Chapitre

XX Polynômes

CONTENU

I L'ensemble $\mathbb{K}[X]$ . . . 1
I.1 Opérations sur $\mathbb{K}[X]$ . . . 2
I.2 Degré d'un polynôme . . . 6
I.3 Notions de polynômes de matrices . . . 7
II Dérivation dans $\mathbb{K}[X]$ . . . 8
II.1 Polynôme dérivé . . . 8
II.2 Degré du polynôme dérivé . . . 9
II.3 Dérivation et opérations . . . 9
II.4 Fonction polynomiale associée à un polynôme . . . 9
II.5 Formules de Taylor . . . 10
III Arithmétique dans $\mathbb{K}[X]$ . . . 12
III.1 Divisibilité . . . 12
III.2 Division euclidienne . . . 13
III.3 Polynômes irréductibles . . . 14
IV Racines d'un polynôme . . . 15
IV.1 Identification entre $Pol(\mathbb{K})$ et $\mathbb{K}[X]$ . . . 16
IV.2 Ordre de multiplicité d'une racine . . . 17
V Décomposition en facteurs irréductibles . . . 18
V.1 Polynôme scindé . . . 18
V.2 Factorisation dans $\mathbb{C}[X]$ . . . 19
V.3 Factorisation dans $\mathbb{R}[X]$ . . . 20
V.4 Algorithme de Hörner . . . 21
VI Somme et produit des racines . . . 22
VI.1 Degré 2 . . . 22
VI.2 Cas général . . . 23

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

Définition 1 : On appelle *polynôme* à une indéterminée à coefficients dans $\mathbb{K}$, toute suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ **nulle à partir d'un certain rang**.

On note $\mathbb{K}[X]$ leur ensemble.

$$\forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X],\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ a_n = 0.$$

Remarque : N peut être aussi grand que l'on veut, mais il est toujours fini.

Exemple 1 : $(1, -2, 3, 0, 0, 4, 0, 0, ...) = 1 - 2X + 3X^2 + 4X^5$.

Vocabulaire :

- Pour n fixé, a_n est le n+1$^{\text{ème}}$ coefficient du polynôme.
- On note X le polynôme défini par $X = (0, 1, 0, 0, ...)$ c'est-à-dire défini par la suite $(a_n)_{n\in\mathbb{N}}$ telle que :

$$a_0 = 0,\ a_1 = 1 \text{ et } \forall\, n \geqslant 2, a_n = 0.$$

ATTENTION X n'est pas un nombre !

- On appelle polynôme constant, tout polynôme de la forme $(\lambda, 0, 0, ...)$ où $\lambda \in \mathbb{K}$.

  On le notera abusivement λ.
- Le polynôme défini par la suite nulle $(0, 0, ...)$ est appelé *polynôme nul* et noté $0_{\mathbb{K}[X]}$, ou dangereusement 0.

Par définition, un polynôme est donc nul si, et seulement si tous ses coefficients sont nuls :

$$\forall\ P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X], \quad P \equiv 0_{\mathbb{K}[X]} \iff \forall\, n \in \mathbb{N},\ a_n = 0.$$

I.1 Opérations sur $\mathbb{K}[X]$

Définition 2 (Somme de polynômes) : Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$.

On appelle *somme* des polynômes P et Q, notée $P + Q$, le polynôme défini par :

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}}.$$

ATTENTION La définition sous-entend que la somme de deux polynômes est un polynôme. C'est la raison de la preuve ci-dessous où nous allons nous en assurer.

La loi

$$\begin{array}{rccc} + : & \mathbb{K}[X] \times \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & (P\,;Q) & \longmapsto & P + Q \end{array}$$

est appelée *loi de composition interne* (à $\mathbb{K}[X]$).

Proposition 1 :
L'addition dans $\mathbb{K}[X]$:
est associative : $\forall\, P, Q, R \in \mathbb{K}[X], (P + Q) + R = P + (Q + R) = P + Q + R$.
est commutative : $\forall\, P, Q \in \mathbb{K}[X], P + Q = Q + P$.

admet un élément neutre : le polynôme nul $0_{\mathbb{K}[X]} = (0, 0, ...)$ vérifie :

$$P + 0_{\mathbb{K}[X]} = 0_{\mathbb{K}[X]} + P = P.$$

est symétrisable : Tout polynôme $P = (a_n)_{n\in\mathbb{N}}$ admet un *symétrique*, noté $-P$, et défini par $-P = (-a_n)_{n\in\mathbb{N}}$ vérifiant

$$P + (-P) = 0_{\mathbb{K}[X]}.$$

Vocabulaire : On dit que $\left(\mathbb{K}[X], +\right)$ est un groupe commutatif (ou abélien)

Corollaire 1.1 :
Deux polynômes sont égaux si, et seulement si leurs coefficients sont égaux :

$$\forall\ P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X], \quad P \equiv_{\mathbb{K}[X]} Q \iff \forall\, n \in \mathbb{N},\ a_n =_{\mathbb{K}} b_n.$$

Définition 3 (Loi externe) : Soient $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

On définit le *produit d'un polynôme par un scalaire*, noté $\lambda.P$ ou λP, le polynôme défini par :

$$\lambda.P = (\lambda \times a_n)_{n\in\mathbb{N}}.$$

Corollaire 1.2 :
L'ensemble $\mathbb{K}[X]$ est stable par combinaisons linéaires.

Vocabulaire : On dit que $\left(\mathbb{K}[X], +, \cdot\right)$ est un espace vectoriel sur $\mathbb{K}$.

Définition 4 (Produit de polynômes) : Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$.

On appelle *produit* des polynômes P et Q, notée $P \times Q$ ou plus simplement PQ, le polynôme défini par :

$$P \times Q = (c_n)_{n\in\mathbb{N}} \quad \text{où } \forall\, n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Vocabulaire : La suite de terme général $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ est appelée *produit de Cauchy* des suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$.

En particulier, on a :

- $c_0 = a_0 b_0$
- $c_1 = a_1 b_0 + a_0 b_1$
- $c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2$
- ...

