ALGEBRE 1 PC/SF-Physique

Fiche 2 : Polynômes à une indéterminée

Une lecture conseillée

A) Les polynômes : des objets formels

Le nombre de solutions d'une équation polynomiale dépend de l'ensemble dans lequel on les cherche. Par exemple, l'équation $2x^2+5x=0$ admet 0 comme unique solution dans $\mathbb{Z}$ alors qu'elle en admet deux dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, tandis que l'équation $x^2-2=0$ n'a pas de solution dans $\mathbb{Z}$, ni même dans $\mathbb{Q}$, elle en admet deux dans $\mathbb{R}$ et pas d'autres dans $\mathbb{C}$, et l'équation $x^2+x+1=0$ n'a aucune solution dans $\mathbb{Z}$, pas plus dans $\mathbb{Q}$, ni dans $\mathbb{R}$, et en admet 2 dans $\mathbb{C}$. Pour déterminer le nombre de solutions d'une équation polynomiale on étudie les propriétés arithmétiques du polynôme associé dans le but de le factoriser au maximum.

Objets d'étude de ce chapitre, les polynômes ressemblent à ce que vous avez déjà croisé par le biais des fonctions polynomiales, mais vous comprendrez bientôt qu'il est important de les considérer comme des objets formels auxquels peuvent être associées des fonctions polynomiales bien différentes les unes des autres, tant par leurs natures que par certaines de leurs propriétés.
Par exemple au polynôme $X^0+X^1-5X^2+8X^3$, il pourra être naturel d'associer, selon le contexte :
- la fonction polynomiale de $\mathbb{Z}$ dans $\mathbb{Z}$ définie par : $s\mapsto 1+s-5s^2+8s^3$
- ou celle de $\mathbb{C}$ dans $\mathbb{C}$ définie par : $z\mapsto 1+z-5z^2+8z^3$
- ou encore celle de $\mathbb{R}^{\mathbb{R}}$ dans lui-même définie par : $f\mapsto Id_{\mathbb{R}}+f-5\ f^{\circ 2}+8f^{\circ 3}$
- ou bien d'autres encore, chaque fois qu'en remplaçant X par un objet mathématique $\heartsuit$, l'objet $\heartsuit^0+\heartsuit^1-5\heartsuit^2+8\heartsuit^3$ aura un sens bien défini.

Le fait d'appeler "**indéterminée**" le symbole X prend ainsi tout son sens.

Nous commencerons par des généralités sur les polynômes à coefficients dans un anneau $\mathcal{A}$ commutatif, unitaire et intègre , puis nous verrons que lorsque les coefficients sont pris dans un corps commutatif $\mathbb{K}$ comme $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'existence d'une division euclidienne permet d'obtenir dans ce cas des propriétés arithmétiques analogues à celles des entiers comme : pgcd, ppcm, irréductibles, identité de Bézout, lemme de Gauss, et un théorème de factorisation.

B) Polynômes sur un anneau commutatif, unitaire, intègre

$\mathcal{A}$ désignera ici un anneau commutatif, unitaire, intègre comme $\mathbb{Z},\mathbb{Q},\mathbb{R}$ ou $\mathbb{C}$.

Un polynôme P à une indéterminée X et à coefficients dans $\mathcal{A}$ est une **combinaison linéaire**

de "puissances" de X c-à-d une expression de la forme :

$$P=a_0X^0+a_1X^1\ +\ \cdots\ +\ a_nX^n\ \text{ en abrégé }\ \sum_{k=0}^{n}a_kX^k\ ,\quad \text{où les } a_k\in\mathcal{A}\ ,\ \text{et } a_n\neq 0\ .$$

Les a_k sont appelés **les coefficients de** P.

Le terme a_0X^0, souvent noté (abusivement) a_0 est appelé **le terme constant de** P.

Un polynôme s'identifie donc à une suite d'éléments de $\mathcal{A}$, indicée sur $\mathbb{N}$, nulle à partir d'un certain rang.

