# Polynômes

## Table des matières

**1 L'anneau $\mathbb{K}[X]$ 2**
1.1 Notion de polynôme . . . 2
1.1.1 Des suites presque nulles à la notation $\sum_{k=0}^{+\infty} a_k X^k$ . . . 2
1.1.2 Degré d'un polynôme et coefficient dominant . . . 3
1.2 Produit de deux polynômes . . . 5
1.3 Structure algébrique de $\mathbb{K}[X]$ . . . 6
1.4 Composition de polynômes . . . 7

**2 Arithmétique des polynômes 8**
2.1 Notion de multiple et de diviseur . . . 8
2.2 Théorème de la division euclidienne . . . 9
2.3 PGCD . . . 9
2.4 Théorème de Bézout et lemme de Gauss . . . 11
2.5 PPCM de deux polynômes . . . 12
2.6 Généralisations . . . 13

**3 Fonctions polynomiales et racines 14**
3.1 Définition . . . 14
3.2 Méthode de Horner (lien avec Python) . . . 15
3.3 Racines d'un polynôme . . . 16
3.4 Racine et multiplicité . . . 17
3.5 Relations coefficients-racines (formules de Viète) . . . 19

**4 Dérivation 20**
4.1 Dérivée formelle d'un polynôme . . . 20
4.2 Formule de Taylor polynomiale . . . 21

**5 Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ 23**
5.1 Notion de polynôme irréductible sur $\mathbb{K}$ . . . 23
5.2 Factorisation dans $\mathbb{C}[X]$ . . . 23
5.3 D'autres conséquences du théorème de D'Alembert-Gauss . . . 24
5.4 Factorisation dans $\mathbb{R}[X]$ . . . 25

**6 Interpolation de Lagrange 27**

Dans tout ce chapitre, $\mathbb{K}$ désigne l'un des corps $\mathbb{R}$ ou $\mathbb{C}$.

# I – L'anneau $\mathbb{K}[X]$

## 1) Notion de polynôme

### (a) Des suites presque nulles à la notation $\sum_{k=0}^{+\infty} a_k X^k$

La définition d'un polynôme est la suivante. Nous utiliserons bientôt une notation plus explicite et plus agréable à manipuler.

**Définition (polynôme)** ⋆ On appelle *polynôme à coefficients dans* $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ *presque nulle*, *i.e.* telle que :

$$\exists\, d \in \mathbb{N},\ \forall n \geqslant d,\ a_n = 0$$

Les termes de cette suite (*i.e.* $a_0, a_1, a_2, \dots, a_d, 0, 0, 0, \dots$) sont appelés les coefficients du polynôme.

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

**Notations.**

⋆ Le polynôme correspondant à la suite nulle sera noté $0_{\mathbb{K}[X]}$ (il s'agit du polynôme dont tous les coefficients sont égaux à 0). On l'appelle le *polynôme nul*.

⋆ Le polynôme correspondant à la suite $(1, 0, 0, \dots)$ est noté 1 ou $X^0$. Plus généralement, on appelle polynôme *constant* tout polynôme de la forme $(\lambda, 0, 0, \dots)$ où $\lambda \in \mathbb{K}$. Un tel polynôme sera plus simplement noté $\lambda$.

⋆ De manière générale, pour tout entier naturel $k$, le polynôme correspondant à la suite $(\delta_{k,n})_{n\in\mathbb{N}}$ sera noté $X^k$.

Rappelons que, pour tous $k, n \in \mathbb{N}$, le symbole de Kronecker $\delta_{k,n}$ est défini par :

$$\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases}$$

Il est clair que l'addition $+$ dans $\mathbb{K}^{\mathbb{N}}$ est une loi de composition interne dans $\mathbb{K}[X]$ (la somme de deux suites presque nulle est encore une suite presque nulle).

**Proposition (structure de groupe dans l'ensemble des polynômes)** Le magma $(\mathbb{K}[X], +)$ est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. Il s'agit donc d'un groupe abélien de neutre $0_{\mathbb{K}[X]} = (0)_{n\in\mathbb{N}}$.

**Démonstration** ⋆ L'élément neutre de $(\mathbb{K}^{\mathbb{N}}, +)$, à savoir $0_{\mathbb{K}[X]} = (0)_{n\in\mathbb{N}}$, appartient à $\mathbb{K}[X]$ (il s'agit du polynôme nul).

⋆ Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$ (il s'agit donc de suites presque nulles). Alors la suite :

$$(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}} = (a_n - b_n)_{n\in\mathbb{N}} \qquad \text{(définition de } + \text{ dans } \mathbb{K}^{\mathbb{N}})$$

est aussi presque nulle.

Donc $(\mathbb{K}[X], +)$ est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. ■

**Remarque :** soient $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

⋆ Avec les notations précédentes, on pourra écrire $P$ sous la forme :

$$P = a_0X^0 + a_1X + a_2X^2 + \cdots = \sum_{k=0}^{+\infty} a_kX^k$$

⋆ De même, comme $\lambda(a_n)_{n\in\mathbb{N}} = (\lambda a_n)_{n\in\mathbb{N}}$ est une suite presque nulle, on peut définir le polynôme $\lambda P \in \mathbb{K}[X]$ par :

$$\lambda P = \sum_{k=0}^{+\infty} \lambda a_kX^k$$

⋆ Enfin, on définit le polynôme $P+Q$ en posant :

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

**Exemple** La suite presque nulle $P = (1,1,2,0,0,\dots)$ est le polynôme :

$$P = (1,0,\dots) + (0,1,0,\dots) + (0,0,2,0,\dots) = 1 + X + 2X^2$$

Le résultat suivant est immédiat (par identification des coefficients d'une suite).