Remarque importante :

$$\forall\, n \in \mathbb{N},\ \sum_{k=0}^{n} a_k b_{n-k} = \sum_{p+q=n} a_p b_q. \tag{XX.1}$$

Proposition 2 :
Le produit dans $\mathbb{K}[X]$:
est associatif : $\forall\, P, Q, R \in \mathbb{K}[X],\ (P \times Q) \times R = P \times (Q \times R) = P \times Q \times R.$
est commutatif : $\forall\, P, Q \in \mathbb{K}[X],\ P \times Q = Q \times P.$
admet un élément neutre : le polynôme $1_{\mathbb{K}[X]} = (1, 0, 0, ...)$.

$$P \times 1_{\mathbb{K}[X]} = 1_{\mathbb{K}[X]} \times P = P.$$

est distributif sur l'addition : $\forall\, P, Q, R \in \mathbb{K}[X],\ P \times (Q + R) = P \times Q + P \times R.$

est compatible avec la loi externe :

$$\forall\, \lambda \in \mathbb{K},\ \forall\, P, Q \in \mathbb{K}[X],\ \lambda.(P \times Q) = (\lambda.P) \times Q = P \times (\lambda.Q)$$

On dit que $\left(\mathbb{K}[X], +, \times\right)$ est un anneau commutatif et que $\left(\mathbb{K}[X], +, \times, \cdot\right)$ est une algèbre commutative (unitaire) sur $\mathbb{K}$.

ATTENTION | $\left(\mathbb{K}[X], \times\right)$ n'est pas un groupe !

ATTENTION | On le démontrera plus loin mais les seuls polynômes inversibles pour la loi $\times$ sont les polynômes constants non nuls.

Définition/Théorème 5 (Notation définitive) : Soit $n \in \mathbb{N}$. On définit la suite des monômes $(X^n)_{n\in\mathbb{N}}$ par :

$$\begin{cases} X^0 = (1, 0, 0, ...) \\ X^{n+1} = X^n \times X \end{cases}$$

$X = (0, 1, 0, ...)$ est appelée l'indéterminée et,

$$\forall\, n \in \mathbb{N},\ X^n = (0, 0, ..., 0, \underset{\substack{\uparrow \\ (n+1)^{\text{ème}} \text{ coefficient}}}{1}, 0, ...) \tag{XX.2}$$

Tout $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ s'écrit alors :

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

Vocabulaire : On appelle *monôme* tout polynôme de la forme $a_k X^k$ où $k \in \mathbb{N}$ et $a_k \in \mathbb{K}$.

Remarque : On adopte diverses notations pour un polynôme comme

- $P = (a_n)_{n\in\mathbb{N}}$,
- P,
- $\sum a_n X^n$,
- $\sum_{k=0}^{n} a_k X^k$,
- $P(X)$,
- $\sum_{k\geqslant 0} a_k X^k$,
- ou $\sum_{k=0}^{+\infty} a_k X^k$,

en convenant toujours que $\forall\, k > n$, $a_k = 0$ *i.e.* la somme est finie et on écrira toujours un polynôme dans l'ordre croissant ou décroissant des puissances de X.

ATTENTION | X n'est pas un nombre !

Définition 6 (Composition) : Soient $P = \sum_{k\geqslant 0} a_k X^k \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$.

On appelle polynôme composé Q par P, noté $P \circ Q$, le polynôme $P \circ Q = \sum_{k\geqslant 0} a_k Q^k$.

Remarque : Si $Q = X + a$ où $a \in \mathbb{K}$ et $P = \sum_{k\geqslant 0} a_k X^k$ alors $P \circ Q = P(X+a) = \sum_{k\geqslant 0} a_k (X+a)^k$.

Exemples 2 (Opérations dans $\mathbb{K}[X]$) : Soient $P = 1 + 3X - X^2$ et $Q = X + X^2$.

Somme : $P + Q = 1 + 4X$.

Loi externe : $2P = 2 + 6X - 2X^2$.

Produit :

k	0	1	2	3	4
a_k	1	3	-1		
b_k	0	1	1		
c_k	0	1	4	2	-1

$$\Longrightarrow \begin{cases} c_0 = a_0 b_0 = 0 \\ c_1 = a_0 b_1 + a_1 b_0 = 1 \\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 4 \\ c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 2 \\ c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = -1 \end{cases}$$

$$PQ = X + 4X^2 + 2X^3 - X^4.$$

Composition : $P \circ Q = 1 + 3(X + X^2) - (X + X^2)^2 = 1 + 3X - 2X^2 - 2X^3 - X^4$.

Exercice 1 : Soient $P(X) = X^2 + 3X - 2$ et $Q(X) = 6X - X^2 + 1$.

Déterminer $P + Q$, $3P - 2Q$, PQ, P^2 et $Q(P(X))$.

Proposition 3 (Binôme de Newton) :
Soient P et Q deux polynômes sur $\mathbb{K}$.

$$\forall\, n \in \mathbb{N},\ (P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k} \quad \text{et} \quad \forall\, n \in \mathbb{N}^*,\ P^n - Q^n = (P-Q)\sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

Exemple 3 : $\forall\, n \in \mathbb{N}^*,\ 1 - X^n = (1-X)\sum_{k=0}^{n-1} X^k$.

Exercice 2 : Démontrer que pour tout $n \in \mathbb{N}^*$,

$$(X^3 + X^2 + X + 1)\sum_{k=0}^{2n}(-1)^k X^k = X^{2n+3} + X^{2n+1} + X^2 + 1.$$

I.2 Degré d'un polynôme

Définition 7 : Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul.

On appelle *degré de* P et on note $\deg(P)$ le plus grand entier k tel que $a_k \neq 0$.

On convient que $\deg\left(0_{\mathbb{K}[X]}\right) = -\infty$.

Exemple 4 : Si $P = X^2 + 5X^3 + X^9$, on a $\deg(P) = 9$.

Remarques :

— si $P = \sum_{k=0}^{n} a_k X^k$, on n'a pas nécessairement $\deg(P) = n$. Ce n'est le cas que si $a_n \neq 0$.

Le coefficient a_n s'appelle alors le *coefficient dominant*, $a_n X^n$ le *monôme dominant*.

— On dit que P est *unitaire* ou *normalisé* si $P \neq 0$ et si son coefficient dominant est égal à 1.

— Si $P = (a_n)_{n\in\mathbb{N}}$ est le polynôme nul alors, par définition, $\forall\, n \in \mathbb{N}$, $a_n = 0$. De fait, il n'existe pas d'entier n tel que $a_n \neq 0$. C'est la raison de la définition ci-dessus.

ATTENTION

— Les polynômes constants ont un degré $\leqslant 0$.

— Les polynômes de degré nul sont les polynômes constants non nuls.

Proposition 4 :

1. $\forall\, P, Q \in \mathbb{K}[X],\quad \deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.
2. $\forall\, \lambda \in \mathbb{K},\ \forall\, P \in \mathbb{K}[X],\quad \deg(\lambda P) = \begin{cases} \deg(P) \text{ si } \lambda \neq 0, \\ -\infty \text{ si } \lambda = 0. \end{cases}$
3. $\forall\, P, Q \in \mathbb{K}[X],\quad \deg(PQ) = \deg(P) + \deg(Q)$.
4. $\forall\, P, Q \in \mathbb{K}[X],\quad \deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Exercice 3 : Déterminer le degré et le coefficient dominant des polynômes suivants :

1. $P_1(X) = X^3 - X(X-2+i)^2$
2. $P_2(X) = (X+1)^n - (X-1)^n$, où $n \in \mathbb{N}$.

