# POLYNOMES

Le but de ce complément est d'approfondir et de systématiser vos connaissances sur les polynômes. Jusqu'à présent, et notamment dans le chapitre 34 de "Toutes les mathématiques" (TLM1), les polynômes ont été vus comme des *fonctions* de $\mathbb{R}$ dans $\mathbb{R}$. Ici, nous les considérons d'un point de vue plus *algébrique*, comme des objets mathématiques sur lesquels sont définies des opérations (addition, multiplication, division euclidienne...). On parle alors de *polynômes formels*. Ce point de vue permet de mieux mettre en valeur la parenté des propriétés des polynômes formels avec celles d'autres objets mathématiques (entiers relatifs par exemple).

Pour indiquer qu'il s'agit de polynômes formels, la variable sera notée $X$ au lieu de $x$. On remarquera que les propriétés des polynômes formels ne remplacent pas celles des fonctions polynômes, bien au contraire ; les deux points de vue s'enrichissent mutuellement.

## 1 Polynômes formels

Dans tout ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Un *polynôme* de l'*indéterminée* $X$, à *coefficients* dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, est une expression de la forme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \tag{1}$$

où les $a_i \in \mathbb{K}$. On note $\mathbb{K}[X]$ l'ensemble des *polynômes à coefficients dans* $\mathbb{K}$.

La *définition théorique* d'un polynôme est un peu plus compliquée, puisqu'un polynôme est une suite $(a_k)_{k\in\mathbb{N}}$ (dite des coefficients) nulle à partir d'un certain rang. Ce qu'il faut comprendre dans cette définition, c'est que l'on peut toujours ajouter des termes dans un polynôme. Par exemple $P = 1 + 2X + 3X^2$ peut aussi s'écrire $P = 1 + 2X + 3X^3 + 0 \times X^4 + 0 \times X^5$, etc. Cela permet d'écrire deux polynômes $P$ et $Q$ sous forme condensée, avec le même domaine de sommation :

$$P = \sum_{k=0}^{n} a_k X^k \ ; \ Q = \sum_{k=0}^{n} b_k X^k, \tag{2}$$

Cela signifie que $P$ et $Q$ sont de degré au plus $n$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus $n$.

Si $P$ est un polynôme, on définit son *degré*, noté $\deg P$ comme l'indice du dernier coefficient non nul. Plus précisément, si la suite des coefficients de $P$ est $(a_k)_{k\in\mathbb{N}}$, alors $d$ est le degré de $P$ si et seulement si $a_d \neq 0$ et si $a_k = 0$ pour $k > d$.

Par définition, le coefficient $a_d$ n'est pas nul. Ce coefficient est dit *coefficient dominant* de $P$. Lorsque le coefficient dominant vaut $1$, on dit que $P$ est *unitaire* ou *normalisé*.

Par convention, le degré du polynôme nul est $-\infty$, et on convient que pour tout entier $n$, $-\infty < n$, $-\infty + n = -\infty$ et que $(-\infty) + (-\infty) = -\infty$.

Nous définissons maintenant, du point de vue formel, les premières opérations sur les polynômes. Si $P$ et $Q$ sont deux polynômes formels écrits comme en (2) , et si $\lambda \in \mathbb{K}$, on pose

$$\lambda P = \sum_{k=0}^{n} (\lambda a_k) X^k ; P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k \tag{3}$$

Puisque les termes dominants de $P$ et $Q$ peuvent s'annuler lorsqu'on les ajoute, il est clair que

$$\deg(P + Q) \leq \max(\deg P, \deg Q). \tag{4}$$

avec égalité si $\deg P \neq \deg Q$. De plus, si $\lambda \neq 0$, on a

$$\deg(\lambda P) = \deg P. \tag{5}$$

**Exemple 1** Soit $P = (X+1)^n$ et $Q = (X-1)^n$ pour $n \in \mathbb{N}$. En développant par la formule du binôme de Newton, on voit que

$$P + Q = \sum_{k=0}^{n} \binom{n}{k} \left(1 + (-1)^{n-k}\right) X^k.$$

Le terme en facteur de $X^n$ est donc 2. Ainsi $\deg(P+Q) = \deg P = \deg Q$.

Par contre on voit que $P - Q = \sum_{k=0}^{n} \binom{n}{k} \left(1 - (-1)^{n-k}\right) X^k$.

Ainsi $\deg(P-Q) < \max[\deg P, \deg(-Q)]$ ; les termes de plus haut degré de $P$ et $Q$ s'éliminent dans ce cas.

Si $P$ et $Q$ sont deux polynômes formels écrits comme en (2), on définit leur produit $PQ$ en distribuant les coefficients de $P$ sur ceux de $Q$ comme lorsqu'on calcule dans $\mathbb{R}$, c'est-à-dire

$$\begin{aligned} PQ &= \left(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n\right)\left(b_0 + b_1 X + b_2 X^2 + \cdots + b_n X^n\right) \\ &= (a_0 b_0) + (a_0 b_1 + a_1 b_0) X + \cdots + (a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0) X^{2n}. \end{aligned}$$

De manière condensée, on a

$$\left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{k=0}^{n} b_k X^k\right) = \sum_{i=0}^{2n} c_i X^i \text{ , avec } c_i = \sum_{k=0}^{i} a_k b_{i-k}. \tag{6}$$

On notera que, dans l'expression du coefficient $c_i$, la somme des indices $k$ et $i-k$ est constante et égale à $i$. En effet, pour obtenir le coefficient de $X^i$ dans le produit $PQ$, on additionne tous les produits $a_k X^k \times b_{i-k} X^{i-k} = a_k b_{i-k} X^i$.

