XX

Polynômes

Avant de s'attaquer vraiment à l'algèbre linéaire, ce chapitre servira d'introduction par l'exemple aux concepts plus généraux développés ensuite dans toute leur généralité sur les espaces vectoriels.

Les polynômes constituent en effet un excellent exemple d'objets mathématiques formels, mais avec lesquels on peut faire des calculs, par le biais d'opérations simples comme la somme, le produit ou la composition. C'est ce genre de notions (opérations « utiles » sur un ensemble) que nous essaierons de généraliser ensuite.

Ce chapitre sera également l'occasion de croiser sous sa forme originale et épurée une formule d'importance capitale en analyse, et que nous retrouverons sous d'autres formes à plusieurs reprises ensuite : la formule de Taylor.

Dans toute ce chapitre, $\mathbb{K}$ désigne soit l'ensemble $\mathbb{R}$ des nombres réels ou l'ensemble $\mathbb{C}$ des nombres complexes. Pour les plus curieux, toute la construction effectuée ici peut être généralisée à un corps $\mathbb{K}$ quelconque, c'est-à-dire à un ensemble muni de deux opérations de somme et de produit « sympathiques » (associatives, commutatives, distributive l'une par rapport à l'autre, admettant chacune un élément neutre et telles que tout élément ait un opposé et un inverse, sauf 0 en ce qui concerne l'inverse)

Contenu

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.

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

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

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

Vocabulaire :

— Pour n fixé, a_n est le n+1$^{\text{ème}}$ coefficient du polynôme.

— On note X le polynôme défini par $X = (0,\ 1,\ 0,\ 0, \ldots)$ 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 $(\lambda,\ 0,\ 0, \ldots)$ 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 :

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

I.1 Opérations sur $\mathbb{K}[X]$

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

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

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

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.

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

On note N_1 et N_2 les deux entiers à partir desquels les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles respectivement.

Posons $N = \max(N_1\,;N_2)$.

Comme $N \geqslant N_1$ et $N \geqslant N_2$ alors $n \geqslant N \implies a_n + b_n = 0$ i.e. la suite $(a_n + b_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang.

On en déduit que $P + Q \in \mathbb{K}[X]$.

La loi $+ :\begin{array}{ccc} \mathbb{K}[X]\times\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ (P\,;Q) & \longmapsto & P+Q \end{array}$ 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 $0_{\mathbb{K}[X]} = (0,\, 0,\, \ldots)$ 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

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

Toutes ces propriétés découlent de celles de $\mathbb{K}$.

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 :

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

En convenant toujours que ces coefficients sont tous nuls à partir d'un certain rang.

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 :

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

On vérifiera, de même que précédemment, que $\lambda.P$ ainsi formé est bien un élément de $\mathbb{K}[X]$.

La loi

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

est alors qualifiée de *loi de composition externe* (à $\mathbb{K}[X]$).

Corollaire I.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 $\mathbb{K}$.

À ce stade, il nous reste à pouvoir multiplier des polynômes entre eux et avoir quelque chose qui ressemble à

$$\left(\sum_{i=0}^{n} a_i X^i\right)\times\left(\sum_{j=0}^{n} b_j X^j\right)=\sum_{k=0}^{2n}\left(a_0b_k+\ldots+a_kb_0\right)X^k=\sum_{k=0}^{2n}\left(\sum_{i=0}^{k}a_ib_{k-i}\right)X^k,$$

calcul au sein duquel on a simplement regroupé les termes degré par degré. Il ne nous reste plus qu'à forcer le destin.

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 :

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

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

En particulier, on a :

- $c_0=a_0b_0$
- $c_1=a_1b_0+a_0b_1$
- $c_2=a_2b_0+a_1b_1+a_0b_2$
- ...

Remarque importante :

$$\boxed{\forall\, n\in\mathbb{N},\ \sum_{k=0}^{n}a_kb_{n-k}=\sum_{p+q=n}a_pb_q.} \tag{XX.1}$$

Ici aussi, assurons-nous de la correcte définition de cette opération :

Preuve : Soient $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$ considérés avec leur entier N_1 et N_2 à partir desquels les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles respectivement.

On considère également $P\times Q=(c_n)_{n\in\mathbb{N}}$ avec, $\forall\, n\in\mathbb{N},\ c_n=\sum_{k=0}^{n}a_kb_{n-k}$.

Montrer que $P\times Q\in\mathbb{K}[X]$ revient à montrer l'existence d'un rang à partir duquel la suite $(c_n)_{n\in\mathbb{N}}$ est nulle.

Posons pour cela $N = N_1 + N_2 + 1$.

$$\forall\, n \geqslant N,\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{N_1} a_k b_{n-k} + \underbrace{\cancel{\sum_{k=N_1+1}^{n} a_k b_{n-k}}}_{=0 \text{ car } k \geqslant N_1+1>N_1}.$$

Or, $n-k = N_1+N_2+1-k = N_2+1+\underbrace{(N_1-k)}_{\geqslant 0 \text{ si } k\leqslant N_1} \geqslant N_2+1 > N_2$.

Donc, $\forall\, n \geqslant N,\ c_n = 0$ i.e. $P\times Q \in \mathbb{K}[X]$.

Comme l'addition, la loi

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

est aussi une loi de composition interne.

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 $1_{\mathbb{K}[X]} = (1,\, 0,\, 0,\, \ldots)$.

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

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

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

Preuve : Tout repose essentiellement sur la relation (XX.1). Considérons les polynômes $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ et $R = (c_n)_{n\in\mathbb{N}}$. On se contente de regarder les coefficients de degré k.

– La commutativité est évidente et découle de celle de $\mathbb{K}$ (et de $\mathbb{N}$) :

$$(PQ)_k = \sum_{p+q=k} a_p b_q = \sum_{q+p=k} b_q a_p = (QP)_k$$

– La distributivité est également assez facile.

$$\Big(P(Q+R)\Big)_k = \sum_{p+q=k} a_p(b_q + r_q) = \sum_{p+q=k} a_p b_q + \sum_{p+q=k} a_p r_q = (PQ)_k + (PR)_k.$$

– L'associativité est à peine plus longue :

$$\Big(P(QR)\Big)_k = \sum_{p+q=k} a_p \sum_{s+t=q} (b_s r_t) = \sum_{p+s+t=k} a_p b_s r_t.$$

Formule totalement symétrique par rapport aux trois polynômes, ce qui prouve l'associativité du produit.

– Il est assez clair que $(P \times 1)_k = \sum_{p+q=k} a_p 1_q = \sum_{p+0=k} a_p 1_0 = a_k = (P)_k$.
– Enfin, la linéarité de la somme nous donne :

$$\Big(\lambda.(PQ)\Big)_k = \lambda \sum_{p+q=k} a_p b_q = \sum_{p+q=k} (\lambda a_p) b_q = \Big((\lambda.P)Q\Big)_k$$
$$= \sum_{p+q=k} a_p (\lambda b_q) = \Big(P(\lambda.Q)\Big)_k.$$

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 :

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

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

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

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

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

Preuve : Montrons par récurrence que $\forall\, n \in \mathbb{N},\ X^n = (0, 0, \dots, 0, \underset{(n+1)^{\text{ème}}\ \text{coefficient}}{\overset{1}{\uparrow}}, 0, \dots)$.