**Proposition (unicité des coefficients d'un polynômes)** Deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients.

**Démonstration** Deux suites sont égales si et seulement si leurs coefficients sont identiques. ■

### (b) Degré d'un polynôme et coefficient dominant

**Définition (degré)** Soit $P \in \mathbb{K}[X]$. On appelle *degré* de $P$, noté $\deg(P)$, l'élément de $\mathbb{N}\cup\{-\infty\}$ suivant :

$$\deg(P) = \begin{cases} \max\left\{d\in\mathbb{N} \,\middle|\, a_d \neq 0\right\} & \text{si } P \neq 0_{\mathbb{K}[X]} \\ -\infty & \text{si } P = 0_{\mathbb{K}[X]} \end{cases}$$

**Remarques :**

⋆ Si $P \neq 0_{\mathbb{K}[X]}$, alors $\left\{d\in\mathbb{N} \,\middle|\, a_d \neq 0\right\}$ est une partie de $\mathbb{N}$ non vide et majorée (puisque la suite $(a_n)_{n\in\mathbb{N}}$ est non nulle et presque nulle) ; cette partie admet donc un maximum. Ceci justifie l'existence du degré de $P$.

⋆ Les polynômes constants (c'est-à-dire de la forme $(\lambda,0,0,\dots)$ où $\lambda\in\mathbb{K}$) sont donc les polynômes de degrés 0 ou $-\infty$.

**Exemple** $\deg(1) = 0$, $\deg(X^3 - X^5) = 5$

**Définition (ensemble des polynômes de degré inférieurs ou égaux à $d$)** Soit $d\in\mathbb{N}$. On note $\mathbb{K}_d[X]$ l'ensemble des polynômes de degré inférieurs ou égaux à $d$, c'est-à-dire :

$$\mathbb{K}_d[X] = \left\{P\in\mathbb{K}[X] \,\middle|\, \deg(P) \leqslant d\right\}$$

**Remarque :** dans $\overline{\mathbb{R}}$, on a $-\infty \leqslant d$ pour tout $d\in\mathbb{N}$ donc $0_{\mathbb{K}[X]} \in \mathbb{K}_d[X]$.

**Exemple** $1 \in \mathbb{K}_3[X]$, $X - X^2 \in \mathbb{K}_3[X]$, $X^4 \notin \mathbb{K}_3[X]$

Si $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ est un polynôme de degré $d \in \mathbb{N}$, alors on pourra écrire :

$$P = \sum_{k=0}^{d} a_k X^k$$

**Définition (coefficient dominant)** Soit $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ un polynôme de degré $d$. Il existe alors $(a_0, \dots, a_{d-1}, a_d) \in \mathbb{K}^d \times \mathbb{K}^*$ tel que $P = \sum_{k=0}^{d} a_k X^k$.

- ⋆ Le scalaire $a_d$ est appelé *coefficient dominant* de $P$.
- ⋆ Si $a_d = 1$, on dit que le polynôme $P$ est *unitaire*.

**Exemple**
- — Le coefficient dominant de $P = 3$ est $a_0 = 3$.
- — Celui de $P = X - 3X^4 + X^2$ est $-3$ (ici $P = (0, 1, 1, 0, -3, 0, 0, \dots)$.

**Proposition** Soient $P, ) \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}^*$. Alors :

$(i)$ $\deg(\lambda P) = \deg(P)$ ;

$(ii)$ $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$.

**Démonstration** Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}^*$.

$(i)$ L'égalité est claire si $P = 0_{\mathbb{K}[X]}$ (les deux degrés valant $-\infty$). Supposons maintenant que $P \neq 0_{\mathbb{K}[X]}$ et notons $d \in \mathbb{N}$ le degré de $P$. Il existe alors $(a_0, \dots, a_d) \in \mathbb{K}^d \times \mathbb{K}^*$ tel que $P = \sum_{k=0}^{d} a_k X^k$. Alors :

$$\lambda P = \sum_{k=0}^{d} \lambda a_k X^k$$

Ainsi, $\deg(\lambda P) \leqslant d$. Comme $\lambda \neq 0$ et $a_d \neq 0$ (par définition du degré de $P$), on a $\lambda a_d \neq 0$ (par intégrité de $\mathbb{K}$) donc $\deg(\lambda P) \geqslant d$. Par antisymétrie de la relation $\leqslant$, on peut conclure que :

$$\deg(\lambda P) = d = \deg(P)$$

$(ii)$ Si $P$ ou $Q$ est le polynôme nul, alors l'inégalité est vraie (et il s'agit d'une égalité). Supposons maintenant que $P \neq 0_{\mathbb{K}[X]}$ et $Q \neq 0_{\mathbb{K}[X]}$. Posons alors $d = \deg(P) \in \mathbb{N}$ et $\delta = \deg(Q) \in \mathbb{N}$. Il existe :

$$(a_0, \dots, a_d) \in \mathbb{K}^d \times \mathbb{K}^* \qquad \text{et} \qquad (b_0, \dots, b_\delta) \in \mathbb{K}^\delta \times \mathbb{K}^*$$

tels que :

$$P = \sum_{k=0}^{d} a_k X^k \qquad \text{et} \qquad Q = \sum_{k=0}^{\delta} b_k X^k$$

- ⋆ Si $d \neq \delta$, alors :

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

On a ici posé $a_k = 0$ si $k > d$ et $b_k = 0$ si $b_k > \delta$. Ainsi, $\deg(P + Q) \leqslant \max(d, \delta)$. De plus :

$$a_{\max(d,\delta)} + b_{\max(d,\delta)} = \begin{cases} a_d & \text{si } d > \delta \\ b_\delta & \text{si } d < \delta \end{cases} \neq 0$$

Ainsi, $\deg(P + Q) \geqslant \max(d, \delta)$. Finalement, $\deg(P + Q) = \max(d, \delta)$, ce qu'il fallait démontrer.

⋆ Supposons maintenant que $d = \delta$. On a alors :

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

ce qui démontre l'inégalité.

**Remarque :** si $P = 1 \in \mathbb{K}[X]$ et $Q = -1 \in \mathbb{K}[X]$, alors $\deg(P) = \deg(Q) = 0$ et $P + Q = 0_{\mathbb{K}[X]}$ est de degré $-\infty$.

## 2) Produit de deux polynômes

**Proposition/définition** Soient $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$ et $Q = \sum_{k=0}^{+\infty} b_k X^k \in \mathbb{K}[X]$. Pour tout entier naturel $n$, on pose :

$$c_n := \sum_{k=0}^{n} a_k b_{n-k}$$

Alors :

⋆ la suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle et on pose $PQ = \sum_{k=0}^{+\infty} c_k X^k$ ;

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

Le polynôme $PQ$ est appelé *polynôme produit* de $P$ et $Q$.