L'expression (6) du coefficient du produit peut être utile dans certains cas.

**Remarque 1** $(\mathbb{K}[X], +, \times)$ est un anneau commutatif (voir le complément de cours "Anneaux et corps").

**Exemple 2** Soit $P = Q = (X+1)^n$. Alors on a

$$PQ = (X+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} X^i. \tag{7}$$

Mais en développant $P$ et $Q$ par la formule du binôme, on a aussi par (6) :

$$PQ = \left(\sum_{k=0}^{n} \binom{n}{k} X^k\right)\left(\sum_{k=0}^{n} \binom{n}{k} X^k\right) = \sum_{i=0}^{2n} \left[\sum_{k=0}^{i} \binom{n}{k}\binom{n}{i-k}\right] X^i, \tag{8}$$

avec la convention $\binom{n}{p} = 0$ si $p > n$. En comparant les termes de degré $i$ dans (7) et (8), on obtient

$$\sum_{k=0}^{i} \binom{n}{k}\binom{n}{i-k} = \binom{2n}{i}. \tag{9}$$

Si nous nous intéressons au degré du produit de deux polynômes, nous voyons immédiatement que

$$\deg(PQ) = \deg P + \deg Q. \tag{10}$$

On notera que cette propriété demeure vraie si $P = 0$. En effet, dans ce cas, on a défini $\deg P = -\infty$, et $-\infty + \deg Q = -\infty$. On en déduit le

**Théorème 1** *Soient $P$ et $Q$ dans $\mathbb{K}[X]$. Alors*

$$PQ = 0 \iff (P = 0 \text{ ou } Q = 0). \tag{11}$$

On traduit ce résultat en disant que l'anneau $\mathbb{K}[X]$ est *intègre* (voir le complément de cours "Anneaux et corps").

**Démonstration** Si $P = 0$ ou $Q = 0$, il est clair que $PQ = 0$. Réciproquement, par contraposition, si $P \neq 0$ et $Q \neq 0$ alors $\deg P \geq 0$ et $\deg Q \geq 0$ car le polynôme nul est le seul qui ait un degré négatif (égal à $-\infty$). Donc $\deg(PQ) \geq 0$. Ainsi $PQ \neq 0$.

# 2 Divisibilité dans $\mathbb{K}[X]$

Cette section est à mettre en parallèle avec le chapitre 28 de TLM1, où on étudie les propriétés arithmétiques des entiers. On peut faire de même avec les polynômes car il existe une *division euclidienne* dans $\mathbb{K}[X]$. L'outil fondamental qui permet d'arithmétiser $\mathbb{K}[X]$ est le degré.

## 2.1 Multiples et diviseurs

**Définition 1** *Soient* $A$ *et* $B$ *dans* $\mathbb{K}[X]$. *On dit que* $B$ divise $A$, *ou que* $B$ *est un* diviseur *de* $A$, *s'il existe* $Q \in \mathbb{K}[X]$ tel que $A = BQ$. *On note alors* $B \mid A$. *On dit également que* $A$ *est un* multiple *de* $B$.

**Exemple 3** Le polynôme $A = X - 1$ divise le polynôme $B = X^n - 1$ pour $n \geq 1$. En effet

$$X^n - 1 = (X-1)\left(X^{n-1} + X^{n-2} + \cdots + 1\right) . \tag{12}$$

Cette formule se vérifie aisément en développant le membre de droite, et doit être connue.

**Remarque 4** Si $B = 0$ dans la définition 1, alors $A = 0$ et $Q$ est quelconque. *Si* $B \neq 0$, *le polynôme* $Q$ *est unique*. En effet si $BQ_1 = BQ_2$ alors $B(Q_1 - Q_2) = 0$. Par intégrité de $\mathbb{K}[X]$, si $B \neq 0$, on a $Q_1 = Q_2$.

**Remarque 5** Le degré d'un produit est la somme des degrés ; on en déduit que si $B$ divise $A$ et si $A \neq 0$, alors $\deg B \leq \deg A$. Par contraposition, il vient : si $\deg B > \deg A$ et si $B$ divise $A$ alors $A = 0$. On mettra cette remarque en parallèle avec la remarque 28.2, page 340 de TLM1. On se convaincra alors que le degré joue, pour les polynômes formels, un rôle *analogue* à celui de la valeur absolue dans $\mathbb{Z}$.

**Définition 2** *On dit que que les polynômes* $A$ *et* $B \in \mathbb{K}[X]$ *sont* associés *s'il existe* $\lambda \in \mathbb{K}^*$ *tel que* $A = \lambda B$.