Corollaire 4.1 :

1. Les seuls polynômes inversibles sont les polynômes constants non nuls.
2. $\forall P, Q \in \mathbb{K}[X], \quad PQ = 0_{\mathbb{K}[X]} \iff P = 0_{\mathbb{K}[X]}$ ou $Q = 0_{\mathbb{K}[X]}$.

Vocabulaire : On dit que $\left(\mathbb{K}[X], +, \times\right)$ est un anneau *intègre*.

Définition 8 : Soit $n \in \mathbb{N}$.

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

Proposition 5 :
$\mathbb{K}_n[X]$ est stable par combinaisons linéaires.

Exercice 4 : Pour tout $P \in \mathbb{R}_3[X]$ on définit $f(P) = P(X+1) - P(X)$.

Calculer $f(X^3), f(X^2), f(X)$ et $f(1)$ puis montrer que, pour tout $P \in \mathbb{R}_3[X]$, $f(P) \in \mathbb{R}_2[X]$.

I.3 Notions de polynômes de matrices

Soit $M \in \mathscr{M}_n(\mathbb{K})$ et $P = \sum_{i=0}^{p} a_i X^i$ un polynôme de $\mathbb{K}[X]$.

Depuis le chapitre sur le calcul matriciel, on sait qu'une combinaison linéaire et un produit de matrices de $\mathscr{M}_n(\mathbb{K})$ sont encore des matrice de $\mathscr{M}_n(\mathbb{K})$, on note alors $P(M)$ la matrice de $\mathscr{M}_n(\mathbb{K})$ définie par :

$$P(M) = \sum_{i=0}^{p} a_i M^i = a_p M^p + \ldots + a_1 M + a_0 I_n \in \mathscr{M}_n(\mathbb{K}).$$

Définition/Théorème 9 :

- Un polynôme en M commute avec la matrice M : $P(M) \times M = M \times P(M)$.
- Lorsque $P(M) = 0_{\mathscr{M}_n(\mathbb{K})}$, on dit que P est un *polynôme annulateur* de M.
- Soient $P, Q \in \mathbb{K}[X]$, $M \in \mathscr{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$.

  Alors,
  - $(P \times_{\mathbb{K}[X]} Q)(M) = P(M) \times_{\mathscr{M}_n(\mathbb{K})} Q(M)$,
  - $(\lambda \cdot_{\mathbb{K}[X]} P +_{\mathbb{K}[X]} Q)(M) = \lambda \cdot_{\mathscr{M}_n(\mathbb{K})} P(M) +_{\mathscr{M}_n(\mathbb{K})} Q(M)$.

Corollaire 5.1 :
Soient $P, Q \in \mathbb{K}[X]$ et $M \in \mathscr{M}_n(\mathbb{K})$. Alors,

$$P(M) \times_{\mathscr{M}_n(\mathbb{K})} Q(M) = Q(M) \times_{\mathscr{M}_n(\mathbb{K})} P(M).$$

Les polynômes de matrices permettent d'introduire de la commutativité là où il n'y en avait pas. Vous verrez que cela a une grande importance.

Exercice 5 : Soit $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$.

Montrer que $A^2 + A - 2I_3 = 0_3$. En déduire que A est inversible et calculer A^{-1}.

II/ Dérivation dans $\mathbb{K}[X]$

II.1 Polynôme dérivé

Définition 10 : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.

On appelle *polynôme dérivé de* P, noté P', le polynôme défini par :

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

On définit également, par récurrence, le *polynôme dérivé k-ième de* P, noté $P^{(k)}$, par

$$\begin{cases} P^{(0)} = P \\ \forall\, k \in \mathbb{N}, \quad P^{(k+1)} = \left(P^{(k)}\right)'. \end{cases}$$

Remarque : Il s'agit d'une dérivation formelle qui peut se décrire par une simple translation de coefficients et une multiplication par leur indice : il n'y a pas de question à se poser sur la dérivabilité d'un polynôme comme pour les fonctions de la variable réelle.

Exemple 5 : $(1 + 3X - X^2)' = 3 - 2X$ et $(20)' = 0$.

II.2 Degré du polynôme dérivé

Proposition 6 :
$$\forall P \in \mathbb{K}[X], \quad \deg(P') = \begin{cases} \deg(P) - 1 \text{ si } \deg(P) \geqslant 1 \\ -\infty \qquad \text{si } \deg(P) \leqslant 0 \end{cases}$$

En particulier, $\forall P \in \mathbb{K}[X], \quad \deg(P) \leqslant n \implies P^{(n+1)} = 0_{\mathbb{K}[X]}$.

Remarque : $\forall P \in \mathbb{K}[X], P' = 0_{\mathbb{K}[X]} \iff \deg(P) \leqslant 0 \iff P$ est constant.

II.3 Dérivation et opérations

Proposition 7 :
1. $\forall P, Q \in \mathbb{K}[X], \forall \lambda, \mu \in \mathbb{K}, \quad (\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
2. $\forall P, Q \in \mathbb{K}[X], \quad (PQ)' = P'Q + PQ'$.
3. $\forall P \in \mathbb{K}[X], \forall n \in \mathbb{N}, \quad (P^n)' = nP' \times P^{n-1}$.

La dérivation des polynômes est donc, comme pour les fonctions, linéaire

Exercice 6 : Déterminer les polynômes :

1. $P \in \mathbb{R}[X]$ tels que $(1-X)P' - P = X^n$.
2. $P \in \mathbb{C}[X]$ tels que $(X^2+1)P' - 6P = 0$.

Proposition 8 :
1. $\forall P, Q \in \mathbb{K}[X], \forall \lambda, \mu \in \mathbb{K}[X], \forall n \in \mathbb{N}, \quad (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.
2. $\forall P, Q \in \mathbb{K}[X], \forall n \in \mathbb{N}, \quad (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Formule de Leibniz

II.4 Fonction polynomiale associée à un polynôme

Définition 11 : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ où $n \in \mathbb{N}$.

La *fonction polynomiale associée à* P est la fonction définie par

$$\begin{array}{rccc} \widetilde{P} : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & \sum_{k=0}^{n} a_k x^k \end{array}$$

On appelle *fonction polynomiale* toute fonction $f \in \mathcal{F}(\mathbb{K},\mathbb{K})$ telle qu'il existe $P \in \mathbb{K}[X]$ vérifiant :

$$f = \widetilde{P}.$$

L'ensemble des fonctions polynomiales définies sur $\mathbb{K}$ à valeurs dans $\mathbb{K}$ est ici noté $Pol(\mathbb{K})$.

