Chapitre 12.A

Polynômes (Partie A)

Plan du chapitre

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

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

1.1 Définition

Définition 1

On dit qu'une suite $(a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est **presque nulle** si elle est nulle à partir d'un certain rang, c'est-à-dire :

$$\exists k_0 \in \mathbb{N} \quad \forall k \in [\![k_0, +\infty[\![\qquad a_k = 0.$$

Cela équivaut à dire que (a_k) a un nombre fini de termes non nuls.

Exemple 1 :

- La suite de terme général $u_k = \dfrac{1}{k+1}$
- La suite de terme général $v_k = \sin \dfrac{k\pi}{2}$
- Soit $n \in \mathbb{N}$. La suite de terme général $w_k = w_k = \begin{cases} \dbinom{10}{k} & \text{si } k \leq 10 \\ 0 & \text{si } k > 10 \end{cases}$

Définition 2

- Un **polynôme à une indéterminée à coefficients dans** $\mathbb{K}$ est une suite $(a_k)_{k\in\mathbb{N}}$ presque nulle à valeurs dans $\mathbb{K}$. Si P est un tel polynôme, on utilise la notation :

$$P = \sum_{k=0}^{+\infty} a_k X^k = a_0 + a_1 X + a_2 X^2 + \cdots \qquad (\text{“convention” } X^0 = 1)$$

  Comme $a_k = 0$ à partir d'un certain rang, cette somme n'a qu'un nombre fini de termes non nuls et donc a toujours un sens.
- X est appelée **l'indéterminée** du polynôme.
- $a_0, a_1, \cdots$ sont appelés les **coefficients** du polynôme.
- L'ensemble de ces polynômes est noté $\mathbb{K}[X]$.
- Deux polynômes P et Q sont dits **égaux** et on note $P = Q$, si leurs coefficients sont égaux deux à deux. Il s'agit d'une relation d'équivalence sur $\mathbb{K}[X]$.

On emploie parfois la notation $P(X)$ au lieu de P.

Exemple 2 :

- $X^2 + X + 1, \quad -X + \pi, \quad 2X^{17} + X, \quad 1$ et 0 sont tous des polynômes.
- $X^{1/2}$ et $1 + X + X^2 + \cdots$ ne sont pas des polynômes.
- $P = 0$ est appelé **polynôme nul**. Il correspond au cas où $0 = a_0 = a_1 = \cdots$.
- Lorsque $a_1 = a_2 = \cdots = 0$, on a $P = a_0$. On dit alors que P est un **polynôme constant**.

1.2 Somme de polynômes et multiplication par un scalaire

Définition 3

Soit $\lambda \in \mathbb{K}$ et

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

deux polynômes. On pose

$$P + Q := \sum_{k=0}^{+\infty} (a_k + b_k) X^k \qquad \lambda P := \sum_{k=0}^{+\infty} (\lambda a_k) X^k$$

Remarques :

- $P+Q$ et λP sont bien des polynômes : puisque (a_k) et (b_k) sont presque nulles, alors les suites $(a_k+b_k)_{k\in\mathbb{N}}$ et $(\lambda a_k)_{k\in\mathbb{N}}$ sont également presque nulles. On en déduit que $+$ est une l.c.i. sur $\mathbb{K}[X]$.
- Les définitions de $P+Q$ et λP sont cohérentes avec la linéarité de la somme : si X était vu comme un élément de $\mathbb{K}$, on aurait bien

$$\lambda \sum_{k=0}^{\cdots} a_k X^k + \mu \sum_{k=0}^{\cdots} b_k X^k = \sum_{k=0}^{\cdots} (\lambda a_k + \mu b_k) X^k.$$

- Toutefois, X ne correspond pas, à proprement parler, à un élément quelconque de $\mathbb{K}$. On introduit ce X comme une notation pratique pour les calculs. On aurait d'ailleurs pu s'en passer et considérer les polynômes uniquement comme des suites presque nulles : la somme des “polynômes” (a_k) et (b_k) serait alors définie comme étant $(a_k + b_k)$.

Propriété 1

L'ensemble $(\mathbb{K}[X],+)$ est un groupe abélien. Son élément neutre est le polynôme nul.

Cela découle directement du fait que $(\mathbb{K}^{\mathbb{N}},+)$ est un groupe abélien.

1.3 Degré d'un polynôme

Définition 4

Soit P un polynôme de coefficients (a_k), tel que $P \neq 0$. On note $n = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$, de telle sorte que

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{avec } a_n \neq 0.$$

- n est appelé **degré de P**, et noté $\deg P$ ou $\deg(P)$.
- a_n est appelé **coefficient dominant** de P.
- $a_n X^n$ est appelé **terme dominant** de P.