**Théorème 2** $A$ *et* $B \in \mathbb{K}[X]$ *sont associés si et seulement si* $A \mid B$ *et* $B \mid A$.

**Démonstration** Si $A$ et $B$ sont associés, il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$. Donc $B \mid A$ car $\lambda \in \mathbb{K}^*$ est un polynôme de degré 0. De même $B = \frac{1}{\lambda} A$, donc $A \mid B$.

Réciproquement, supposons que $A \mid B$ et $B \mid A$. Alors il existe deux polynômes $P$ et $Q$ tels que $B = AP$ et $A = BQ$. En prenant les degrés, il vient $\deg B = \deg A + \deg P$ et $\deg A = \deg B + \deg Q$. Par addition de ces deux égalités, il vient $\deg P + \deg Q = 0$. La seule valeur négative du degré étant $-\infty$, ceci implique $\deg P = \deg Q = 0$. Donc $Q$ est un polynôme de degré 0, c'est-à-dire $Q = \lambda \in \mathbb{K}^*$. Ainsi $A$ et $B$ sont associés.

## 2.2 Division euclidienne

**Théorème 3** *Soient* $A$ *et* $B$ *dans* $\mathbb{K}[X]$ *avec* $B \neq 0$ *; alors il existe un unique couple* $(Q, R)$ *dans* $\mathbb{K}[X]$ *tel que* $A = BQ + R$ *et* $\deg R < \deg B$.

**Démonstration** On commence par l'unicité. Supposons l'existence de deux couples $(Q_1, R_1)$ et $(Q_2, R_2)$. Alors :

$$A = BQ_1 + R_1 = BQ_2 + R_2 \Longrightarrow B(Q_1 - Q_2) = R_2 - R_1 .$$

On en déduit que $B$ divise $R_2 - R_1$. Mais $\deg(R_2 - R_1) \leq \max(\deg R_1, \deg R_2) < \deg B$. On en déduit (remarque 5) que $R_2 - R_1 = 0$, puis par intégrité ($B \neq 0$) que $Q_1 = Q_2$.

Prouvons maintenant l'existence, ce qui donnera l'algorithme de la division euclidienne dans $\mathbb{K}[X]$.

Si $\deg A < \deg B$ alors $A = B \times 0 + A$ ce qui fournit le couple $(0, A)$.

Si maintenant $\deg A \geq \deg B$, posons $A = a_n X^n + \cdots$ et $B = b_q X^q + \cdots$.

Alors le polynôme

$$A_1 = A - \frac{a_n}{b_q} X^{n-q} B = a_n X^n + \cdots - \frac{a_n}{b_q} X^{n-q} (b_q X^q + \cdots) \tag{13}$$

est de degré strictement plus petit que $n$ puisqu'on s'est arrangé pour éliminer les termes de degré $n$. Si $\deg A_1 < \deg B$, la division euclidienne est terminée ; en effet, d'après (13) on a $A = \frac{a_n}{b_q} X^{n-q} B + A_1 = \alpha_1 X^{\beta_1} B + A_1$.

Sinon, on recommence le procédé avec $A_1$. On élimine le terme de plus haut degré de $A_1$ en multipliant $B$ par un facteur $\alpha_2 X^{\beta_2}$ et en définissant donc $A_2$ tel que $\deg A_2 < \deg A_1$ et $A_1 = \alpha_2 X^{\beta_2} B + A_2$.

En poursuivant de même, on définit une suite $A_n$ de degré *strictement décroissant* telle que $A_{n-1} = \alpha_n X^{\beta_n} B + A_n$.

Puisque $\deg A_n$ est une suite d'*entiers* qui décroît strictement, il existe un entier $N$ tel que $\deg A_N < \deg B$. On a alors

$$\begin{aligned} A = \quad & \alpha_1 X^{\beta_1} B + A_1 = \alpha_1 X^{\beta_1} B + \alpha_2 X^{\beta_2} B + A_2 = \cdots \\ & = \left(\alpha_1 X^{\beta_1} + \alpha_2 X^{\beta_2} + \cdots + \alpha_N X^{\beta_N}\right) B + A_n . \end{aligned}$$

Le théorème de division euclidienne est démontré.

On notera que la démonstration proposée ici traduit très exactement, dans le cas général, le *procédé pratique* de division euclidienne tel qu'il a été exposé dans l'exemple 34.5 de TLM1, auquel on se reportera. La formule 13 exprime, en fait, que l'on multiplie $B$ par un facteur convenable de façon à éliminer, par soustraction, le terme de plus haut degré de $A$. On répète ensuite le procédé jusqu'à obtenir un reste de degré plus petit que celui du diviseur $B$.

**Remarque 6** $B$ divise $A$ si et seulement si $R = 0$.

**Remarque 7** On notera l'analogie avec la division euclidienne dans $\mathbb{Z}$. De nouveau, le degré joue dans $\mathbb{K}[X]$ le même rôle que la valeur absolue dans $\mathbb{Z}$.

