Rudiments sur les polynômes

1 Rudiments sur les polynômes.

a. Définition

- On note par $\mathbb{K}$ le corps des nombres réels $\mathbb{R}$ ou celui des nombres complexes $\mathbb{C}$.

  On appelle polynôme à une indéterminée, notée X, à coefficients dans $\mathbb{K}$, toute expression de la forme :

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

  où (a_k) est une suite d'éléments, dans $\mathbb{K}$, tous nuls sauf un nombre fini de ces éléments qui sont appelés les **coefficients** du polynômes. On admet que $X^0 = 1$. On a également :

  $$a_0 + \sum_{k=1}^{+\infty} a_k\, X^k$$

  Deux polynômes sont **égaux** si et seulement s'ils ont les mêmes coefficients. Ce qui fait que la somme précédente est finie. On note par $P(X)$, ou P, cette somme finie. L'ensemble des polynômes, de l'indéterminée X, à coefficients dans $\mathbb{K}$, se note $\mathbb{K}[X]$.

En considérant la situation dans laquelle seul le coefficient a_0 est non nul, qui s'identifie à $\mathbb{K}$, on constate que l'ensemble $\mathbb{K}[X]$ contient l'ensemble $\mathbb{K}$. Donc on a :

$$\boxed{\mathbb{K} \subset \mathbb{K}[X]}$$

On appelle le **polynôme nul**, le polynôme dont tous les coefficients sont nuls. On le note simplement $P = 0$.

On appelle **monôme**, tout polynôme dont tous les coefficients, sauf un, sont nuls. Un **monôme** est donc de la forme $a_k\, X^k$.

On appelle **degré** d'un polynôme P non nul le plus grand entier naturel n tel que $a_n \neq 0$. On le note $n = \deg(P)$ ou $\mathrm{d}^\circ(P)$.

Si $\deg(P) = n$ alors $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ avec $a_n \neq 0$. On note ceci : $P(X) = \sum_{k=0}^{n} a_k\, X^k$

Le monôme $a_n\, X^n$ est appelé **monôme dominant** et a_n s'appelle le **coefficient dominant** Si $a_n = 1$ alors le polynôme est dit **unitaire** ou **normalisé**.

$\triangleleft$ **Important :**

Le degré du polynôme nul n'est pas défini.

On appelle **valuation** d'un polynôme P **non nul** le plus petit entier naturel n tel que $a_n \neq 0$. On note ceci par : $\mathrm{val}(P) = n$.

b. Addition des polynômes

◁ Définition :

On pose $P = \sum_{k=0}^{+\infty} a_k\, X^k$ et $Q = \sum_{k=0}^{+\infty} b_k\, X^k$ deux polynômes de $\mathbb{K}[X]$. On appelle le polynôme somme, noté $P + Q$, le polynôme suivant :

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

Ce qui implique que :

$$\boxed{\deg(P+Q) \leqslant \max\left(\deg(P)\,;\,\deg(Q)\right)}$$

On appelle **le symétrique** de $P = \sum_{k=0}^{+\infty} a_k\, X^k$, pour l'addition, **l'opposé**, et est noté $-P$. Et on a :

$$-P = -\sum_{k=0}^{+\infty} a_k\, X^k = \sum_{k=0}^{+\infty} (-a_k)\, X^k$$

L'addition confère à l'ensemble des polynômes une structure de groupe abélien. On note $\left(\mathbb{K}[X]\,;\,+\right)$ ce groupe abélien.

c. Multiplication des polynômes

◁ Définition :

On pose $P = \sum_{k=0}^{+\infty} a_k\, X^k$ et $Q = \sum_{k=0}^{+\infty} b_k\, X^k$ deux polynômes de $\mathbb{K}[X]$. On appelle le polynôme produit, noté $PQ = P \times Q$, le polynôme suivant :

$$PQ = \sum_{k=0}^{+\infty} c_k\, X^k$$

Avec :

$$c_k = \sum_{i=0}^{n} a_{k-i} b_i = a_k b_0 + a_{k-1} b_1 + a_{k-2} b_2 + \cdots + a_2 b_{k-2} + a_1 b_{k-1} + a_0 b_k$$

Ce qui implique que :

$$\boxed{\deg(PQ) = \deg(P) + \deg(Q)}$$

La multiplication des polynômes est commutative, associative, distributive par rapport à l'addition et admet le polynôme $P = 1$ comme élément neutre.