Ainsi, par construction même, deux polynômes sont égaux s'ils ont la même suite de coefficients.

L'ensemble de ces polynômes est noté $\mathcal{A}[X]$.

Un polynôme qui se réduit à un seul terme est plutôt appelé un **monôme**, exemple : $15X^6$.

Si P n'est pas le polynôme nul, la plus grande puissance de X présente dans P est appelée **le degré de** P.

$$\deg(P)\underset{déf}{=}\max\{k\in\mathbb{N}\mid a_k\neq 0\}$$

Pour $a\neq 0$, on a $\deg(aX^0)=0$ et par convention le degré du polynôme nul $0X^0$ est pris égal à $-\infty$
(on verra pourquoi un peu plus loin).

Le coefficient $a_{\deg(P)}$ s'appelle le **coefficient dominant** de P.

Un polynôme est dit **unitaire** si son coefficient dominant est égal à 1 (l'unité de $\mathcal{A}$).
Exemples : $2X^0-5X+X^3$ est un polynôme de $\mathbb{Z}[X]$, unitaire, de degré 3.
$3X^0-\sqrt{5}X+X^3-2X^5\in\mathbb{R}[X]$ est de degré 5, non unitaire car de coefficient dominant -2 .

Fonction polynomiale sur $\mathcal{A}$ associée à un polynôme de $\mathcal{A}[X]$:

Pour $P=\sum_{k=0}^{n}\lambda_kX^k\in\mathcal{A}[X]$, on notera $\widetilde{P}$ la fonction polynomiale sur $\mathcal{A}$ définie par : $\forall a\in\mathcal{A}$, $\widetilde{P}(a)=\sum_{k=0}^{n}\lambda_ka^k$.

Si $\deg(P)<1$ on dit que P est un polynôme constant, $\widetilde{P}$ est alors une fonction constante.

C) Les Opérations dans $\mathcal{A}[X]$, et leurs propriétés.

L'addition

$$\sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{p} b_k X^k \underset{déf}{=} \sum_{k=0}^{\max(n,p)} (a_k + b_k) X^k$$

où par convention $a_k = 0$ si $n < k \leqslant p$ et $b_k = 0$ si $p < k \leqslant n$,
est associative, commutative, admet pour neutre le polynôme nul, et l'opposé d'un polynôme est le polynôme de coefficients opposés.

Degré d'une somme : $\forall P, Q \in \mathcal{A}[X]$ on a $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$, avec égalité si les coefficients dominants de P et Q ne sont pas opposés .

La multiplication

$$\sum_{k=0}^{n} a_k X^k \times \sum_{k=0}^{p} b_k X^k \underset{déf}{=} \sum_{k=0}^{n+p} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

est associative, commutative, admet pour neutre X^0 (souvent identifié à l'unité de $\mathcal{A}$ notée 1) , admet le polynôme nul comme élément absorbant, et elle est distributive par rapport à l'addition.
Les polynômes inversibles sont ceux de la forme αX^0 avec α inversible dans $\mathcal{A}$, et $\left(\alpha X^0\right)^{-1} = \alpha^{-1} X^0$.

Degré d'un produit : $\forall P, Q \in \mathcal{A}[X]$ on a $\deg(PQ) = \deg(P) + \deg(Q)$
On voit que pour que cette propriété reste vraie quand l'un des polynômes est nul, on est amené à convenir que le degré du polynôme nul est égal à $-\infty$.

Multiples, diviseurs et racines :

Soient $P, Q \in \mathcal{A}[X]$, on dit que P est un **multiple** de Q, ou que Q **divise** P et on note $Q|P$, s'il existe $T \in \mathcal{A}[X]$ tel que $P = QT$.

Un élément $\alpha \in \mathcal{A}$ est une **racine de** $P \underset{déf}{\iff} (X - \alpha X^0)$ divise P.