## 2.3 Arithmétique des polynômes

De la même manière que pour les entiers relatifs, on définit les notions de pgcd et de ppcm. Le théorème 3 de la division euclidienne des polynômes prouve que les diviseurs communs à $A$ et $B$ sont ceux communs à $B$ et $R$, où $R$ est le reste de la division de $A$ par $B$ (comparer avec le théorème 28.3 de TLM1, page 343). Si on réitère le procédé en divisant $B$ par $R$, on obtient un nouveau reste $R_1$ ; en notant $\delta(A,B)$ l'ensemble des diviseurs communs à $A$ et $B$, on a $\delta(A,B) = \delta(R,R_1)$. Puisque $\deg R_1 < \deg R < \deg B$, au bout d'un nombre fini d'étape (le degré diminue d'une unité au moins à chaque étape) on obtient un reste nul. Si on note $D$ le dernier reste non nul, on a $\delta(A,B) = \delta(D,0)$, ensemble des diviseurs de $D$.

Le polynôme obtenu en *normalisant* $D$ (c'est-à-dire en le divisant par son coefficient dominant) est appelé le pgcd de $A$ et $B$ et se note $A \wedge B$. On a donc

$$P \mid A \ \text{ et } \ P \mid B \Longleftrightarrow P \mid (A \wedge B) . \tag{14}$$

et on dispose d'un procédé pratique pour déterminer $D$. Ce procédé, que l'on vient d'exposer, est l'*algorithme d'Euclide.*

**Exemple 4** Déterminons le pgcd de $A = 8X^4 - 26X^3 + 21X^2 - X - 2$ et de $B = X^3 - 2X^2$. On effectue la division euclidienne de $A$ par $B$ :

$$A = B \times (8X - 10) + X^2 - X - 2.$$

On a donc $R = X^2 - X - 2$. On divise ensuite $B$ par $R$ et on obtient

$$B = (X - 1) \times R + (X - 2) .$$

Enfin la division de $R$ par $X - 2$ donne $R = (X - 2)(X + 1) + 0$.

Le dernier reste non nul est le polynôme unitaire $X - 2$, qui est le pgcd de $A$ et $B$.

Comme pour les entiers, on peut "remonter" l'algorithme d'Euclide et en déduire l'existence de deux polynômes $U$ et $V$ tels que $AU + BV = D$. Ce résultat porte encore le nom de *théorème de Bézout.*

**Exemple 5** On reprend les polynômes de l'exemple 4. On a

$$A = B \times (8X - 10) + \left(X^2 - X - 2\right) \ ; \ B = (X - 1) \times \left(X^2 - X - 2\right) + (X - 2) .$$

On en déduit que

$$\begin{aligned} X - 2 \quad & = B - (X - 1) \times \left(X^2 - X - 2\right) = B - (X - 1)(A - B \times (8X - 10)) \\ & = -(X - 1) A + \left(8X^2 - 18X + 11\right) B. \end{aligned}$$

Si le pgcd de $A$ et $B$ est le polynôme constant égal à $1$, on dit que $A$ et $B$ sont *premiers entre eux*. Alors le *théorème de Bézout* s'écrit :

**Théorème 4** *Les polynômes $A$ et $B$ sont premiers entre eux si et seulement si il existe deux polynômes $U$ et $V$ tels que $AU + BV = 1$.*

**Remarque 8** Si $A$ est premier avec $B$ et $C$, alors $A$ est premier avec $BC$ (voir corollaire 28.1). On en déduit l'important résultat suivant :

**Théorème 5** *Soient $a$ et $b \in \mathbb{K}$, avec $a \neq b$, et soient $n$, $p \in \mathbb{N}^*$. Alors les polynômes $(X-a)^n$ et $(X-b)^p$ sont premiers entre eux.*

**Démonstration** D'abord on a $\frac{1}{b-a}(X-a) - \frac{1}{b-a}(X-b) = 1$.
Donc $X-a$ et $X-b$ sont premiers entre eux en vertu du théorème de Bézout.
Par la remarque 8, on obtient par récurrence sur $p$ que $X-a$ et $(X-b)^p$ sont premiers entre eux, puis par récurrence sur $n$ que $(X-a)^n$ et $(X-b)^p$ sont premiers entre eux.

Le *théorème de Gauss* est encore valable pour les polynômes :

**Théorème 6** *Si $A$ et $B$ sont premiers entre eux, et si $A \mid BC$, alors $A \mid C$.*

Pour la démonstration, voir le théorème 28.7 de TLM1.

Pour finir, définissons le ppcm de deux polynômes. Soit $\mu(A,B)$ est l'ensemble des multiples communs à $A$ et $B$, et $\mathcal{M}$ l'ensemble des degrés des polynômes non nuls de $\mu(A,B)$, c'est-à-dire $\mathcal{M} = \{\deg P,\ P \in M(A,B) \text{ et } P \neq 0\}$. $\mathcal{M}$ est une partie non vide de $\mathbb{N}$ (elle contient $\deg A + \deg B$ car $AB \in \mu(A,B)$). Elle admet donc un plus petit élément $m$. Soit $M$ un polynôme de $\mu(A,B)$ de degré $m$. Alors $\forall \lambda \in \mathbb{K}^*$, $\lambda M$ est encore un multiple commun à $A$ et $B$ de degré $m$. On définit le ppcm de $A$ et $B$ en normalisant $M$ ; on le note $A \vee B$.