L'addition et la multiplication confère à l'ensemble des polynômes une structure d'anneau commutatif intègre. On note $\left(\mathbb{K}[X]\,;\,+\,;\,\times\right)$ cet anneau commutatif intègre.

L'ensemble $\mathbb{K}[X]$ n'est pas un corps.

d. Multiplication par un scalaire

$\triangleleft$ **Définition :**

On pose $P = \displaystyle\sum_{k=0}^{+\infty} a_k\, X^k$ un polynôme de $\mathbb{K}[X]$, et λ un nombre réel. On pose :

$$\lambda P = \lambda \sum_{k=0}^{+\infty} a_k\, X^k = \sum_{k=0}^{+\infty} (\lambda a_k)\, X^k$$

Si on pose λ et μ deux scalaire de $\mathbb{K}$, et P et Q deux polynômes de $\mathbb{K}[X]$. On a les quatre propriétés suivantes :

$1 - \lambda(\mu P) = (\lambda\mu)P$

$2 - (\lambda + \mu)P = \lambda P + \mu P$

$3 - 1P = P$

$4 - \lambda(P + Q) = \lambda P + \lambda Q$

De ces quatre propriétés, on en déduit que l'ensemble des polynômes, relativement à l'addition et la multiplication par un scalaire, à une structure d'**espace vectoriel** sur $\mathbb{K}$ (souvent noté en abrégé $\mathbb{K} - $ **ev**).

D'ailleurs, les $n+1$ $(n \in \mathbb{N})$ monômes $X^0 = 1$, $X^1 = 1$, X^2, X^3, ... , X^n constituent une base de dimension $n+1$ pour l'espace vectoriel des polynômes de degré au plus égal à n. Autrement dit, il est possible d'écrire de **manière unique**, juste à l'aide des monômes $X^0 = 1$, $X^1 = 1$, X^2, X^3, ... , X^n, n'importe quel polynôme de degré maximal n.

e. Polynôme dérivé

$\triangleleft$ **Définition :**

On appelle **polynôme dérivé** de $P = \displaystyle\sum_{k=0}^{+\infty} a_k\, X^k$ le polynôme, noté P', suivant :

$$P' = \sum_{k=0}^{+\infty} k a_k\, X^{k-1} = \sum_{k=1}^{+\infty} k a_k\, X^{k-1}$$

Comme le premier terme de cette (première) somme est nul (cas $k = 0$). Il est possible de réindicer cette somme de manière à ne plus avoir le premier terme nul. On a alors :

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

Et on a les dix propriétés suivantes :

$1 - (P+Q)' = P' + Q'$

$1 - (P-Q)' = P' - Q'$

$2 - (\lambda P)' = \lambda P'$

$3 - 1P = P$

$4 - (PQ)' = P'Q + PQ'$

$5 - \left(\dfrac{P}{Q}\right)' = \dfrac{P'Q - PQ'}{Q^2}$

$6 - (P^n)' = nP'P^{n-1}$

$7 - P^{(0)} = P$

$8 - P^{(1)} = P'$

$9 - P^{(2)} = \left(P^{(1)}\right)' = (P')' = P''$

$10 - \left(P^{(n)}\right)' = P^{(n+1)}$

f. Polynôme Mac Laurin et Taylor

◁ Définition :

Un polynôme non nul P de degré n s'écrit sous la forme :

$$P = \sum_{k=0}^{n} a_k\, X^k = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \cdots + a_n X^n \quad \Longrightarrow \quad P(0) = a_0$$