Exemple 6 : Si $P = X^2+1$, alors $\widetilde{P} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2+1 \end{array}$.

Corollaire 8.1 :

L'application $\Phi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & Pol(\mathbb{K}) \\ P & \longmapsto & \widetilde{P} \end{array}$ est surjective.

ATTENTION X n'est toujours pas un nombre ! On ne dit pas « Posons $X = 1$ », mais « Évaluons en 1 ».

Proposition 9 :
Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On a :

1. $\widetilde{\lambda P + \mu Q} = \lambda\widetilde{P} + \mu\widetilde{Q}$.
2. $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$.
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.
4. $\widetilde{P'} = \left(\widetilde{P}\right)'$.

ATTENTION

$\mathbb{R}[X]$ et $\mathbb{R}^{\mathbb{R}}$ sont dotés de notions différentes d'addition, multiplication, composition et dérivation.

Dans la formule $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$ par exemple, ce ne sont pas les mêmes « $\circ$ » qu'on trouve à gauche et à droite.

Pire, dans la formule $\widetilde{P'} = \widetilde{P}'$, la dérivée P' est une dérivée formelle alors que la dérivée $\widetilde{P}'$ est la dérivée d'une fonction définie comme limite d'un taux d'accroissement.

Sachant que $\widetilde{1}$ est la fonction constante $x \longmapsto 1$, élément neutre de $\mathbb{K}^{\mathbb{K}}$ l'application $P \longmapsto \widetilde{P}$ s'avère être un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$.

II.5 Formules de Taylor

Théorème 10 (Théorème de Taylor) :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On suppose que $\deg(P) = p$.

Alors :

$$\begin{aligned} P &= \sum_{n=0}^{p} \frac{\widetilde{P}^{(n)}(a)}{n!}(X-a)^n \\ &= \widetilde{P}(a) + \widetilde{P}'(a)(X-a) + \frac{\widetilde{P}''(a)}{2!}(X-a)^2 + \cdots + \frac{\widetilde{P}^{(p)}(a)}{p!}(X-a)^p. \end{aligned}$$

Exemple 7 : Soit $f(x) = \dfrac{2x^3+2x^2+3x-4}{(x-1)^3}$.

Imaginons que nous voulions effecteur sa décomposition en éléments simples dans le but de calculer une primitive de f par exemple.

On souhaite donc écrire $f(x)$ sous la forme $a + \dfrac{b}{x-1} + \dfrac{c}{(x-1)^2} + \dfrac{d}{(x-1)^3}$.

Il suffirait de savoir écrire $2x^3+2x^2+3x-4$ sous la forme $a(x-1)^3+b(x-1)^2+c(x-1)+d$ pour conclure.

La formule de Taylor permet d'éviter les développements, l'identification, et la résolution du système.

$$\begin{array}{ll} P = 2X^3+2X^2+3X-4 & \text{donc } P(1) = 3 \\ P' = 6X^2+4X+3 & \text{donc } P'(1) = 13 \\ P'' = 12X+4 & \text{donc } P''(1) = 16 \\ P^{(3)} = 12 & \text{donc } P^{(3)}(1) = 12 \end{array}$$

D'après le théorème de Taylor : $P = P(1) + P'(1)(X-1) + \dfrac{P''(1)}{2}(X-1)^2 + \dfrac{P^{(3)}(1)}{3!}(X-1)^3$.

D'où $P = 3 + 13(X-1) + 8(X-1)^2 + 2(X-1)^3$ et $f(x) = \dfrac{3}{(x-1)^3} + \dfrac{13}{(x-1)^2} + \dfrac{8}{x-1} + 2$.

Exercice 7 : Donner la décomposition en éléments simples de $f : x \longmapsto \dfrac{4x^3-3x^2+7x-1}{(x-2)^3}$.

Corollaire 10.1 :
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On suppose que $\deg(P) = p$.

Alors :

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

Théorème 11 (Théorème de Taylor-Mac Laurin [1]) :
Soit $P \in \mathbb{K}[X]$. On suppose que $\deg(P) = p$.

Alors :

$$P = \sum_{n=0}^{p} \frac{\widetilde{P}^{(n)}(0)}{n!} X^n.$$

En particulier, si $P = \sum_{n=0}^{p} a_n X^n$, alors, par identification, $a_n = \frac{\widetilde{P}^{(n)}(0)}{n!}$ et $\widetilde{P}^{(n)}(0) = n! a_n$.

III/ Arithmétique dans $\mathbb{K}[X]$

III.1 Divisibilité

Définition 12 : Soient $A, P \in \mathbb{K}[X]$.

— On dit que A *divise* P, noté $A|P$, s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = AQ$.

On dit alors que A est *un diviseur* de P ou que P est *un multiple* de A.

— On dit que A et P sont *associés* s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda A$.

Exemples 8 :

— $X - 1 | X^2 - 1$ car $X^2 - 1 = (X-1)(X+1)$.
— $X - 3$ et $2X - 6$ sont associés car $2X - 6 = 2(X-3)$.
— Tous les polynômes divisent le polynôme nul.
— $\forall P \in \mathbb{K}[X], \quad 0|P \iff P = 0$.

Proposition 12 :

1. $\forall A \in \mathbb{K}[X], \quad A|A$ et $A|0$
2. $\forall A, B \in \mathbb{K}[X], \quad \begin{cases} A|B \\ B|A \end{cases} \iff \exists \lambda \in \mathbb{K}^*, \quad B = \lambda A.$
3. $\forall A, B, C \in \mathbb{K}[X], \quad \begin{cases} A|B \\ B|C \end{cases} \implies A|C.$

Remarque : La divisibilité dans $\mathbb{K}[X]$ n'est pas une relation d'ordre.

[1]. Colin Mac Laurin : écossais, 1698-1746

Proposition 13 (Compatibilité avec les opérations) :

1. $\forall A, P, Q \in \mathbb{K}[X]$, $A|P \implies A|PQ$
2. $\forall A, P, Q \in \mathbb{K}[X]$, $\begin{cases} A|P \\ A|Q \end{cases} \implies A|P+Q$
3. $\forall A, P, B, Q \in \mathbb{K}[X]$, $\begin{cases} A|P \\ B|Q \end{cases} \implies AB|PQ$
4. $\forall A, P \in \mathbb{K}[X], \forall n \in \mathbb{N}$, $A|P \implies A^n|P^n$

ATTENTION $\begin{cases} A|P \\ B|P \end{cases}$ n'implique pas $AB|P$.