Par définition de X^0 la propriété est clairement initialisée.

Supposons alors que cette propriété soit vraie pour un certain $n \in \mathbb{N}$ i.e. $X^n = (0, 0, \dots, 0, 1, 0, \dots)$ où le nombre 1 et le $(n+1)^{\text{ème}}$ coefficient.

Posons $X^n = (a_p)_{p\in\mathbb{N}}$, $X = (b_p)_{p\in\mathbb{N}}$ et $X^{n+1} = X^n \times X = (c_p)_{p\in\mathbb{N}}$. En particulier, tous les coefficients b_p et les a_p sont nuls sauf $b_1 = 1$ et $a_n = 1$.

On a : $c_p = \displaystyle\sum_{k=0}^{p} a_k b_{p-k} = \sum_{k'=0}^{p} a_{p-k'} b_{k'}$ en effectuant le changement d'indice $k' = p - k$.

- Si $p = 0$ alors $c_0 = a_p b_0 = 0$ car $b_0 = 0$.
- Si $p \geqslant 1$ alors $c_p = a_{p-1}b_1 = a_{p-1} = \begin{cases} 1 \text{ si } p-1=n \\ 0 \text{ sinon} \end{cases} = \begin{cases} 1 \text{ si } p=n+1 \\ 0 \text{ sinon} \end{cases}$.

On a donc montré que $X^{n+1} = (0, 0, \dots, 0, \underset{(n+2)^{\text{ème}} \text{ coefficient}}{\underset{\uparrow}{1}}, 0, \dots)$.

La propriété est donc héréditaire. Étant initialisée pour $n = 0$, elle est vraie pour tout $n \in \mathbb{N}$. ┘

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

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

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

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

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

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

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

Correction : Soit $n \in \mathbb{N}^*$, on a :

$$\begin{aligned}(X^3+X^2+X+1)\sum_{k=0}^{2n}(-1)^k X^k &= \frac{1-X^4}{1-X}\times\frac{1+X^{2n+1}}{1+X}\\ &= \frac{(1-X^2)(1+X^2)}{1-X}\times\frac{1+X^{2n+1}}{1+X} = \frac{(1-X)(1+X)(1+X^2)}{1-X}\times\frac{1+X^{2n+1}}{1+X}\\ &= (1+X^2)(1+X^{2n+1})\\ &= X^{2n+3}+X^{2n+1}+X^2+1.\end{aligned}$$

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

Preuve :

1 Déjà vu. À noter qu'on peut avoir $\deg(P+Q) < \max(\deg(P), \deg(Q))$ (lorsque P et Q sont de même degré et de coefficients dominants opposés).

2 Si $\lambda = 0$ on a $\lambda P = 0$ donc $\deg(\lambda P) = -\infty$.

Si $\lambda \neq 0$, posons $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ (i.e. $\deg(P) = p$).

On a vu que $\forall\, k > p, \quad \lambda a_k = 0$ donc $\deg(\lambda P) \leqslant p$.

Par ailleurs, $\lambda a_p \neq 0$ car $\lambda \neq 0$ et $a_p \neq 0$.

D'où $\deg(\lambda P) = p = \deg(P)$.

3 Si $P = 0$ ou $Q = 0$, on a $PQ = 0$ donc $\deg(PQ) = -\infty$. Par ailleurs, $\deg(P) + \deg(Q) = -\infty$ donc $\deg(PQ) = \deg(P) + \deg(Q)$.

Si $P \neq 0$ et $Q \neq 0$, posons $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ et $Q = \sum_{k=0}^{q} b_k X^k$ avec $b_q \neq 0$.

Soit $PQ = \sum_{k=0}^{+\infty} c_k X^k$. On a vu que $\forall\, k > p+q, \quad c_k = 0$ donc $\deg(PQ) \leqslant p+q$.

Par ailleurs, $c_{p+q} = \sum_{i=0}^{p+q} a_i b_{p+q-i} = \cancel{\underbrace{\sum_{i=0}^{p-1} a_i b_{p+q-i}}_{=0 \text{ car } p+q-i>q}} + a_p b_q + \cancel{\underbrace{\sum_{i=p+1}^{p+q} a_i b_{p+q-i}}_{=0 \text{ car } i \geqslant p+1>p}} = a_p b_q \neq 0$.

Donc $\deg(PQ) = p + q = \deg(P) + \deg(Q)$.

4 On a $P \circ Q = \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{p} b_i X^i \right)^k$, dont le terme dominant vaut (si on développe tout brutalement à coup de formules du binôme de Newton) $a_n b_p^n X^{pn}$.

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 $\forall\, P, Q \in \mathbb{K}[X], \quad PQ = 0 \iff P = 0 \text{ ou } Q = 0$.

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

Preuve :

1 $P \in \mathbb{K}[X]$ est inversible dans $\mathbb{K}[X]$ pour la loi $\times$ si, et seulement si il existe un polynôme Q de $\mathbb{K}[X]$ tel que $PQ = 1$. Nécessairement, P ne peut être nul.

Mais alors, $\deg(P) + \deg(Q) = 0$ i.e. $\deg(P) = 0$.

P est donc un polynôme constant non nul.

Réciproquement, il est clair que les polynômes constants non nuls, les scalaires non nuls de $\mathbb{K}$ donc, sont inversibles.

2 Supposons que $PQ = 0$.

Alors $\deg(P) + \deg(Q) = -\infty$. Si $P \neq 0$ et $Q \neq 0$, alors $\deg(P) + \deg(Q) \in \mathbb{N}$: absurde.

En conclusion, $P = 0$ ou $Q = 0$.

La réciproque est claire.

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.

Preuve : Soient $P, Q \in \mathbb{K}_n[X]$, $\lambda, \mu \in \mathbb{K}$.

$$\deg(\lambda P + \mu Q) \leqslant \max(\deg(\lambda P) ; \deg \mu Q) \leqslant \max(\deg(P) ; \deg(Q)) \leqslant n.$$

En conclusion, $\lambda P + \mu Q \in \mathbb{K}_n[X]$.

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

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

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

Preuve : Soit $P = \sum_{k\geqslant 0} a_k X^k$ alors $P' = \sum_{k\geqslant 0} k a_k X^{k-1}$.

- Si $\deg(P) \leqslant 0$ alors P est constant et $\forall\, k \in \mathbb{N}^*$, $a_k = 0$ d'où $P' = 0$ et $\deg(P') = -\infty$.
- Si $N = \deg(P) \geqslant 1$ alors $P = \sum_{k=0}^{N} a_k X^k$ avec $a_N \neq 0$.

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

Or, $\mathrm{N}a_{\mathrm{N}} \neq 0$.

Donc $\deg(\mathrm{P}') = \mathrm{N} - 1 = \deg(\mathrm{P}) - 1$.