Pour le polynôme nul, on pose par convention $\deg(0) = -\infty$. Pour tout $n \in \mathbb{N}$, on note

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

l'ensemble des polynômes de degré au plus n.

Exemple 3 :

- Le degré de $P = a_0 + a_1 X + a_2 X^2$ est ...
- $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants (y compris le polynôme nul) ; il peut être identifié à $\mathbb{K}$.
- $\mathbb{K}_1[X] = \left\{aX + b \mid (a,b) \in \mathbb{K}^2\right\}$ est l'ensemble des polynômes constants ou de degré 1.

Définition 5

Soit $P \in \mathbb{K}[X]$. On dit que P est **unitaire** si $P \neq 0$ et son coefficient dominant est égal à 1.

Exemple 4 :

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

Définition 6

Un **monôme** est un polynôme possédant exactement un coefficient non nul.

Exemple 5 : X^3, $\quad -2X$ et -3 sont des monômes, tandis que $X^2 + 1$ et 0 n'en sont pas.

Propriété 2 : degré de la somme

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

$$\deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \in \mathbb{K}^* \\ -\infty & \text{si } \lambda = 0 \end{cases}$$

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

$$\deg(P+Q) = \max(\deg P, \deg Q) \qquad \text{lorsque } \deg P \boxed{\neq} \deg Q$$

Démonstration

Remarque : Somme de polynômes de même degré. Si $\deg P = \deg Q = p$, alors en notant (a_k) et (b_k) les coefficients respectifs de P et Q, on a

$$\begin{aligned} P &= a_p X^p + a_{p-1} X^{p-1} + \cdots + a_0 \qquad \text{avec ...} \\ Q &= b_p X^p + b_{p-1} X^{p-1} + \cdots + b_0 \qquad \text{avec ...} \end{aligned}$$

Dans ce cas :

- Si $b_p \neq -a_p$, alors $\deg(P+Q) = p$.
- Si $b_p = -a_p$, alors $\deg(P+Q) < p$.

Par exemple, avec $P = X^3 + X, \quad Q = -X^3 + X \quad \text{et} \quad R = X^3 - X$:

Propriété 3

$$\begin{array}{lllllll} P \text{ est constant} & \text{ssi} & P = \lambda \in \mathbb{K} & \text{ssi} & P \in \mathbb{K}_0[X] & \text{ssi} & \deg(P) \leq 0 \\ P \text{ est constant non nul} & \text{ssi} & P = \lambda \in \mathbb{K}^* & \text{ssi} & P \in \mathbb{K}_0[X] \setminus \{0\} & \text{ssi} & \deg(P) = 0 \end{array}$$

1.4 Produit de polynômes

Définition 7

Soit $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ des polynômes à coefficients dans $\mathbb{K}$.

Le produit de P et Q est le polynôme $P \times Q = PQ := \sum_{n=0}^{p+q} c_n X^n$, avec pour tout $n \in \mathbb{N}$:

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} =$$

Remarque : Pour tout entier $n > p+q$, on a

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{p} a_k b_{n-k} + \sum_{k=p+1}^{n} a_k b_{n-k}.$$

Or, pour tout entier $k \geqslant p+1$, $a_k =$, et pour tout $k \in [\![0,p]\!]$, $n-k \geqslant$ donc $b_{n-k} =$, donc

$$c_n =$$

Cela justifie que la suite (c_n) est presque nulle, et que la somme s'arrête à l'indice $n = p+q$ dans l'écriture de $P \times Q$. On en déduit ainsi que $\times$ est une l.c.i. sur $\mathbb{K}[X]$.

Produit avec un polynôme constant : Soit $\lambda \in \mathbb{K}$, $P = \lambda X^0$ et $Q \in \mathbb{K}[X]$. Alors :

$$P \times Q = \sum_{n=0}^{p+q} c_n X^n \qquad \text{avec} \quad c_n =$$

Ainsi $(\lambda X^0) \times Q = \lambda Q$: le produit de polynômes $\lambda X^0 \times Q$ coïncide avec le produit λQ introduit dans la définition 3. En particulier, $1X^0 \times P = P$: le polynôme constant 1 est ainsi élément neutre de la loi $\times$.

Produit de deux monômes : Si $P = a_p X^p$ et $Q = b_q X^q$ sont deux monômes, alors PQ aussi et $PQ = a_p b_q X^{p+q}$.

En effet, $PQ = \sum_{n=0}^{p+q} c_n X^n$ avec, pour tout $n \in \mathbb{N}$:

$$c_n =$$

Ainsi $(a_p X^p)(b_q X^q) = a_p b_q X^{p+q}$.