III.2 Division euclidienne

Théorème 14 :
Soient $(A, B) \in \mathbb{K}[X]^2$, avec $B \neq 0$.

Il existe un unique couple $(Q, R) \in \mathbb{R}[X]^2$ tel que :

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Lorsqu'on a obtenu cette écriture, on dit qu'on a effectué la *division euclidienne* de A par B.

A est le *dividende*, B le *diviseur*, Q le *quotient* et R le *reste*.

Exemple 9 : $2X^4 - X^3 + 6X^2 + 7X - 14 = (X^2 + X + 1)(2X^2 - 3X + 7) + (3X - 21)$

Exercice 8 : Montrer que $\forall n \in \mathbb{N}$, $X^2|(X+1)^n - nX + 1$.

Exemple 10 : Soit $P = X^4 + 5X^3 + 5X^2 - 5X - 6$. Effectuons la division euclidienne de P par $X - 1$.

$$\begin{array}{rcrcrcrcr|l}
1X^4 & + & 5X^3 & + & 5X^2 & - & 5X & - & 6 & X-1 \\
\cline{10-10}
-(X^4 & - & X^3) & & & & & & & 1X^3+6X^2+11X+6 \\
\cline{1-3}
 & & 6X^3 & + & 5X^2 & - & 5X & - & 6 & \\
 & & -(6X^3 & - & 6X^2) & & & & & \\
\cline{3-5}
 & & & & 11X^2 & - & 5X & - & 6 & \\
 & & & & -(11X^2 & - & 11X) & & & \\
\cline{5-7}
 & & & & & & 6X & - & 6 & \\
 & & & & & & -(6X & - & 6) & \\
\cline{7-9}
 & & & & & & & & 0 &
\end{array}$$

On obtient donc, $P = (X-1)(X^3 + 6X^2 + 11X + 6)$.

Cette méthode de calcul est une alternative à l'identification lorsqu'on cherche à factoriser un polynôme comme ici, par exemple, après avoir trouvé 1 comme racine évidente.

Exercice 9 : Soit la matrice $M = \begin{pmatrix} 2 & -2 & 1 \\ 2 & -3 & 2 \\ -1 & 2 & 0 \end{pmatrix}$.

1. Vérifier que $M^2 + 2M - 3I_3 = 0_3$.
2. En déduire que M est inversible.
3. On définit le polynôme $P = X^2 + 2X - 3$.
   (a) Factoriser P.
   (b) Déterminer le reste R de la division euclidienne de X^n par P.
   (c) En déduire M^n

Méthode 1 (Calcul de la puissance d'une matrice) :
Si P est un polynôme annulateur de la matrice A *i.e.* si $P(A) = 0$, on écrit la division euclidienne de X^n par P :

$$\exists\, Q_n, R_n \in \mathbb{K}[X], X^n = Q_n P + R_n \quad \text{et} \quad \deg(R_n) < \deg(P).$$

La relation matricielle $A^n = \underbrace{P(A)}_{=0} \times Q_n(A) + R_n(A)$ donne $A^n = R_n(A)$. Il suffit donc de connaître R_n.

Proposition 15 :
Soient A et B deux polynômes avec B non nul.

$$B|A \iff \text{le reste dans la division euclidienne de A par B est nul.}$$

Exercice 10 : Démontrer que $X^2 - 3X + 2$ divise le polynôme $(X-2)^{2n} + (X-1)^n - 1$.

III.3 Polynômes irréductibles

Définition 13 : Un polynôme de $\mathbb{K}[X]$ est dit *irréductible* ou *premier* si :
- $\deg(P) \geqslant 1$.
- P n'admet comme diviseurs que les λ (avec $\lambda \in \mathbb{K}^\star$) et les μP (avec $\mu \in \mathbb{K}^\star$).

ATTENTION

Un même polynôme peut être irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$:
- $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$.
- $X^2 + 1 = (X + i)(X - i)$ dans $\mathbb{C}[X]$ et donc il est non irréductible.

Théorème 16 (Admis) :
Tout polynôme de $\mathbb{K}[X]$ de degré $\geqslant 1$ admet une décomposition en produit de polynômes irréductibles, unique à l'ordre près des facteurs et aux constantes multiplicatives près.

On dit que $\mathbb{K}[X]$, tout comme $\mathbb{Z}$, est un anneau *factoriel*.

Exemples 11 : Dans $\mathbb{R}[X]$, $X^3-1=(X-1)(X^2+X+1)=\left(\frac{1}{2}X+\frac{1}{2}\right)(2X^2+2X+2)$.

Dans $\mathbb{C}[X]$, $X^3-1=(X-1)(X-j)(X-\overline{j})=\left(\frac{1}{6}X+\frac{1}{6}\right)(2X-2j)(3X-3\overline{j})$.

Corollaire 16.1 :
Tout polynôme de $\mathbb{K}[X]$ de degré $\geqslant 1$ admet (au moins) un diviseur irréductible.

Proposition 17 :
Les polynômes de $\mathbb{K}[X]$ de degré 1 sont irréductibles.

IV/ Racines d'un polynôme

Définition 14 : Soit $P\in\mathbb{K}[X]$ et $\alpha\in\mathbb{K}$.

On dit que α est *une racine de* P (ou *un zéro* P) lorsque $\widetilde{P}(\alpha)=0$.

Exemple 12 : 1 est une racine de $P=X^2-1$ car $\widetilde{P}(x)=x^2-1$ et $\widetilde{P}(1)=1^2-1=0$.

Théorème 18 :
Soit $P\in\mathbb{K}[X]$ et $\alpha\in\mathbb{K}$.

$$\alpha \text{ est une racine de } P \iff P \text{ est divisible par } X-\alpha.$$

Remarque : On a vu, au cours de la démonstration que le reste dans la division euclidienne de P par $X-\alpha$ est $\widetilde{P}(\alpha)$.

Corollaire 18.1 :
Soit $P\in\mathbb{K}[X]$.

Si P admet n racines distinctes $\alpha_1, \cdots, \alpha_n$, alors P est divisible par $\prod_{k=1}^{n}(X-\alpha_k)$.

Exercice 11 : À quelle condition nécessaire et suffisante sur $n \in \mathbb{N}$ le polynôme X^2+1 divise-t-il X^n+1 ?

Théorème 19 :
Soit $P \in \mathbb{K}[X]$ non nul, de degré $n \geqslant 0$.

Alors, P possède au maximum n racines.

ATTENTION Dans $\mathbb{R}$, un polynôme de degré n ne possède pas forcément n racines.

Corollaire 19.1 :
1. Tout polynôme non nul possède un nombre fini de racines.
2. Le seul polynôme admettant une infinité de racines et le polynôme nul.

