Polynômes

Table des matières

Polynôme et fonction polynomiale

Le terme de « polynôme » peut entraîner des confusions.

Pour les lycéens, polynôme renvoie à la fonction polynomiale, c'est à dire qu'un polynôme est une fonction. Soit par exemple le polynôme P du second degré : $P : \quad x \mapsto x^2 - 3x + 2$. La lettre x désigne alors la variable de la fonction. Cette variable est réelle ou éventuellement complexe.

Dans ce chapitre nous nous intéresserons aux polynômes dans le sens formel. Par exemple le polynôme : $P = X^2 - 3X + 2$. La lettre X ne désigne plus un élément variant dans $\mathbb{R}$ mais sert seulement à repérer les coefficients du polynôme, on dit que X est une **indéterminée**. Dans notre exemple le coefficient de degré 2 du polynôme P vaut 1, celui de degré 1 vaut -3, et le coefficient constant vaut 2.

Un polynôme (formel), n'est rien d'autre qu'une liste de coefficients repérés par la puissance de l'indéterminée X. Deux polynômes seront égaux si, et seulement si, ils ont les mêmes coefficients : c'est le principe d'identification.

Il est cependant facile de retourner du polynôme à la fonction polynomiale dans $\mathbb{R}$ ou $\mathbb{C}$. Il suffit pour cela de substituer à l'indéterminée X la variable réelle ou complexe x dans le polynôme. On pourra ainsi évaluer un polynôme en n'importe qu'elle valeur de x.

Pourquoi n'a t-on pas défini *a priori* un polynôme comme une fonction polynomiale sur laquelle on effectue des calculs dans $\mathbb{R}$ ou $\mathbb{C}$? La raison est qu'en procédant ainsi, on n'aurait pas pu donner de signification mathématique précise à la lettre X, en sorte que la définition des polynômes s'en trouverait imprécise. Il est, en effet parfois impossible de retourner à un polynôme formel à partir d'une fonction polynomiale (c'est le cas dans le corps fini $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier).

On aura donc soin de **ne pas considérer** la lettre X comme représentant un « élément variable » d'un corps $\mathbb{K}$. La lettre X comme on le verra par la suite désigne un polynôme particulier dont le seul coefficient non nul est celui du 1er degré.

1 Construction de l'anneau des polynômes

1.1 Définition

Dans la suite, $\mathbb{K}$ désigne le corps des réels $\mathbb{R}$ ou le corps des complexes $\mathbb{C}$.

Définition 1 : On appelle **polynôme** à une indéterminée à coefficients dans $\mathbb{K}$ toute suite $(a_i)_{i\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ dont tous les termes sont nuls à partir d'un certain rang.

Si tous les termes ne sont pas nul, le plus grand indice n, pour lequel $a_n \neq 0$ est appelé le **degré du polynôme** noté $d^\circ P = n$.
a_n est le coefficient dominant et si $a_n = 1$ le polynôme est unitaire.

Pour le **polynôme nul**, noté 0, dont tous les termes sont nuls, on note $d^\circ 0 = -\infty$

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ dont X est l'indéterminée.

Exemple : P un polynôme : $P = (a_i)_{i\in\mathbb{N}} = (a_0, a_1, \dots, a_n, 0, 0, \dots)$ et $d^\circ P = n$

Théorème 1 : Principe d'identification.
Deux polynômes sont égaux si, et seulement si, leurs coefficients sont égaux

1.2 Somme et produit

Définition 2 : On définit dans $\mathbb{K}[X]$ la somme et le produit de deux polynômes. Soient $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$:

- $P + Q = (a_i + b_i)_{i\in\mathbb{N}}$
- $PQ = (c_n)_{n\in\mathbb{N}}$ avec $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

La définition du produit de deux polynômes correspond au **développement usuel** de deux fonctions polynomiales.
Comme x^n s'obtient en multipliant x^k par x^{n-k} pour k compris entre 0 et n, la somme des produits des coefficients devant x^k et x^{n-k} correspond au coefficient devant x^n.

Propriété : La somme et le produit de deux polynômes sont des lois internes car les suites des coefficients $(a_i + b_i)_{i\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ ont tous leurs termes nuls à partir d'un certain rang.

Démonstration : Soit $m = \max(d^\circ P\ ,\ d^\circ Q)$

- Si $i > m$ alors, $a_i = b_i = 0$ et donc $a_i + b_i = 0$
- Si $n > 2m$ alors, $c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{m} a_k \underbrace{b_{n-k}}_{=0} + \sum_{k=m+1}^{n} \underbrace{a_k}_{=0} b_{n-k} = 0$

1.3 Notation

Définition 3 : Dans $\mathbb{K}[X]$, on note $1 = (1, 0, 0, \dots)$ et $X = (0, 1, 0, 0, \dots)$.
On en déduit alors : $X^2 = (0, 0, 1, 0, 0 \dots)$, $X^3 = (0, 0, 0, 1, 0, 0 \dots)$ etc.