Compatibilité du produit avec la notation $\sum$: La définition du produit est également compatible avec le produit de deux sommes (cf chapitre 2) :

$$PQ = \left(\sum_{i=0}^{p} a_i X^i\right)\left(\sum_{j=0}^{q} b_j X^j\right) = \sum_{i=0}^{p}\sum_{j=0}^{q} a_i b_j X^{i+j} = \sum_{n=0}^{p+q}\left(\sum_{i+j=n} a_i b_j X^{i+j}\right) = \sum_{n=0}^{p+q} \underbrace{\left(\sum_{i+j=n} a_i b_j\right)}_{c_n} X^n$$

Propriété 4 : Bilinéarité du produit

Pour tous $P,Q \in \mathbb{K}[X]$, pour tout $\lambda \in \mathbb{K}$,

$$\lambda(P \times Q) = (\lambda P) \times Q = P \times (\lambda Q)$$

Propriété 5

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

La démonstration est laissée en exercice. Il reste à démontrer ...

Propriété 6 : degré d'un produit

Pour tous $P, Q \in \mathbb{K}[X]$, on a $\deg(PQ) = \deg P + \deg Q$.

Si P ou Q est nul, $PQ = 0$ donc l'égalité reste vraie avec la convention $-\infty + n = -\infty$ pour tout $n \in \mathbb{N} \cup \{-\infty\}$.

Démonstration

Notons $(p,q) = (\deg P, \deg Q)$ ainsi que $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$. Nécessairement $a_p \neq 0$ et $b_q \neq 0$.

Ainsi :

- $a_p \neq 0$ et pour tout entier $k > p$, $a_k = 0$.
- $b_q \neq 0$ et pour tout entier $k > q$, $b_k = 0$.

□

Remarque : La démonstration montre également que le coefficient dominant de PQ est le produit des coefficients dominants de P et de Q.

Corollaire 7

- Pour tous polynômes $P, Q \in \mathbb{K}[X]$, $PQ = 0 \implies (P = 0 \text{ ou } Q = 0)$. Autrement dit, $(\mathbb{K}[X], +, \times)$ est un anneau intègre.
- Pour tout polynôme $P \in \mathbb{K}[X]$, il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$ si et seulement si P est constant et non nul (c'est-à-dire $P \in \mathbb{K}^*$).

Conséquence : Pour tous polynômes $A, B, C \in \mathbb{K}[X]$ avec A non nul, $AB = AC \Leftrightarrow B = C$.

En effet,

$$AB = AC \quad \Leftrightarrow \quad AB - AC = 0 \quad \Leftrightarrow \quad A(B - C) = 0 \quad \Leftrightarrow \quad A = 0 \text{ ou } B - C = 0.$$

Par ailleurs, le second point équivaut à dire qu'un polynôme est inversible si et seulement s'il est de degré zéro. On ne peut donc pas définir la division de deux polynômes comme une "multiplication par l'inverse." On aura recours à la place à une division euclidienne, comme dans $\mathbb{Z}$ (voir partie 3).

1.5 Puissances d'un polynôme

Définition 8

Soit $P \in \mathbb{K}[X]$. On définit de manière récursive P^n en posant :

- $P^0 = 1$,
- pour tout entier naturel n, $P^{n+1} = P^n \times P$.

Remarque : Le polynôme X^n correspond bien à la puissance n-ième du polynôme X : la notation est cohérente.

Attention, la notation P^{-1} n'a de sens que si P est ....! S'en servir est donc risqué...

Propriété 8

Pour tout $P \in \mathbb{K}[X]$ non nul, pour tout $n \in \mathbb{N}$, $\deg(P^n) = n \deg(P)$.

Si P est nul, l'égalité reste vraie avec la convention $n \times (-\infty) = \begin{cases} -\infty & \text{si } n \geq 1 \\ 0 & \text{si } n = 0 \end{cases}$.

La preuve résulte d'une récurrence immédiate en utilisant la propriété 6.

Exemple 6 : Soit $n \in \mathbb{N}$. Déterminer le degré de $P = (X^2+1)^n - (X+1)^n$.

Les propriétés sur les sommes et puissances de nombres complexes restent valables pour les polynômes, notamment les identités remarquables et le fait que pour tous $n, m \in \mathbb{N}$, $P^n \times P^m = P^{n+m}$.

