Chapitre 16 : Polynômes

Dans ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 Définitions et règles de calcul

Définition 1. On appelle *polynôme à coefficients dans* $\mathbb{K}$ un objet mathématique « formel » qui s'écrit de manière unique sous la forme

$$\begin{aligned} P(X) &= a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n \\ &= \sum_{k=0}^{n} a_k X^k \end{aligned}$$

où n est un entier naturel, $a_0, a_1, \ldots, a_{n-1}, a_n$ sont des éléments de $\mathbb{K}$, appelés *coefficients* du polynôme, et X est un objet qui porte le nom d'*indéterminée*.
L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

On peut également construire les polynômes en les définissant de la manière suivante :

Un *polynôme à coefficients dans* $\mathbb{K}$ est une suite finie de $\mathbb{K}^{\mathbb{N}}$, c'est-à-dire nulle à partir d'un certain rang :

$$(a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, 0 \ldots).$$

Remarque 1. Les coefficients d'un polynôme sont uniques, ce qui permet d'identifier les coefficients de deux polynômes égaux. Par définition, deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

Remarque 2. Les éléments de $\mathbb{K}$ sont des polynômes. On les appelle *polynômes constants.*

Remarque 3. On a $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Exemple. $1 + X + X^2 \in \mathbb{R}[X]$ et $1 + iX^4 \in \mathbb{C}[X] \setminus \mathbb{R}[X]$.

Définition 2. (Degré) Soit $P = (a_k)_{k \in \mathbb{N}}$ un polynôme non nul.
On appelle *degré de* P et on note $\deg P$ le plus grand entier naturel n tel que $a_n \neq 0$.
Par convention, le degré du polynôme nul vaut $-\infty$:

$$\deg 0 = -\infty.$$

Exemple. Soit P un polynôme non nul. Alors le polynôme P est constant si et seulement si $\deg P = 0$. On pensera à toujours traiter à part le cas du polynôme nul.

Définition 3. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus n.

Exemple. On a $X^3 + X^2 + X + 1 \in \mathbb{K}_3[X]$, mais on a aussi $X^3 + X^2 + X + 1 \in \mathbb{K}_4[X]$.

Définition 4. (Coefficient dominant, polynôme unitaire)
Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ un polynôme non nul de degré n.
Alors a_n s'appelle le *coefficient dominant de* P et $a_n X^n$ s'appelle le *monôme de plus haut degré de* P.
De plus, si $a_n = 1$, on dit que le polynôme P est *unitaire.*

Exemple. $3X^4 + 2X + 1$ est un polynôme de degré 4. Son coefficient dominant est 3. Son monôme de plus haut degré est $3X^4$.
Le polynôme $X^3 - 1$ est un polynôme unitaire de degré 3.
5 est un polynôme constant de degré 0.

1.1 Opérations sur les polynômes

Soient P et Q deux polynômes à coefficients dans $\mathbb{K}$, dont on note $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ les coefficients.
Rappel : Les suites (a_k) et (b_k) sont des suites finies, c'est-à-dire nulles à partir d'un certain rang.

Égalité de deux polynômes

$$\boxed{P = Q \iff \forall k \in \mathbb{N},\ a_k = b_k.}$$

Somme de deux polynômes

Soient $P = a_nX^n + a_{n-1}X^{n-1}\cdots + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1}\cdots + b_1X + b_0$. On définit :

$$\boxed{P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1}\cdots + (a_1 + b_1)X + (a_0 + b_0)}$$

Multiplication par un scalaire

Soient $P = a_nX^n + a_{n-1}X^{n-1}\cdots + a_1X + a_0$ et $\lambda \in \mathbb{K}$, On définit :

$$\boxed{\lambda P = (\lambda a_n)X^n + (\lambda a_{n-1})X^{n-1}\cdots + (\lambda a_1)X + (\lambda a_0)}$$

Règles de calcul

Pour tous polynômes P, Q, R à coefficients dans $\mathbb{K}$ et pour tout $(\alpha, \beta) \in \mathbb{K}^2$, on a :

$$(P + Q) + R = P + (Q + R) \quad \text{et ce polynôme est noté } P + Q + R,$$

$$P + Q = Q + P, \quad P + 0 = P, \quad P - P = 0, \quad 1P = P,$$

$$\alpha(P + Q) = \alpha P + \alpha Q, \quad (\alpha + \beta)P = \alpha P + \beta P,$$

$$\alpha(\beta P) = (\alpha\beta)P.$$

Produit de deux polynômes

On définit

$$\boxed{\begin{aligned} PQ &= \sum_{k=0}^{\deg P + \deg Q} \left(\sum_{\ell=0}^{k} a_\ell b_{k-\ell}\right) X^k \\ &= \sum_{k=0}^{\deg P + \deg Q} (a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0)\, X^k \\ &= \sum_{k=0}^{\deg P + \deg Q} \left(\sum_{i+j=k} a_ib_j\right) X^k \end{aligned}}$$