Pour tout polynôme : $P = a_0 + a_1 X + \cdots + a_n X^n = \sum_{i=0}^{n} a_i X^i$

Remarque : On peut aussi écrire : $P = \sum_{i=0}^{+\infty} a_i X^i$.
Cette notation peut rendre service dans la rédaction par exemple dans un produit des polynômes de degrés différents.

Démonstration : On montre que $\forall i \in \mathbb{N},\ X^i = (0, 0, \dots, 0, 1, 0, 0, \dots)$ par récurrence. On utilise la propriété : $X^{i+1} = X \times X^i$ qui décale le coefficient 1 d'un rang.

⚠ X n'est pas une variable mais correspond au polynôme dont le seul coefficient non nul, égal à 1, est celui du 1er degré.

Exemples :
- $P = X^3 - 2X + 1$ est un polynôme unitaire de degré 3.
- $Q = 5X^4 + 3X^3 + 1$ est un polynôme de degré 4 et de coefficient dominant 5

1.4 L'anneau des polynômes

Théorème 2 : $\mathbb{K}[X]$ muni de la somme et du produit forme un anneau commutatif.

Démonstration : On montre facilement que $(\mathbb{K}[X]\ ,\ +)$ est un groupe commutatif avec le polynôme nul 0 comme élément neutre et comme opposé $-P$ dont tous les coefficients sont multipliés par (-1).

De même, on montre facilement que $(\mathbb{K}[X]\ ,\ \times)$ est commutatif, associatif et possède un élément neutre, le polynôme noté 1.

Enfin le produit est distributif par rapport à la somme.

Théorème 3 : Soient P et Q deux polynômes de $\mathbb{K}[X]$
- Degré de la somme : $d^\circ(P+Q) \leqslant \max(d^\circ P\ ,\ d^\circ Q)$
- Degré du produit : $d^\circ(PQ) = d^\circ P + d^\circ Q$

Démonstration :

$P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$ et p et q les degrés respectifs de P et Q
- Pour le degré de la somme cela est immédiat.
- Pour le degré du produit : si P ou Q nuls immédiat ($d^\circ P$ ou $d^\circ Q$ vaut $-\infty$), sinon

  1) $c_{p+q} = \sum_{k=0}^{p+q} a_k b_{p+q-k} = \sum_{k=0}^{p-1} a_k \underbrace{b_{p+q-k}}_{=0} + a_p b_q + \sum_{k=p+1}^{p+q} \underbrace{a_k}_{=0} b_{p+q-k} = a_p b_q \neq 0$

  2) $n > p+q,\quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{p} a_k \underbrace{b_{n-k}}_{=0} + \sum_{k=p+1}^{n} \underbrace{a_k}_{=0} b_{n-k} = 0$

  De 1) et 2), on a bien $d^\circ(PQ) = p+q$

Théorème 4 : $\mathbb{K}[X]$ est un anneau intègre c'est à dire :

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

Démonstration : Par le degré du produit (vraiment efficace) :
- $PQ = 0 \ \Rightarrow\ d^\circ(PQ) = -\infty$
- or $d^\circ(PQ) = d^\circ P + d^\circ Q$ donc $d^\circ P + d^\circ Q = -\infty$

Nécessairement $d^\circ P = -\infty$ ou $d^\circ Q = -\infty$ donc $P = 0$ ou $Q = 0$

1.5 Composition de polynômes

Définition 4 : Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q \in \mathbb{K}[X]$

On appelle composée de P par Q, le polynôme $P \circ Q = P(Q) = \sum_{k=0}^{+\infty} a_k Q^k$

On a alors si $d^\circ Q \geqslant 1$, $d^\circ(P \circ Q) = d^\circ P \times d^\circ Q$

Démonstration : Par produit sur Q : $\forall k \in [\![0, n]\!]$, $d^\circ(Q^k) = k\, d^\circ Q$.

Par somme si $d^\circ Q \geqslant 1$, $d^\circ(P \circ Q) = d^\circ\left(\sum_{k=0}^{p} a_k Q^k\right) \overset{a_p \neq 0}{=} d^\circ(Q^p) = d^\circ P \times d^\circ Q$

1.6 Dérivée d'un polynôme formel

Définition 5 : Soit $P \in \mathbb{K}[X]$ tel que : $P = \sum_{k=0}^{+\infty} a_k X^k$.

- On appelle polynôme dérivé le polynôme, noté P', tel que : $P' = \sum_{k=0}^{+\infty} k a_k X^{k-1}$
- On définit ensuite par récurrence les polynômes dérivés successifs avec la relation $P^{(n+1)} = \left(P^{(n)}\right)'$

  Pour $n = 2$, on utilisera la notation P''.

Exemple : Si $P = 2X^3 - X^2 - 5X + 1$, on a :

$P' = 6X^2 - 2X - 5$, $P'' = 12X - 2$, $P^{(3)} = 12$ puis $\forall n > 3$, $P^{(n)} = 0$

Remarque : Contrairement aux fonctions polynomiales, la dérivée des polynômes formels ne fait pas appel à la notion de limite.