Exemple 13 : La fonction cos n'est pas polynomiale.

Exercice 12 (Polynômes de Tchebychev) :
1. Démontrer qu'il existe une unique suite de polynômes $(T_n)_{n\in\mathbb{N}}$ telle que :
$$\forall\, n \in \mathbb{N},\ \forall\, x \in \mathbb{R},\ T_n(cos(x)) = \cos(nx).$$
2. Calculer T_2 et T_3.

IV.1 Identification entre $Pol(\mathbb{K})$ et $\mathbb{K}[X]$

Proposition 20 :
L'application $\Phi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & Pol(\mathbb{K}) \\ P & \longmapsto & \widetilde{P} \end{array}$ est bijective.

Chaque fonction polynomiale f est donc associée de manière unique à un et un seul polynôme P.

On se permettra donc par la suite d'identifier P et $\widetilde{P}$, ce que l'on avait commencé à faire avec les polynômes constants.

Corollaire 20.1 (Polynômes de Lagrange) :
Soient $n \in \mathbb{N}^*$, $x_1, x_2, \dots, x_{n+1} \in \mathbb{K}$ distincts deux à deux et $y_1, y_2, \dots, y_{n+1} \in \mathbb{K}$.

Il existe un unique polynôme de degré inférieur ou égal à n tel que :

$$\forall\, i \in [\![1\,;n+1]\!]\,, \quad \mathrm{P}\,(x_i) = y_i.$$

Il s'agit du polynôme défini par la formule :

$$\mathrm{P} = \sum_{i=1}^{n+1} \left(\prod_{k \neq i} \frac{\mathrm{X} - x_k}{x_i - x_k} \right) y_i.$$

Remarque : Lorsque $\mathbb{K} = \mathbb{R}$, cela signifie qu'il existe une unique fonction polynômiale P de degré inférieur au égal à n dont le graphe passe par les $n+1$ points du plan $\mathrm{M}_1\,(x_1, y_1)\,, \dots, \mathrm{M}_{n+1}\,(x_{n+1}, y_{n+1})$.

IV.2 Ordre de multiplicité d'une racine

Définition 15 : Soit P un polynôme non nul de $\mathbb{K}[\mathrm{X}]$ et $\alpha \in \mathbb{K}$.

Si α est une racine de P, on appelle *ordre de multiplicité de la racine α dans* P le plus grand entier n tel que $(\mathrm{X} - \alpha)^n | \mathrm{P}$.

Théorème 21 :
Soit P un polynôme non nul de $\mathbb{K}[\mathrm{X}]$ et $\alpha \in \mathbb{K}$.

Les trois propositions suivantes sont équivalentes :

1. α est une racine de P de multiplicité m.
2. $\exists\, \mathrm{Q} \in \mathbb{K}[\mathrm{X}]$, $\mathrm{P} = (\mathrm{X} - \alpha)^m \mathrm{Q}$ et $\mathrm{Q}(\alpha) \neq 0$.
3. $\mathrm{P}(\alpha) = \mathrm{P}'(\alpha) = \cdots = \mathrm{P}^{(m-1)}(\alpha) = 0$ et $\mathrm{P}^{(m)}(\alpha) \neq 0$.

À retenir 1 :
On dit que $\alpha \in \mathbb{K}$, est racine de $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ d'ordre de multiplicité au moins $m \in \mathbb{N}^*$ si $(\mathrm{X} - a)^m | \mathrm{P}$ ou s'il existe $\mathrm{Q} \in \mathbb{K}[\mathrm{X}]$ tel que $\mathrm{P} = (\mathrm{X} - a)^m \mathrm{Q}$ ou si $\forall\, m \in [\![0\,;m-1]\!]$, $\mathrm{P}^{(k)}(\alpha) = 0$.

Exemples 14 :

— Déterminer les racines de $\mathrm{P} = (\mathrm{X}-1)(\mathrm{X}^2-1)(\mathrm{X}^3-1)(\mathrm{X}^4-1) \in \mathbb{R}[\mathrm{X}]$ et leur multiplicité.

$$\begin{aligned}\mathrm{P} &= (\mathrm{X}-1)(\mathrm{X}^2-1)(\mathrm{X}^3-1)(\mathrm{X}^4-1)\\ &= (\mathrm{X}-1)[(\mathrm{X}-1)(\mathrm{X}+1)][(\mathrm{X}-1)(\mathrm{X}^2+\mathrm{X}+1)][(\mathrm{X}-1)(\mathrm{X}+1)(\mathrm{X}^2+1)]\\ &= (\mathrm{X}-1)^4(\mathrm{X}+1)^2(\mathrm{X}^2+\mathrm{X}+1)(\mathrm{X}^2+1)\end{aligned}$$

X^2+X+1 n'a pas de racines réelles ($\Delta=-3$) et X^2+1 non plus.

P a donc deux racines réelles : 1 de multiplicité 4 et -1 de multiplicité 2.

— $P=aX^2+bX+c$ avec $a\neq 0$.

Si $\Delta=0$, $x_0=-\dfrac{b}{2a}$ est une racine double de P : $P=a(X-x_0)^2$.

Exercice 13 : Montrer que, $\forall\, n\in\mathbb{N}$, $P_n=nX^{n+1}-(n+1)X^n+1$ est divisible par $(X-1)^2$.

Corollaire 21.1 :
Soit $P\in\mathbb{K}[X]$.

Si P admet n racines distinctes α_1, $\cdots$, α_n de multiplicités respectives m_1, m_2, $\cdots$, m_n, alors P est divisible par $\prod_{k=1}^{n}(X-\alpha_k)^{m_k}$.

Exercice 14 : Montrer que le polynôme $P_n=\sum_{k=0}^{n}\dfrac{X^k}{k!}$ n'admet que des racines simples.

V/ Décomposition en facteurs irréductibles

V.1 Polynôme scindé

Définition 16 : Soit $P\in\mathbb{K}[X]$ un polynôme non nul.

On dit que P est *scindé* lorsqu'il est constant, ou s'il s'écrit comme un produit de facteurs de degré 1.

Plus précisément, P est scindé si, et seulement si il existe $\lambda\in\mathbb{K}^*$ et a_1, a_2, ..., $a_n\in\mathbb{K}$ tels que :

$$P=\lambda\prod_{k=1}^{n}(X-a_k).$$

Exemples 15 :

— $(X-2)(X-3)$ est scindé.

— $(X-1)^8$ est scindé.

— X^2+1 ne peut s'écrire sous la forme $(X-\alpha)(X-\beta)$ dans $\mathbb{R}[X]$. Sinon, α et β seraient des racines réelles de X^2+1 qui n'en a pas !

Par conséquent, X^2+1 n'est pas scindé dans $\mathbb{R}[X]$.