Proposition : $\alpha \in \mathcal{A}$ est une racine de $P \iff \widetilde{P}(\alpha) = 0$. *Preuve en factorisant* $(X^k - \alpha^k X^0)$ *par* $(X - \alpha X^0)$

Une racine α de P est dite **de multiplicité** $m \underset{déf}{\iff} m$ est le plus grand entier tel que $(X - \alpha X^0)^m$ divise P.

Propriété fondamentale du nombre de racines :
Un polynôme $P \in \mathcal{A}[X]$ de degré n admet au plus n racines comptées avec multiplicité.
Preuve : par l'absurde sur le degré de P.

Diviseurs triviaux d'un polynôme et polynômes irréductibles :

Tous les polynômes de la forme αX^0 ou $\alpha X^0\ P$ avec α inversible dans $\mathcal{A}$ divisent trivialement le polynôme P, on les appelle les **diviseurs triviaux** de P.

Un polynôme non inversible est dit **irréductible** dans $\mathcal{A}[X]$ si ses seuls diviseurs sont ses diviseurs triviaux.

Propriété : Les polynômes unitaires de degré 1 sont irréductibles dans $\mathcal{A}[X]$.

Deux polynômes P et Q sont dits **associés** si ($P|Q$ et $Q|P$), il existe alors α inversible dans $\mathcal{A}$ tel que $P = \alpha X^0\ Q$.

Propriété fondamentale des diviseurs communs : Si D divise P et Q alors $\forall\ U, V \in \mathcal{A}[X]$ D divise $PU + QV$.

Deux polynômes sont dits **premiers entre eux** s'ils n'ont aucun diviseur commun irréductible.

Le produit externe

$\forall a \in \mathcal{A}$ et $\forall P \in \mathcal{A}[X]$, on définit $aP \in \mathcal{A}[X]$ par : $aP \underset{déf}{=} aX^0 \times P$

Si $a = 0$ on obtient $aP = 0X^0$ et si $a \neq 0$ on a $\deg(aP) = \deg(P)$.

De plus on peut vérifier que $\forall a, b \in \mathcal{A}$ et $\forall P, Q \in \mathcal{A}[X]$,
$$\begin{cases} (a+b)P &= aP + bP \\ (ab)P &= a(bP) \\ a(P+Q) &= aP + aQ \\ a(P \times Q) &= (aP) \times Q = P \times (aQ) \end{cases}$$

La composition

Pour $P, Q \in \mathcal{A}[X]$, en substituant Q à X dans P, on définit dans $\mathcal{A}[X]$ le composé $P \circ Q \underset{déf}{=} P(Q)$.

Propriétés :

Généralement $P \circ Q \neq Q \circ P$.

Si P et Q sont non nuls alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

D'autre part, $\forall P_1, P_2, Q \in \mathcal{A}[X]$ et $\forall a_1, a_2 \in \mathcal{A}$,
$$\begin{cases} (a_1 P_1 + a_2 P_2) \circ Q = & a_1\ P_1 \circ Q + a_2\ P_2 \circ Q \\ (P_1 P_2) \circ Q = & (P_1 \circ Q) \times (P_2 \circ Q) \end{cases}$$

On peut remarquer aussi que $\forall \alpha \in \mathcal{A}$, $P \circ (\alpha X^0) = \widetilde{P}(\alpha) X^0$

La dérivation formelle

Par analogie avec la dérivation des fonctions polynomiales réelles, pour $P = \left(\sum_{k=0}^{n} a_k X^k\right)$ on définit

le polynôme dérivé formel : $P' \underset{déf}{=} \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$.

Remarques : $P' = 0 \Longleftrightarrow P$ est un polynôme constant.
Si P n'est pas constant on a $\deg(P') = \deg(P) - 1$.