**Démonstration** ⋆ Si $P$ ou $Q$ est le polynôme nul, alors $(c_n)_{n\in\mathbb{N}}$ est la suite nulle qui est bien un polynôme ($0_{\mathbb{K}[X]}$). La formule annoncée dans le deuxième point est clairement vérifiée d'après les règles de calculs dans $\overline{\mathbb{R}}$ (en effet, $-\infty + (-\infty) = -\infty$ et, pour tout $d \in \mathbb{N}$, on a $-\infty + d = -\infty$).

⋆ On suppose maintenant que les polynômes $P$ et $Q$ sont non nuls. Notons alors $d \in \mathbb{N}$ et $\delta \in \mathbb{N}$ les degrés respectifs de $P$ et $Q$. Pour tout entier $k > d + \delta$, on a :

$$c_k = \sum_{j=0}^{k} a_k b_{k-j} = 0$$

En effet, pour tout $j \in [\![0, k]\!]$ :

— si $j > d$, alors $a_j = 0$ ;

— si $j \leqslant d$, alors $k - j > \delta$ et donc $b_{k-j} = 0$.

Le produit $PQ$ défini ci-dessus est donc bien un polynôme (suite presque nulle). De plus, le raisonnement ci-dessus implique (par définition du degré d'un polynôme) que :

$$\deg(PQ) \leqslant d + \delta \qquad \text{c'est-à-dire} \qquad \deg(PQ) \leqslant \deg(P) + \deg(Q)$$

De plus :

$$c_{d+\delta} = a_d b_\delta \neq 0$$

par définition de $d$ et de $\delta$ donc $\deg(PQ) \geqslant d + \delta$ (par définition du degré). On a donc bien l'égalité :

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

ce qui achève la démonstration. ■

**Remarques :**

⋆ Par définition du produit de deux polynômes, on a la formule suivante :

$$\left(\sum_{k=0}^{+\infty} a_k X^k\right) \times \left(\sum_{k=0}^{+\infty} b_k X^k\right) = \sum_{k=0}^{+\infty} \left(\sum_{j=0}^{k} a_j b_{k-j}\right) X^k$$

⋆ Avec cette formule, on vérifie facilement que $X \times X = X^2$. Par récurrence, on vérifie aussi que :

$$\forall n \in \mathbb{N}^*, \qquad \prod_{k=1}^{n} X = X^n$$

### 3) Structure algébrique de $\mathbb{K}[X]$

**Proposition (structure d'anneau de l'ensemble des polynômes)** Le triplet $(\mathbb{K}[X], +, \times)$ est un anneau commutatif. L'élément neutre pour $\times$ (produit de deux polynômes) est le polynôme $1 = X^0$.

**Démonstration** On sait déjà que $(\mathbb{K}[X], +)$ est un groupe commutatif (en tant que sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$).

⋆ On a vu dans la démonstration précédente que $\times$ définit une loi de composition interne dans $\mathbb{K}[X]$. De plus, avec le notations précédentes, on a (en effectuant le changement d'indice $i = k - j$ dans la somme) :

$$PQ = \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} a_j b_{k-j} \right) X^k = \sum_{k=0}^{+\infty} \left( \sum_{i=0}^{k} a_{k-i} b_i \right) X^k = QP$$

donc la loi $\times$ est commutative.

⋆ Vérifions maintenant que le produit est associatif. Soit $R = \sum_{k=0}^{+\infty} c_k X^k$. Montrons que $(PQ)R = P(QR)$. Par définition du produit de deux polynômes, on a :

$$\begin{aligned}(PQ)R &= \left( \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} a_j b_{k-j} \right) X^k \right) \left( \sum_{k=0}^{+\infty} c_k X^k \right) \\ &= \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} \alpha_j c_{k-j} \right) X^k\end{aligned}$$

où :

$$\begin{aligned}\forall k \in \mathbb{N}, \qquad \sum_{j=0}^{k} \alpha_j c_{k-j} = \sum_{j=0}^{k} \left( \sum_{i=0}^{j} a_i b_{j-i} \right) c_{k-j} &= \sum_{i=0}^{k} a_i \sum_{j=i}^{k} b_{j-i} c_{k-j} \\ &= \sum_{i=0}^{k} a_i \sum_{\ell=0}^{k-i} b_\ell c_{k-i-\ell}\end{aligned}$$

Ainsi :

$$(PQ)R = \left( \sum_{k=0}^{+\infty} a_k X^k \right) \left( \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} b_j c_{k-j} \right) X^k \right) = P(QR)$$

⋆ Il est clair que $1 = X^0$ est l'élément neutre pour la multiplication $\times$ dans $\mathbb{K}[X]$.

⋆ Il reste à montrer que $\times$ est distributive par rapport à l'addition $+$. Or (par définition du produit de deux polynômes) :

$$\begin{aligned}P(Q+R) &= \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} a_j (b_{k-j} + c_{k-j}) \right) X^k \\ &= \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} a_j b_{k-j} \right) X^k + \sum_{k=0}^{+\infty} \left( \sum_{j=0}^{k} a_j b_{k-j} \right) X^k \\ &= PQ + PR\end{aligned}$$

Finalement, $(\mathbb{K}[X], +, \times)$ est un anneau commutatif. ■

**Proposition** L'anneau $\mathbb{K}[X]$ est intègre, *i.e.* :

$$\forall P, Q \in \mathbb{K}[X], \qquad PQ = 0_{\mathbb{K}[X]} \iff (P = 0_{\mathbb{K}[X]} \text{ ou } Q = 0_{\mathbb{K}[X]})$$

**Démonstration** Soient $P, Q \in \mathbb{K}[X]$.

- ⋆ Il est clair que si $P = 0_{\mathbb{K}[X]}$ ou $Q = 0_{\mathbb{K}[X]}$, alors $PQ = 0_{\mathbb{K}[X]}$.
- ⋆ Réciproquement, supposons que $PQ = 0_{\mathbb{K}[X]}$. Alors $\deg(P) + \deg(Q) = -\infty$, ce qui implique que $P$ ou $Q$ est de degré $-\infty$, d'où le résultat. ■