Théorème 5 : Soient $P, Q \in \mathbb{K}[X]$ et $d^\circ P = p$.

- $\forall n \leqslant p$, $d^\circ P^{(n)} = p - n$ et $\forall n > p$, $P^{(n)} = 0$
- $(P + Q)^{(n)} = P^{(n)} + Q^{(n)}$
- $(PQ)' = P'Q + PQ'$
- Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$
- $(P \circ Q)' = Q' \times P' \circ Q$

Démonstration :

- Degré : mis à part le polynôme nul, la dérivée fait baisser le degré du polynôme de 1. Par récurrence, tant que $n \leqslant p$, on montre $d^\circ P^{(n)} = p - n$.
- Somme : rien à dire, immédiat.

- Produit de la dérivée 1re. Les coefficients sont un peu délicat à trouver.

  On pose : $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$.

  $PQ = \sum_{n=0}^{+\infty} c_n X^n$ avec $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

  Dans $(PQ)'$ pour obtenir le coefficient devant X^n, il faut dériver $c_{n+1}X^{n+1}$ qui donne $c'_n = (n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k}$

  Pour obtenir le coefficient devant X^n
  – Dans $P'Q$, il faut dériver chaque terme $a_{k+1}X^{k+1}$ et laisser le terme $b_{n-k}X^{n-k}$.
  – Dans PQ', il faut dériver chaque terme $b_{n+1-k}X^{n+1-k}$ et laisser le terme $a_k X^k$.

  On obtient alors dans $P'Q + PQ'$ pour le terme d_n devant X^n :

$$\begin{aligned} d_n &= \sum_{k=0}^{n} (k+1)\, a_{k+1} b_{n-k} + \sum_{k=0}^{n} (n+1-k)\, a_k b_{n+1-k} \\ &\overset{k=k+1}{=} \sum_{k=1}^{n+1} k\, a_k b_{n+1-k} + \sum_{k=0}^{n} (n+1-k)\, a_k b_{n+1-k} \\ &= \sum_{k=0}^{n+1} \left[k\, a_k b_{n+1-k} + (n+1-k)\, a_k b_{n+1-k}\right] = (n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k} = c'_n \end{aligned}$$

- Formule de Leibniz : par récurrence.

  Initialisation : : $n = 0$, $PQ^{(0)} = PQ$. La proposition est initialisée.

  Hérédité : Soit $n \in \mathbb{N}$. Supposons que $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$, montrons qu'elle reste vraie à l'ordre $n+1$.

$$\begin{aligned} (PQ)^{(n+1)} &= \left[PQ^{(n)}\right]' \overset{\text{HR}}{=} \left[\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\right]' \\ &= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\ &\overset{k=k+1}{=} \sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\ &= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n} \binom{n}{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{k=1}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} \\ &= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k}\right] P^{(k)} Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} \\ &\overset{\text{formule Pascal}}{=} P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)} \end{aligned}$$

  La proposition est héréditaire.

  Par initialisation et hérédité, la formule de Leibniz est donc vraie.

- Pour la composée : $P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k$ donc $(P \circ Q)' = \sum_{k=0}^{+\infty} a_k (Q^k)'$.

  On montre facilement par récurrence que $(Q^k)' = k Q' Q^{k-1}$ pour $k \in \mathbb{N}$

  On a alors : $(P \circ Q)' = \sum_{k=0}^{+\infty} a_k k Q' Q^{k-1} = Q' \times P' \circ Q$.

1.7 Fonction polynomiale

Théorème 6 : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.

On appelle valeur de P en un point $x \in \mathbb{K}$, l'élément de $\mathbb{K}$: $P(x) = \sum_{k=0}^{n} a_k x^k$

La fonction $x \mapsto P(x)$ de $\mathbb{K}$ dans $\mathbb{K}$ est appelée fonction polynomiale associée à P. Cette fonction est notée $\widetilde{P}$ lorsqu'on veut la distinguer de P.

$\forall P, Q \in \mathbb{K}[X]$, $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, et $\widetilde{(P')} = (\widetilde{P})'$

Remarque : La plupart du temps, on n'utilisera pas la notation $\widetilde{P}$, lorsqu'on voudra évaluer le polynôme en un point. On écrira par exemple $P(1)$, pour l'évaluation de P en 1.

2 Divisibilité et division euclidienne

Tout comme $\mathbb{Z}$ qui est un anneau commutatif, on peut définir dans l'anneau commutatif $\mathbb{K}[X]$ la notion de diviseur et multiple ainsi que de division euclidienne. La grande proximité de $\mathbb{Z}$ et $\mathbb{K}[X]$ permet de développer une arithmétique sur $\mathbb{K}[X]$

2.1 Multiple, diviseur

Définition 6 : Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B, s'il existe $P \in \mathbb{K}[X]$ tel que : $B = PA$. Cette relation se note $A|B$

Remarque : D'autre formulation sont possible :
« A est un diviseur de B », « B est divisible par A »,« B est un multiple de A »

Exemple : $X-2$ divise X^2+X-6 car $X^2 + X - 6 = (X-2)(X+3)$

Théorème 7 : Soient $A, B, C, D \in \mathbb{K}[X]$.