La dérivation formelle des polynômes a les mêmes propriétés algébriques que la dérivation usuelle des fonctions :

Elle est linéaire : $\forall P, Q \in \mathcal{A}[X]$ et $\forall a \in \mathcal{A}$, $\begin{cases} (P+Q)' = & P' + Q' \\ (aP)' = & a\ P' \end{cases}$

Dérivation d'un produit : $\forall P, Q \in \mathcal{A}[X]$ on a $(PQ)' = P'Q + PQ'$

Dérivation d'un composé : $\forall P, Q \in \mathcal{A}[X]$ on $(P \circ Q)' = (P' \circ Q) \times Q'$

Dérivés d'ordres supérieurs : Pour tout $P \in \mathcal{A}[X]$ et $k \in \mathbb{N}$ on pose $\begin{cases} P^{(0)} = & P \\ P^{(k+1)} = & \left(P^{(k)}\right)' \end{cases}$ et pour $s \in \mathbb{N}$ on appelle **dérivé d'ordre s de P** le polynôme $P^{(s)}$ ainsi défini par récurrence.

On a en particulier : $\left(X^k\right)^{(s)} = \begin{cases} \frac{k!}{(k-s)!}\ X^{k-s} & \text{quand } s < k \\ s!\ X^0 & \text{quand } s = k \\ 0 & \text{quand } s > k \end{cases}$

Pour $P = \sum_{k=0}^{n} a_k X^k$ on obtient alors $P^{(s)} = \begin{cases} 0 & \text{quand } s > n \\ \sum_{k=s}^{n} \left(\frac{k!}{(k-s)!} a_k X^{k-s}\right) & \text{quand } s \leqslant n \end{cases}$.

On remarque que $\forall k \geqslant s$, $\frac{k!}{(k-s)!} = s!\ C_k^s$ où C_k^s est le *nombre de combinaisons* de s éléments pris parmi k,

on peut ainsi réécrire pour $s \leqslant n$: $P^{(s)} = s! \sum_{k=s}^{n} \left(C_k^s\ a_k\ X^{k-s}\right)$

Propriété : Soit $P, Q \in \mathcal{A}[X]$ et m un entier $\geqslant 1$.
Si Q^m divise P alors Q^{m-1} divise P', et par suite $\forall k \in \{1, \cdots, m-1\}$, Q^{m-k} divise $P^{(k)}$.

Preuve : Si Q^m divise P, on a $P = Q^m P_1$ et donc $P' = mQ^{m-1}Q'P_1 + Q^m P_1' = Q^{m-1} \times (mQ'P_1 + QP_1')$
ce qui met en évidence que Q^{m-1} divise P'.

Remarque : Les définitions et propriétés vues jusqu'ici sont valables pour les polynômes à coefficients dans un anneau $\mathcal{A}$ commutatif, unitaire et intègre. Comme certains coefficients peuvent ne pas être inversibles, l'étude des propriétés arithmétiques de ces polynômes : diviseurs, diviseurs communs, irréductibles, décomposition en produit d'irréductibles etc... qui permettent de simplifier la recherche des racines, est une tache ardue dans ce contexte. Déjà avec $\mathcal{A} = \mathbb{Z}$, un polynôme de degré 1 peut ne pas avoir de racine, un de degré 2 peut posséder aucune, une seule ou deux racines. Pour appréhender les propriétés de ces polynômes, l'idée est alors de les "plonger" dans un ensemble plus grand dont l'arithmétique est plus simple à étudier.
On le fait en "plongeant" $\mathcal{A}$ dans un corps commutatif $\mathbb{K}$, où seul le coefficient 0 ne sera pas inversible.

D) Arithmétique des polynômes sur un corps commutatif $\mathbb{K}$ (exemples $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$)

$\mathbb{K}[X]$ désigne l'anneau des polynômes à coefficients dans $\mathbb{K}$, les éléments de $\mathbb{K} \setminus \{0\}$ sont inversibles.

Les inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0 (constants non nuls).