Règles de calcul

Pour tous polynômes P, Q, R à coefficients dans $\mathbb{K}$, on a :

$$PQ = QP, \quad P(Q+R) = PQ + PR,$$

$$P(QR) = (PQ)R \quad \text{et ce polynôme est noté } PQR.$$

Notation

Soit P un polynôme.

$$\begin{array}{rcl} P^0 & = & 1 \\ P^{n+1} & = & P \cdot P^n \quad \forall n \in \mathbb{N}. \end{array}$$

Binôme de Newton

Soient P et Q deux polynômes, et $n \in \mathbb{N}$.

$$\boxed{(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}.}$$

Exemple. Déterminer $(X-1)^5$.

Exercice 1. Soient

$$P = aX^2 + bX + c,\ Q = 2X^4 + X^2 + 9 \text{ et } R = X^4 + 3X$$

trois polynômes de $\mathbb{R}[X]$. Déterminer une condition nécessaire et suffisante sur a, b, c pour que $P^2 = Q - 2R$.

Composée de deux polynômes

Soient P et Q des polynômes. Le polynôme composé de P et Q, noté $P \circ Q$, est défini de la manière suivante :

si P est constant, alors $P \circ Q = P$

et si $\deg P > 0$, $P = a_n X^n + \cdots + a_1 X + a_0$, alors

$$P \circ Q = a_n Q^n + \cdots + a_1 Q + a_0.$$

Exemple. Déterminer $P \circ Q$ lorsque :

1. $P = X^2 + 1$ et $Q = 2X + 3$,
2. $P = 3$ et $Q = 2X + 3$.

Proposition 1. *Soient P et Q des polynômes de $\mathbb{K}[X]$. Alors :*

$$\deg(P + Q) \leqslant \max\left(\deg P, \deg Q\right).$$

et

$$\deg(PQ) = \deg P + \deg Q.$$

2 Arithmétique dans $\mathbb{K}[X]$

Définition 5. Soient A et B deux polynômes. On dit que

- A divise B,
- ou que A est un diviseur de B,
- ou encore que B est un multiple de A

s'il existe un polynôme Q tel que

$$B = AQ.$$

Exemple.

1. Tout polynôme divise le polynôme nul.
2. Le seul multiple de 0 est 0.
3. Soient P un polynôme non nul est $a \in \mathbb{K}^\star$. Alors aP et a sont des diviseurs de P.
4. Le polynôme $X^5 - 1$ est un multiple de $X - 1$.
   Plus généralement, si $n \in \mathbb{N}^\star$, $X - 1$ divise $X^n - 1$:
   $$X^n - 1 = (X - 1)(X^{n-1} + \cdots + X + 1).$$

Proposition 2. *Soient A et B deux polynômes.*
Si A divise B, alors $\deg A \leqslant \deg B$.

Démonstration.

Proposition 3. *Soient A, B, C des polynômes non nuls.*

1. *Si A divise B et si B divise C, alors A divise C.*
2. *Si A divise B et si B divise A, alors $B = \lambda A$ avec $\lambda \in \mathbb{K}^\star$.*
3. *Si A divise B et A divise C, alors A divise $B + C$.*

Démonstration.

Proposition 4. *(Division euclidienne) Soient A un polynôme et B un polynôme non nul.*
Il existe des polynômes Q et R uniques tels que

$$\boxed{A = BQ + R \quad \text{et} \quad \deg R < \deg B}$$

Le polynôme Q s'appelle le quotient et le polynôme R s'appelle le reste de la division euclidienne de A par B.

MÉTHODOLOGIE : EFFECTUER UNE DIVISION EUCLIDIENNE DANS $\mathbb{K}[X]$

Exercice 2. Déterminer le quotient et le reste de la division euclidienne de $X^5 + X^2 + 1$ par $X^2 + X + 1$.

3 Dérivation

3.1 Dérivée première

Définition 6. Soit $P = \sum_{k=0}^{n} a_k X^k = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$.
On appelle *polynôme dérivé de* P, et on note P', le polynôme défini par :

$$\begin{aligned} P' &= a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \\ &= \sum_{k=1}^{n} k a_k X^{k-1} \\ &= \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k. \end{aligned}$$

Exemple. Si $P = X^4 + 5X + 3$, alors $P' = 4X^3 + 5$.

Proposition 5. *Si $P \in \mathbb{K}[X]$ est constant, alors $P' = 0$.*
Si $P \in \mathbb{K}[X]$ n'est pas constant, alors $\deg P' = \deg P - 1$.