Soit $P$ un multiple commun à $A$ et $B$. En divisant $P$ par $A \vee B$, on a $P = (A \vee B)Q + R$ avec $\deg R < \deg(A \vee B)$. Puisque $A$ et $B$ divisent $P$ et $(A \vee B)$, ils divisent aussi $R$. Ainsi $R$ est un multiple commun à $A$ et $B$, de degré plus petit que celui de $A \vee B$ ; par définition de $A \vee B$, on a $R = 0$. On a donc prouvé que tout multiple commun à $A$ et $B$ est un multiple de $A \vee B$. La réciproque étant immédiate, on a :

$$A \mid P \text{ et } B \mid P \iff A \vee B \mid P. \tag{15}$$

**Remarque 9** Dans "pgcd" et "ppcm" les termes "grand" et "petit" doivent donc être compris au sens de la divisibilité : $P$ est plus "petit" que $Q$ si $P$ divise $Q$.

Les propriétés du pgcd et du ppcm vues au chapitre 28 de TLM1 s'étendent aux polynômes. Les théorèmes 33.2, 33.6 et 33.8 donnent des théorèmes aux *formulations identiques* pour les polynômes. En revanche, le théorème 28.9 s'énonce ainsi :

**Théorème 7** *Soient $A$ et $B \in \mathbb{K}[X]$. Alors $AB$ et $(A \wedge B)(A \vee B)$ sont associés (c'est-à-dire sont égaux à une constante multiplicative près).*

En particulier, si $A$ et $B$ sont premiers entre eux, leur ppcm est $A \vee B = \lambda AB$ où $\lambda$ est l'inverse du produit des coefficients dominants de $A$ et $B$ (n'oublions pas que le ppcm est un polynôme unitaire).

# 3 Formule de Taylor

Dans cette section, nous montrons comment exprimer un polynôme à l'aide de ses dérivées successives en un point. Cependant, puisque nous travaillons sur des *polynômes formels*, nous ne pouvons pas utiliser la notion usuelle de dérivée, qui utilise les propriétés de $\mathbb{R}$ et notamment la notion de limite (définition 10.1 de TLM1). Nous devons donc donner d'abord une *définition de la dérivée formelle d'un polynôme*. Celle-ci s'obtient par "dérivation terme à terme" et redonne bien sûr la dérivée de la fonction polynôme correspondante de $\mathbb{R}$ dans $\mathbb{R}$.

## 3.1 Dérivation formelle d'un polynôme

**Définition 3** *Soit* $P = a_0 + a_1 X + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.

*On appelle* polynôme dérivé *de* $P$ *le polynôme*

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} = \sum_{k=0}^{n} k a_k X^{k-1} \tag{16}$$

Il est immédiat que $P$ est constant si et seulement si $P' = 0$. En effet, d'après la définition 3,

$$P' = 0 \Leftrightarrow a_1 = a_2 = \ldots = a_n = 0 \Leftrightarrow P = a_0.$$

Par ailleurs $\deg P' = \deg(P) - 1$ si $P$ n'est pas constant.

D'après la définition, on a pour tout $(P, Q) \in \mathbb{K}[X]^2$, $(\lambda, \mu) \in \mathbb{K}$ :

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q'. \tag{17}$$

Cette propriété porte le nom de *linéarité de la dérivation.*

La formule de dérivation d'un produit déjà rencontrée pour les fonctions reste valable pour la dérivée formelle des polynômes : pour tout $(P, Q) \in \mathbb{K}[X]^2$,

$$(PQ)' = P'Q + PQ' \tag{18}$$

Dans ce cas cependant, elle n'est pas du tout évidente car la démonstration du théorème 10.4, page 108 de TLM 1, n'est pas valable. Il faut démontrer la formule de dérivation d'un produit *à partir de* (16) . Pour ce faire, posons

$$P = \sum_{i=0}^{p} a_i X^i \ ; \ Q = \sum_{j=0}^{q} b_j X^j.$$

En utilisant la distributivité de la multiplication sur l'addition dans $\mathbb{K}[X]$ et la linéarité de la dérivation [formule (17)], on a

$$\begin{aligned}
(PQ)' &= \left(\sum_{i=0}^{p} a_i X^i \times \sum_{j=0}^{q} b_j X^j\right)' = \left[\sum_{i=0}^{p} a_i \left(X^i \times \sum_{j=0}^{q} b_j X^j\right)\right]' = \left[\sum_{i=0}^{p} a_i \left(\sum_{j=0}^{q} b_j X^{i+j}\right)\right]' \\
&= \sum_{i=0}^{p} a_i \left(\sum_{j=0}^{q} b_j X^{i+j}\right)' = \sum_{i=0}^{p} a_i \left(\sum_{j=0}^{q} (i+j)\, b_j X^{i+j-1}\right) = \sum_{i=0}^{p} a_i \left(\sum_{j=0}^{q} i b_j X^{i+j-1}\right) + \sum_{i=0}^{p} a_i \left(\sum_{j=0}^{q} j b_j X^{i+j-1}\right) \\
&= \sum_{i=0}^{p} i a_i X^{i-1} \left(\sum_{j=0}^{q} b_j X^j\right) + \sum_{i=0}^{p} a_i X^i \left(\sum_{j=0}^{q} j b_j X^{j-1}\right) \\
&= \left(\sum_{i=0}^{p} i a_i X^{i-1}\right)\left(\sum_{j=0}^{q} b_j X^j\right) + \left(\sum_{i=0}^{p} a_i X^i\right)\left(\sum_{j=0}^{q} j b_j X^{j-1}\right) = P'Q + PQ'.
\end{aligned}$$