Tout $P \neq 0$ de $\mathbb{K}[X]$ est associé dans $\mathbb{K}[X]$ à un unique polynôme unitaire, le normalisé P_u de P :

$$P_u \underset{déf}{=} \frac{1}{a_{\deg(P)}}\ P$$

Division euclidienne dans $\mathbb{K}[X]$:

Théorème : $\forall A, B \in \mathbb{K}[X]$ avec $B \neq 0X^0$, il existe un couple unique $(Q, R) \in (\mathbb{K}[X])^2$, tel que

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

Q s'appelle le **quotient** et R le **reste** de la division euclidienne de A par B.
Conséquence : Dans $\mathbb{K}[X]$ on a alors $B|A \Longleftrightarrow R = 0$.

Pgcd de deux polynômes de $\mathbb{K}[X]$:

Si D divise A et B, on a $\deg(D) \leqslant \min(\deg(A), \deg(B))$. Parmi tous les diviseurs communs à A et B, certains sont donc de degré maximal, on les appelle "des pgcd" de A et B.

Propriété-Définition :
Tout diviseur commun à A et B divise les restes successifs de l'**algorithme d'Euclide** appliqué à A et B.
Cela permet de voir que le dernier reste non nul R_d de cet algorithme est un pgcd de A et B.

Ainsi tous "les pgcd" de A et B divisent R_d et ont même degré (maximal) que lui, on en déduit qu'ils sont tous associés entre eux, ils ont donc le même normalisé :

$$\textbf{le pgcd de } A \textbf{ et } B \text{ noté } A \wedge B \underset{déf}{=} (R_d)_u$$

Conséquence : Les diviseurs communs à A et B sont les diviseurs de $A \wedge B$.

Deux polynômes **sont dits premiers entre eux** s'ils n'ont comme seuls diviseurs communs que les diviseurs triviaux : les inversibles de $\mathbb{K}[X]$, c'est à dire les polynômes de degré 0. Ainsi A et B sont premiers entre eux si $A \wedge B = X^0$.

Théorème de Bézout : A et $B \in \mathbb{K}[X]$ sont premiers entre eux $\iff \exists\, U, V \in \mathbb{K}[X]$ tels que $AU + BV = X^0$.

De plus, $\forall A, B, C \in \mathbb{K}[X]$, l'équation $AU + BV = C$ admet dans $(\mathbb{K}[X])^2$ des couples (U, V) solutions
si et seulement si C est multiple de $A \wedge B$.

Lemme de Gauss : Soit $A, B, C \in \mathbb{K}[X]$, si A divise BC et A est premier avec B , alors A divise C.

Propriété des diviseurs premiers entre eux :
Si B et C sont premiers entre eux et chacun d'eux divise A alors leur produit BC divise A aussi.

Propriété des irréductibles :
Soit P un irréductible et $A \in \mathbb{K}[X]$. Si P ne divise pas A alors il est premier avec A
ou sa contraposée : si un irréductible P n'est pas premier avec A alors il le divise.

Lemme d'Euclide : Si un irréductible P divise BC alors il divise B ou C (ou les deux).

Remarque : Les polynômes de degré 1 sont des irréductibles dans $\mathbb{K}[X]$.

Racines d'un polynôme de $\mathbb{K}[X]$:
$\forall P \in \mathbb{K}[X]$ et $\forall \alpha \in \mathbb{K}$, $\quad \alpha$ est **une racine de** $P \underset{déf}{\iff}$ le reste de la division euclidienne de P par $(X - \alpha X^0)$ est nul
$\iff \widetilde{P}(\alpha) = 0.$

Multiplicité d'une racine :
On rappelle que $\alpha \in \mathbb{K}$ est une racine de P de multiplicité m si m est le plus grand entier tel que $(X - \alpha X^0)^m$ divise P, et qu'un polynôme de degré $n \geqslant 1$ admet au plus n racines comptées avec leurs multiplicités.

Théorème fondamental de d'Alembert-Gauss : (admis)

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.

Corollaire : Tout $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$ admet exactement n racines comptées avec leurs multiplicités.