Propriété 9 : Calcul dans un anneau, version polynôme

Pour tous $P, Q \in \mathbb{K}[X]$, pour tout $n \in \mathbb{N}$,

$$(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}.$$

et si $n \in \mathbb{N}^*$,

$$P^n - Q^n = (P-Q) \sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

1.6 Composition de polynômes

Définition 9

Soit $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ des polynômes. On définit le **polynôme composé** $P \circ Q$ par

$$P \circ Q := \sum_{k=0}^{p} a_k Q^k = \sum_{k=0}^{p} a_k \left(\sum_{j=0}^{q} b_j X^j \right)^k.$$

Exemple 7 : Soit $P = X^2 + 1$, $\quad Q = 2X - 2$, $\quad R = 3$. Calculer $P \circ Q$, $Q \circ P$, $P \circ R$ et $Q \circ R$.

On constate que

Propriété 10

La composition de polynômes est **associative** : pour tous polynômes P, Q et R, $(P\circ Q)\circ R = P\circ(Q\circ R)$.

Remarques :

- Il n'existe pas de formule simple pour les coefficients de la composée de deux polynômes. En règle générale, il n'y a pas d'autre méthode que faire le calcul "à la main" pour déterminer un polynôme composé.
- La composée $P\circ Q$ peut s'écrire $P(Q)$. On utilisera cette notation avec précaution (ce n'est pas un produit !). Cela donne en particulier, pour tout polynôme $P=\sum_{k=0}^{n} a_k X^k$, pour tout $\alpha\in\mathbb{K}$:

$$P(X) =$$

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

Avant d'aborder la suite, on rappelle la propriété suivante (cf propriété 2) : si $P\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$, alors

$$\deg(\lambda P) = \begin{cases} \deg(0) = -\infty & \text{si } \lambda = 0 \\ \deg(P) & \text{si } \lambda \neq 0 \end{cases}$$

En particulier, on a toujours $\deg(\lambda P)\leq \deg P$.

Propriété 11 : degré de $P\circ Q$

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

1. Si Q est non constant, alors $\deg(P\circ Q) = \deg P\times\deg Q$.

2. Si Q est constant $\deg(P\circ Q)\leq 0$ (en particulier $P\circ Q$ est constant).

$P\circ Q$		Q : 0	Q : $\lambda\in\mathbb{K}^*$	Q : $\deg Q\geq 1$
P	0	0	0	0
	$\lambda\in\mathbb{K}^*$	λ	λ	λ
	$\deg P\geq 1$	$\deg(P\circ Q)\leq 0$	$\deg(P\circ Q)\leq 0$	$\deg(P\circ Q)=\deg P\times\deg Q$

Commentons un peu ce tableau.

- Si P est constant, alors $P\circ Q = P$: cela correspond aux deux premières lignes.
- La première assertion de la propriété se vérifie sur la colonne de droite.
- Lorsque $\deg P\geq 1$ et que Q est constant, on peut seulement dire que $P\circ Q$ est constant. Tous les cas sont possibles, par exemple :

$$\begin{cases} P = X-1 \\ Q = 1 \end{cases} \Longrightarrow P\circ Q = 0 \qquad\qquad \begin{cases} P = X+1 \\ Q = 0 \end{cases} \Longrightarrow P\circ Q = 1$$

1.7 Lien avec les fonctions polynomiales

Définition 10

Soit $P=\sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$.

La **fonction polynomiale** associée à P est la fonction $\widetilde{P} : \begin{array}{l} \mathbb{K}\to\mathbb{K} \\ x\mapsto \sum_{k=0}^{n} a_k x^k. \end{array}$

Les opérations $+$, $\lambda\cdot$, $\times$ et $\circ$ vues précédemment sont “compatibles” avec les opérations $+$, $\lambda\cdot$, $\times$ et $\circ$ entre fonctions qu'on a vu au chapitre de fonctions usuelles. Cela signifie que pour tous polynômes P,Q et pour tout $\lambda \in \mathbb{K}$, on a :

- La fonction polynomiale associée à $P+Q$ est $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$.
- $\widetilde{\lambda P} = \lambda \widetilde{P}$.
- La fonction polynomiale associée à $P \times Q$ est $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$.
- La fonction polynomiale associée à $P \circ Q$ est la composée $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Remarque : Malgré le lien fort entre les polynômes et les fonctions polynomiales, il faut distinguer les deux. Pour cela, il est d'usage d'écrire X pour l'indéterminée d'un polynôme et x pour la variable d'une fonction polynômiale.

On verra à la partie 2.2 que l'application $P \mapsto \widetilde{P}$ est bijective de $\mathbb{K}[X]$ sur l'ensemble des fonctions polynomiales (la surjectivité découle de la définition ci-dessus). Cela montrera que la connaissance d'une fonction polynomiale détermine de manière unique le polynôme auquel elle est associée.