Il est scindé dans $\mathbb{C}[X]$ puisqu'on peut écrire $X^2+1=(X-i)(X+i)$.

ATTENTION La notion de polynôme scindé dépend du corps $\mathbb{K}$.

V.2 Factorisation dans $\mathbb{C}[X]$

Théorème 22 (de D'Alembert-Gauss) :
Dans $\mathbb{C}[X]$, tout polynôme *non constant* admet au moins une racine (dans $\mathbb{C}$).

Corollaire 22.1 :
Dans $\mathbb{C}[X]$, tout polynôme est scindé.

On dit que $\mathbb{C}$ est algébriquement clos.

Corollaire 22.2 :
Dans $\mathbb{C}[X]$, tout polynôme P s'écrit sous la forme :

$$P=\lambda\prod_{k=1}^{n}(X-\alpha_k)^{m_k}$$

Factorisation dans $\mathbb{C}[X]$

où $\alpha_1,\alpha_2,\cdots,\alpha_n$ sont les racines de P de multiplicités $m_1,m_2,\cdots,m_n$ et λ est le coefficient dominant de P.

Corollaire 22.3 :
Les polynômes irréductibles dans $\mathbb{C}[X]$ sont **exactement** les polynômes de degré 1.

Exemple 16 : Soit $P=X^n-1$ avec $n\geqslant 1$.

Dans $\mathbb{C}$, les racines de P sont les racines $n^{\text{èmes}}$ de l'unité. Il y en a n distinctes.

Donc $\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right)|P$.

On a donc $P=\left[\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\right]Q$ avec $Q\in\mathbb{C}[X]$.

Or, $\deg(P)=n+\deg(Q)$ d'où $\deg(Q)=0$ et $Q=\lambda$ avec $\lambda\in\mathbb{C}^\star$.

D'où, $P=\lambda\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right)$.

Enfin, par identification des coefficients dominants, $\lambda = 1$.

$$\text{En conclusion, } \mathrm{X}^n - 1 = \prod_{k=0}^{n-1} \left(\mathrm{X} - e^{\frac{2ik\pi}{n}}\right) = \prod_{\zeta \in \mathbb{U}_n} (\mathrm{X} - \zeta).$$

Exercice 15 : Pour $n \in \mathbb{N}$, on pose $\mathrm{P} = (\mathrm{X} + \mathrm{i})^{2n+1} - (\mathrm{X} - \mathrm{i})^{2n+1}$.

Factoriser P dans $\mathbb{C}[\mathrm{X}]$.

V.3 Factorisation dans $\mathbb{R}[\mathrm{X}]$

Proposition 23 (Racines complexes d'un polynôme réel) :
Soit $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ et $\alpha \in \mathbb{C}$.

Si α est une racine de P, alors $\overline{\alpha}$ est aussi une racine de P.

ATTENTION

i est une racine de $(\mathrm{X} - i)(\mathrm{X} + 2)$ mais $\overline{i}$ ne l'est pas.

Pas de contradiction avec la propriété ci-dessous car $(\mathrm{X} - i)(\mathrm{X} + 2) \notin \mathbb{R}[\mathrm{X}]$.

Proposition 24 :
Soit $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ et $\alpha \in \mathbb{C}$.

Si α est une racine de P de multiplicité m, alors $\overline{\alpha}$ est une racine de P de multiplicité m également.

En pratique,

Corollaire 24.1 :
Dans $\mathbb{R}[\mathrm{X}]$, tout polynôme P s'écrit sous la forme :

$$\mathrm{P} = \lambda \prod_{k=1}^{r} (\mathrm{X} - \alpha_k)^{m_k} \prod_{\ell=1}^{s} [\mathrm{X}^2 + u_\ell \mathrm{X} + v_\ell]^{\mu_\ell} \tag{XX.3}$$

Factorisation dans $\mathbb{R}[\mathrm{X}]$

où :

- λ est le coefficient dominant de P.
- $\alpha_1, \alpha_2, \cdots, \alpha_r$ sont les racines réelles de P de multiplicités $m_1, m_2, \cdots, m_r$.
- $(u_1, v_1), (u_2, v_2), \cdots, (u_s, v_s)$ sont des couples de réels tels que $\forall\, k \in [\![1\,;s]\!]$, $u_k^2 - 4v_k < 0$, *i.e.* $\mathrm{X}^2 + u_k \mathrm{X} + v_k$ n'a pas de racines réelles.
- $\mu_1, \mu_2, \cdots, \mu_s \in \mathbb{N}$.

Corollaire 24.2 :
Les seuls polynômes normalisés irréductibles dans $\mathbb{R}[X]$ sont :
- Les polynômes de degré 1 de la forme $X-\alpha$ avec $\alpha \in \mathbb{R}$;
- Les polynômes de degré 2 irréductibles de la forme X^2+uX+v avec $u,v \in \mathbb{R}$ et $u^2-4v<0$.

ATTENTION

Un polynôme peut très bien ne pas avoir de racines dans $\mathbb{K}$ et ne pas être irréductible :

$X^4+1=(X^2+X\sqrt{2}+1)(X^2-X\sqrt{2}+1)$ n'a pas de racines réelles.

Exemple 17 : Comment factoriser $P=X^6-1$ dans $\mathbb{R}[X]$?

On le factorise dans $\mathbb{C}[X]$, puis on regroupe les racines avec leur conjugué.

$$\begin{aligned}P&=\prod_{k=0}^{5}\left(X-e^{\frac{2ik\pi}{6}}\right)\\&=(X-1)\left(X-e^{\frac{i\pi}{3}}\right)\left(X-e^{\frac{2i\pi}{3}}\right)(X+1)\left(X-e^{\frac{4i\pi}{3}}\right)\left(X-e^{\frac{5i\pi}{3}}\right)\\&=(X-1)(X+1)\left(X-e^{\frac{i\pi}{3}}\right)\left(X-e^{-\frac{i\pi}{3}}\right)\left(X-e^{\frac{2i\pi}{3}}\right)\left(X-e^{-\frac{2i\pi}{3}}\right)\\&=(X-1)(X+1)\left(X^2-X+1\right)\left(X^2+X+1\right).\end{aligned}$$

Finalement, $X^6-1=(X-1)(X+1)\left(X^2-X+1\right)\left(X^2+X+1\right)$.

Remarque : Bien sûr, on peut également reconnaître que $X^6-1=\left(X^3\right)^2-1$ ou $X^6-1=\left(X^2\right)^3-1$ puis factoriser, à la main, chaque facteur.

Exercice 16 : Factoriser X^6+1 dans $\mathbb{R}[X]$.