**Proposition** Dans l'anneau $\mathbb{K}[X]$, les éléments inversibles (pour la multiplication), sont les polynômes constants non nuls (c'est-à-dire les polynômes de degré 0). Autrement dit :

$$\mathbb{K}[X]^\times = \mathbb{K}_0[X] \setminus \{0_{\mathbb{K}[X]}\}$$

**Démonstration** On raisonne par analyse-synthèse.

- ⋆ Supposons que $P \in \mathbb{K}[X]$ soit inversible dans $\mathbb{K}[X]$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. En considérant les degrés, on obtient que $\deg(P) + \deg(Q) = 0$. Comme les degrés de $P$ et $Q$ sont des éléments de $\mathbb{N} \cup \{-\infty\}$, cette égalité implique que $P$ et $Q$ sont de degrés 0.
- ⋆ Réciproquement, si $P$ est de degré 0, alors il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda X^0 = \lambda$. Le polynôme $\tilde{P} = \frac{1}{\lambda} X^0 = \frac{1}{\lambda}$ est tel que $P\tilde{P} = 1$ donc $P$ est inversible (d'inverse $\tilde{P}$). ■

## 4) Composition de polynômes

**Définition (composition)** Soient $P, Q \in \mathbb{K}[X]$. On pose $P = \sum_{k=0}^{+\infty} a_k X^k$. On appelle *composée de $P$ par $Q$* le polynôme noté $P \circ Q$ défini par :

$$P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k$$

**Remarque :** $P \circ Q$ est bien un polynôme car tout produit et combinaisons linéaires d'éléments de $\mathbb{K}[X]$ appartient à $\mathbb{K}[X]$.

**Exemple** Si $P = X^2$ et $Q = X + 1$, alors $P \circ Q = (X+1)^2$ et $Q \circ P = X^2 + 1$.

**Proposition** Soit $(P, Q) \in (\mathbb{K}[X])^2$. Si $Q$ est non constant (c'est-à-dire si $\deg(Q) \in \mathbb{N}^*$), alors :

$$\deg(P \circ Q) = \deg(P) \deg(Q)$$

**Remarque :** c'est faux si $\deg(Q) = 0$. Par exemple, la composée de $X - 1$ par 1 est de degré $-\infty$ (puisque la composée est $0_{\mathbb{K}[X]}$).

**Démonstration** La formule est évidente si $P$ est le polynôme nul (en effet, $P \circ Q = 0_{\mathbb{K}[X]}$ dans ce cas et car $-\infty \times d = -\infty$ pour tout $d \in \mathbb{N}^*$). Supposons maintenant que $P \neq 0_{\mathbb{K}[X]}$ et notons $d \in \mathbb{N}$ le degré de $P$. Il existe alors $(a_0, \dots, a_d) \in \mathbb{K}^d \times \mathbb{K}^*$ tel que :

$$P = \sum_{k=0}^{d} a_k X^k \qquad \text{et alors} \qquad P \circ Q = \sum_{k=0}^{d} a_k Q^k$$

Pour tout $k \in [\![0, d-1]\!]$, on a :

$$\deg(a_k Q^k) = \begin{cases} -\infty & \text{si } a_k = 0 \\ k \deg(Q) & \text{si } a_k \neq 0 \end{cases}$$

et :

$$\deg(a_d Q^d) = \deg(Q^d) = d \deg(Q)$$

car $a_d \neq 0$. En particulier,

$$\deg\left(\sum_{k=0}^{d-1} a_k Q^k\right) \leqslant (d-1)\deg(Q) < d\deg(Q) = \deg\left(a_d Q^d\right)$$

car $Q$ est non constant. D'après les propriétés sur le degré, on a :

$$\deg(P \circ Q) = \deg(a_d Q^d) = d \deg(Q) = \deg(P)\deg(Q),$$

ce qu'il fallait démontrer. ■

# II – Arithmétique des polynômes

## 1) Notion de multiple et de diviseur

**Définition (multiple, diviseur)** Soit $A, B \in \mathbb{K}[X]$.

- ⋆ On dit que $A$ *divise* $B$ (ou que $B$ *est un multiple de* $A$), noté $A \mid B$, s'il existe $C \in \mathbb{K}[X]$ tel que $B = AC$.
- ⋆ On note $\mathscr{D}(A)$ l'ensemble des diviseurs de $A$.

**Remarques :**

- ⋆ Comme dans $\mathbb{Z}$, le polynôme nul $0_{\mathbb{K}[X]}$ est divisible par tout polynôme (en effet, pour tout $A \in \mathbb{K}[X]$, on a $0_{\mathbb{K}[X]} = A \times 0_{\mathbb{K}[X]}$).
- ⋆ Soient $A, B \in \mathbb{K}[X]$ tels que $A \mid B$ et $B \neq 0_{\mathbb{K}[X]}$. Alors $\deg(A) \leqslant \deg(B)$ (d'après la formule donnant le degré d'un produit de polynômes).
- ⋆ Soient $P \in \mathbb{K}[X]$ et $\lambda$ un polynôme constant non nul. Alors $P = (\lambda P) \times \frac{1}{\lambda}$ et $\frac{1}{\lambda}$ définit un polynôme donc $\lambda \mid P$.
- ⋆ La relation $\mid$ est réflexive et transitive.

**Démonstration (du dernier point)** Soient $A, B, C \in \mathbb{K}[X]$.

- ⋆ On a clairement $A \mid A$ car $1 \in \mathbb{K}[X]$ et $A = A \times 1$. La relation $\mid$ est donc réflexive.
- ⋆ Si $A \mid B$ et $B \mid C$, alors il existe $Q, R \in \mathbb{K}[X]$ tels que $B = AQ$ et $C = BR$. Par conséquent, $C = A(QR)$ et comme $QR$ est un polynôme, $A \mid C$. Donc la relation $\mid$ est transitive. ■

**Proposition (relation $\mid$ dans l'anneau des polynômes)** Soient $A, B \in \mathbb{K}[X]$. Alors :

$$(A \mid B \text{ et } B \mid A) \iff (\exists \lambda \in \mathbb{K}^*,\ A = \lambda B)$$

Les polynômes $A$ et $B$ sont dits *associés*.