- Si A divise B et B divise A alors A et B sont égaux au produit d'une constante près. On dit que A et B sont associés sur $\mathbb{K}$.

$$A|B \text{ et } B|A \Leftrightarrow \exists \lambda \in \mathbb{K}^*, \ A = \lambda B$$

- Si D divise A et B alors D divise toute combinaison de A et de B :

$$D|A \text{ et } D|B \Rightarrow D|(AU + BV) \text{ avec } U, V \in \mathbb{K}[X]$$

- La divisibilité est compatible avec le produit :

$$A|B \text{ et } C|D \Rightarrow AC|BD \text{ et } A^k|B^k \text{ avec } k \in \mathbb{N}$$

2.2 Division euclidienne

Théorème 8 : Soient $A, B \in \mathbb{K}[X]$ et $B \neq 0$.

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

$$A = BQ + R \text{ avec } d^\circ R < d^\circ B$$

On appelle A le dividende, B le diviseur, Q le quotient et R le reste.

Démonstration : Il faut montrer l'existence et l'unicité du couple (Q, R).

- **Existence** : on pose $b = d^\circ B$ et β son coefficient dominant.
  1) Si B divise A alors il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On peut alors prendre $R = 0$ pour obtenir $A = BQ + R$.
  2) Si B ne divise pas A, alors l'ensemble des polynômes $A - BS$ avec $S \in \mathbb{K}[X]$ ne contient pas le polynôme nul et donc $d^\circ(A - BS) \in \mathbb{N}$.

     Toute partie non vide de $\mathbb{N}$ admet un plus plus petit élément. L'ensemble $\mathcal{E} = \{d^\circ(A - BK)\}_{K \in \mathbb{K}[X]}$ admet un plus petit élément r obtenu pour $S = Q$.

     On pose alors $R = A - BQ$ et ρ son coefficient principal avec $d^\circ R = r$.

     Raisonnons par l'absurde en supposant que $r \geqslant b$.

     $d^\circ\left(R - \dfrac{\rho}{\beta}X^{r-b}B\right) < r$ car $\dfrac{\rho}{\beta}X^{r-b}B$ supprime le terme dominant de R.

     Or $R - \dfrac{\rho}{\beta}X^{r-b}B = A - BQ - \dfrac{\rho}{\beta}X^{r-b}B = A - B\left(Q + \dfrac{\rho}{\beta}X^{r-b}\right)$

     est de la forme $A - BS$ et donc $d^\circ\left(R - \dfrac{\rho}{\beta}X^{r-b}B\right) \in \mathcal{E}$.

     Contradiction car r est le plus petit élément. On en déduit que $r < b$.

- **Unicité** : Supposons qu'il existe deux couples (Q_1, R_1) et (Q_2, R_2) vérifiant :

  $BQ_1 + R_1 = BQ_2 + R_2 \Leftrightarrow B(Q_1 - Q_2) = R_2 - R_1$ avec $r_1 < b$ et $r_2 < b$.

  Si $Q_1 \neq Q_2 \Rightarrow d^\circ(Q_1 - Q_2) \geqslant 0 \Rightarrow d^\circ[B(Q_1 - Q_2)] \geqslant b \Rightarrow d^\circ(R_2 - R_1) \geqslant b$

  Contradiction car $r_2 < b$ et $r_1 < b$. On en déduit alors que $Q_1 = Q_2$ et par suite que $R_1 = R_2$

Remarque : Ce que l'on pratiquait par exemple pour la décomposition en éléments simples s'en trouve justifié.

Par exemple : $\underbrace{2X^4 - X^3 - 2X^2 + 3X - 1}_{A} = \underbrace{(X^2 - X + 1)}_{B}\underbrace{(2X^2 + X - 3)}_{Q}\underbrace{-X + 2}_{R}$

$$\begin{array}{r|l}
2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\
\cline{2-2}
-2X^4 + 2X^3 - 2X^2 & 2X^2 + X - 3 \\
\cline{1-1}
0X^4 + X^3 - 4X^2 + 3X & \\
-X^3 + X^2 - X & \\
\cline{1-1}
0X^3 - 3X^2 + 3X - 1 & \\
3X^2 - 3X + 3 & \\
\cline{1-1}
0X^2 - X + 2 &
\end{array}$$

3 Racines d'un polynôme

3.1 Racines

Définition 7 : Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

On dit que λ est une racine de P sur $\mathbb{K}$ si, et seulement si, $P(\lambda) = 0$

Théorème 9 : Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$

λ est une racine de P sur $\mathbb{K}$ si, et seulement si, P est divisible par $(X - \lambda)$

Démonstration :

- Supposons que $P(\lambda) = 0$.