Définition 11

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

L'**évaluation de $\boldsymbol{P}$ en $\boldsymbol{\alpha}$** est le nombre $\widetilde{P}(\alpha) = \sum_{k=0}^{n} a_k \alpha^k$, aussi noté $P(\alpha)$.

Propriété 12

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$.

- $P(0)$ est égal au premier coefficient de P : $P(0) = a_0$.
- $P(1)$ est la somme des coefficients de P : $P(1) = \sum_{k=0}^{n} a_k$.

2 Dérivation formelle dans $\mathbb{K}[X]$

2.1 Définitions et premières propriétés

Définition 12

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. Le **polynôme dérivé** (ou dérivée formelle) de P est le polynôme

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

Remarque : Si $\mathbb{K} = \mathbb{R}$, la fonction polyomiale $\widetilde{P}$ est dérivable, et il y a “compatibilité” entre ces notions : $\widetilde{P}' = \widetilde{P'}$. Mais la dérivée formelle reste définie si $\mathbb{K} = \mathbb{C}$, alors qu'on ne sait pas dériver une fonction définie sur $\mathbb{C}$: c'est notamment pour cela que l'on parle de dérivée *formelle*.

Propriété 13

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

1. Degré du polynôme dérivé :

- Si $\deg(P) \geqslant 1$, alors $\deg(P') = \deg(P) - 1$.
- $P' = 0$ si et seulement si P est constant.

2. Opérations et dérivation formelle :

- Linéarité de la dérivation : pour tous $\lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
- Produit : $(P \times Q)' = P' \times Q + P \times Q'$.
- Composition : $(P \circ Q)' = Q' \times (P' \circ Q)$.

Démonstration

▶ **Éléments de démonstration pour la composition :** En utilisant le point précédent, on montre par récurrence que pour tout $k \in \mathbb{N}$, $(Q^k)' = kQ'Q^{n-1}$. On a alors $P \circ Q = \sum_{k=0}^{n} a_k Q^k$, donc par linéarité de la dérivation,

$$\begin{aligned}(P \circ Q)' &= \sum_{k=0}^{n} a_k (Q^k)' = \sum_{k=0}^{n} a_k k Q' Q^{k-1} \\ &= Q' \sum_{k=0}^{n} a_k k Q^k = Q' \times (P' \circ Q).\end{aligned}$$

□

Exemple 8 : Déterminer la dérivée formelle du polynôme $P = (2X - 1)^4$.

Définition 13

Soit $P \in \mathbb{K}[X]$. On définit récursivement le polynôme dérivé d'ordre k de P en notant :

- $P^{(0)} = P$,
- pour tout $k \in \mathbb{N}$, $P^{(k+1)} = (P^{(k)})'$.

Exemple 9 : Pour tous $n, k \in \mathbb{N}$, $(X^n)^{(k)} =$

Remarque : Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

La dérivée formelle de $P(X + \alpha)$ est

Par une récurrence immédiate, la dérivée d'ordre k de $P(X + \alpha)$ est

En combinant cette remarque avec l'exemple précédent, on a notamment

$$((X + \alpha)^n)^{(k)} =$$

On peut généraliser les propriétés de la dérivée formelle aux dérivées successives :

Propriété 14

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

1. Degré de $P^{(n)}$:

- Si $\deg(P) \geqslant n$, alors $\deg(P^{(n)}) = \deg(P) - n$.
- $P^{(n)} = 0$ si et seulement si $\deg P \leqslant n-1$.

2. Opérations :

- Linéarité : pour tous $\lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.
- Formule de Leibniz : $(P \times Q)^{(n)} = \displaystyle\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

2.2 Formule de Taylor

Theorème 15 : Formule de Taylor

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{K}$,

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

Remarque : Si $\deg P < n$, la formule ci-dessus reste valable. Si par exemple $\deg P = n-1$, alors le théorème ci-dessus entraine $P = \displaystyle\sum_{k=0}^{n-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$ et comme $P^{(n)} = 0$, on retrouve que $P = \displaystyle\sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$

<u>**Démonstration**</u>

▶ **Cas $\alpha = 0$:** Notons $P(X) = \displaystyle\sum_{k=0}^{n} a_k X^k$. Pour tout $i \in [\![0, n]\!]$,

$$P^{(i)}(X) = \sum_{k=i}^{n} a_k k(k-1)\dots(k-i+1)X^{k-i},$$

$$\text{donc} \quad P^{(i)}(0) =$$

Cela donne $a_i =$. Ainsi $P(X) = \displaystyle\sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$.

▶ **Cas général :** Notons $Q(X) = P(X+\alpha)$. D'après le point précédent, $Q(X) = \displaystyle\sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k$. De plus :

- Pour tout $k \in [\![0, n]\!]$, $Q^{(k)}(X) =$ (remarque suivant la définition 13), donc $Q^{(k)}(0) =$
- $Q(X-\alpha) = P(X-\alpha+\alpha) = P(X)$.