**Remarque :** en particulier, la relation $\mid$ n'est pas une relation d'ordre car elle n'est pas antisymétrique.

**Démonstration** Soient $A, B \in \mathbb{K}[X]$.

- ⋆ S'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$, alors il est clair que $A \mid B$ et $B \mid A$ (puisque $\lambda$ et $\frac{1}{\lambda}$ sont des polynômes).
- ⋆ Réciproquement, supposons que $A \mid B$ et $B \mid A$. Il existe alors $P, Q \in \mathbb{K}[X]$ tel que $A = PB$ et $B = AQ$. Par conséquent, $A = PQA$, c'est-à-dire $A(1 - PQ) = 0_{\mathbb{K}[X]}$. Comme l'anneau des polynômes est intègre, on a nécessairement $A = 0_{\mathbb{K}[X]}$ (et alors $B = 0_{\mathbb{K}[X]}$ et $\lambda = 1$ conviennent) ou $PQ = 1$, ce qui est possible que si $P$ et $Q$ sont des constantes non nulles. ■

## 2) Théorème de la division euclidienne

Le résultat suivant est fondamental.

**Théorème (de la division euclidienne dans l'anneau des polynômes)** Soient $A, B \in \mathbb{K}[X]$ tel que $B \neq 0_{\mathbb{K}[X]}$. Il existe un unique couple de polynômes $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

$(i)$ $A = BQ + R$ ;

$(ii)$ $\deg(R) < \deg(B)$.

On dit que l'on a effectué la division euclidienne de $A$ par $B$ ; le polynôme $Q$ est appelé *quotient* tandis que $R$ est le *reste*.

**Exemple** $X^2 + X + 1 = X(X + 1) + 1$ est la division euclidienne de $X^2 + X + 1$ par $X$

**Démonstration** On traite séparément l'existence et l'unicité.

- ⋆ **Existence :** notons $b$ le degré de $B$ et $\beta \in \mathbb{K}^*$ son coefficient dominant.
  - — Si $B$ divise $A$, alors il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. En posant $R = 0_{\mathbb{K}[X]}$, le couple $(Q, R)$ vérifie les propriétés $(i)$ et $(ii)$.
  - — Supposons maintenant que $B$ ne divise pas $A$ et considérons l'ensemble :

$$\mathscr{D} = \left\{ \deg(A - BK) \,\middle|\, K \in \mathbb{K}[X] \right\}$$

L'ensemble $\mathscr{D}$ est une partie de $\mathbb{N}$ (pour tout $K \in \mathbb{K}[X]$, on a $A \neq BK$ par hypothèse) qui est non vide (elle contient $\deg(A)$). Donc $\mathscr{D}$ admet un plus petit élément noté $r \in \mathbb{N}$. Par définition de $r$, il existe $Q \in \mathbb{K}[X]$ tel que $\deg(A - BQ) = r$ ; posons encore $R = A - BQ \in \mathbb{K}[X]$ de sorte que l'égalité $(i)$ soit vérifiée. Il reste à montrer que $\deg(R) < \deg(B)$. Notons $\rho$ le coefficient dominant de $R$ et supposons par l'absurde que $r \geqslant b$. Alors :

$$\deg\left(R - \frac{\rho}{\beta} X^{r-b} B\right) < r$$

En posant $K = Q + \dfrac{\rho}{\beta} X^{r-b}$, on a :

$$\deg\left(R - \frac{\rho}{\beta} X^{r-b} B\right) = \deg(A - BK) \in \mathscr{D}$$

Ceci contredit la minimalité de $r$. Finalement, $r < b$ et l'existence est démontrée.

- ⋆ **Unicité :** soient $(Q_1, R_1)$ et $(Q_2, R_2)$ deux couples de polynômes vérifiant les conditions $(i)$ et $(ii)$. Alors :

$$B(Q_1 - Q_2) = R_2 - R_1$$

Si $Q_1 \neq Q_2$, alors $\deg(Q_2 - Q_1) \geqslant 0$ et alors :

$$\deg\big(B(Q_1 - Q_2)\big) = \deg(B) + \deg(Q_1 - Q_2) \geqslant \deg(B)$$

tandis que $\deg(R_2 - R_1) < \deg(B)$ par définition de $R_1$ et $R_2$. On obtient donc une absurdité. Ainsi, $Q_1 = Q_2$ puis $R_1 = R_2$, d'où l'unicité. ■

## 3) PGCD

**Proposition/définition (PGCD de deux polynômes)** Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0_{\mathbb{K}[X]}$. On appelle *plus grand commun diviseur de $A$ et $B$* (en abrégé PGCD) tout élément de $\mathscr{D}(A) \cap \mathscr{D}(B)$ de degré maximal.

**Démonstration** Justifions l'existence d'un PGCD pour $A$ et $B \neq 0_{\mathbb{K}[X]}$. On sait que $\mathscr{D}(A) \cap \mathscr{D}(B)$ est non vide (en effet, cet ensemble contient $\mathbb{K}^*$) donc l'ensemble :

$$\left\{ \deg(P) \,\middle|\, P \in \mathscr{D}(A) \cap \mathscr{D}(B) \right\}$$

est une partie non vide de $\mathbb{N}$ (car $B \neq 0_{\mathbb{K}[X]}$ donc $\mathscr{D}(B)$ ne contient pas $0_{\mathbb{K}[X]}$) non vide (elle contient 0) et est majorée par $\max(\deg(A), \deg(B))$. Ceci justifie l'existence d'un PGCD pour $A$ et $B$. ■

**Remarques :**

- ⋆ Considérons les polynômes $A = X^2$ et $B = X^2 + X$. Alors $X$ et $-X$ sont deux PGCD de $A$ et $B$. Il n'y a donc pas unicité dans la notion de PGCD.
- ⋆ Si $D$ est un PGCD de $A$ et $B$, alors tout polynôme de la forme $\lambda D$ où $\lambda \in \mathbb{K}^*$ est un PGCD de $A$ et $B$.
- ⋆ Comme dans $\mathbb{Z}$, on peut montrer que :

$$\forall \Delta \in \mathbb{K}[X], \qquad \Delta \text{ est un PGCD de } A \text{ et } B \iff \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta)$$

**Proposition** Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0_{\mathbb{K}[X]}$ et $\Delta, \Delta'$ deux PGCD de $A$ et $B$. Alors $\Delta$ et $\Delta'$ sont associés, *i.e.* :

$$\exists \lambda \in \mathbb{K}^*, \qquad \Delta' = \lambda \Delta$$

**Démonstration** C'est une conséquence immédiate de la proposition 8. ■

**Remarque :** si $\Delta$ est un PGCD de $A$ et $B$, alors l'ensemble des PGCD de $A$ et $B$ est (d'après la proposition précédente) :

$$\left\{ \lambda \Delta \,\middle|\, \lambda \in \mathbb{K}^* \right\}$$

Cet ensemble contient un unique polynôme unitaire. Ceci nous permet de définir « *le* » PGCD de deux polynômes.

