de la division euclidienne de P par $(X - \alpha)$, on a :

$$P(X) = (X - \alpha)Q(X) + \lambda, \quad \lambda \in \mathbb{K}.$$

$$\text{Or, } P(\alpha) = 0 \implies \lambda = 0.$$

$$P(X) = (X - \alpha)Q(X).$$

$$\text{Donc } (X - \alpha) \mid P.$$

1.2. DIVISION DES POLYNÔMES DANS $\mathbb{K}[X]$

Définition :

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

1. a est une racine d'ordre de multiplicité m si et seulement si $(X-a)^m/P$ et $(X-a)^{m+1}$ ne divisent pas P .

2. Soit a une racine d'ordre de multiplicité m alors :

- Si $m = 1$, on dit que a est une racine simple de P .
- Si $m = 2$, on dit que a est une racine double de P .
- Si $m = 3$, on dit que a est une racine triple de P .

Exemple :

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

$$P(X) = (X-1)(X-4)^2(X+3)^5.$$

- 1 est une racine simple de P .
- 4 est une racine double de P .
- -3 est une racine d'ordre 5 de P .

Théorème : (admis)

Soient $P \in \mathbb{K}[X]$ et a_1, a_2, \dots, a_m des racines de P deux à deux distinctes d'ordres de multiplicité respectifs k_1, k_2, \dots, k_m . Alors, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P(X) = (X-a_1)^{k_1}(X-a_2)^{k_2}\dots(X-a_m)^{k_m}Q(X), \quad \text{et } Q(a_i) \neq 0, \quad \forall i = 1, 2, \dots, m.$$

Corollaire :

Soit P un polynôme de $\mathbb{K}[X]$ de degré n . Alors P ne peut pas avoir plus de n racines distinctes.

Preuve :

Supposons que P admet $n+1$ racines a_1, a_2, \dots, a_{n+1} . Alors, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P(X) = (X-a_1)(X-a_2)\dots(X-a_{n+1})Q(X), \quad Q \in \mathbb{K}[X]$$

donc,

$$\begin{aligned} \deg(P) &= \deg((X-a_1)(X-a_2)\dots(X-a_{n+1})Q(X)) \\ &\geq n+1. \quad \text{Absurde!} \end{aligned}$$

Définition :

Soit P un polynôme de $\mathbb{K}[X]$ de degré $n > 1$. P est dit scindé sur \mathbb{K} s'il admet n racines dans \mathbb{K} .

1.2. DIVISION DES POLYNÔMES DANS $\mathbb{K}[X]$

Exemple :

a) $P(X) = X^3 - 3X^2 - X + 3 = (X-1)(X+1)(X-3)$ est scindé sur \mathbb{R} .

b) $Q(X) = X^2 + 1 = (X-i)(X+i)$ est scindé sur \mathbb{C} .

Théorème d'Alémbert : (admis)

Tout polynôme de $\mathbb{C}[X]$ de degré $n > 1$ est scindé sur \mathbb{C} .

1.2.3 Décomposition en facteurs irréductibles :

Définition :

Soit P un polynôme de $\mathbb{K}[X]$. P est irréductible dans \mathbb{K} s'il n'a pour diviseurs dans $\mathbb{K}[X]$ que les polynômes constants et les polynômes λP où $\lambda \neq 0$.

Théorème : (Polynôme irréductible dans \mathbb{C})

Un polynôme P est irréductible dans \mathbb{C} si et seulement si $\deg(P) = 1$.

Corollaire :

Tout polynôme P non nul de $\mathbb{C}[X]$ admet une décomposition en facteurs irréductibles du type suivant :

$$P(X) = \lambda \prod_{i=1}^k (X - \lambda_i)^{m_i},$$

où $\{\lambda_1, \dots, \lambda_k\}$ est l'ensemble des racines de P , m_i est la multiplicité de λ_i et λ est le coefficient du terme dominant de P .

Théorème : (Polynôme irréductible dans \mathbb{R})

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

- Les polynômes de degré 1.
- Les polynômes de degré 2 à discriminant strictement négatifs.
 $P(X) = aX^2 + bX + c$ avec $a \neq 0$ et $\Delta = b^2 - 4ac < 0$.