II.3 Dérivation et opérations

Cette dérivation, bien que définie de façon formelle, coïncide évidemment avec la dérivation usuelle sur les fonctions polynômiales, et de ce fait vérifie toutes les formules de dérivation usuelles. En particulier celles rappelées ci-dessous :

Proposition 7 :

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

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

Preuve :

1. Il suffit d'écrire...
2. Posons $\mathrm{P} = \sum_{k=0}^{p} a_k \mathrm{X}^k$ et $\mathrm{Q} = \sum_{k=0}^{q} b_k \mathrm{X}^k$.

   – D'une part, par définition du produit : $\mathrm{PQ} = \sum_{k=0}^{p+q} d_k \mathrm{X}^k$ avec $\forall k \in \mathbb{N}, d_k = \sum_{i=0}^{k} a_i b_{k-i}$

   Et donc
$$(\mathrm{PQ})' = \sum_{k=1}^{p+q} k d_k \mathrm{X}^{k-1} = \sum_{k=0}^{p+q-1} (k+1) d_{k+1} \mathrm{X}^k$$
$$= \sum_{k=0}^{p+q-1} d'_k \mathrm{X}^k \text{ avec } \forall k \in \mathbb{N},\ d'_k = (k+1)d_{k+1} = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}.$$

   – D'autre part,
$$\mathrm{P}' = \sum_{k=1}^{p} k a_k \mathrm{X}^{k-1} = \sum_{k=0}^{p-1} (k+1) a_{k+1} \mathrm{X}^k$$
$$= \sum_{k=0}^{p-1} a'_k \mathrm{X}^k \text{ avec } \forall k \in \mathbb{N},\ a'_k = (k+1)a_{k+1}.$$

   On obtient alors le produit : $\mathrm{P}'\mathrm{Q} = \sum_{k=0}^{p+q-1} \alpha_k \mathrm{X}^k$ avec $\forall k \in \mathbb{N},\ \alpha_k = \sum_{i=0}^{k} a'_i b_{k-i}$

De même, en posant $\mathrm{Q}' = \sum_{k=1}^{q} b'_k \mathrm{X}^k$ avec $b'_k = (k+1)b_{k+1}$, on a :

$\mathrm{PQ}' = \sum_{k=0}^{p+q-1} \beta_k \mathrm{X}^k$ avec $\forall k \in \mathbb{N},\ \beta_k = \sum_{i=0}^{k} a_i b'_{k-i}$

En réunissant ces résultats, $P'Q + PQ' = \sum_{k=0}^{p+q-1} \gamma_k X^k$ avec :

$$\begin{aligned}
\forall\, k \in \mathbb{N}, \gamma_k &= \alpha_k + \beta_k \\
\gamma_k &= \sum_{i=0}^{k} a'_i b_{k-i} + \sum_{i=0}^{k} a_i b'_{k-i} \\
\gamma_k &= \sum_{i=0}^{k} (i+1) a_{i+1} b_{k-i} + \sum_{i=0}^{k} a_i (k-i+1) b_{k-i+1} \\
\gamma_k &= \sum_{i=1}^{k+1} i a_i b_{k-i+1} + \sum_{i=0}^{k} (k-i+1) a_i b_{k-i+1} \\
\gamma_k &= \underbrace{(k+1) a_0 b_{k+1}}_{i=0} + \left[\sum_{i=1}^{k} i a_i b_{k-i+1}\right] + \left[\sum_{i=1}^{k} (k-i+1) a_i b_{k-i+1}\right] + \underbrace{(k+1) a_{k+1} b_0}_{i=k+1} \\
\gamma_k &= (k+1) a_0 b_{k+1} + \sum_{i=1}^{k} [i a_i b_{k-i+1} + (k-i+1) a_i b_{k-i+1}] + (k+1) a_{k+1} b_0 \\
\gamma_k &= (k+1) a_0 b_{k+1} + \sum_{i=1}^{k} [(k+1) a_i b_{k-i+1}] + (k+1) a_{k+1} b_0 \\
\gamma_k &= (k+1) \sum_{i=0}^{k+1} a_i b_{k+1-i} \\
\gamma_k &= d'_k
\end{aligned}$$

Par conséquent, on a bien : $(PQ)' = P'Q + PQ'$

Je vous accorde que cette démonstration n'a d'intérêts que techniques.

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 $\widetilde{P} : \begin{array}{rcl} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2+1 \end{array}$.

Par construction,

Corollaire 8.1 : L'application $\Phi : \begin{array}{rcl} \mathbb{K}[X] & \longrightarrow & Pol(\mathbb{K}) \\ P & \longmapsto & \widetilde{P} \end{array}$ 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. $\widetilde{\lambda P + \mu Q} = \lambda\widetilde{P} + \widetilde{Q}$.
2. $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$.
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.
4. $\widetilde{P'} = \widetilde{P}'$.

Preuve : Soient $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ deux polynômes où $p, q \in \mathbb{N}$.

Quitte à rajouter des coefficients dans l'un des deux polynômes, en notant $n = \max(p\,;q)$, on peut écrire $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$.

Pour tout $x \in \mathbb{K}$,

$$(\widetilde{\lambda P + \mu Q})(x) = \sum_{k=0}^{n} (\lambda a_k + \mu b_k) x^k = \lambda \sum_{k=0}^{n} a_k x^k + \mu \sum_{k=0}^{n} b_k x^k = \lambda\widetilde{P}(x) + \mu\widetilde{Q}(x).$$

La démonstration est identique pour le produit.

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 $\tilde{1}$ 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 :

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

Preuve : En trois temps :

1. Posons $Q_k = X^k$. Alors $\forall n \in \mathbb{N}$, $\quad Q_k^{(n)} = \begin{cases} \dfrac{k!}{(k-n)!}X^{k-n} & \text{si } n \leqslant k \\ 0 & \text{si } n > k \end{cases}$

2. On montre la formule de Taylor pour Q_k :

$$\begin{aligned} Q_k = X^k = (a + X - a)^k &= \sum_{n=0}^{k} \binom{k}{n} a^{k-n}(X-a)^n \\ &= \sum_{n=0}^{k} \frac{k!}{n!(k-n)!} a^{k-n}(X-a)^n \\ &= \sum_{n=0}^{k} \frac{\widetilde{Q}_k^{(n)}(a)}{n!}(X-a)^n \\ &= \sum_{n\geqslant 0} \frac{\widetilde{Q}_k^{(n)}(a)}{n!}(X-a)^n \end{aligned}$$

3. On étend à tous les polynômes par linéarité :

Soit $P = \sum_{k\geqslant 0} a_k X^k = \sum_{k\geqslant 0} a_k Q_k$. En dérivant, on a $P^{(n)} = \sum_{k\geqslant 0} a_k Q_k^{(n)}$.

$$\begin{aligned} P = \sum_{k\geqslant 0} a_k Q_k &= \sum_{k\geqslant 0} a_k \sum_{n\geqslant 0} \frac{\widetilde{Q}_k^{(n)}(a)}{n!}(X-a)^n \\ &= \sum_{n\geqslant 0} \frac{1}{n!} \left[\sum_{k\geqslant 0} a_k \widetilde{Q}_k^{(n)}(a) \right] (X-a)^n \\ &= \sum_{n\geqslant 0} \frac{1}{n!} \widetilde{P}^{(n)}(a)(X-a)^n \end{aligned}$$

Les formules de Taylor sont un outil complètement fondamental en analyse, permettant d'effectuer les calculs de développements limités qui nous permettront de voir sous un jour nouveau les calculs de limites. Le principe en est simple : généraliser la notion de droite tangente à une courbe en approchant le plus possible une courbe donnée (en un point donné) par la courbe d'une fonction polynômiale.