Donc :

$$P' = \sum_{k=1}^{n} k a_k\, X^{k-1} = a_1 + 2a_2 X + 3a_3 X^2 + \cdots + n a_n X^{n-1} \quad \Longrightarrow \quad P'(0) = a_1$$

Puis :

$$P'' = \sum_{k=1}^{n} k(k-1) a_k\, X^{k-2} = 2a_2 + 6a_3 X + \cdots + n(n-1) a_n X^{n-1} \quad \Longrightarrow \quad P''(0) = 2a_2 = 1 \times 2a_2$$

D'où :

$$P''' = \sum_{k=1}^{n} k(k-1)(k-2) a_k\, X^{k-3} = 6a_3 + \cdots + n(n-1)(n-2) a_n X^{n-2} \quad \Longrightarrow \quad P'''(0) = 6a_3 = 1 \times 2 \times 3a_3$$

On constate alors que, de proche en proche, nous obtenons :

$$P^{(n)}(0) = 1 \times 2 \times 3 \cdots \times n\, a_n = n!\, a_n$$

On a donc :

$$a_n = \frac{P^{(n)}(0)}{n!}$$

En se souvenant que dans le cas $n=0$ on a $a_0 = \dfrac{P^{(0)}(0)}{0!} = \dfrac{P(0)}{1} = P(0)$, on peut donc écrire le polynômes P sous la forme suivante :

$$P = \sum_{k=0}^{n} a_k\, X^k = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}\, X^k = P(0) + P'(0)X + \frac{P''(0)}{2}X^2 + \frac{P'''(0)}{6}X^3 + \cdots + \frac{P^{(n)}(0)}{n!}X^n$$

Finalement, on obtient **la formule de MacLaurin** (Colin MacLaurin, mathématicien écossais, 1698-1746) :

$$\boxed{P(X) = P(0) + P'(0)\,X + \frac{1}{2!}P''(0)\,X^2 + \frac{1}{3!}P'''(0)\,X^3 + \cdots + \frac{1}{n!}P^{(n)}(0)\,X^n}$$

Soit $h \in \mathbb{K}$. Posons $Q(X) = P(X+h)$. La **formule de MacLaurin** nous donne alors :

$$Q(X) = Q(0) + Q'(0)\,X + \frac{1}{2!}Q''(0)\,X^2 + \frac{1}{3!}Q'''(0)\,X^3 + \cdots + \frac{1}{n!}Q^{(n)}(0)\,X^n$$

On a alors, par dérivation composée :

$$Q'(X) = \big(P(X+h)\big)' = (X+h)'P'(X+h) = 1 \times P'(X+h) = P'(X+h)$$

D'où :

$$Q'(0) = P'(0+h) = P'(h)$$

On trouve alors que $Q^{(n)}(0) = P^{(n)}(h)$. De plus, $Q(0) = P(0+h) = P(h)$. La **formule de MacLaurin** nous donne alors :

$$\boxed{P(X+h) = P(h) + P'(h)\,X + \frac{1}{2!}P''(h)\,X^2 + \frac{1}{3!}P'''(h)\,X^3 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^n}$$

Il s'agit de **la formule de Taylor** (Brook Taylor, mathématicien anglais, 1685-1731)

De la formule précédente, on tire que :

$$P(X+h) - P(h) = P'(h)\,X + \frac{1}{2!}P''(h)\,X^2 + \frac{1}{3!}P'''(h)\,X^3 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^n$$

Soit encore :

$$\frac{P(X+h) - P(h)}{X} = P'(h) + \frac{1}{2!}P''(h)\,X + \frac{1}{3!}P'''(h)\,X^2 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^{n-1}$$

D'où :

$$\lim_{X \longrightarrow 0} \frac{P(X+h) - P(h)}{X} = \lim_{X \longrightarrow 0} \left(P'(h) + \frac{1}{2!}P''(h)\,X + \frac{1}{3!}P'''(h)\,X^2 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^{n-1}\right)$$