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

Théorème de factorisation dans $\mathbb{C}[X]$:
Tout polynôme non constant $P \in \mathbb{C}[X]$ se factorise complètement, de manière unique à l'ordre près des facteurs, sous la forme

$$P = \lambda \prod_{k=1}^{p} \left(X - \alpha_k X^0\right)^{m_k}$$

où λ est le coefficient dominant de P, $\alpha_1, \cdots, \alpha_p$ sont les racines complexes distinctes de P, et $m_1, \cdots, m_p$ leurs multiplicités respectives.

Relations symétriques de Viète sur les racines de $P \in \mathbb{C}[X]$:

Pour $P = \sum_{k=0}^{n} a_k X^k$ de degré n et $\alpha_1, \cdots, \alpha_n$ ses n racines complexes (certaines étant éventuellement égales) on a :

$$\forall k \in \{1, \cdots, n\}, \qquad \frac{(-1)^k a_{n-k}}{a_n} = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \alpha_{i_1} \cdots \alpha_{i_k} \qquad \textit{la somme des produits } k \textit{ à } k \textit{ des racines de } P.$$

Propriété fondamentale des racines d'un polynôme $P \in \mathbb{R}[X]$:
Comme $\mathbb{R} \subset \mathbb{C}$, on a aussi $P \in \mathbb{C}[X]$ et si β est une racine complexe de P de multiplicité μ alors son conjugué $\bar{\beta}$ est aussi une racine de P de multiplicité μ.

Conséquence : Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Théorème de factorisation dans $\mathbb{R}[X]$

Tout polynôme non constant $P \in \mathbb{R}[X]$ se factorise complètement de manière unique, à l'ordre près des facteurs, sous la forme

$$P = \lambda \prod_{k=1}^{p} \left(X - \alpha_k X^0\right)^{m_k} \times \prod_{\ell=1}^{s} \left(X^2 - 2Re(\beta_\ell)\ X + |\beta_\ell|^2\ X^0\right)^{\mu_\ell}$$

où λ est le coefficient dominant de P, $\alpha_1, \cdots, \alpha_p$ sont les racines réelles distinctes de P avec $m_1, \cdots, m_p$ leurs multiplicités respectives, et $\beta_1, \cdots, \beta_s$ les racines complexes distinctes de P de partie imaginaires strictement positives (ou strictement négatives, au choix), avec $\mu_1, \cdots, \mu_s$ leurs multiplicités respectives.

Remarque Le nombre $m_1 + \cdots + m_p$ des racines réelles, comptées avec leurs multiplicités respectives, d'un polynôme $P \in \mathbb{R}[X]$ est donc de même parité que le degré de P.
Par exemple, un polynôme de degré impair qui admet deux racines réelles (éventuellement égales) admet forcément au moins une troisième racine réelle (éventuellement égale à l'une des deux précédentes).

E) Caractérisation et remarques sur les racines d'un polynôme et leurs multiplicités

Pgcd de n polynômes $P_1, \cdots, P_n \in \mathbb{K}[X]$

Parmi tous les diviseurs communs à $P_1, \cdots, P_n$ ceux de degré maximal sont associés entre eux, ils ont donc le même polynôme unitaire qu'on appelle **le pgcd de** $P_1, \cdots, P_n$ et qui est noté $P_1 \wedge P_2 \wedge \cdots \wedge P_n$.

Propriétés :

a) Les diviseurs communs à $P_1, \cdots, P_n$ sont les diviseurs de $P_1 \wedge P_2 \wedge \cdots \wedge P_n$.

b) Pour calculer $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ on peut regrouper les termes comme bon nous semble, on dit que $\wedge$ est associatif.
Par exemple $P_1 \wedge P_2 \wedge P_3 = P_1 \wedge (P_2 \wedge P_3) = (P_1 \wedge P_2) \wedge P_3$.
On peut tout autant les permuter à notre guise, $\wedge$ est commutatif, on a ainsi par exemple
$P_1 \wedge P_2 \wedge P_3 = P_1 \wedge (P_3 \wedge P_2) = (P_2 \wedge P_3) \wedge P_1 = \cdots$
Pour calculer $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ on peut donc remplacer quelques polynômes de notre choix par leur pgcd.