On définit ensuite les dérivées successives de $P$. Par définition, $P''$ est le polynôme dérivé du polynôme $P'$. Plus généralement, on définit par récurrence le polynôme dérivé $k^{ième}$ de $P$, noté $P^{(k)}$, par $P^{(k)} = \left(P^{(k-1)}\right)'$. Par convention $P^{(0)} = P$.

**Exemple 6** Pour $0 \leq k \leq n$ entiers :

$$(X^n)^{(k)} = n(n-1)(n-2)\cdots(n-k+1)\, X^{n-k} = \frac{n!}{(n-k)!} X^{n-k}. \tag{19}$$

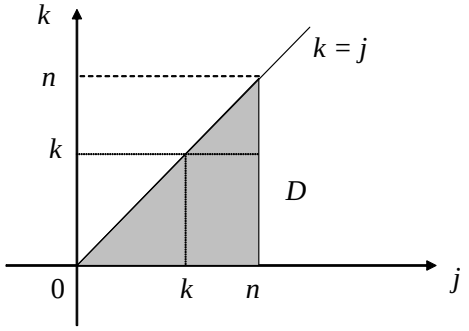
En particulier $(X^n)^{(n)} = n!$ et $(X^n)^{(n+1)} = 0$. Ainsi, par linéarité de la dérivation, si $P$ est de degré au plus $n$ on a $P^{(n+1)} = 0$.

## 3.2 Formule de Taylor

Soit $a \in \mathbb{K}$ et $P = \sum_{j=0}^{n} a_j X^j$. En utilisant la formule du binôme de Newton, on a

$$P = \sum_{j=0}^{n} a_j \left(X - a + a\right)^j = \sum_{j=0}^{n} a_j \sum_{k=0}^{j} \binom{j}{k} (X-a)^k \, a^{j-k} = \sum_{j=0}^{n} \sum_{k=0}^{j} a_j \binom{j}{k} (X-a)^k \, a^{j-k}.$$

Cette somme double est analogue à une intégrale double (chapitre 24 de TLM1). On l'obtient en sommant pour $j$ allant de $0$ à $n$, puis pour $k$ allant de $0$ à $j$, de $a_j \binom{j}{k} (X-a)^k \, a^{j-k}$ pour tous les points à coordonnées entières du domaine $D$ ci-dessous :




Si nous décidons de sommer d'abord par rapport à $k$, nous voyons que $k$ varie de $0$ à $n$ pour décrire $D$. Pour $k$ fixé, $j$ varie de $k$ à $n$. Donc

$$\begin{aligned} P &= \sum_{k=0}^{n} \sum_{j=k}^{n} a_j \binom{j}{k} (X-a)^k \, a^{j-k} = \sum_{k=0}^{n} \left( \sum_{j=k}^{n} a_j \binom{j}{k} a^{j-k} \right) (X-a)^k \\ &= \sum_{k=0}^{n} \left( \sum_{j=k}^{n} a_j \frac{j!}{k!\,(j-k)\,!} a^{j-k} \right) (X-a)^k = \sum_{k=0}^{n} \frac{1}{k!} \left( \sum_{j=k}^{n} a_j \frac{j!}{(j-k)\,!} a^{j-k} \right) (X-a)^k . \end{aligned}$$

Or en utilisant (19), on voit que $P^{(k)} = \sum_{j=k}^{n} a_j \frac{j!}{(j-k)\,!} X^{j-k}$. Nous avons donc obtenu la *formule de Taylor* :

**Théorème 8** *Soit $P \in \mathbb{K}[X]$, de degré au plus $n$, et $a \in \mathbb{K}$. Alors*

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k . \tag{20}$$

On peut donc maintenant voir un polynôme de degré $n$ d'une nouvelle manière : la suite des $n+1$ dérivées en un point $a$ de $\mathbb{K}$. Dans le cas particulier où $a = 0$, on obtient la formule dite *de Mac-Laurin* :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k . \tag{21}$$

**Exemple 7** Déterminer $P$ tel que $P(1) = 1$ et

$$4P(X) = (X-1)\,P'(X) + P''(X) \tag{E}$$

On peut tout d'abord chercher le degré de $P$.