Exemple :

Le polynôme $P(X) = X^3 + 3X^2 + 2X + 6$ se décompose en facteurs irréductibles dans :

a) $\mathbb{C}[X]$ en $(X-3)(X+i\sqrt{2})(X-i\sqrt{2})$.

b) $\mathbb{R}[X]$ en $(X-3)(X^2+2)$.

1.3. DÉRIVATION DES POLYNÔMES

1.2.4 Division suivant les puissances croissantes :

Théorème (admis)

Soient A et B deux polynômes de $\mathbb{K}[X]$ tel que $B(0) \neq 0$ et n un entier strictement positif, alors il existe deux polynômes uniques Q_n et R_n de $\mathbb{K}[X]$ tels que :

$$\begin{cases} A = B \cdot Q_n + X^{n+1}R_n, \\ \deg(Q_n) \leq n \end{cases}$$

On effectue cette division un peu comme la division euclidienne classique, mais en écrivant les polynômes suivant les puissances croissantes, et en cherchant à éliminer d'abord les termes constants, puis les termes en X , etc...

Exemple :

Effectuer la division suivant les puissances croissantes à l'ordre 2 de $A = 4 + X^2$ par $B = 1 + X + X^2$.

On a :

$$\begin{array}{r} 4 + 0X + X^2 \\ 4 + 4X + 4X^2 \\ \hline -4X - 3X^2 \\ -4X - 4X^2 - 4X^3 \\ \hline X^2 + 4X^3 \\ X^2 + X^3 + X^4 \\ \hline 3X^3 - X^4 \end{array}$$

D'où :

$$A = BQ_2 + X^3R_2, \quad \text{avec } Q_2 = 4 - 4X + X^2 \text{ et } R_2 = 3 - X.$$

1.3 Dérivation des polynômes

1.3.1 Définition :

Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_2 X^2 + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$. On appelle polynôme dérivé de P et on note P' le polynôme suivant :

$$P'(X) = \begin{cases} na_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \dots + 2a_2 X + a_1 = \sum_{k=1}^n k a_k X^{k-1}, & \text{Si } n \geq 1 \\ 0, & \text{Si } n = 0 \end{cases}$$

1.3.2 Propriétés :

Soient P et Q deux polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on a les propriétés suivantes :

1. Si $\deg(P) > 0$ alors $\deg(P') = \deg(P) - 1$.

1.3. DÉRIVATION DES POLYNÔMES

2. Si P est constant alors $P' = 0$.
3. $(P + Q)' = P' + Q'$.
4. $(\lambda P)' = \lambda P'$.
5. $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$.

1.3.3 Remarque :

On définit par récurrence le polynôme dérivé d'ordre n du polynôme P , que l'on note $P^{(n)}$ comme suit :

$$P^{(0)} = P, \quad \text{et} \quad \forall k \in \{0, \dots, n\}, \quad P^{(k)} = (P^{(k-1)})'.$$

Et on a le résultat suivant entre les dérivées successives de P et ses coefficients :

1.3.4 Proposition : (Formule de Mac-Laurin)

Soit $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$. On a :

$$\begin{aligned} a_k &= \frac{P^{(k)}(0)}{k!}, \quad \forall k \in \{1, \dots, n\} \\ P(X) &= P(0) + \frac{P'(0)}{1!} X + \frac{P''(0)}{2!} X^2 + \dots + \frac{P^{(n)}(0)}{n!} X^n \\ &= \sum_{k=0}^n \frac{P^{(k)}(0)}{k!} X^k. \end{aligned}$$

Preuve :

Soit $P(X) = \sum_{k=0}^n a_k X^k$.

Pour tout $j \leq n$, on a :

$$\begin{aligned} P^{(j)}(X) &= \sum_{k=0}^n a_k (X^k)^{(j)} \\ &= \sum_{k=j}^n a_k (k(k-1) \dots (k-j+1)) X^{k-j} \\ &= a_j j! + \sum_{k=j+1}^n a_k (k(k-1) \dots (k-j+1)) X^{k-j} \end{aligned}$$

On en déduit que $P^{(j)}(0) = j! a_j$.