Donc

$$\begin{aligned} P(X) = Q(X-\alpha) &= \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!}(X-\alpha)^k \\ &= \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k. \end{aligned}$$

□

Remarque : En particulier, si $P = \sum_{k=0}^{n} a_k X^k$, alors $a_k = \dfrac{P^{(k)}(0)}{k!}$.

Conséquence : Si deux polynômes P et Q ont la même fonction polynômiale ($\widetilde{P} = \widetilde{Q}$), alors $P = Q$.
En effet, pour tout $k \in \mathbb{N}$, $P^{(k)}(0) = (\widetilde{P})^{(k)}(0)$, donc avec la relation ci-dessus, les coefficients de P sont déterminés par la fonction polynômiale $\widetilde{P}$.
En d'autre termes, l'application $P \mapsto \widetilde{P}$ est injective de $\mathbb{K}[X]$ sur l'ensemble des fonctions polynomiales (donc bijective, puisque l'on a déjà justifié la surjectivité).

3 Divisibilité et division euclidienne de polynômes

3.1 Divisibilité dans $\mathbb{K}[X]$

Définition 14

Soit $A, B \in \mathbb{K}[X]$.
On dit que ***B* divise *A***, et on note $B \mid A$, s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$.
On dit alors que B est un **diviseur** de A, et que A est un **multiple** de B.

Propriété 16

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

- Si $B \mid A$, alors $\deg B \leq \deg A$.
- Si $B \mid A$ et $\deg B = \deg A$, alors $B = \lambda A$ avec $\lambda \in \mathbb{K}^*$.

En effet, comme $B \mid A$, on a $A = BQ$ et donc $\deg A = \deg B + \deg Q$. Or, $Q \neq 0$ (sinon on aurait $A = 0$). On en déduit que $\deg Q \geq 0$. D'où $\deg B \leq \deg A$.
Si en outre $\deg B = \deg A$, alors $\deg Q = 0$, ce qui entraine que $Q = \mu \in \mathbb{K}^*$. D'où $B = \lambda A$ avec $\lambda = \dfrac{1}{\mu} \in \mathbb{K}^*$.

Exemple 10 :

- $X^2 - 4$ est-il divisible par $X + 2$ dans $\mathbb{R}[X]$?
- $X^2 - 4$ est-il divisible par $5X + 10$ dans $\mathbb{R}[X]$?
- $X^2 - 4$ est-il divisible par $X^2 + 1$ dans $\mathbb{R}[X]$?

- Soit $P \in \mathbb{K}[X]$. Alors $P \mid 0$ car et $1 \mid P$ car .
- Pour tous λ,$\mu \in \mathbb{K}^*$ et P,$Q \in \mathbb{K}[X]$, on a $P \mid Q$ ssi $\lambda P \mid \mu Q$.

Exemple 11 : Soit $n \in \mathbb{N}^*$. Donner un diviseur de degré 1 de $X^n - 1$.

Propriété 17

Soient A, B, D des polynômes.

$$D \mid A \quad \text{et} \quad D \mid B \implies \forall (U,V) \in \mathbb{K}[X]^2 \quad D \mid AU + BV$$

Démonstration

Supposons que $D \mid A$ et $D \mid B$: il existe des polynômes Q_A et Q_B tels que $A = DQ_A$ et $B = DQ_B$.
Pour tous polynômes U et V,

$$AU + BV = DQ_AU + DQ_BV = D(Q_AU + Q_BV),$$

donc D divise $AU + BV$. □

Propriété 18

La relation de divisibilité a les propriétés suivantes :

- **Réflexivité :** Pour tout polynôme A, $A \mid A$.
- **Transitivité :** Pour tous polynômes A, B, C, si $A \mid B$ et $B \mid C$, alors $A \mid C$.
- Pour tous polynômes A et B :

$$(A \mid B \text{ et } B \mid A) \quad \Longleftrightarrow$$

On dit alors que les polynômes A et B sont **associés**.

Remarque : La relation de divisibilité entre polynômes n'est ni symétrique, ni antisymétrique.

Démonstration

La réflexivité et la transitivité sont évidentes. Montrons la dernière assertion. Soit A, B des polynômes.
▶ Sens réciproque : Supposons qu'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$. Alors il est clair que $B \mid A$ (le quotient est λ). Et par ailleurs $B = \frac{1}{\lambda} A$ donc de même $A \mid B$.