Soit :

$$\lim_{X \longrightarrow 0} \frac{P(X+h) - P(h)}{X} = \lim_{X \longrightarrow 0} P'(h) + \lim_{X \longrightarrow 0} \left(\frac{1}{2!}P''(h)\,X + \frac{1}{3!}P'''(h)\,X^2 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^{n-1}\right)$$

Or, $P'(h) \in \mathbb{K}$, donc $\lim\limits_{X \longrightarrow 0} P'(h) = P'(h)$. Ce qui nous donne immédiatement :

$$\lim_{X \longrightarrow 0} \frac{P(X+h) - P(h)}{X} = P'(h) + \lim_{X \longrightarrow 0} \left(\frac{1}{2!}P''(h)\,X + \frac{1}{3!}P'''(h)\,X^2 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^{n-1}\right)$$

De plus, on a $\lim\limits_{X \longrightarrow 0} \left(\frac{1}{2!}P''(h)\,X + \frac{1}{3!}P'''(h)\,X^2 + \cdots + \frac{1}{n!}P^{(n)}(h)\,X^{n-1}\right) = 0$. Ainsi, on obtient :

$$\lim_{X \longrightarrow 0} \frac{P(X+h)-P(h)}{X} = P'(h)$$

On reconnais la formule qui sert de définition de dérivée de P en h, usuellement écrite sous la forme :

$$P'(h) = \lim_{X \longrightarrow 0} \frac{P(h+X)-P(h)}{X}$$

Ceci montre la cohérence de l'ensemble des développements.

2 Multiplicité d'une racine d'un polynôme

a. Définition

◁ **Définition :**

Soit $r \in \mathbb{K}$.

On appelle **racine** d'un polynôme P, le scalaire r qui vérifie $\boxed{P(r)=0}$.

On appelle **ordre de multiplicité de la racine** r, de $P \neq 0$, de degré $n \in \mathbb{N}$, le plus grand nombre entier naturel $p \leqslant n$

qui rend le polynôme (non nul) P **divisible** par $(X-r)^p$. Autrement écrit :

$$\boxed{P(X) \big| (X-r)^p \iff \frac{P(X)}{(X-r)^p} = Q(X) \in \mathbb{K}[X] \quad \deg(Q) = n-p}$$

Dans **la formule de Taylor** de $P \neq 0$, posons $h=r$ et $X = \mathrm{X} - r$.

Dans ce cas :

$X + h = \mathrm{X} - r + h = \mathrm{X} - r + r = \mathrm{X}$

On a alors :

$$P(\mathrm{X}) = P(r) + P'(r)\left(\mathrm{X}-r\right) + \frac{1}{2!}P''(r)\left(\mathrm{X}-r\right)^2 + \frac{1}{3!}P'''(r)\left(\mathrm{X}-r\right)^3 + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^n$$

Dans cette expression, faisons clairement apparaitre le nombre entier naturel $p \leqslant n$. On a alors :

$$\begin{aligned} P(\mathrm{X}) &= P(r) + P'(r)\left(\mathrm{X}-r\right) + \frac{1}{2!}P''(r)\left(\mathrm{X}-r\right)^2 + \frac{1}{3!}P'''(r)\left(\mathrm{X}-r\right)^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\left(\mathrm{X}-r\right)^{p-1} \\ &+ \frac{1}{p!}P^{(p)}(r)\left(\mathrm{X}-r\right)^p + \frac{1}{(p+1)!}P^{(p+1)}(r)\left(\mathrm{X}-r\right)^{p+1} + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^n \end{aligned}$$

Soit encore :

$$\begin{aligned} P(\mathrm{X}) &= P(r) + P'(r)\left(\mathrm{X}-r\right) + \frac{1}{2!}P''(r)\left(\mathrm{X}-r\right)^2 + \frac{1}{3!}P'''(r)\left(\mathrm{X}-r\right)^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\left(\mathrm{X}-r\right)^{p-1} \\ &+ \left(\mathrm{X}-r\right)^p \left(\frac{1}{p!}P^{(p)}(r) + \frac{1}{(p+1)!}P^{(p+1)}(r)\left(\mathrm{X}-r\right) + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^{n-p}\right) \end{aligned}$$