  La division de P par $(X - \lambda)$ donne $P = (X - \lambda)Q + R$ avec $r < 1$.

  R est donc un polynôme constant. Or $P(\lambda) = (\lambda - \lambda)Q + R(\lambda) = R(\lambda) = 0$ donc $R = 0$ et donc P est divisible par $(X - \lambda)$.
- Réciproquement : P est divisible par $(X - \lambda)$ donc $P = (X - \lambda)Q$. On a alors $P(\lambda) = (\lambda - \lambda)Q(\lambda) = 0$

Exemple : Soit $n \in \mathbb{N}$, déterminer le reste de la division de X^n par $X^2 - 6X + 5$.

- 1 et 5 sont racines de $X^2 - 6X + 5$ donc $X^2 - 6X + 5 = (X - 1)(X - 5)$
- Divisons X^n par $(X^2 - 6X + 5)$, $X^n = (X - 1)(X - 5)Q + R$ avec $d^\circ R \leqslant 2$

  R est du 1er degré donc $R = aX + b$ donc $X^n = (X - 1)(X - 5)Q + aX + b$
- Évaluons en 1 et 5, on obtient : $\begin{cases} a + b = 1 \\ 5a + b = 5^n \end{cases}$

  On obtient alors $a = \dfrac{5^n - 1}{4}$ et $b = \dfrac{3 - 5^n}{4}$ donc $R = \left(\dfrac{5^n - 1}{4}\right) X + \dfrac{3 - 5^n}{4}$

3.2 Multiplicité des racines

Définition 8 : Soient $P \in \mathbb{K}[X]$ non nul et $\lambda \in \mathbb{K}$

L'ensemble des entiers naturels k tel que $(X-\lambda)^k$ divise P possède un plus grand élément m appelé multiplicité de la racine λ dans P ou λ racine d'ordre m.

- Si $m = 0$ signifie que λ n'est pas racine de P car la multiplicité de λ est 0.
- Si $m = 1$ la racine λ est simple,
- Si $m = 2$ la racine λ est double, etc.

m est caractérisé par les deux propositions équivalentes suivantes :

- P est divisible par $(X-\lambda)^m$ mais pas par $(X-\lambda)^{m+1}$
- Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\lambda)^m Q$ avec $Q(\lambda) \neq 0$

Démonstration :
Soit $\mathcal{M}$ l'ensemble des entiers naturels k tel que $(X-\lambda)^k$ divise P.

- $\mathcal{M}$ est non vide car pour $k=0$, $(X-\lambda)^0 = 1$ qui divise P
- $\mathcal{M}$ est majoré par $d^\circ P$. En effet $\forall k \in \mathcal{M}$, $P = (X-k)^k Q$ avec $Q \in \mathbb{K}[X]$. P non nul donc Q non nul et donc $d^\circ Q \geqslant 0$. On a alors $d^\circ P = k + d^\circ Q \geqslant k$.

Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément donc m existe.

Théorème 10 : Formule de Taylor.

$$\forall P \in \mathbb{K}[X] \text{ et } \lambda \in \mathbb{K} : \quad P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$$

Démonstration : En deux temps.

- Pour $\lambda = 0$: on pose $P = \sum_{i=0}^{+\infty} a_i X^i$ et on dérive k fois, avec $k \in \mathbb{N}$:

  $P^{(k)} = \sum_{i=k}^{+\infty} \frac{i!\, a_i}{(i-k)!} X^{i-k}$ on évalue en 0 : $P^{(k)}(0) = \sum_{i=k}^{+\infty} \frac{i!}{(i-k)!} \underbrace{0^{i-k}}_{=0 \text{ sauf } i=k} = k!\, a_k$.

  D'où $a_k = \frac{P^{(k)}(0)}{k!}$ et par sommation $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} X^k$

- λ quelconque. On compose P avec $(X+\lambda)$. On remarquera $(X+\lambda)' = 1$

  $Q = P \circ (X+\lambda) = P(X+\lambda)$, on dérive k fois $Q^{(k)} = P^{(k)}(X+\lambda)$.

  Évaluation en 0 : $Q^{(k)}(0) = P^{(k)}(\lambda)$ donc $Q = \sum_{k=0}^{+\infty} \frac{Q^{(k)}(0)}{k!} X^k = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} X^k$

  $P = Q \circ (X-\lambda) = Q(X-\lambda) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$

Théorème 11 : Dérivées et multiplicité d'une racine.

λ racine d'ordre m dans $P \iff \forall k \in [\![0, m-1]\!]$, $P^{(k)}(\lambda) = 0$ et $P^{(m)}(\lambda) \neq 0$

Démonstration : Par double implication.