□

Propriété 19

Pour tous polynômes A, B et C, avec A non nul, on a

$$AB \mid AC \quad \Longleftrightarrow \quad B \mid C.$$

Démonstration

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

▶ **Sens direct :** Supposons que AB divise AC : il existe $Q \in \mathbb{K}[X]$ tel que $AC = ABQ$.
A est non nul donc $C = BQ$ (on peut simplifier par $A \neq 0$ car l'anneau $\mathbb{K}[X]$ est intègre).
Ainsi B divise C.

▶ **Réciproque :** Supposons que B divise C : il existe $Q \in \mathbb{K}[X]$ tel que $C = BQ$.
Alors $AC = ABQ$, donc AC divise AB. □

3.2 Division euclidienne

Theorème 20 : division euclidienne dans $\mathbb{K}[X]$

Soit $A,B \in \mathbb{K}[X]$, avec $B \neq 0$. Il existe un *unique* couple (Q,R) de polynômes à coefficients dans $\mathbb{K}$ tel que

$$A = BQ + R \qquad \text{et} \qquad \deg R < \deg B.$$

On dit que Q est le **quotient** de la division euclidienne de A par B, et que R est le **reste**.

Démonstration de l'existence

Soit B un polynôme non nul. Pour tout $n \in \mathbb{N}$, on note

$$\mathcal{P}_n : \qquad \forall A \in \mathbb{K}_n[X] \quad \exists Q,R \in \mathbb{K}[X] \qquad A = BQ + R \quad \text{et} \quad \deg R < \deg B$$

▶ **Initialisation :** Montrons $\mathcal{P}_0$. Soit $A \in \mathbb{K}_0[X]$: le polynôme A est constant.

- Si A est nul, le couple $(Q,R) = (0,0)$ convient.
- Si $A \in \mathbb{K}^*$ et $\deg B > 0$, le couple $(Q,R) = (0,A)$ convient : $A = 0B + A$ et $\deg R = \deg A = 0 < \deg B$.
- Si $A \in \mathbb{K}^*$ et $\deg B = 0$, on a $B = \lambda \in \mathbb{K}^*$. Alors $A = \dfrac{1}{\lambda}AB + 0$ et $\deg 0 < \deg B$, donc le couple $(Q,R) = \left(\dfrac{1}{\lambda}A, 0\right)$ convient.

▶ **Hérédité :** Soit $n \in \mathbb{N}$. On suppose que $\mathcal{P}_n$ est vraie. Montrons que $\mathcal{P}_{n+1}$ est vraie. Soit $A \in \mathbb{K}_{n+1}[X]$.

- Si $\deg A \leq n$, l'existence du couple (Q,R) découle directement de $\mathcal{P}_n$.
- Si $\deg A < \deg B$, le couple $(Q,R) = (0,A)$ convient.
- Il reste donc à traiter le cas où $\deg A = n+1$ et $\deg B \leqslant n+1$. On pose $p = \deg B$ et

$$\begin{aligned} A &= a_{n+1}X^{n+1} + a_nX^n + \cdots + a_0 \qquad &\text{avec } a_{n+1} \neq 0 \\ B &= b_pX^p + b_{p-1}X^{p-1} + \cdots + b_0 \qquad &\text{avec } b_p \neq 0 \end{aligned}$$

Considérons le polynôme $A_0 := A - \dfrac{a_{n+1}}{b_p}X^{n+1-p}B$. Or, il existe $S \in \mathbb{K}[X]$ tel que

$$\frac{a_{n+1}}{b_p}X^{n+1-p}B = a_{n+1}X^{n+1} + S \qquad \text{avec } \deg S \leq n$$

On en déduit que $A_0 = a_nX^n + \cdots + a_0 - Q$ et donc $\deg A_0 \leq n$. Par hypothèse de récurrence, il existe donc un couple (Q_0,R) de polynômes tel que

$$A_0 = BQ_0 + R \qquad \text{et} \qquad \deg R < \deg B.$$

On a donc

$$A = B\left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_0\right) + R \qquad \text{et} \qquad \deg R < \deg B.$$

Ainsi le couple $\left(\dfrac{a_{n+1}}{b_p}X^{n+1-p} + Q_0, R\right)$ convient. Ainsi $\mathcal{P}_{n+1}$ est vraie.

Finalement, pour tout $n \in \mathbb{N}$, $\mathcal{P}_n$ est vraie. □

Remarque : On notera que tous les polynômes (Q_0,R,S,A_0) sont bien tous à coefficients dans $\mathbb{K}$.