Proposition 6. $P' = 0 \iff P$ *est un polynôme constant.*

Proposition 7. $\forall \lambda, \mu \in \mathbb{K}$, $\forall P, Q \in \mathbb{K}[X]$,

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q' \quad \text{et} \quad (PQ)' = P'Q + PQ'.$$

Proposition 8. $\forall P, Q \in \mathbb{K}[X]$,

$$\boxed{(P \circ Q)' = Q' \times P' \circ Q.}$$

3.2 Dérivée d'ordre supérieur

Définition 7. (Dérivées d'ordre supérieur) Soit $P \in \mathbb{K}[X]$. On définit les dérivées successives du polynôme P par

$$P^{(0)} = P \quad \text{et} \quad \forall n \in \mathbb{N},\ P^{(n+1)} = \left(P^{(n)}\right)'.$$

Le polynôme $P^{(n)}$ est appelé *polynôme dérivé d'ordre n de P*.

Exemple. Soient $n \in \mathbb{N}$ et $k \in [\![0, n]\!]$. Le polynôme dérivé d'ordre k de $P = X^n$ est : $n(n-1)\cdots(n-k+1)X^{n-k} = \dfrac{n!}{(n-k)!} X^{n-k}$. En particulier, $(X^n)^{(n)} = n!$.

Théorème 1. *(Formule de Leibniz) Soient P et Q deux polynômes de $\mathbb{K}[X]$, et $n \in \mathbb{N}$. On a*

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

Exemple. Écrire la formule de Leibniz dans le cas où $n = 1, 2, 3$ et 4.

Théorème 2. *(Formule de Taylor) Soient P un polynôme de $\mathbb{K}[X]$ de degré inférieur ou égal à n et a un élément de $\mathbb{K}$. Alors :*

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

Exemple. Écrire la formule de Taylor pour $P = X^4 + 1$ et $a = 1$.

4 Racines d'un polynôme

Définition 8. (Fonction polynomiale) Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$. On appelle *fonction polynomiale associée à P*, et on note $\widetilde{P}$, la fonction

$$\begin{array}{rccc} \widetilde{P}: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & a_n x^n + \cdots + a_1 x + a_0. \end{array}$$

Exemple. Si $P = X^2 + X + 1$, alors $\tilde{P}(2) =$............................
Si $Q = 3$, alors $\tilde{Q}(2) =$..

Proposition 9. *Soient P, Q des polynômes et λ, a des éléments de $\mathbb{K}$. On a :*

$$(\widetilde{\lambda P})(a) = \lambda \widetilde{P}(a), \quad (\widetilde{P+Q})(a) = \widetilde{P}(a) + \widetilde{Q}(a) \quad \textit{et} \quad (\widetilde{PQ})(a) = \widetilde{P}(a)\widetilde{Q}(a).$$

Exemple. Si $P = X^2 + X + 1$ et $Q = 3$, alors $(\widetilde{P+2Q})(2) =$...........

Définition 9. (Racine) Soient P un polynôme et a un élément de $\mathbb{K}$. On dit que a est une *racine* de P si $\widetilde{P}(a) = 0$.

Exemple. $X^2 - 1$ admet deux racines réelles : 1 et -1.
$X^2 + 1$ n'admet aucune racine réelle, mais deux racines complexes : i et $-i$.

Proposition 10. *Soient P un polynôme et a un élément de $\mathbb{K}$.*
a est une racine de P si et seulement si $X - a$ divise P.

Démonstration.

Proposition 11. *Soit P est un polynôme non nul de $\mathbb{K}[X]$ de degré n, alors P admet au plus n racines dans $\mathbb{K}$.*

Remarque. Le polynôme nul admet une infinité de racines. Un polynôme constant non nul n'admet aucune racine.

Démonstration.

Définition 10. (Ordre de multiplicité) Soient P un polynôme non constant et $a \in \mathbb{K}$ une racine de P. Le plus grand entier r tel que $(X-a)^r$ divise P s'appelle l'*ordre de multiplicité de la racine a de P*. Dans ce cas,

$$P = (X-a)^r Q \quad \text{avec} \quad \widetilde{Q}(a) \neq 0.$$

Remarque.
1. Si $r = 1$, on dit que a est une racine simple de P.
2. Si $r = 2$, on dit que a est une racine double de P.
3. Si $r \geqslant 2$, on dit que a est une racine multiple de P.

Exemple.
1. 1 et -1 sont des racines simples de $X^2 - 1$ car $X^2 - 1 = (X+1)(X-1)$.
2. 1 est une racine double de $X^2 - 2X + 1$ car $X^2 - 2X + 1 = (X-1)^2$.
3. Soit $P = X^4 - 3X^3 + 3X^2 - X$.
   0 est une racine simple et de P et 1 est une racine triple de P car

$$P = X^1(X-1)^3.$$

Proposition 12. *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le nombre a est une racine double de P si et seulement si*

$$P(a) = P'(a) = 0 \quad \textit{et} \quad P''(a) \neq 0.$$

Plus généralement, le nombre a est une racine de P d'ordre de multiplicité r si et seulement si pour tout $k \in [\![0, r-1]\!]$, $P^{(k)}(a) = 0$ et $P^{(r)}(a) \neq 0$.