- λ racine d'ordre m dans P donc $P = (X-\lambda)^m Q$ avec $Q(\lambda) \neq 0$. (1)

$$P \overset{\text{Taylor}}{=} \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k}_{=R} + (X-\lambda)^m \underbrace{\sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m}}_{=Q}$$

$$= (X-\lambda)^m Q + R \quad (2)$$

(1) et (2) sont la division euclidienne de P par $(X-\lambda)^k$, en identifiant :

$R = 0 \overset{\text{par composition}}{\Rightarrow} R(X+\lambda) = 0 \Rightarrow \sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!} X^k = 0$ et par identification $P^{(k)}(\lambda) = 0, \quad \forall k \in [\![0, m-1]\!]$

- Réciproquement, $\forall k \in [\![0, m-1]\!]$, $P^{(k)}(\lambda) = 0$ et $P^{(m)}(\lambda) \neq 0$

$$P \overset{\text{Taylor}}{=} \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k}_{=0} + (X-\lambda)^m \underbrace{\sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m}}_{=Q}$$

$$= (X-\lambda)^m Q$$

de plus $Q(\lambda) = \underbrace{\sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} 0^{k-m}}_{=0 \text{ sauf } k=m} = \frac{P^{(m)}(\lambda)}{m!} \neq 0$

λ est donc une racine d'ordre m dans P.

3.3 Nombre maximale de racines

Théorème 12 : Soient $P \in \mathbb{K}[X]$ non nul.

Si $\lambda_1, \lambda_2, \ldots, \lambda_r$ sont des racines de multiplicité respectives $m_1, m_2, \ldots, m_r$, alors $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\ldots(X-\lambda_r)^{m_r}$ divise P et $\sum_{k=1}^{r} m_i \leqslant d^\circ P$

Le nombre de racines sur P, comptées avec multiplicité, est majoré par $d^\circ P$

Démonstration :
Par récurrence : $\forall k \in [\![1, r]\!]$, $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\ldots(X-\lambda_r)^{m_r}$ divise P.

Remarque : Le polynôme nul possède une infinité de racines.

Un polynôme de degré n n'a pas nécessairement n racines comptées avec multiplicité pour $\mathbb{K} = \mathbb{R}$, c'est la cas, par contre pour $\mathbb{K} = \mathbb{C}$ (corps algébriquement clos)

Exemple : Soit $P \in \mathbb{R}[X]$, de degré n et pour tous $k \in [\![1, n+1]\!]$, $P(k) = \frac{1}{k}$.
Montrer alors que $P(-1) = n+1$

L'astuce consiste à passer par un polynôme formel.

Soit le polynôme $Q = XP - 1$. On vérifie que pour tous $k \in [\![1, n+1]\!]$, $Q(k) = 0$.

- Détermination de Q.

  Donc $1, 2, \ldots, n+1$ sont $(n+1)$ racines de Q.

  Or le degré de Q vaut $(n+1)$ donc $Q = \lambda \prod_{k=1}^{n+1}(X-k)$.

  On détermine λ en évaluant en 0 : $Q(0) = \lambda \prod_{k=1}^{n+1}(-k) = (-1)^{n+1}\lambda\,(n+1)!$

  Or $Q(0) = -1$ donc $(-1)^{n+1}\lambda(n+1)! = -1 \Leftrightarrow \lambda = \dfrac{(-1)^n}{(n+1)!}$

  On a alors : $Q = \dfrac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(X-k)$.

- Calcul de $P(-1)$: $Q(-1) = -P(-1) - 1 \Leftrightarrow P(-1) = -1 - Q(-1)$

$$P(-1) = -1 - \frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(-1-k) = -1 - \frac{(-1)^n(-1)^{n+1}(n+2)!}{(n+1)!}$$
$$= -1 + (n+2) = n+1$$

3.4 Polynômes scindés et relations coefficient-racines

Définition 9 : Soit $P \in \mathbb{K}[X]$.

On dit que P est scindé sur $\mathbb{K}$ s'il est constant ou s'il s'écrit : $P = a\prod_{k=1}^{r}(X-\lambda_k)^{m_k}$ où $\lambda_1, \lambda_2, \ldots, \lambda_r$ sont les racines de P dans $\mathbb{K}$, de multiplicités respectives $m_1, m_2, \ldots, m_r$ et a son coefficient dominant.

P possède alors exactement $d^\circ P$ racines comptées avec multiplicité.

Remarque : Tout polynôme de $\mathbb{C}[X]$ est scindé ce qui n'est pas le cas de $\mathbb{R}[X]$.

Exemple : $\forall n \in \mathbb{N}^*, \quad X^n - 1 = \prod_{k=0}^{n-1}\left(X - e^{i\frac{2k\pi}{n}}\right)$

$X^n - 1$ admet comme racines les n racines de l'unité $e^{i\frac{2k\pi}{n}}$ pour $k \in [\![0, n-1]\!]$

Théorème 13 : Relations coefficients-racines.

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ scindé de degré n. Soit $\lambda_1, \lambda_2, \ldots, \lambda_n$ les n racines de P distinctes ou confondues.

$$\forall K \in [\![1, n]\!], \quad \sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_k} \quad \Rightarrow \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Remarque : σ_k, dont la définition peut dérouter au premier abord, correspond à la somme des produits de racines prises par 1, 2, ... n.