V.4 Algorithme de Hörner

Soit f une fonction polynomiale de degré $n>0$ et $a \in \mathbb{R}$ une racine de f.

Il existe donc un polynôme Q de degré $n-1$ tel que $\forall\, x \in \mathbb{R}$, $f(x)=(x-a)\mathrm{Q}(x)$.

On pose : $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ $\quad a_n\neq 0$
$\mathrm{Q}(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\ldots+b_1x+b_0$.

Cette méthode, appelée aussi algorithme de Ruffini-Hörner, consiste à calculer les coefficients de Q de proche en proche à partir de b_{n-1} puis en descendant jusqu'à b_0.

$$\begin{array}{ll}a_n=b_{n-1} & b_{n-1}=a_n\\ \forall\, k\in[\![1\,;n-1]\!]\,,\ a_k=b_{k-1}-ab_k & b_{k-1}=a_k+ab_k\\ a_0=-ab_0. & b_0=-\dfrac{a_0}{a}.\end{array}$$

On calcule, en général, ces coefficients à partir d'un tableau que l'on remplit de gauche à droite :

a_n	a_{n-1}	...	a_2	a_1	a_0
$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + ab_{n-1}$		$b_1 = a_2 + ab_2$	$b_0 = a_1 + ab_1$	$b_0 = -\dfrac{a_0}{a}$

La redondance des deux dernières colonnes permettant de vérifier ses calculs...

Exemple 18 : Soit la fonction polynômiale définie par

$$f(x) = x^4 + 5x^3 + 5x^2 - 5x - 6 \quad \text{avec} \quad a = 1.$$

L'algorithme d'Hörner s'écrit :

	1	5	5	-5	-6
(Calcul de b_3)	1				
(Calcul de b_2)	1	$6 = 5 + 1 \times 1$			
(Calcul de b_1)	1	6	$11 = 5 + 1 \times 6$		
(Calcul de b_0)	1	6	11	6	$-\dfrac{-6}{1} = 6$

On retrouve : $\forall\, x \in \mathbb{R},\ f(x) = (x-1)(x^3 + 6x^2 + 11x + 6)$.

Et on continue avec $a = -1$:

	1	6	11	6
(Avec $a = -1$)	1	5	6	6
(Avec $a = -2$)	1	3	3	

On retrouve encore, $\forall\, x \in \mathbb{R}$,
$$\begin{aligned} f(x) &= (x-1)(x+1)(x^2 + 5x + 6) \\ &= (x-1)(x+1)(x+2)(x+3). \end{aligned}$$

Exercice 17 : Factoriser $\mathrm{P} = 4\mathrm{X}^3 - 16\mathrm{X}^2 - 19\mathrm{X} - 5$ à l'aide de l'algorithme de Hörner sachant que 5 est une des racines.

VI/ Somme et produit des racines

VI.1 Degré 2

Proposition 25 :
Soit $\mathrm{P} = a\mathrm{X}^2 + b\mathrm{X} + c \in \mathbb{K}[\mathrm{X}]$ avec $a \in \mathbb{K}^*$.

α_1 et α_2 sont racines de P si, et seulement si $\begin{cases} \alpha_1+\alpha_2 = -\dfrac{b}{a} \\ \alpha_1\alpha_2 = \dfrac{c}{a}. \end{cases}$

Exemple 19 : $\forall\, \alpha \in \mathbb{C},\quad (\mathrm{X}-\alpha)(\mathrm{X}-\overline{\alpha}) = \mathrm{X}^2 - 2\mathrm{Re}\,(\alpha) + |\alpha|^2.$

En particulier : $\forall\, \theta \in \mathbb{R},\quad (\mathrm{X}-\mathrm{e}^{\mathrm{i}\theta})\,(\mathrm{X}-\mathrm{e}^{-\mathrm{i}\theta}) = \mathrm{X}^2 - 2\cos(\theta)\mathrm{X} + 1.$

VI.2 Cas général

Considérons $\mathrm{P} = a_n\mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$.

Posons $\mathrm{P} = a_n(\mathrm{X}-\alpha_1)(\mathrm{X}-\alpha_2)\cdots(\mathrm{X}-\alpha_n)$ (les α_i éventuellement identiques en cas de racines multiples).

En développant, on a $\mathrm{P} = a_n\Big(\mathrm{X}^n - (\alpha_1+\alpha_2+\cdots+\alpha_n)\mathrm{X}^{n-1} + \cdots + (-1)^n\alpha_1\alpha_2\cdots\alpha_n\Big)$

En identifiant, on a (entre autres) $\begin{cases} a_{n-1} = -a_n(\alpha_1+\alpha_2+\cdots+\alpha_n) \\ a_0 = a_n(-1)^n\alpha_1\alpha_2\cdots\alpha_n \end{cases}$.

On peut donc trouver facilement la somme et le produit des racines ainsi que d'autres sommes remarquables :

Proposition 26 :
Soient $n \in \mathbb{N}^*$ et $\mathrm{P} = \sum_{k=0}^{n} a_k\mathrm{X}^k \in \mathbb{K}[\mathrm{X}]$ un polynôme scindé de degré n *i.e.* $a_n \neq 0$.

Si α_1, α_2, ..., α_n sont les racines de P alors,

$$\begin{cases} \alpha_1+\alpha_2+\cdots+\alpha_n = -\dfrac{a_{n-1}}{a_n} \\ \displaystyle\sum_{1\leqslant i<j\leqslant n} \alpha_i\alpha_j = \dfrac{a_{n-2}}{a_n} \\ \vdots \\ \displaystyle\sum_{1\leqslant i_1<i_2<\ldots<i_p\leqslant n} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_p} = (-1)^p\dfrac{a_{n-p}}{a_n} \\ \vdots \\ \alpha_1\alpha_2\cdots\alpha_n = (-1)^n\dfrac{a_0}{a_n}. \end{cases}$$

Exemple 20 : Soit $n \geqslant 2$. On a vu que $\mathrm{X}^n - 1 = \prod_{\zeta\in\mathbb{U}_n}(\mathrm{X}-\zeta)$.

Donc $\sum_{\zeta\in\mathbb{U}_n}\zeta = 0$: la somme des racines $n^{\text{èmes}}$ de l'unité est nulle.

Exercice 18 : Soient a, b, c les trois racines complexes de $\mathrm{P} = \mathrm{X}^3 - 3\mathrm{X} - 1$.

Calculer :

1. $a + b + c$,
2. $ab + ac + bc$,
3. abc,
4. $a^2 + b^2 + c^2$,
5. $a^3 + b^3 + c^3$,
6. $\dfrac{1}{a} + \dfrac{1}{b} + \dfrac{1}{c}$,
7. $a^7 + b^7 + c^7$.