Posons $\deg P = n$ avec $n \geq 0$ ($P \neq 0$ car $P(1) = 1$) et $P = \sum_{k=0}^{n} a_k X^k$, avec $a_n \neq 0$. Alors :

$$4P = 4a_n X^n + \cdots = (X-1)\left(n a_n X^{n-1} + \cdots\right) + n(n-1)\,a_n X^{n-2} + \cdots ,$$

d'où $4a_n = na_n$ et ainsi $n = 4$. Cherchons $P$ en utilisant la formule de Taylor au point $1$. Avec $X = 1$ dans $(E)$, on obtient $4P(1) = 4 = P''(1)$. Dérivons $(E)$ :

$$4P'(X) = P'(X) + (X-1)P''(X) + P^{(3)}(X) \tag{E'}$$

donne, en $X = 1$, $3P'(1) = P^{(3)}(1)$. Dérivons $(E')$ :

$$3P''(X) = P''(X) + (X-1)P^{(3)}(X) + P^{(4)}(X). \tag{E''}$$

Il vient $2P''(1) = 8 = P^{(4)}(1)$. Une dernière dérivation :

$$2P^{(3)}(X) = (X-1)P^{(4)}(X) + P^{(5)}(X) \tag{E'''}$$

fournit $2P^{(3)}(1) = P^{(5)}(1) = 0$ car $\deg P = 4$.

Pour conclure, on a $P'(1) = P^{(3)}(1) = 0$, $P(1) = 1$, $P''(1) = 4$, $P^{(4)}(1) = 8$ et

$$P(X) = 1 + \frac{4}{2!}(X-1)^2 + \frac{8}{4!}(X-1)^4 = 1 + 2(X-1)^2 + \frac{1}{3}(X-1)^4.$$

# 4 Formule de Leibniz

Soient $(P, Q) \in \mathbb{K}[X]^2$ et $a \in \mathbb{K}$. Soit $N = \max(\deg P, \deg Q)$.

En utilisant la formule de Taylor pour les polynômes $P$, $Q$ et $PQ$, et la formule (6), on a

$$PQ = \left(\sum_{n=0}^{N} \frac{P^{(n)}(a)}{n!}X^n\right)\left(\sum_{n=0}^{N} \frac{Q^{(n)}(a)}{n!}X^n\right) = \sum_{n=0}^{2N}\left(\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}\frac{Q^{(n-k)}(a)}{(n-k)!}\right)X^n = \sum_{n=0}^{2N}\frac{(PQ)^{(n)}(a)}{n!}X^n.$$

Par identification des coefficients de $X^n$, on obtient

$$(PQ)^{(n)}(a) = \sum_{k=0}^{n}\frac{n!}{k!(n-k!)}P^{(k)}(a)\,Q^{(n-k)}(a) = \sum_{k=0}^{n}\binom{n}{k}P^{(k)}(a)\,Q^{(n-k)}(a).$$

L'égalité ci-dessus, vraie pour tout $a \in \mathbb{K}$, entraîne l'égalité des polynômes correspondants (car un polynôme n'a qu'un nombre fini de racines) et on obtient la *formule de Leibniz* pour les polynômes formels :

**Théorème 9** *Soit* $(P, Q) \in \mathbb{K}[X]^2$. *Alors*

$$(PQ)^{(n)} = \sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)} \tag{22}$$

**Exemple 8** On a $X^{2n} = X^n \times X^n$, d'où

$$\left(X^{2n}\right)^{(n)} = \frac{(2n)!}{n!}X^n = \sum_{k=0}^{n}\binom{n}{k}\left(X^n\right)^{(k)}\left(X^n\right)^{(n-k)} = \sum_{k=0}^{n}\binom{n}{k}\frac{n!}{(n-k)!}X^{n-k} \times \frac{n!}{k!}X^k = n!\sum_{k=0}^{n}\binom{n}{k}^2 X^n.$$

Ceci prouve que $\binom{2n}{n} = \sum_{k=0}^{n}\binom{n}{k}^2$, résultat qui se déduit aussi de (9).

# Exercices

**Exercice 1** Déterminer $p$ et $q$ dans $\mathbb{R}$ pour que $P = X^3 + pX + q$ soit divisible par $Q = X^2 + 3X - 1$.

**Exercice 2** Montrer que $X^2 - X + 1$ divise $P = (X-1)^{n+2} + X^{2n+1}$ pour tout $n \in \mathbb{N}$.

**Exercice 3** Calculer, pour $n \geq 2$, les restes de la division euclidienne de $P = (X-3)^{2n} + (X-2)^n - 2$ par $(X-2)^2$.

**Exercice 4** Soit $\theta \in \mathbb{R}$ et, pour $n \in \mathbb{N}^*$, $P_n = [\cos((n-1)\theta)]X^{n+1} - [\cos n\theta]X^n - (\cos\theta)X + 1$.
Montrer que $P_1$ divise $P_n$ et expliciter le quotient.

**Exercice 5** Soit $P \in \mathbb{C}[X]$. On suppose que $\forall x \in \mathbb{R}$, $P(x) \in \mathbb{R}$.
Montrer que les coefficients de $P$ sont tous réels.

**Exercice 6** Déterminer les polynômes $P$ tels que $P'$ divise $P$.

# Solutions des exercices

**Exercice 1** On fait la division euclidienne de $X^3 + pX + q$ par $X^2 + 3X - 1$. On obtient, après calcul, $X^3 + pX + q = (X-3)\left(X^2 + 3X - 1\right) + (10 + p)X + q - 3$. Le polynôme $Q$ divise $P$ si et seulement si le reste $R = (10+p)X + q - 3$ est le polynôme nul. La seule solution est $p = -10$ et $q = 3$.