Théorème sur les racines multiples : Les racines multiples de P sont les racines de $P \wedge P'$.

Plus précisément, les racines de multiplicité m ($\geqslant 2$) de P sont les racines de $P \wedge P' \wedge \cdots \wedge P^{(m-1)}$ qui ne sont pas racine de $P^{(m)}$.
Pour les déterminer, on pourra utiliser l'associativité de $\wedge$, par exemple en commençant par chercher les racines de $P^{(m-2)} \wedge P^{(m-1)}$ (qui est de degré $\leqslant \deg(P) - m + 1$), et vérifier lesquelles d'entre elles sont aussi racines de $P^{(m-3)}$, et de $\cdots$, et de P', et de P, mais pas de $P^{(m)}$.

Formule de Taylor formelle et racines multiples

Formule de Taylor formelle de P en $a \in \mathcal{A}$
Il s'agit d'écrire le polynôme P sous forme d'une combinaison linéaire des puissances de "$X-a$" c'est-à-dire de $X - aX^0$

Remarquons tout d'abord que $X = \left(aX^0 + X\right) \circ \left(X - aX^0\right)$,
il s'ensuit que $P \circ X = P \circ \left(aX^0 + X\right) \circ \left(X - aX^0\right)$.

Comme $P \circ X = P$ et que la composition est associative on en déduit que $P = \left[P \circ \left(aX^0 + X\right)\right] \circ \left(X - aX^0\right)$.

Pour $P = \sum_{k=0}^{n} a_k X^k$ on a successivement

$$\begin{aligned}
P \circ \left(aX^0 + X\right) &= \sum_{k=0}^{n} a_k \left(aX^0 + X\right)^k \\
&= \sum_{k=0}^{n} a_k \left(\sum_{s=0}^{k} C_k^s\ a^{k-s} X^s\right) \\
&= \sum_{k=0}^{n} \left(\sum_{s=0}^{k} C_k^s\ a_k\ a^{k-s} X^s\right) \qquad \text{(somme triangulaire ligne par ligne)} \\
&= \sum_{s=0}^{n} \left(\sum_{k=s}^{n} C_k^s\ a_k\ a^{k-s} X^s\right) \qquad \text{(somme triangulaire colonne par colonne)} \\
&= \sum_{s=0}^{n} \left(\sum_{k=s}^{n} C_k^s\ a_k\ a^{k-s}\right) X^s
\end{aligned}$$

En composant maintenant par $(X - aX^0)$ et en reconnaissant l'expression $\sum_{k=s}^{n} C_k^s \; a_k \; a^{k-s}$ liée au polynôme dérivé d'ordre s de P, on obtient la forme escomptée :

Formule de Taylor formelle de P en $a \in \mathcal{A}$ $\qquad P = \sum_{s=0}^{n} \frac{\widetilde{P^{(s)}}(a)}{s!} \left(X - aX^0\right)^s$

On voit alors facilement sur cette expression que a est une racine de P de multiplicité au moins m si et seulement si $\sum_{s=0}^{m-1} \frac{\widetilde{P^{(s)}}(a)}{s!} \left(X - aX^0\right)^s$ est divisible par $\left(X - aX^0\right)^m$, or ce polynôme est de degré $< m$, ce qui permet de voir que cela est équivalent à sa nullité, c'est à dire à la nullité de tous ses coefficients.
On retrouve ainsi le théorème sur les racines de multiplicité m.
Le lecteur averti notera ici que ce théorème est donc valable pour les polynômes de $\mathcal{A}[X]$, à condition que les simplifications par les $s!$ soient licites dans l'anneau $\mathcal{A}$, c'est le cas pour les *anneaux de caractéristique zéro* , comme $\mathbb{Z}$ par exemple.

Deux lectures sur le nombre des racines réelles d'un polynôme de $\mathbb{R}[X]$

La règle des signes de Descartes

Le théorème des suites de Sturm