Rien d'étonnant donc à en retrouver un énoncé dans ce chapitre consacré aux polynômes. Ici, pas question d'approximation, puisqu'un polynôme est évidemment simplement égal à à son développement limité, mais l'idée est de comprendre qu'il existe plusieurs façons différentes de décrire un même polynôme.

L'ensemble $\mathbb{R}_n[X]$ étant ce qu'on appelle un espace vectoriel de dimension $n+1$ (on expliquera cela plus tard), on peut décrire un polynôme de degré n en donnant $n+1$ réels.

On peut le faire d'au moins trois façons :

1. donner les coefficients du polynôme. C'est la façon la plus classique de procéder, mais l'information donnée est finalement assez peu commode à exploiter autrement que très globalement (que signifie le fait qu'un polynôme de degré 8 a un coefficient de degré 3 égal à 5 ? Essentiellement rien).
2. donner les valeurs du polynôme en $n+1$ réels distincts. Nous détaillerons sûrement cette méthode dans un devoir sur les polynômes dits de Lagrange qui donne une information très concrète mais éparpillée à $n+1$ endroits différents.
3. la troisième méthode que nous allons voir concentre réellement toute l'information au même endroit, puisque la formule de Taylor reconstitue le polynôme à partir des valeurs de ses différentes dérivées en un même réel a.

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.

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

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

D'où $\mathrm{P} = 3+13(\mathrm{X}-1)+8(\mathrm{X}-1)^2+2(\mathrm{X}-1)^3$ 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 $f : x \longmapsto \dfrac{4x^3-3x^2+7x-1}{(x-2)^3}$.

Correction : Posons $\mathrm{P} = 4\mathrm{X}^3-3\mathrm{X}^2+7\mathrm{X}-1$. On a $\tilde{\mathrm{P}}(2) = 33$ et

$$\mathrm{P}' = 12\mathrm{X}^2-6\mathrm{X}+7 \quad \text{et} \quad \tilde{\mathrm{P}}'(2) = 43$$
$$\mathrm{P}'' = 24\mathrm{X}-6 \quad \text{et} \quad \tilde{\mathrm{P}}''(2) = 42$$
$$\mathrm{P}^{(3)} = 24 \quad \text{et} \quad \tilde{\mathrm{P}}^{(3)}(2) = 24$$

D'après la formule de Taylor au point 2, on obtient :

$$\begin{aligned} \mathrm{P} &= 33+43(\mathrm{X}-2)+\frac{42}{2}(\mathrm{X}-2)^2+\frac{24}{6}(\mathrm{X}-2)^3 \\ &= 33+43(\mathrm{X}-2)+21(\mathrm{X}-2)^2+4(\mathrm{X}-2)^3. \end{aligned}$$

D'où,

$$f(x) = \frac{33}{(x-2)^3} + \frac{43}{(x-2)^2} + \frac{21}{x-2} + 4.$$

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 :

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

Preuve : Cas Particulier de Taylor avec $a = 0$.

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. $\forall A, B \in \mathbb{K}[X], \quad \begin{cases} A|B \\ B|A \end{cases} \iff \exists \lambda \in \mathbb{K}^\star, \quad B = \lambda A.$

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

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.

Preuve :

1. *Soit* $A \in \mathbb{K}[X]$.

   $A = A \times 1 \implies A|A$ *et* $0 = 0 \times A \implies A|0$.

2. *Soient* A, $B \in \mathbb{K}[X]$, *tels que* $\begin{cases} A|B \\ B|A \end{cases}$ *i.e.* $\exists\, Q_1, Q_2 \in \mathbb{K}[X]$ *tels que* $\begin{cases} B = Q_1A \\ A = Q_2B \end{cases}$.

   On a alors $B = Q_1Q_2B \iff B(1 - Q_1Q_2) = 0$.

   Comme $\mathbb{K}[X]$ *est intègre, alors* $B = 0$ *ou* $Q_1Q_2 = 1$.

   - *Si* $B = 0$ *alors* $B|A \implies A = 0$ *et tout* $\lambda \in \mathbb{K}$ *convient : A et B sont associés.*
   - *Si* $Q_1Q_2 = 1$ *alors* $\begin{cases} Q_1 \neq 0 \\ Q_2 \neq 0 \end{cases}$ *et* $\deg(Q_1Q_2) = \deg(Q_1)+\deg(Q_2) = 0 \implies \begin{cases} \deg(Q_1) = 0 \\ \deg(Q_2) = 0 \end{cases}$.

     Ainsi Q_1, *par exemple, est constant non nul i.e.* $\exists\, \lambda \in \mathbb{K}^*$ *tel que* $B = Q_1A = \lambda A$: *A et B sont associés.*

   Réciproquement, si $\exists\, \lambda \in \mathbb{K}^*$ *tel que* $B = \lambda A$ *alors* $B = \dfrac{1}{\lambda}A$ *qui entraîne* $A|B$ *et* $B|A$.

3. *Il suffit d'écrire.*

Proposition 13 (Compatibilité avec les opérations) :

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

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

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

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*.

Preuve :

Existence : Par récurrence (forte) sur $d = \deg(A)$.

- Si $d \leqslant 0$, alors :
  si $\deg(B) \geqslant 1$, on peut poser $A = QB + R$ avec $Q = 0$ et $R = A$ (et on a bien $\deg R < \deg(B)$.
  si $\deg(B) = 0$, B est inversible, et on peut écrire $A = (AB^{-1})B + 0$.
- Supposons que pour tout polynôme de degré $\leqslant d$ (avec $d \geqslant 0$) la propriété soit vraie.
  On considère alors $A = \sum_{k=0}^{d+1} a_k X^k = a_{d+1}X^{d+1} + \sum_{k=0}^{d} a_k X^k$ un polynôme de degré $d+1$ et $B = \sum_{k=0}^{p} b_k X^k$ avec $b_p \neq 0$.
  - si $d + 1 < p$, on pose $Q = 0$ et $R = A$.
  - si $d + 1 \geqslant p$, on écrit $A = B \times \dfrac{a_{d+1}}{b_p} X^{d+1-p} + A'$ et $A' = A - B \times \dfrac{a_{d+1}}{b_p} X^{d+1-p}$.

    Le coefficient de X^{d+1} de A' est donc, par construction, $a_{d+1} - b_p \dfrac{a_{d+1}}{b_p} = 0$.

    D'où, $\deg(A') \leqslant d$.
    Par HR, on peut écrire $A' = BQ_1 + R_1$ avec $\deg R_1 < \deg(B)$.