- Pour $n = 2$, il y a deux coefficients que l'on connaît bien avec $P = aX^2 + bX + c$:
  1) $\sigma_1 = \lambda_1 + \lambda_2 = -\dfrac{b}{c}$ qui est la somme des racines
  2) $\sigma_2 = \lambda_1\lambda_2 = \dfrac{c}{a}$ qui est le produit des racines.
- Pour $n = 3$, il y a trois coefficients avec $P = a_3X^3 + a_2X^2 + a_1X + a_0$:
  1) $\sigma_1 = \lambda_1 + \lambda_2 + \lambda_3 = -\dfrac{a_2}{a_3}$ qui est la somme des racines
  2) $\sigma_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = \dfrac{a_1}{a_3}$
  3) $\sigma_3 = \lambda_1\lambda_2\lambda_3 = -\dfrac{a_0}{a_3}$ qui est le produit des racines.
- Pour $n = 4$, il y a quatre coefficients avec $P = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$:
  1) $\sigma_1 = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = -\dfrac{a_3}{a_4}$ qui est la somme des racines
  2) $\sigma_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_1\lambda_4 + \lambda_2\lambda_3 + \lambda_2\lambda_4 + \lambda_3\lambda_4 = \dfrac{a_2}{a_4}$
  3) $\sigma_3 = \lambda_1\lambda_2\lambda_3 + \lambda_1\lambda_2\lambda_4 + \lambda_1\lambda_3\lambda_4 + \lambda_2\lambda_3\lambda_4 = -\dfrac{a_1}{a_4}$
  4) $\sigma_4 = \lambda_1\lambda_2\lambda_3\lambda_4 = \dfrac{a_0}{a_4}$ qui est le produit des racines.

Démonstration : Développement de la factorisation de P qui donne :

$$P = a_n \prod_{k=1}^{n}(X - \lambda_k) = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \cdots + (-1)^n \sigma_n\right)$$

Exemple : Somme et produit des racines de l'unité avec le polynôme $X^n - 1$:

$$\sigma_1 = \sum_{k=0}^{n} e^{i\frac{2k\pi}{n}} = 0 \ \ (a_{n-1} = 0) \quad \text{et} \quad \sigma_n = \prod_{k=0}^{n} e^{i\frac{2k\pi}{n}} = (-1)^{n+1} \ \ (a_0 = -1)$$

4 Formule d'interpolation de Lagrange

Le but de l'interpolation de Lagrange est d'approcher une fonction f par un polynôme en faisant correspondre un certain nombre n d'images de f avec une fonction polynomiale.
Par exemple si $n = 2$ l'interpolation est linéaire et si $n = 3$ l'interpolation est de Simpson (polynôme du second degré).

Définition 10 : Symbole de Kronecker. Soit I un ensemble d'indices.
On appelle symbole de Kronecker la fonction $\delta : \mathrm{I} \times \mathrm{I} \longrightarrow \{0, 1\}$ définie par :

$$\begin{cases} \delta(i,j) = 0 & \text{si } i \neq j \\ \delta(i,j) = 1 & \text{si } i = j \end{cases}$$

Il est d'usage de remplacer la notation $\delta(i,j)$ par δ_{ij}

Définition 11 : Polynômes de Lagrange. Soit $\mathrm{I} = [\![1, n]\!]$

Soit $x_1, x_2, \ldots, x_n \in \mathbb{K}$ distincts. On pose $\forall i \in \mathrm{I}, \quad L_i = \prod_{k \in \mathrm{I} \text{ et } k \neq i} \dfrac{X - x_k}{x_i - x_k}$

Les polynômes $L_1, L_2, \ldots, L_n$ sont appelés polynôme de Lagrange de $x_1, \ldots, x_n$.

On alors : $\forall i \in \mathrm{I}, \quad L_i(x_j) = \delta_{ij}$

Exemple : Pour $n = 3$

$$L_1 = \frac{(X - x_2)(X - x_3)}{(x_1 - x_2)(x_1 - x_3)}, \quad L_2 = \frac{(X - x_1)(X - x_3)}{(x_2 - x_1)(x_2 - x_3)}, \quad L_3 = \frac{(X - x_1)(X - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

Théorème 14 : Polynôme d'interpolation minimal.

Soient $x_1, x_2, \ldots, x_n \in \mathbb{K}$ et $y_1, y_2, \ldots, y_n \in \mathbb{K}$.

$P = \sum_{i=1}^{n} y_i L_i$ est l'unique polynôme de $\mathbb{K}_{n-1}[X]$ pour lequel $P(x_i) = y_i$ avec $i \in \mathrm{I}$

Remarque : $\mathbb{K}_{n-1}[X]$: ensemble des polynômes de degré inférieur ou égal à $(n-1)$

Démonstration :

- **Existence :** Soient $P = \sum_{i=1}^{n} y_i L_i$ et $\mathrm{I} = [\![1, n]\!]$.