Définition 11. Un polynôme P de $\mathbb{K}[X]$ est dit *scindé* dans $\mathbb{K}[X]$ si l'on peut l'écrire sous la forme :

$$P = \lambda (X - x_1) \cdots (X - x_n) \quad \text{avec } \lambda \in \mathbb{K}^\star \text{ et } x_1, \ldots, x_n \in \mathbb{K}.$$

Exemple.
1. $X^2 - 2$ est scindé dans $\mathbb{R}[X]$: $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.
2. $X^2 - 2X + 1$ est scindé dans $\mathbb{R}[X]$:
   $X^2 - 2X + 1 = (X-1)^2 = (X-1)(X-1)$.
3. $X^2 + 1$ n'est pas scindé dans $\mathbb{R}[X]$, mais l'est dans $\mathbb{C}[X]$.

Théorème 3. *(Théorème de d'Alembert-Gauss) Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine complexe.*

Corollaire 1. *Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.*

Ce résultat très important est admis.

5 Décomposition en facteurs irréductibles

Pour tout polynôme $P \in \mathbb{K}[X]$ et pour tout $\lambda \in \mathbb{K}^\star$, on a $P = \frac{1}{\lambda}\lambda P$. Il existe des polynômes pour lesquels il n'y a pas d'autres factorisations possibles : les polynômes *irréductibles*. La notion correspondante en arithmétique est celle de nombre premier.

Définition 12. Un *polynôme irréductible* est un polynôme P non constant dont les seuls diviseurs sont les polynômes constants non nuls et les polynômes de la forme λP, où $\lambda \in \mathbb{K}^\star$.

Exemple.
1. Les polynômes de degré 1 sont des polynômes irréductibles.
2. Le polynôme $X^2 + 1$ est un polynôme irréductible de $\mathbb{R}[X]$.
   Par contre, ce n'est pas un polynôme irréductible de $\mathbb{C}[X]$.

Remarque. Un polynôme irréductible de $\mathbb{R}[X]$ de degré 2 n'admet pas de racine dans $\mathbb{R}$.

Théorème 4. *(Polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$)*
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Exemple. Le polynôme $X^2 - 2X + 2$ est irréductible dans $\mathbb{R}[X]$.........

Théorème 5. *(Décomposition en facteurs irréductibles) Soit P un polynôme non constant de $\mathbb{K}[X]$. Il existe $\lambda \in \mathbb{K}$ et $P_1, \ldots, P_r$ des polynômes irréductibles unitaires tels que*

$$P = \lambda P_1 \times \cdots \times P_r.$$

De plus, cette décomposition est unique à l'ordre des facteurs près.

Exemple. Soit $P = X^4 - 3X^3 + 3X^2 - X$. Écrire la décomposition de P en facteurs irréductibles.

6 Somme et produit des racines d'un polynôme

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ un polynôme scindé unitaire.

On note $x_1, \ldots, x_n$ les racines de P (comptées avec multiplicité, c'est-à-dire que si a est une racine double de P, a apparaît deux fois dans la liste).

Alors :

$$\boxed{\begin{cases} x_1 + \cdots + x_n &= -a_{n-1} \\ x_1 \times \cdots \times x_n &= (-1)^n a_0 \end{cases}.}$$

En d'autres termes, le coefficient de X^{n-1} d'un polynôme scindé unitaire permet d'obtenir la somme de ses racines (au signe près), et le coefficient constant d'un polynôme scindé unitaire permet d'obtenir le produit de ses racines (à un facteur $(-1)^{\deg P}$ près).

Cas des polynômes de degré 2

Soit $P = X^2 + a_1 X + a_0$. On note x_1 et x_2 ses racines. Alors

$$P = (X - x_1)(X - x_2).$$

Donc

$$\begin{aligned} X^2 + a_1 X + a_0 &= (X - x_1)(X - x_2) \\ &= X^2 - (x_1 + x_2)X + x_1 x_2. \end{aligned}$$

Par unicité des coefficients d'un polynôme, on a

$$\boxed{\begin{cases} x_1 + x_2 &= -a_1 \\ x_1 x_2 &= a_0 \end{cases}.}$$

Il s'agit des relations coefficients-racines étudiées en début d'année.

Application

Résoudre le système

$$\begin{cases} x + y &= 1 \\ xy &= -1 \end{cases}$$

d'inconnue $(x, y) \in \mathbb{R}^2$.