Notons par $\mathcal{R}(\mathrm{X})$ la première ligne du développement précédent de $P(\mathrm{X})$. Donc :

$$\begin{aligned} P(\mathrm{X}) &= \mathcal{R}(\mathrm{X}) \\ &+ \left(\mathrm{X}-r\right)^p \left(\frac{1}{p!}P^{(p)}(r) + \frac{1}{(p+1)!}P^{(p+1)}(r)\left(\mathrm{X}-r\right) + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^{n-p}\right) \end{aligned}$$

Avec :

$$\mathcal{R}(\mathrm{X}) = P(r) + P'(r)\left(\mathrm{X}-r\right) + \frac{1}{2!}P''(r)\left(\mathrm{X}-r\right)^2 + \frac{1}{3!}P'''(r)\left(\mathrm{X}-r\right)^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\left(\mathrm{X}-r\right)^{p-1}$$

Supposons maintenant que r soit une racine d'ordre p du polynôme P. Ainsi le polynôme P est divisible par les tous les termes suivants : $\left(\mathrm{X}-r\right)$, $\left(\mathrm{X}-r\right)^2$, $\left(\mathrm{X}-r\right)^3, \cdots, \left(\mathrm{X}-r\right)^{p-1}$ et $\left(\mathrm{X}-r\right)^p$. De plus, on a bien évidemment $P(r) = 0$.

Dans ce cas, avec $Q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$, on a

$$\frac{P(\mathrm{X})}{\left(\mathrm{X}-r\right)^p} = Q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$$

Soit :

$$\frac{\mathcal{R}(\mathrm{X}) + \left(\mathrm{X}-r\right)^p\left(\frac{1}{p!}P^{(p)}(r) + \frac{1}{(p+1)!}P^{(p+1)}(r)\left(\mathrm{X}-r\right) + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^{n-p}\right)}{\left(\mathrm{X}-r\right)^p} = Q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$$

Soit encore :

$$\frac{\mathcal{R}(\mathrm{X})}{\left(\mathrm{X}-r\right)^p} + \frac{1}{p!}P^{(p)}(r) + \frac{1}{(p+1)!}P^{(p+1)}(r)\left(\mathrm{X}-r\right) + \cdots + \frac{1}{n!}P^{(n)}(r)\left(\mathrm{X}-r\right)^{n-p} = Q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$$

On doit donc avoir obligatoirement $\mathcal{R}(\mathrm{X}) = 0$.

Nous pouvons imaginer que l'indéterminée de $\mathcal{R}$ ne soit pas X mais $\mathrm{X}-r$. Posons donc $\mathrm{X}-r = T$, et de fait :

$$\mathcal{R}(T) = P(r) + P'(r)\,T + \frac{1}{2!}P''(r)\,T^2 + \frac{1}{3!}P'''(r)\,T^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\,T^{p-1}$$

A savoir :

$$0 = P(r) + P'(r)\,T + \frac{1}{2!}P''(r)\,T^2 + \frac{1}{3!}P'''(r)\,T^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\,T^{p-1}$$

Or, rappelons que $P(r) = 0$ car, par hypothèse, r est une racine du polynôme P. Donc :

$$0 = 0 + P'(r)\,T + \frac{1}{2!}P''(r)\,T^2 + \frac{1}{3!}P'''(r)\,T^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\,T^{p-1}$$

Soit :

$$P'(r)\,T + \frac{1}{2!}P''(r)\,T^2 + \frac{1}{3!}P'''(r)\,T^3 + \cdots + \frac{1}{(p-1)!}P^{(p-1)}(r)\,T^{p-1} = 0$$

Ceci implique donc que $P'(r) = P''(r) = P'''(r) = \cdots = P^{(p-1)}(r) = 0$

Finalement, nous arrivons à la conclusion suivante :

$$\boxed{\textbf{Si } r \textbf{ est une racine d'ordre } p \leqslant n \textbf{ du polynôme } P \textbf{ alors } P(r) = P'(r) = \cdots = P^{(p-1)}(r) = 0 \textbf{ et } P^{(p)}(r) \neq 0}$$