**Définition (PGCD de deux polynômes)** Soient $A, B \in \mathbb{K}[X]$.

- ⋆ Si $A$ ou $B$ est non nul, alors le PGCD de $A$ et $B$ est l'unique PGCD unitaire de $A$ et $B$. On le note $A \wedge B$.
- ⋆ Si $A = B = 0_{\mathbb{K}[X]}$, alors on pose $A \wedge B = 0_{\mathbb{K}[X]}$.

Ainsi, le PGCD de $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ est caractérisé par :

$$\Delta = A \wedge B \iff \begin{cases} \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta) \\ \Delta \text{ est unitaire} \end{cases}$$

**Remarque :** si $A \neq 0_{\mathbb{K}[X]}$, alors $A \wedge 1 = 1$ et $A \wedge A = \alpha^{-1} A$ où $\alpha \in \mathbb{K}^*$ est le coefficient dominant de $A$.

Pour trouver le PGCD de deux polynômes, on procèdera comme pour trouver le PGCD de deux entiers relatifs : on utilise l'algorithme d'Euclide étendu. Il sera important de diviser le dernier reste non nul par son coefficient dominant.

**Exemple** ⋆ $(X^2+3X+1)\wedge(X+1)=1$ ;
⋆ $(X^2-3X+2)\wedge(X^3-2X^2+X-2)=X-2$.

Comme dans $\mathbb{Z}$, l'algorithme d'Euclide étendu permet de trouver un *couple de Bézout*.

**Proposition** Soient $A,B\in\mathbb{K}[X]$. Il existe $U,V\in\mathbb{K}[X]$ tels que :

$$AU+BV=A\wedge B$$

**Démonstration** Si $B=0_{\mathbb{K}[X]}$, alors :

$$\forall A\in\mathbb{K}[X],\qquad A+B=A=A\wedge B$$

donc le résultat est vrai. Si $B$ est non nul, on utilise une récurrence forte en raisonnant sur le degré du polynôme $B$. Pour tout $d\in\mathbb{N}$ considérons la proposition suivante :

$$\mathscr{P}_d : \text{« pour tous polynômes } A,B\in\mathbb{K}[X] \text{ tels que } \deg(B)=d, \text{ il existe } U,V\in\mathbb{K}[X] \text{ tels que } AU+BV=A\wedge B\text{ »}$$

⋆ Soient $A,B\in\mathbb{K}[X]$ tels que $\deg(B)=0$. Il existe donc $\lambda\in\mathbb{K}^*$ tel que $B=\lambda X^0=\lambda$ et $A\wedge B=1$. On a la relation $0\times A+\dfrac{1}{\lambda}B=1$ et comme $0,\dfrac{1}{\lambda}\in\mathbb{K}[X]$, la propriété $\mathscr{P}_0$ est vraie.

⋆ Soit $d\in\mathbb{N}$. On suppose que, pour tout $k\in[\![0,d]\!]$, la proposition $\mathscr{P}_k$ est vraie. Montrons que la proposition $\mathscr{P}_{d+1}$ est vraie. Soient $A,B\in\mathbb{K}[X]$ tels que $\deg(B)=d+1$. Comme $B\neq 0_{\mathbb{K}[X]}$, on peut effectuer la division euclidienne de $A$ par $B$ : il existe $Q,R\in\mathbb{K}[X]$ tels que $A=BQ+R$ et $\deg(R)\leqslant d$.

— Si $R=0_{\mathbb{K}[X]}$, alors l'égalité $A=BQ$ se réécrit $A+(1-Q)B=B$, ce qui fournit une relation de Bézout pour les polynômes $A$ et $B$.

— Sinon, on pose $r=\deg(\mathbb{R})\in[\![0,d]\!]$ et on utilise le fait que la proposition $\mathscr{P}_r$ soit vraie : il existe $U,V\in\mathbb{K}[X]$ tels que :

$$BU+RV=B\wedge R=A\wedge B\qquad\text{(algorithme d'Euclide)}$$

Ainsi :

$$BU+(A-BQ)V=A\wedge B\qquad\text{c'est-à-dire}\qquad AV+B(U-QV)=A\wedge B$$

La proposition $\mathscr{P}_{d+1}$ est donc vraie.

La proposition est donc vraie par principe de récurrence forte. ■

**Remarque :** il n'y a pas unicité d'un couple de Bézout.

**Exemple** Reprendre l'un des deux exemples précédents.

## 4) Théorème de Bézout et lemme de Gauss

**Définition (polynômes premiers entre eux)** Soient $A,B\in\mathbb{K}[X]$. On dit que $A$ et $B$ sont premiers entre eux si $A\wedge B=1$.

**Exemple** ⋆ Les polynômes $X^2+1$ et $X^2+X$ sont premiers entre eux.
⋆ Par contre, $X$ et $X^2+X$ ne sont pas premiers entre eux (en effet, $X\wedge(X^2+X)=X$).

Le théorème de Bézout permet de caractériser les polynômes premiers entre eux.