    D'où $A = A' + BQ_0 = B(Q_0 + Q_1) + R_1$ avec $\deg R_1 < \deg(B)$.

  La propriété est encore vraie jusqu'au rang $d + 1$.

Unicité : Supposons que $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$. avec $\deg R_1 < \deg(B)$ et $\deg R_2 < \deg(B)$.

Alors $B(Q_1 - Q_2) = R_2 - R_1$ et $\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1)$.
D'où $\deg(Q_1 - Q_2) = \deg(R_2 - R_1) - \deg(B) < 0$ i.e. $Q_1 = Q_2$.
Par suite $R_1 = A - BQ_1 = A - BQ_2 = R_2$.

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

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

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

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 $(M - I_3)(M + 3I_3) = 0_3$.
2. En déduire l'expression de M^2 en fonction de M et de I_3.
3. On définit le polynôme $P = X^2 + 2X - 3$.
   - (a) Déterminer le reste R de la division euclidienne de X^n par P.
   - (b) En déduire M^n
4. M est-elle inversible ?

La méthode exposée dans l'exercice est générale :

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 :

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

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.

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

Preuve :
($\Leftarrow$) Si $R = 0$, on a $A = BQ + 0$ avec $Q \in \mathbb{K}[X]$ donc $B|A$.
($\Rightarrow$) Supposons que $B|A$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ = BQ + 0$.

Comme on a bien $\deg 0 < \deg(B)$, le reste dans la division euclidienne A par B est nul.

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

Correction : Écrivons la division euclidienne de $(X-2)^{2n} + (X-1)^n - 1$ par $X^2 - 3X + 2$.
Avec les degrés, il existe donc un polynôme Q et deux scalaires a et b tels que :

$$(X-2)^{2n} + (X-1)^n - 1 = Q(X^2 - 3X + 2) + aX + b.$$

En remarquant que 1 et 2 sont les racines de $(X^2 - 3X + 2)$, on obtient le système trivial :

$$\begin{cases} a+b & = 0 \\ 2a+b & = 0 \end{cases} \iff \begin{cases} a = 0 \\ b = 0 \end{cases} \iff X^2 - 3X + 2 | (X-2)^{2n} + (X-1)^n - 1.$$

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.

Preuve : Soit $P \in \mathbb{K}[X]$ de degré 1.

Supposons qu'il existe $A \in \mathbb{K}[X]$ tel que $A|P$ i.e. $\exists Q \in \mathbb{K}[X]$ tel que $P = AQ$.

On a alors $1 = \deg(P) = \deg(A) + \deg(Q) \implies \begin{cases} \deg(A) = 0 \\ \deg(Q) = 1 \end{cases}$ ou $\begin{cases} \deg(A) = 1 \\ \deg(Q) = 0 \end{cases}$

- Si $\deg(A) = 0$ alors A est un polynôme constant non nul.
- Si $\begin{cases} \deg(A) = 1 \\ \deg(Q) = 0 \end{cases}$ alors Q est un polynôme constant non nul, soit $Q = \lambda \in \mathbb{K}^*$ qui entraîne $P = \lambda A$: P et A sont associés.

Finalement, si $P \in \mathbb{K}[X]$ est de degré 1 alors les seuls diviseurs de P sont les polynômes constants non nuls et les polynômes associés à P i.e. le polynôme P est irréductible.

Toute la question va être de savoir si la réciproque est vraie ou non *i.e.* les polynômes irréductibles SONT les polynômes de degré 1. Cela va dépendre de $\mathbb{K}$.

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 $\alpha \in \mathbb{K}$.

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

Preuve :

($\Leftarrow$) Si P est divisible par $X - \alpha$, alors on peut écrire $P = (X - \alpha)Q$, avec $Q \in \mathbb{K}[X]$.

Alors, $\forall x \in \mathbb{K}$, $\widetilde{P}(x) = (\widetilde{X - \alpha)Q}(x) = (x - \alpha)\widetilde{Q}(x)$.

Par conséquent, $\widetilde{P}(\alpha) = (\alpha - \alpha)\widetilde{Q}(\alpha) = 0$ donc α est une racine de P.

($\Rightarrow$) Effectuons la division euclidienne de P par $X - \alpha$: $P = (X - \alpha)Q + R$ avec $Q, R \in \mathbb{K}[X]$ et $\deg R < \deg(X - \alpha) = 1$. On en déduit que $\deg R \leqslant 0$, i.e. R est un polynôme constant.

Posons $R = r_0$.

On a donc $P = (X - \alpha)Q + r_0$ et donc $\forall x \in \mathbb{K}$, $\widetilde{P}(x) = (x - \alpha)\widetilde{Q}(x) + r_0$.

En évaluant en $x = \alpha$, on obtient $\widetilde{P}(\alpha) = r_0$.

D'où $P = (X - \alpha)Q + \widetilde{P}(\alpha)$.

Par hypothèse, α est une racine de P, donc $\widetilde{P}(\alpha) = 0$ et $P = (X - \alpha)Q$, i.e. $(X - \alpha)|P$.

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 $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$.

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

Preuve : Par récurrence sur n :

1. Si $n=1$, c'est le théorème précédent.
2. Supposons que la propriété soit vraie pour n racines ($n \geqslant 1$).

   Soit P admettant $n+1$ racines $\alpha_1, \cdots, \alpha_n, \alpha_{n+1}$.

   En utilisant le théorème, on peut écrire $\mathrm{P} = (\mathrm{X}-\alpha_{n+1})\mathrm{Q}$.

   On a donc $\forall x \in \mathbb{K}, \quad \widetilde{\mathrm{P}}(x) = (x-\alpha_{n+1})\widetilde{\mathrm{Q}}(x)$.

   Pour $k \in [\![1, n]\!], \quad (\alpha_k - \alpha_{n+1})\widetilde{\mathrm{Q}}(\alpha_k) = \widetilde{\mathrm{P}}(\alpha_k) = 0$.

   Or, les racines sont supposées distinctes, d'où $\alpha_k - \alpha_{n+1} \neq 0$ et donc $\widetilde{\mathrm{Q}}(\alpha_k) = 0$: les $\alpha_1, \cdots, \alpha_n$ sont racines de Q.