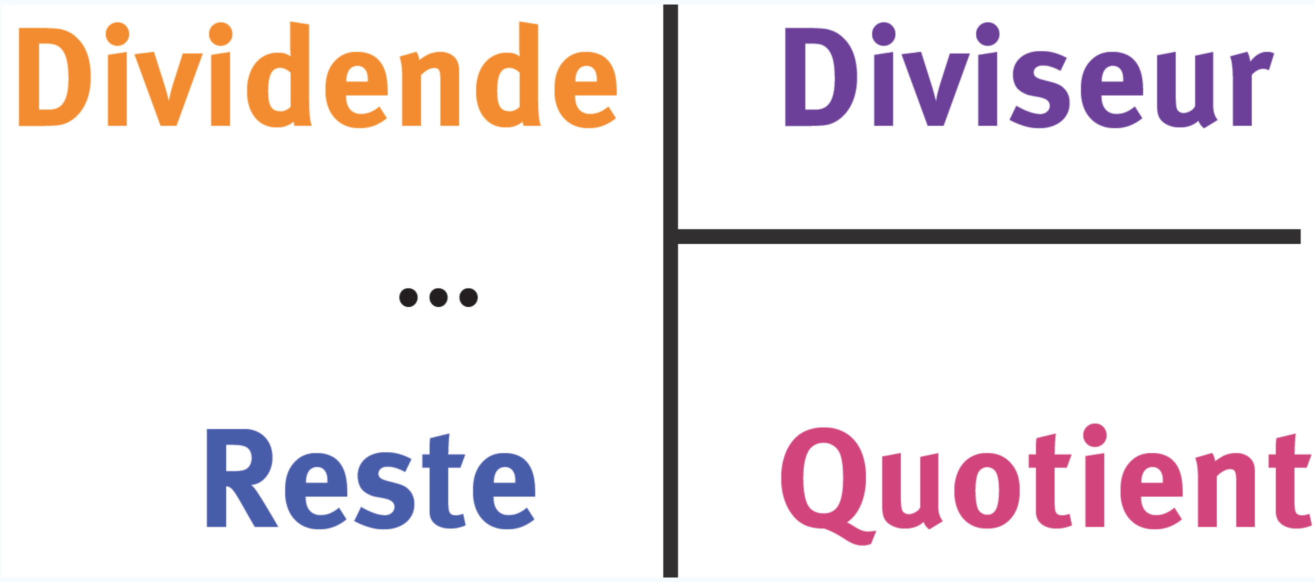
3 Division euclidienne de deux polynômes

a. Le théorème de la division euclidienne de deux polynômes

Soient A et B deux polynômes à coefficients dans $\mathbb{K}$, avec B non nul, il existe **un unique** couple $(Q\,;\,R)$ tel que :

$A = BQ + R$

Avec le degré de R est **strictement plus petit** que celui de B. Le polynôme A est le dividende et le polynôme B est le diviseur. Le polynôme Q est le quotient et le polynôme R est le reste. On retiendra :



Lorsque le reste $R = 0$, on dit que A est **divisible** par B ou, de manière équivalente, que B **divise** A. On note ceci : $A \big| B$.

Bien souvent, dans la pratique, on a $\deg(A) \geqslant \deg(B)$. Dans ce cas, on obtient séquence type que nous allons illustrer.

Pour l'exécution d'une division euclidienne, on écrit les deux polynômes A et B selon les puissances décroissantes. Donc on écrit les deux polynômes A et B en commençant par leur monôme dominant respectif.

Rappelons que l'on stoppe la séquence calculatoire lorsqu'à gauche, à l'issue de la soustraction (donc sous un trait horizontal), le degré du polynôme obtenu est inférieur à celui du diviseur.