**Théorème (de Bézout)** Soient $A, B \in \mathbb{K}[X]$. Alors :

$$(A \text{ et } B \text{ sont premiers entre eux}) \iff (\exists\, U, V \in \mathbb{K}[X],\ AU + BV = 1)$$

**Démonstration** On raisonne par double implication.

- ⋆ Si $A$ et $B$ sont premiers entre eux, alors $A \wedge B = 1$ et il suffit d'utiliser la proposition précédente (sur les relations de Bézout).
- ⋆ Supposons qu'il existe $U, V \in \mathbb{K}[X]$ tels que $AU+BV = 1$ et posons $\Delta = A \wedge B$. Alors $\Delta \mid A$ et $\Delta \mid B$ donc $\Delta \mid AU+BV$, *i.e.* $\Delta \mid 1$. Ainsi, $\Delta$ est un polynôme constant, et comme il est unitaire, on a nécessairement $\Delta = 1$. ■

**Exemple** Soient $a, b \in \mathbb{K}$ tels que $a \neq b$. Alors $(X-a) \wedge (X-b) = 1$. En effet :

$$\frac{1}{b-a}(X-a) + \left(-\frac{1}{b-a}\right)(X-b) = 1$$

De la même manière, le lemme de Gauss est aussi valable dans $\mathbb{K}[X]$.

**Lemme (de Gauss)** Soient $A, B, C \in \mathbb{K}[X]$. Si :

$$A \mid BC \qquad \text{et} \qquad A \wedge B = 1,$$

alors $A$ divise $C$.

**Démonstration** Comme $A \wedge B = 1$, on sait d'après le théorème de Bézout qu'il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. En multipliant par $C$, on obtient $ACU + BCV = C$. Comme $A \mid BC$, on a $A \mid (ACU + BCV)$, *i.e.* $A \mid C$. ■

✎✎✎ **Exercice** Résoudre dans $\mathbb{K}[X]$ l'équation $(X^3-1)U + (X^2+1)V = 2X^2$.

**Une solution.** On procède comme dans $\mathbb{Z}$ pour résoudre une équation diophantienne.

- ⋆ Comme $(X^3-1) \wedge (X^2+1) = 1$, on peut trouver deux polynômes $U$ et $V$ tels que :

  $$(X^3-1)U + (X^2+1)V = 2$$

  en utilisant l'algorithme d'Euclide étendu. Les polynômes $U = X-1$ et $V = -X^2+X+1$ conviennent.
- ⋆ On en déduit que le couple formé par les polynômes :

  $$U_0 = X^2(X-1) \qquad \text{et} \qquad V_0 = X^2(1+X-X^2)$$

  est solution de l'équation. Ensuite, en utilisant le lemme de Gauss, on montre que les seules solutions sont nécessairement de la forme :

  $$(U_0 + (X^2+1)C, V_0 - (X^3-1)C),$$

  où $C \in \mathbb{K}[X]$.

## 5) PPCM de deux polynômes

Pour tout $A \in \mathbb{K}[X]$, on note $\mathscr{M}(A)$ l'ensemble des polynômes multiples de $A$, *i.e.* :

$$\mathscr{M}(A) = \{AQ \mid Q \in \mathbb{K}[X]\}$$

**Proposition/définition (PPCM)** Soient $A, B \in \mathbb{K}[X]$.

- ⋆ Si $A$ et $B$ sont non nuls, alors il existe un unique polynôme unitaire, noté $A \vee B$, tel que :
$$\mathscr{M}(A) \cap \mathscr{M}(B) = \mathscr{M}(A \vee B)$$
Ce polynôme $A \vee B$ est appelé le PPCM de $A$ et $B$.
- ⋆ Si $A = 0_{\mathbb{K}[X]}$ ou $B = 0_{\mathbb{K}[X]}$, alors on pose $A \vee B = 0_{\mathbb{K}[X]}$.

**Démonstration** La justification de l'existence du PPCM est analogue à celle du PGCD. ■

**Remarques :**

- ⋆ $A \vee B$ est l'unique polynôme unitaire de degré minimal de l'ensemble $\mathscr{M}(A) \cap \mathscr{M}(B)$.
- ⋆ Comme dans le cas entier, les polynômes $(A \wedge B)(A \vee B)$ et $AB$ sont associés (ils sont égaux si le polynôme $AB$ est unitaire).

**Exemple** $(3X^2(X+1)) \vee (X^4(X+2)^2) = X^4(X+1)(X+2)^2$

### 6) Généralisations

**Définition (PGCD d'une famille finie de polynômes)** Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$ une famille de polynômes dont au moins l'un d'entre eux est non nul. On appelle PGCD de $A_1, \dots, A_n$ tout diviseur commun de $A_1, \dots, A_n$ de degré maximal.

On peut montrer que les PGCD de $A_1, \dots, A_n$ sont associés ; il en existe donc un seul qui est unitaire. C'est ce polynôme qu'on appelle *le* PGCD de $A_1, \dots, A_n$ que l'on note $A_1 \wedge \cdots \wedge A_n$.

**Remarque :** si tous les polynômes sont nuls, on pose $A_1 \wedge \cdots \wedge A_n = 0_{\mathbb{K}[X]}$.

**Proposition (relation de Bézout)** Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$ une famille de polynômes dont au moins l'un d'entre eux est non nul. Il existe $(U_1, \dots, U_n) \in (\mathbb{K}[X])^n$ tel que :
$$A_1 \wedge \cdots \wedge A_n = A_1U_1 + \cdots + A_nU_n$$
Une telle relation est appelée *une relation de Bézout de* $A_1, \dots, A_n$.

**Démonstration** Il s'agit de procéder par récurrence sur le nombre de polynômes de la famille. On utilise la relation de Bézout connue pour deux polynômes. ■

**Définition (polynômes premiers entre eux )** Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$ une famille de polynômes dont au moins l'un d'entre eux est non nul.

- ⋆ On dit que $A_1, \dots, A_n$ sont *premiers entre eux dans leur ensemble* si 1 est leur seul diviseur commun unitaire, c'est-à-dire si :
$$A_1 \wedge \cdots \wedge A_n = 1$$
- ⋆ On dit que $A_1, \dots, A_n$ sont *deux à deux premiers entre eux* si :
$$\forall (i,j) \in [\![1,n]\!]^2, \quad i \neq j \implies A_i \wedge A_j = 1$$

Si $A_1, \dots, A_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. La réciproque est fausse.