Plus généralement, on a la formule de Taylor pour les polynômes.

1.3.5 Proposition : (Formule de Taylor)

Soit P un polynôme de $\mathbb{K}[X]$ de degré n et $\alpha \in \mathbb{K}$. On a la relation suivante :

$$\begin{aligned} P(X) &= P(\alpha) + \frac{P'(\alpha)}{1!} (X - \alpha) + \frac{P''(\alpha)}{2!} (X - \alpha)^2 + \dots + \frac{P^{(n)}(\alpha)}{n!} (X - \alpha)^n \\ &= \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k. \end{aligned}$$

1.3.6 Théorème :

Soient P un polynôme de $\mathbb{K}[X]$, $m \in \mathbb{N}^*$ et $\alpha \in \mathbb{K}$. Les propriétés suivantes sont équivalentes :

1. α est une racine d'ordre m de P .
2. $P^{(k)}(\alpha) = 0, \forall k \in \{0, \dots, m-1\}$ et $P^{(m)}(\alpha) \neq 0$.

LEMME



Travaux Dirigés. Polynômes de $\mathbb{K}[X]$

Algèbre 2 Série n^o1

Pr. Nouh IZEM

Exercice 1

- 1 Effectuer la division euclidienne (suivant les puissances décroissantes) de
 - (a) $3X^5 + 4X^2 + 1$ par $X^2 + 2X + 3$;
 - (b) $X^5 + 2X^3 + 3X + 1$ par $X^3 + 1$;
 - (c) $X^4 + (1+i)X^2 + 1$ par $X^2 - 1$;
 - (d) $2X^4 + 2iX^3 + 5X^2 + (8i-5)X + 1$ par $X^2 - iX + 2$;
- 2 Effectuer la division suivant les puissances croissantes de:
 - (a) $A = X^4 + X^3 - 2X + 1$ par $B = X^2 + X + 1$ à l'ordre 2;
 - (b) $A = X^6 + 2X^4 + X^3 + 1$ par $B = X^3 + X^2 + 1$ à l'ordre 4;

Exercice 2

- 1 Déterminer le reste de la division euclidienne de $X^n + X + b$ par $(X-a)^2$, pour $n \in \mathbb{N}$, $n \geq 2$.
- 2 Déterminer le reste de la division euclidienne de $(\cos a + X \sin a)^n$ par $1 + X^2$, pour $a \in \mathbb{R}$, $n \in \mathbb{N}$, $n \geq 2$.
- 3 Montrer que le polynôme $P = nX^{n+1} - (n+1)X^n + 1$ est divisible par $(X-1)^2$ et calculer le quotient.

Exercice 3

- 1 Factoriser en produit de polynômes irréductibles dans $\mathbb{R}[X]$ les polynômes suivants :
 - a) $X^4 + 4$;
 - b) $X^6 + 27$;
 - c) $X^4 + X^2 + 1$;
 - d) $X^8 + X^4 + 1$;
- 2 Décomposer dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme $X^n - 1$ pour $n = 5$ et $n = 6$.

Exercice 4

Soit $P = X^7 - 5X^6 + 8X^5 - 4X^4 - 4X^3 + 8X^2 - 5X + 1$ un polynôme de $\mathbb{C}[X]$.

- 1 Montrer que 1 et -1 sont des racines de P .
- 2 Déterminer P_1 tel que $P = (X-1)^\alpha (X+1)^\beta P_1$ avec $P_1(1) \neq 0$ et $P_1(-1) \neq 0$.
- 3 Montrer que $P_1(z) = 0$ si et seulement si $z + \frac{1}{z}$ est solution d'un polynôme de second degré.
- 4 En déduire la décomposition de P dans $\mathbb{C}[X]$.

Exercice 5

Soit $P \in \mathbb{R}[X]$ défini par:

$$P = X^8 + 2X^6 + 3X^4 + 2X^2 + 1$$

- 1 Montrer que $j = e^{\frac{2i\pi}{3}}$ est une racine multiple de P .
- 2 En remarquant que P est un polynôme pair, donner toutes les racines de ainsi que leur multiplicité.
- 3 Factoriser P dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.