  Les polynômes $(L_i)_{i \in I}$ sont de degré $(n-1)$ et donc par somme P aussi.

  De plus $\forall j \in \mathrm{I}, \quad P(x_j) = \sum_{i=1}^{n} y_i L_i(x_j) = \sum_{i=1}^{n} y_i \delta_{ij} = y_j$

- **Unicité :** Soient $P_1, P_2 \in \mathbb{K}_{n-1}[X]$ tels que $\forall i \in \mathrm{I}, \ P_1(x_i) = P_2(x_i) = y_i$.

  Le polynôme $P_1 - P_2$ admet $x_1, \ldots, x_n$ pour racines distinctes, donc le polynôme $P_1 - P_2$ admet au moins n racines et comme $d^\circ(P_1 - P_2) \leqslant n-1$, nécessairement $P_1 - P_2 = 0$ et donc $P_1 = P_2$.

Exemple : Soit la fonction f définie sur $[-1\,;\,1]$ par $f(x) = x\sin(\pi x)$ et $n = 5$

i	1	2	3	4	5
x_i	-1	$-0,5$	0	0,5	1
$y_i = f(x_i)$	0	0,5	0	0,5	0

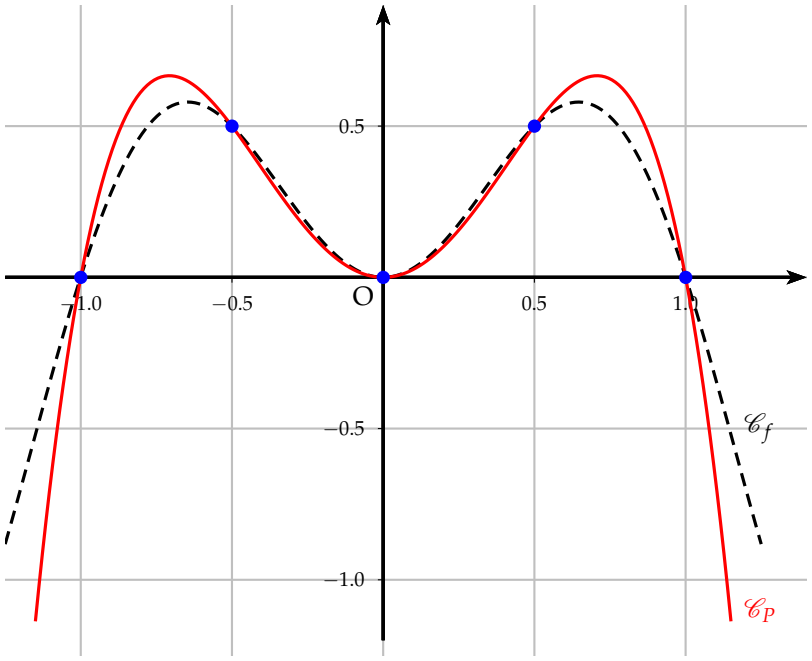
Le polynôme d'interpolation est alors $P = \sum_{i=1}^{5} y_i L_i = 0,5L_2 + 0,5L_4$

$$L_2 = \frac{(X+1)X(X-0,5)(X-1)}{(-0,5+1)(-0,5)(-0,5-0,5)(-0,5-1)} = \frac{-8X(X^2-1)(X-0,5)}{3}$$

$$L_4 = \frac{(X+1)(X+0,5)(X)(X-1)}{(0,5+1)(0,5+0,5)(0,5)(0,5-1)} = \frac{-8X(X^2-1)(X+0,5)}{3}$$

D'où : $P = \dfrac{-4X(X^2-1)(X-0,5)}{3} + \dfrac{-4X(X^2-1)(X+0,5)}{3} = \dfrac{-8X^2(X^2-1)}{3}$

On peut visualiser cette interpolation par le graphe suivant :



Théorème 15 : Polynômes d'interpolation, cas général.

En gardant les mêmes notation et en notant $P_{\min} = \sum_{i=1}^{n} y_i L_i$.

Les polynômes P pour lesquels $P(x_i) = y_i$ sont les polynômes de la forme :

$$P = P_{\min} + Q\prod_{k=1}^{n}(X - x_i), \quad Q \in \mathbb{K}[X]$$

Démonstration : Soit $P \in \mathbb{K}[X]$ et $\mathrm{I} = [\![1, n]\!]$.

$\forall i \in \mathrm{I},\ P(x_i) = y_i \ \Leftrightarrow\ \forall i \in \mathrm{I},\ P(x_i) = P_{\min}(x_i) \ \Leftrightarrow$

$(P - P_{\min})$ admet $x_1, \ldots, x_n$ pour racines $\Leftrightarrow\ \prod_{k=1}^{n}(X - x_i)$ divise $(P - P_{\min}) \ \Leftrightarrow$

$\exists Q \in \mathbb{K}[X], \quad P - P_{min} = Q\prod_{k=1}^{n}(X - x_i)$