Posons $A = 2X^3 - X^2 - 2X + 1$ et $B = X^2 + X + 1$. Dans ce cas, on a la séquence calculatoire suivante :

$$\begin{array}{r|l}
2X^3 - X^2 - 2X + 1 & \underline{X^2 + X + 1} \\
\underline{2X^3 + 2X^2 + 2X\phantom{{}+1}} & 2X - 3 \\
-3X^2 - 4X + 1 & \\
\underline{-3X^2 - 3X - 3} & \\
-X + 4 &
\end{array}$$

Et on a :

$2X^3 - X^2 - 2X + 1 = (X^2 + X + 1) \times (2X - 3) + (-X + 4)$

Le quotient est $Q = 2X - 3$ et le reste est $R = -X + 4$.

Illustrons maintenant la situation dans laquelle le reste est nul, c'est-à-dire le cas pour lequel B divise A (le diviseur divise le dividende, ou encore le dividende est divisible par le diviseur).

Posons $A = X^3 + 4X^2 + X - 6$ et $B = 2X^2 + 10X + 12$. Dans ce cas, on a la séquence calculatoire suivante :

$$
\begin{array}{rrr|l}
X^3 & +4X^2 + & X - 6 & 2X^2 + 10X + 12 \\
\cline{4-4}
-X^3 & -5X^2 - 6X & & \dfrac{1}{2}X - \dfrac{1}{2} \\
\cline{1-3}
 & - & X^2 - 5X - 6 & \\
 & + & X^2 + 5X + 6 & \\
\cline{2-3}
 & & 0 &
\end{array}
$$

Et on a :

$$X^3 + 4X^2 + X - 6 = \left(2X^2 + 10X + 12\right) \times \left(\frac{1}{2}X - \frac{1}{2}\right) + (0)$$

Le quotient est $Q = \dfrac{1}{2}X - \dfrac{1}{2}$ et le reste est $R = 0$.

Dans le dividiende, lorsqu'un coefficient (se trouvant devant un terme $X^i, \ i \in [\![1\,;\,n]\!]$) est nul, on l'indique clairement dans la division euclidienne en écrivant $0X^i$.

4 Division selon les puissances croissantes de deux polynômes

a. Définition

Il est également possible d'écrire les deux polynômes A et B selon les puissances croissantes de leur indéterminée. Cette technique est utile pour effectuer des décomposition en éléments simples de fractions rationnelles polynomiales.

On considère les deux polynômes non nul A et B suivants :

$$\left\{\begin{array}{lcl} A & = & a_0 + a_1X + \cdots + a_nX^n \\ B & = & b_0 + b_1X + \cdots + b_nX^n \end{array}\right.$$

Avec $b_0 \neq 0$, autrement dit $\mathrm{val}(B) = 0$.

Dans ce cas, pour tout nombre entier naturel m, il existe un couple unique de polynôme $(Q\,;\,R)$, tel que $\deg(Q) \leqslant m$, et qui permet d'écrire :

$A = BQ + X^{m+1}R$. Le polynôme Q s'appelle le quotient et le polynôme $X^{m+1}R$ s'appelle le reste de la division suivant les puissances croissantes de A et B **à l'ordre m**.

Si le reste de la division suivant les puissances croissantes de A et B est nul, à un certain moment, alors A est divisible par B.

Contrairement à la division euclidienne, on peut la continuer indéfiniment : on ne s'arrête que quand l'ordre désiré est atteint. Par exemple, pour diviser $A = X + 1$ par $B = X^2 + 1$, à l'ordre 2, on écrit :

$$
\begin{array}{ccccc|c}
1 & +X & & & & 1+X^2 \\
1 & & +X^2 & & & \hline 1+X-X^2 \\
\cline{1-5}
 & X & -X^2 & & & \\
 & X & & +X^3 & & \\
\cline{1-5}
 & & -X^2 & -X^3 & & \\
 & & -X^2 & & -X^4 & \\
\cline{1-5}
 & & & -X^3 & +X^4 &
\end{array}
$$

Ainsi, on écrit que :

$X + 1 = (1 + X^2) \times (1 + X - X^2) + (-X^3 + X^4)$

Soit encore :