   Par hypothèse de récurrence, on peut écrire $\mathrm{Q} = \left(\displaystyle\prod_{k=1}^{n}(\mathrm{X}-\alpha_k)\right)\mathrm{Q}_1$, et donc :

$$\mathrm{P} = (\mathrm{X}-\alpha_{n+1})\mathrm{Q} = (\mathrm{X}-\alpha_{n+1})\left(\prod_{k=1}^{n}(\mathrm{X}-\alpha_k)\right)\mathrm{Q}_1 = \left(\prod_{k=1}^{n+1}(\mathrm{X}-\alpha_k)\right)\mathrm{Q}_1.$$

3. Initialisée pour $n=1$ et héréditaire, la propriété est vraie pour tout entier non nul.

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

Correction : Pour tout $n \in \mathbb{N}$:

$$\begin{aligned}
\mathrm{X}^2+1 \text{ divise } \mathrm{X}^n+1 &\iff \mathrm{i} \text{ et } -\mathrm{i} \text{ sont racines de } \mathrm{X}^n+1 \\
&\iff \mathrm{i} \text{ est racine de } \mathrm{X}^n+1 \qquad \text{car } \mathrm{X}^n+1 \text{ est à coefficients réels.} \\
&\iff \mathrm{i}^n+1=0 \iff \mathrm{e}^{\frac{\mathrm{i}n\pi}{2}} = \mathrm{e}^{\mathrm{i}\pi} \\
&\iff \frac{n\pi}{2} \equiv \pi \ [2\pi] \iff n \equiv 2 \ [4].
\end{aligned}$$

C'est le corollaire (18.1) qui donne l'implication

$$\mathrm{i} \text{ et } -\mathrm{i} \text{ sont racines de } \mathrm{X}^n+1 \implies \mathrm{X}^2+1 \text{ divise } \mathrm{X}^n+1.$$

Théorème 19 : Soit $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ 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.

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

Supposons que P possède au moins $n+1$ racines distinctes $\alpha_1, \cdots, \alpha_n, \alpha_{n+1}$.

Alors, on peut écrire $P = \left(\prod_{k=1}^{n+1}(X - \alpha_k)\right) Q$ avec $Q \in \mathbb{K}[X]$.

D'où $\deg(P) = n + 1 + \deg(Q)$ et $\deg(Q) = -1$. Absurde !

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 :
   $T_0 = 1$, $T_1 = X$ et pour tout $n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n$.
2. Calculer T_2, T_3, et T_4.
3. Démontrer que $T_n(\cos\theta) = \cos n\theta$ pour tout $\theta \in \mathbb{R}$.

   En déduire les racines de T_n.

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

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

Preuve :

- Soit $f \in Pol(\mathbb{K})$ alors, par définition, il existe $P \in \mathbb{K}[X]$ $f = \widetilde{P}$.

  Φ est donc surjective (par construction). Ce que l'on avait déjà vu au corollaire (8.1) .
- Montrons que Φ est injective.

  Soient P, $Q \in \mathbb{K}[X]$ tel que $\Phi(P) = \Phi(Q) \iff \widetilde{P} = \widetilde{Q}$.

  Ainsi, $\forall\, x \in \mathbb{K}$, $(\widetilde{P - Q})(x) = 0$.

  Le polynôme $P - Q$ admet une infinité de racines (car $\mathbb{K}$ est infini) donc $P - Q \equiv 0$ i.e. $P \equiv Q$ et Φ est injective.

Des deux alinéas précédents, on en déduit que Φ 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.

On écrira donc en particulier à partir de maintenant $P(\alpha)$ au lieu de $\widetilde{P}(\alpha)$ $(\alpha \in \mathbb{K})$.

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 :

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

Preuve : Le polynôme proposé convient bien.

L'unicité est donné par la proposition (20) .

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 $(\mathrm{X}-\alpha)^n|\mathrm{P}$.

Remarques :

— Comme α est une racine de P, $\mathrm{E} = \{n \in \mathbb{N}, (\mathrm{X}-\alpha)^n|\mathrm{P}\}$ est non vide, puisque $1 \in \mathrm{E}$.

D'autre part, E est majoré par le degré de P. Donc $\mathrm{E} \subset \mathbb{N}$ admet un plus grand élément *i.e.* la multiplicité d'une racine est bien définie.

— Si la multiplicité de α est 1, 2, 3, ... on parle de racine simple, double, triple.

On convient que si l'ordre est 0, α n'est pas une racine de P.

— Par définition de l'ordre de multiplicité, si n est celui d'une racine α alors $(\mathrm{X}-\alpha)^{n+1}$ ne divise pas 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. $\mathrm{P}(\alpha) = \mathrm{P}'(\alpha) = \dots = \mathrm{P}^{(m-1)}(\alpha) = 0$ et $\mathrm{P}^{(m)}(\alpha) \neq 0$.

Preuve :

$\boxed{1} \Rightarrow \boxed{2}$: Si α est une racine de P de multiplicité m, par définition $(\mathrm{X}-\alpha)^m|\mathrm{P}$ et $(\mathrm{X}-\alpha)^{m+1}\nmid\mathrm{P}$.
On peut donc écrire $\mathrm{P} = (\mathrm{X}-\alpha)^m\mathrm{Q}$.

Si l'on avait $Q(\alpha) = 0$, on pourrait écrire $Q = (X-\alpha)Q_1$ et donc $P = (X-\alpha)^{m+1}Q_1$. Absurde.

2 $\Rightarrow$ **3** : Supposons que $P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$. Posons $R = (X-\alpha)^m$.

D'après la formule de Leibniz $P^{(k)} = (RQ)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} R^{(i)} Q^{(k-i)}$.

Or, $R^{(i)} = \begin{cases} \dfrac{m!}{(m-i)!}(X-\alpha)^{m-i} & \text{si } i \leqslant m \\ 0 & \text{si } i > m \end{cases}$ d'où $R^{(i)}(\alpha) = \begin{cases} 0 & \text{si } i < m \\ m! & \text{si } i = m \\ 0 & \text{si } i > m \end{cases}$.

D'où $P^{(k)}(\alpha) = \sum_{i=0}^{k} \binom{k}{i} R^{(i)}(\alpha) Q^{(k-i)}(\alpha) = \begin{cases} 0 & \text{si } k < m \\ \binom{k}{m} R^{(m)}(\alpha) Q^{(k-m)}(\alpha) & \text{si } k \geqslant m \end{cases}$.

Ainsi, $P^{(m)}(\alpha) = 1 \times m! \times Q(\alpha) \neq 0$.

3 $\Rightarrow$ **1** : Supposons que $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

On applique la formule de Taylor à P :

$$\begin{aligned} P &= \sum_{n=0}^{p} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n \\ &= \sum_{n=m}^{p} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n \\ &= (X-\alpha)^m \underbrace{\sum_{n=m}^{p} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^{n-m}}_{Q} \\ &= (X-\alpha)^m Q \end{aligned}$$

Avec, $Q(\alpha) = \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!} \underbrace{(a-a)^{k-m}}_{\neq 0 \text{ ssi } k=m} = \frac{P^{(m)}(\alpha)}{m!} \neq 0$.

Donc, α est une racine de multiplicité m de P.

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

Exemples 14 :

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

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

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 $\alpha_1, \cdots, \alpha_n$ de multiplicités respectives $m_1, m_2, \cdots, m_n$, alors P est divisible par $\displaystyle\prod_{k=1}^{n}(X - \alpha_k)^{m_k}$.

Preuve : Par récurrence sur n

Si $n = 1$, c'est le théorème précédent.

Supposons que la propriété soit vraie pour n racines ($n \geqslant 1$).

Soit P admettant $n+1$ racines $\alpha_1, \cdots, \alpha_n, \alpha_{n+1}$ de multiplicités respectives $m_1, m_2, \cdots, m_n, m_{n+1}$.