**Exercice 2** Les racines de $X^2 - X + 1$ sont $-j$ et $-j^2 = \overline{(-j)}$ où $j = e^{\frac{2i\pi}{3}}$ (exemple 34.1 de TLM1). On calcule $P(-j) = (-j-1)^{n+2} + (-j)^{2n+1}$. Puisque $1 + j + j^2 = 0$, on a $P(-j) = j^{2n+4} - j^{2n+1} = 0$ car $j^3 = 1$. On en déduit que $-j$ est racine de $P$. Ainsi $X + j$ divise $P$.
Puisque $P$ est à coefficients réels, $-j^2 = \overline{(-j)}$ est aussi racine de $P$. Ainsi $X + j^2$ divise $P$.
Puisque $X + j$ et $X + j^2$ sont premiers entre eux (théorème 5), $(X + j)\left(X + j^2\right) = X^2 - X + 1$ divise $P$.

**Exercice 3** On a l'égalité $P(X) = (X-2)^2 Q(X) + \gamma X + \delta$, qui donne avec $X = 2$, $2\gamma + \delta = P(2) = -1$. On dérive l'égalité précédente pour obtenir $P'(X) = 2(X-2)Q(X) + (X-2)^2 Q'(X) + \gamma$, ce qui donne avec $X = 2$, $P'(2) = -2n = \gamma$. Le reste cherché est $-2nX + 4n - 1$.

**Exercice 4** Supposons $n \geq 2$ et écrivons le début de la division euclidienne de $P_n$ par $P_1 = X^2 - 2\cos(\theta)X + 1$.

| | |
|---|---|
| $\cos((n-1)\theta)X^{n+1} - \cos(n\theta)X^n - \cos(\theta)X + 1$ | $X^2 - 2\cos(\theta)X + 1$ |
| $-\cos((n-1)\theta)X^{n+1} - 2\cos(\theta)\cos((n-1)\theta)X^n + \cos((n-1)\theta)X^{n-1}$ | $\cos((n-1)\theta)X^{n-1}$ |
| $(2\cos(\theta)\cos((n-1)\theta) - \cos(n\theta))X^n - \cos((n-1)\theta)X^{n-1}$ | |
| $-\cos(\theta)X + 1$ | |

Le premier reste obtenu ressemble beaucoup à $P_{n-1}$. Cela sera vrai si :

$$2\cos(\theta)\cos(n-1)\theta - \cos(n\theta) = \cos(n-2)\theta,$$

ce qui découle d'une formule connue de trigonométrie (formule 1.17 de TLM1). On a donc

$$P_n = \cos((n-1)\theta)X^{n-1}P_1 + P_{n-1}.$$

Par récurrence il vient $P_n = \left(\sum_{k=1}^{n} \cos((k-1)\theta)X^{k-1}\right)P_1 = \left(\sum_{k=0}^{n-1} \cos(k\theta)X^k\right)P_1$.

**Exercice 5** Si $P = \sum_{k=0}^{n} a_k X^k$, on définit $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$ le polynôme conjugué de $P$. Alors, si $z \in \mathbb{C}$, $\overline{P(z)} = \overline{P}(\overline{z})$. D'après les hypothèses, pour tout $x \in \mathbb{R}$, $P(x) = \overline{P(x)} = \overline{P}(\overline{x}) = \overline{P}(x)$. Les polynômes $P$ et $\overline{P}$ coïncident sur $\mathbb{R}$ qui est infini,

ils sont donc égaux (car $P - \overline{P}$ a une infinité de racines distinctes). Ceci se traduit par $a_k = \overline{a_k}$ pour tout $k$, c'est-à-dire $P \in \mathbb{R}[X]$.

**Exercice 6** Le polynôme nul est solution et c'est le seul polynôme constant. Si on écrit que $P = QP'$, alors $\deg Q = 1$. Si $P = a_n X^n + \cdots$ avec $a_n \neq 0$, on en déduit qu'il existe $\alpha$ tel que $Q = \frac{1}{n}(X - \alpha)$. Ainsi

$$P = \frac{1}{n}(X - \alpha) P' \tag{R}$$

On en déduit que $\alpha$ est racine de $P$. Dérivons l'égalité (R), on obtient $P' = \frac{1}{n}(X - \alpha) P'' + \frac{1}{n} P'$, d'où $\left(1 - \frac{1}{n}\right) P'(\alpha) = 0$.

Si $n = 1$, alors $P = a_n (X - \alpha)$. Sinon, on a $P'(\alpha) = 0$. Supposons $n \geq 1$, on dérive la relation (R) $k$ fois avec Leibniz pour obtenir :

$$P^{(k)} = \frac{1}{n}(X - \alpha) P^{(k+1)} + \frac{k}{n} P^{(k)} \Longrightarrow \left(1 - \frac{k}{n}\right) P^{(k)}(\alpha) = 0$$
$$\Longrightarrow P^{(k)}(\alpha) = 0 \text{ si } 0 \leq k \leq n - 1.$$

Conclusion : $\alpha$ est racine d'ordre $n$ de $P$ et $P = a_n (X - \alpha)^n$.