Démonstration de l'unicité

Soit (Q_1, R_1) et (Q_2, R_2) deux couples de polynômes tels que

$$\begin{aligned} A = BQ_1 + R_1 \quad &\text{et} \quad \deg R_1 < \deg B \\ A = BQ_2 + R_2 \quad &\text{et} \quad \deg R_2 < \deg B. \end{aligned}$$

Par différence, $B(Q_1 - Q_2) = -(R_1 - R_2)$, donc $B(Q_1 - Q_2)$ et $R_1 - R_2$ sont de même degré.

Supposons que $Q_1 - Q_2 \neq 0$. Alors $\deg(Q_1 - Q_2) \geqslant 0$ donc $\deg(B(Q_1 - Q_2)) \geqslant \deg B + \deg Q \geq \deg B$.

Par ailleurs, $\deg(R_1 - R_2) \leq \max(\deg R_1, \deg(-R2)) < \deg B$.
Or, on doit avoir $\deg(B(Q_1 - Q_2)) = \deg(R_1 - R_2)$: contradiction.

Ainsi $Q_1 = Q_2$, et en conséquence $R_1 = R_2$. □

La démonstration de l'existence donne de plus une méthode algorithmique pour déterminer le couple (Q,R) de la division euclidienne de A par B. En pratique, le calcul se fait ainsi :

Exemple 12 : Déterminer le quotient et le reste de la division euclidienne de A par B, dans chacun des cas suivants :

(a) $A = X^4 + 4X^3 + X + 1$ et $B = X + 1$.

(b) $A = X^4 + 2X^3 + 1$ et $B = X^2 - 1$.

(c) $A = X^3 + X + 1$ et $B = X^4$.

Remarque : Si on demande seulement le reste (sans le quotient) de la division euclidienne de A par B, il est possible de conclure sans effectuer la division euclidienne complète. Par exemple, sur les divisions ci-dessus :

(a) $A = X^4 + 4X^3 + X + 1$ et $B = X + 1$. :

Si on note R le reste de la division euclidienne de A par B, alors R est nécessairement un polynôme constant. Notons $R = \lambda \in \mathbb{R}$. On a $A = (X + 1)Q + \lambda$, donc en évaluant en -1 :

$$\begin{aligned} A(-1) &= 0 \times Q(-1) + \lambda \\ -3 &= \lambda. \end{aligned}$$

(b) $A = X^4 + 2X^3 + 1$ et $B = X^2 - 1$:
Le reste R de la division euclidienne de A par B est un polynôme de degré au plus 1. Notons $R = \lambda X + \mu$, avec $(\lambda, \mu) \in \mathbb{R}^2$. On a $A = (X^2 - 1)Q + \lambda X + \mu$, donc :

- en évaluant en :

- en évaluant en :

Ainsi

Propriété 21

Soient $A, B \in \mathbb{K}[X]$, avec B non nul.
B divise A dans $\mathbb{K}[X]$ si et seulement si le reste de la division euclidienne de A par B est nul.

Démonstration

▶ **Sens direct :** Supposons que B divise A : il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$, donc $A = BQ + 0$. Par unicité du couple (quotient, reste), le reste de la division euclidienne de A par B est 0.

▶ **Réciproque :** Supposons que le reste de la division euclidienne de A par B est nul : il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + 0$. Alors B divise A dans $\mathbb{K}[X]$. □

Propriété 22 : Bilan sur les formules du degré

Soit P,$Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$ et $n \in \mathbb{N}$. Alors

1.
$$\deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \in \mathbb{K}^* \\ -\infty & \text{si } \lambda = 0 \end{cases}$$

2.
$$\deg(P+Q) \leq \max(\deg P, \deg Q)$$
$$\deg(P+Q) = \max(\deg P, \deg Q) \qquad \text{si} \quad \deg P \boxed{\neq} \deg Q$$

3.
$$\deg(PQ) = \deg P + \deg Q$$

4.
$$\deg P^n = \begin{cases} n \deg P & \text{si } n \geq 1 \\ 0 & \text{si } n = 0 \end{cases}$$

5.
$$\deg P' = \begin{cases} \deg P - 1 & \text{si } \deg P \geq 1 \\ -\infty & \text{si } \deg P < 1 \end{cases}$$

6.
$$\deg P^{(n)} = \begin{cases} \deg P - n & \text{si } \deg P \geq n \\ -\infty & \text{si } \deg P < n \end{cases}$$

7.
$$\deg(P \circ Q) \begin{cases} = \deg P \times \deg Q & \text{si } \deg Q \geq 1 \\ \leq 0 & \text{si } \deg Q \leq 0 \end{cases}$$

Avec les conventions suivantes : pour tout $m \in \mathbb{N}$,

- $m + (-\infty) = -\infty$
- Si $m \geq 1$, $m \times (-\infty) = -\infty$