En utilisant le théorème précédent, on peut écrire $P = (X - \alpha_{n+1})^{m_{n+1}}Q_1$.

Soit $k \in [\![1, n]\!]$. On va montrer que α_k est encore une racine de multiplicité m_k dans Q_1.

Considérons pour cela μ_k la multiplicité (éventuellement nulle) de α_k dans Q_1.

On a donc $Q_1 = (X - \alpha_k)^{\mu_k}Q_2$ avec $Q_2(\alpha_k) \neq 0$.

$P = (X - \alpha_{n+1})^{m_{n+1}}Q_1 = (X - \alpha_{n+1})^{m_{n+1}}(X - \alpha_k)^{\mu_k}Q_2 = (X - \alpha_k)^{\mu_k}[(X - \alpha_{n+1})^{m_{n+1}}Q_2]$

Or $\alpha_k \neq \alpha_{n+1}$ (les racines sont supposées distinctes) et $Q_2(\alpha_k) \neq 0$, donc $(X - \alpha_{n+1})^{m_{n+1}}Q_2$ est non nul en α_k.

On en déduit que μ_k est la multiplicité de α_k dans P, i.e. $\mu_k = m_k$. CQFD.

Les α_k sont de multiplicité m_k dans Q_1.

Par H.R, on peut écrire $Q_1 = \left[\displaystyle\prod_{k=1}^{n}(X - \alpha_k)^{m_k}\right]Q_3$.

Par conséquent, $P = \left[\displaystyle\prod_{k=1}^{n+1}(X - \alpha_k)^{m_k}\right]Q_3$. La propriété est héréditaire. Étant initialisée à partir de 1, elle est donc vraie pour tout entier non nul.

Exercice 14 : Montrer que le polynôme $P_n = \displaystyle\sum_{k=0}^{n}\frac{X^k}{k!}$ 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 $\mathbb{C}[X]$

Dans $\mathbb{C}$, le problème est résolu depuis longtemps sous le nom du théorème de D'Alembert-Gauss :

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 :

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

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

Preuve : À la proposition (17), on a déjà vu que les polynômes de degré 1 sont irréductibles.

Réciproquement, soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Par définition, $\deg(P) \geqslant 1$ donc P est non constant.

D'après le théorème de D'Alembert-Gauss, P admet au moins une racine $a \in \mathbb{C}$ et alors $X - a|P$.

Or, P est irréductible donc les seuls polynômes qui divisent P sont les polynômes constants non nul ou les polynômes associés à P.

$X - a$ est un polynôme non constant donc $X - a$ ne peut-être qu'un polynôme associé à P. Il existe donc $\lambda \in \mathbb{K}^*$ tel que $P = \lambda(X - a)$.

P est donc un polynôme 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, $\lambda = 1$.

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

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

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

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

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

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

Preuve : Soit $P = \sum_{k=0}^{p} a_k X^k$ avec $a_k \in \mathbb{R}$. Il suffit d'utiliser la compatibilité du conjugué avec les lois de $\mathbb{C}$ ainsi que la caractérisation des réels à partir du conjugué : $z \in \mathbb{R} \iff \overline{z} = z$.

$$P(\overline{\alpha}) = \sum_{k=0}^{p} a_k (\overline{\alpha})^k = \sum_{k=0}^{p} a_k \overline{\alpha^k} = \sum_{k=0}^{p} \overline{a_k}\,\overline{\alpha^k} = \overline{\sum_{k=0}^{p} a_k \alpha^k} = 0.$$

ATTENTION i est une racine de $(X-i)(X+2)$ mais $\overline{i}$ ne l'est pas.
Pas de contradiction avec la propriété ci-dessous car $(X-i)(X+2) \notin \mathbb{R}[X]$.

On a même un peu mieux :

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

Preuve : Soit $P \in \mathbb{K}[X]$.
Pour tout $k \in \mathbb{N}$, $P^{(k)} \in \mathbb{R}[X]$.
Pour tout $k \in [\![1, m-1]\!]$, $P^{(k)}(\alpha) = 0$ donc $P^{(k)}(\overline{\alpha}) = 0$ (proposition précédente).
Supposons qu'on ait $P^{(m)}(\overline{\alpha}) = 0$. On aurait alors $P^{(m)}(\overline{\overline{\alpha}}) = 0$: absurde.
On en déduit que $P(\overline{\alpha}) = P'(\overline{\alpha}) = \cdots = P^{(m-1)}(\overline{\alpha}) = 0$ et $P^{(m)}(\overline{\alpha}) \neq 0$.
$\overline{\alpha}$ est donc une racine de P de multiplicité m.

V.4 En pratique,

Soit $P \in \mathbb{R}[X]$. En particulier, $P \in \mathbb{C}[X]$ et on sait factoriser P dans $\mathbb{C}[X]$ connaissant son coefficient dominant λ et ses racines notées :

- Racines réelles : $\alpha_1, \alpha_2, \cdots, \alpha_r$ de multiplicité $m_1, m_2, \cdots, m_r$.
- Racines complexes : $\beta_1, \overline{\beta}_1, \beta_2, \overline{\beta}_2, \cdots, \beta_s, \overline{\beta}_s$ de multiplicité $\mu_1, \mu_2, \cdots, \mu_s$.

$$\begin{aligned} P &= \lambda \prod_{k=1}^{r} (X-\alpha_k)^{m_k} \prod_{\ell=1}^{s} (X-\beta_\ell)^{\mu_\ell} (X-\overline{\beta}_\ell)^{\mu_\ell} \\ &= \lambda \prod_{k=1}^{r} (X-\alpha_k)^{m_k} \prod_{\ell=1}^{s} \Big[(X-\beta_\ell)(X-\overline{\beta}_\ell)\Big]^{\mu_\ell} \\ &= \lambda \prod_{k=1}^{r} (X-\alpha_k)^{m_k} \prod_{\ell=1}^{s} \Big[X^2 - (\beta_\ell + \overline{\beta}_\ell)X + \beta_\ell\overline{\beta}_\ell\Big]^{\mu_\ell} \end{aligned}$$

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

en posant $\begin{cases} u_\ell = -(\beta_\ell + \overline{\beta}_\ell) = -2\mathrm{Re}\,(\beta_\ell) \in \mathbb{R} \\ v_\ell = \beta_\ell \overline{\beta}_\ell = |\beta_\ell|^2 \in \mathbb{R} \end{cases}$.

Et on a $\Delta_\ell = (u_\ell)^2 - 4v_\ell = 4\mathrm{Re}\,(\beta_\ell)^2 - 4|\beta_\ell|^2 = 4(\mathrm{Re}\,(\beta_\ell)^2 - |\beta_\ell|^2) < 0$.
En effet, $|\mathrm{Re}\,(\beta_\ell)| \leqslant |\beta_\ell|$ avec égalité uniquement si $\beta_\ell \in \mathbb{R}$, ce qui n'est pas le cas ici.

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

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

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

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.* $X^2 + u_k X + v_k$ 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 $u^2 - 4v < 0$.