$X + 1 = (1 + X^2) \times (1 + X - X^2) + X^3(-1 + X)$

Finalement :

$X + 1 = (1 + X^2) \times (1 + X - X^2) + X^{2+1}(-1 + X)$

On peut, par exemple, s'en servir pour décomposer la fraction rationnelle $\dfrac{A}{X^3 B} = \dfrac{1+X}{X^3(1+X^2)}$ en éléments simples. En effet, nous avons :

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

Illustrons cette méthode sur un autre exemple avec les polynômes suivants :

$A = 1 + 3X + 2X^2 - 7X^3$ et $B = 1 + X - 2X^2$

On a alors, à l'ordre 3, la séquence calculatoire suivante :

$$
\begin{array}{cccccc|cccc}
1 & +3X & +2X^2 & -7X^3 & & & 1 & +X & -2X^2 & \\
\cline{7-10}
 & +2X & +4X^2 & -7X^3 & & & 1 & +2X & +2X^2 & -5X^3 \\
 & & +2X^2 & -3X^3 & & & & & & \\
 & & & -5X^3 & +4X^4 & & & & & \\
 & & & & +9X^4 & -10X^5 & & & &
\end{array}
$$

Et on peut alors écrire :

$$\underbrace{1 + 3X + 2X^2 - 7X^3}_{A} = \underbrace{(1 + X - 2X^2)}_{B}\underbrace{(1 + 2X + 2X^2 - 5X^3)}_{Q} + X^{3+1}\underbrace{(9 - 10X)}_{R}$$

b. Division par le terme $X - a$

La division de P par $X-a$ s'écrit :

$$P(X)=(X-a)Q(X)+R(X)$$

Posons $X=a$, et dans ce cas, nous obtenons :

$$P(a)=(a-a)Q(a)+R(a) \iff P(a)=R(a)$$

Donc, on en déduit que :

$$\boxed{\big(P(X)\big|(X-a)\big) \iff P(a)=0}$$

Si un polynôme P admet $k \in \mathbb{N}$ racines $r_1, r_2, \cdots, r_k$ (pas forcément distinctes entre elles, donc certaines peuvent être multiples) alors ce polynôme P peut se factoriser sous la forme suivante :

$$P=(X-r_1)(X-r_2)\cdots(X-r_k)Q$$

Avec $Q \in \mathbb{K}[X]$, et $\deg(Q)=\deg(P)-k$.

Un polynôme P de $\mathbb{K}[X]$, de degré $n \in \mathbb{N}^\star$ est dit $\textbf{scindé}$ sur $\mathbb{K}$ s'il se factorise sous la forme :

$$P=a_n(X-r_1)(X-r_2)\cdots(X-r_n)$$

où $r_1, r_2, \cdots, r_n$ sont les n racines de P et a_n est le coefficient dominant de P.

Autrement dit, P est $\textbf{scindé}$ s'il s'écrit comme produit de polynômes de degré 1 à coefficients dans $\mathbb{K}$. D'où :

$$P(X)=\prod_{k=1}^{n}(X-r_k)$$

c. Le théorème de D'Alembert et Gauss

Historiquement, ce théorème est démontré rigoureusement par $Gauss$ en 1815. Il s'agit en fait de sa deuxième preuve car la première (incomplète) était proposée dans sa thèse de Doctorat en 1799. Ce théorème est tellement important qu'il se nomme aujourd'hui :

$\textit{théorème fondamental de l'algèbre}$.

Le théorème s'énonce ainsi :

$\clubsuit$ $\textbf{Le théorème fondamental de l'algèbre :}$

$\boxed{\textbf{Tout polynôme non constant, à coefficients complexes, admet au moins une racine complexe}}$.

Ce qui conduit facilement à l'énoncé suivant :

$\boxed{Tout\ polynôme\ de\ degré\ n \geqslant 1\ admet\ n\ racines\ réelles\ ou\ complexes\ distinctes\ ou\ confondues}$.