Preuve :

- Depuis la proposition (17), on sait que les polynômes de degré 1 sont irréductibles.
- Montrons que les polynômes de degré 2 à discriminant négatif sont irréductibles.

  Soit $P \in \mathbb{K}[X]$ de degré 2 et de discriminant $\Delta < 0$.

  Supposons qu'il existe $A \in \mathbb{R}[X]$ tel que $A|P$ i.e. $\exists\, Q \in \mathbb{R}[X]$ tel que $P = AQ$.

  On a alors $2 = \deg(P) = \deg(A) + \deg(Q) \implies \begin{cases}\deg(A) = 0\\ \deg(Q) = 2\end{cases}$ ou $\begin{cases}\deg(A) = 1\\ \deg(Q) = 1\end{cases}$ ou $\begin{cases}\deg(A) = 2\\ \deg(Q) = 0\end{cases}$

  - Si $\begin{cases}\deg(A) = 1\\ \deg(Q) = 1\end{cases}$ alors P s'écrit comme le produit de deux polynômes de degré 1.

    P a donc deux racines réelles ce qui contredit l'hypothèse $\Delta < 0$.
  - Si $\begin{cases}\deg(A) = 0\\ \deg(Q) = 2\end{cases}$ alors A est constant non nul.
  - Si $\begin{cases}\deg(A) = 2\\ \deg(Q) = 0\end{cases}$ alors $Q = \lambda \in \mathbb{K}^*$ et $P = \lambda A$: P et A sont associés.

Finalement, si $P \in \mathbb{K}[X]$ est de degré 2 de discriminant strictement négatif alors les seuls diviseurs de P sont les polynômes constants non nuls et les polynômes associés à P i.e. le polynôme P est irréductible.

Réciproquement, soit $P \in \mathbb{K}[X]$ irréductible. On a déjà $\deg(P) \geqslant 1$.

Dans sa factorisation (XX.3), il ne peut figurer qu'un seul facteur non constant sinon, P admettrait deux (ou plus) facteurs non constants et ne serait pas irréductible.

P est donc de la forme $\lambda(X-a)$ ou $\lambda(X^2+uX+v)$ avec $\begin{cases}\lambda \in \mathbb{R}^* \\ a \in \mathbb{R} \\ u,\, v \in \mathbb{R} \,/\, u^2-4v<0.\end{cases}$

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

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

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 $\mathbb{R}[X]$.

Correction :

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

$$X^6+1=\left(X^2+1\right)\left(X^2-X\sqrt{3}+1\right)\left(X^2+X\sqrt{3}+1\right).$$

V.5 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 $\forall\, x\in\mathbb{R},\ f(x)=(x-a)Q(x)$.

On pose : $f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$ $\qquad a_n\neq 0$

$Q(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\dots+b_1x+b_0$.

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.

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

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	

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

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.

Correction : $\mathrm{P} = (2\mathrm{X}+1)^2(\mathrm{X}-5)$.

VI Somme et produit des racines

Il est très difficile d'exprimer les racines en fonction des coefficients d'un polynôme. C'est même impossible dans le cas général à partir du degré 5.

En revanche on peut facilement exprimer les coefficients en fonction des racines d'un polynôme scindé :

VI.1 Degré 2

Dans le cas du degré 2, en identifiant $P = aX^2 + bX + c$ et $P = a(X - \alpha_1)(X - \alpha_2)$, on obtient :

Proposition 25 : Soit $P = aX^2 + bX + c \in \mathbb{K}[X]$ 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 : $\forall\, \alpha \in \mathbb{C}, \quad (X - \alpha)(X - \overline{\alpha}) = X^2 - 2\mathrm{Re}\,(\alpha) + |\alpha|^2$.

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

VI.2 Cas général

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

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

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

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 $P = \displaystyle\sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$ 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,

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

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

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

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

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. $a^7 + b^7 + c^7$.

Correction : Soient a, b, c les trois racines complexes de $P = X^3 - 3X - 1$.

$$\begin{aligned} P &= 1(X-a)(X-b)(X-c) \\ &= X^3 - (a+b+c)X^2 + (ab+ac+bc)X - abc \end{aligned}$$

1. Par identification,

$$\begin{cases} a+b+c = 0 \\ ab+ac+bc = -3 \\ abc = 1 \end{cases}$$

4. $$\begin{aligned} a^2+b^2+c^2 &= (a+b+c)^2 - 2(ab+ac+bc) \\ &= 0^2 - 2\times(-3) \\ &= 6. \end{aligned}$$

5. **Par identification :**

   – $(a+b+c)^3 = a^3+b^3+c^3+3(a^2b+a^2c+b^2a+b^2c+c^2a+c^2b)+6abc.$

   Donc,

   $$\begin{aligned} a^3+b^3+c^3 &= (a+b+c)^3 - 3(a^2b+a^2c+b^2a+b^2c+c^2a+c^2b) - 6abc \\ &= -3(a^2b+a^2c+b^2a+b^2c+c^2a+c^2b) - 6 \end{aligned}$$

   – Par ailleurs :

   $$(ab+ac+bc)(a+b+c) = a^2b+a^2c+b^2a+b^2c+c^2a+c^2b+3abc.$$

   Donc,

   $$\begin{aligned} a^2b+a^2c+b^2a+b^2c+c^2a+c^2b &= (ab+ac+bc)(a+b+c) - 3abc \\ &= -3 \end{aligned}$$

   – Bilan : $a^3+b^3+c^3 = -3\times(-3) - 6 = 3.$

   À l'aide de la division euclidienne : Effectuons la division euclidienne de X^3 par $P = X^3-3X-1$:

   $$X^3 = 1P + (3X+1) \implies \begin{cases} a^3 = 1P(a) + (3a+1) \\ b^3 = 1P(b) + (3b+1) \\ c^3 = 1P(c) + (3c+1) \end{cases}$$

   D'où,

   $$\begin{aligned} a^3+b^3+c^3 &= 3(a+b+c) + 3\times 1 \\ &= 3\times 0 + 3\times 1 \end{aligned}$$

   Finalement, $a^3+b^3+c^3 = 3.$

6. $\dfrac{1}{a}+\dfrac{1}{b}+\dfrac{1}{c} = \dfrac{bc+ac+ab}{abc} = \dfrac{-3}{1} = -3.$

7. Effectuons la division euclidienne de X^7 par $P = X^3 - 3X - 1$:

$$X^7 = (X^4+3X^2+X+9)P + (6X^2+28X+9) \implies \begin{cases} a^7 = (a^4+3a^2+a+9)P(a) + (6a^2+28a+9) \\ b^7 = (b^4+3b^2+b+9)P(b) + (6b^2+28b+9) \\ c^7 = (c^4+3c^2+c+9)P(c) + (6c^2+28c+9) \end{cases}$$

D'où,

$$\begin{aligned} a^7+b^7+c^7 &= 6(a^2+b^2+c^2)+28(a+b+c)+3\times 9 \\ &= 6\times 6+28\times 0+3\times 9. \end{aligned}$$

Finalement, $a^7+b^7+c^7=63.$

Index