**Exemple** Soient $A = X(X+1)$, $B = X(X+2)$ et $C = (X+1)(X+2)$. Alors $A$, $B$ et $C$ sont premiers entre eux dans leur ensemble mais :

$$X(X+1) \wedge X(X+2) = X \neq 1$$

donc ils ne sont pas deux à deux premiers entre eux.

**Proposition** Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $P_1, \dots, P_n, Q \in \mathbb{K}[X]$. On suppose que pour tout $k \in [\![1, n]\!]$, on a $P_k \wedge Q = 1$. Alors $(P_1 \dots P_n) \wedge Q = 1$.

**Démonstration** On raisonne par récurrence sur le nombre $n$ de polynômes.

- ⋆ Démontrons la propriété pour $n = 2$. Soient $P_1, P_2, Q \in \mathbb{K}[X]$ tels que $P_1 \wedge Q = 1$ et $P_2 \wedge Q = 1$. D'après le théorème de Bézout, il existe $U_1, U_2, V_1, V_2 \in \mathbb{K}[X]$ tels que :

$$P_1U_1 + QV_1 = 1 \qquad \text{et} \qquad P_2U_2 + QV_2 = 1$$

  En multipliant membre à membre ces égalités, on obtient :

$$(P_1U_1 + QV_1)(P_2U_2 + QV_2) = 1 \qquad i.e. \qquad P_1P_2 \underbrace{U_1U_2}_{\in \mathbb{K}[X]} + Q\underbrace{(P_1U_1V_2 + V_1P_2U_1 + QV_1V_2)}_{\in \mathbb{K}[X]} = 1$$

  D'après le théorème de Bézout, on a bien $P_1P_2 \wedge Q = 1$.
- ⋆ Supposons que la propriété soit vérifiée au rang $n \in \mathbb{N} \setminus \{0,1\}$ et soient $P_1, \dots, P_{n+1}, Q \in \mathbb{K}[X]$ tels que, pour tout $k \in [\![1, n+1]\!]$, on ait $P_k \wedge Q = 1$. Par hypothèse de récurrence, on a $(P_1 \dots P_n) \wedge Q = 1$ puis, en utilisant le résultat démontré au premier point, il vient $(P_1 \dots P_nP_{n+1}) \wedge Q = 1$, ce qu'il fallait démontrer.

La proposition est donc vraie par principe de récurrence simple. ■

**Corollaire** Soient $n \in \mathbb{N} \setminus \{0,1\}$, $P_1, \dots, P_n, R \in \mathbb{K}[X]$. On suppose que :

- ⋆ les polynômes $P_1, \dots, P_n$ sont deux à deux premiers entre eux ;
- ⋆ pour tout $k \in [\![1, n]\!]$, le polynôme $P_k$ divise $R$.

Alors le produit $P_1 \dots P_n$ divise $R$.

**Démonstration** On procède à nouveau par récurrence.

- ⋆ Soient $P_1, P_2, R \in \mathbb{K}[X]$ tels que $P_1 \wedge P_2 = 1$, $P_1 \mid R$ et $P_2 \mid R$. Comme $P_2 \mid R$, il existe $Q \in \mathbb{K}[X]$ tel que $R = P_2Q$. Or $P_1 \mid R$ et $P_1 \wedge P_2 = 1$ donc (d'après le lemme de Gauss) $P_1 \mid Q$. Ainsi, $P_1P_2 \mid P_2Q$, c'est-à-dire $P_1P_2 \mid R$.
- ⋆ Soient $n \in \setminus\{0,1\}$, $P_1, \dots, P_{n+1}, \mathbb{R} \in \mathbb{K}[X]$. On suppose que les polynômes $P_1, \dots, P_n, P_{n+1}$ sont deux à deux premiers entre eux et que, pour tout $k \in [\![1, n+1]\!]$, on a $P_k \mid R$. Par hypothèse de récurrence, on a $P_1 \dots P_n \mid R$. Or, d'après la proposition précédente, les polynômes $P_1 \dots P_n$ et $P_{n+1}$ sont premiers entre eux (car pour tout $k \in [\![1, n]\!]$, on a $P_k \wedge P_{n+1} = 1$) donc, d'après ce qui a été établi au point précédent, on peut conclure que $P_1 \dots P_nP_{n+1} \mid R$.

Le corollaire est donc démontré par principe de récurrence simple. ■

# III – Fonctions polynomiales et racines

## 1) Définition

Un polynôme est un objet formel qui n'est pas une fonction. On définit ici la *fonction polynomiale* associée à un polynôme.

**Définition (fonction polynomiale)** Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. On appelle *fonction polynomiale associée à $P$* l'application :

$$\tilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \sum_{k=0}^{+\infty} a_k x^k \end{array} \right.$$

**Notation.** L'ensemble des fonctions polynomiales à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[x]$.

**Remarque :** si $P \in \mathbb{K}[X]$ et $x \in \mathbb{K}$, alors la quantité « $P(x)$ » n'a a priori aucun sens. Par contre, si $\tilde{P}$ est la fonction polynomiale associée à $P$, alors $\tilde{P}(x)$ est bien défini. On dit qu'on a *évalué* le polynôme $P$ en $x$.

**Exemple** La fonction polynomiale associé à $P = X^2 + 1 \in \mathbb{R}[X]$ est :

$$\tilde{P} : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 + 1 \end{array} \right.$$

**Remarques :**

- ⋆ On montre facilement que $(\mathbb{K}[x], +, \times)$ est un sous-anneau de $\mathbb{K}^{\mathbb{K}}$.
- ⋆ On peut démontrer que, pour tous $P, Q \in \mathbb{K}[X]$, on a les égalités :

$$\tilde{P+Q} = \tilde{P} + \tilde{Q}, \qquad \tilde{PQ} = \tilde{P}\tilde{Q} \qquad \text{et} \qquad \tilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$$

Cette dernière assertion n'est pas évidente : les additions, multiplication et composition sont des opérations différentes dans $\mathbb{K}[X]$ et dans $\mathbb{K}^{\mathbb{K}}$.

## 2) Méthode de Horner (lien avec Python)

La méthode de Horner est un algorithme permettant d'évaluer efficacement un polynôme en un point. Si l'on souhaite calculer :

$$\tilde{P}(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \qquad (\text{où } x \in \mathbb{K}), \tag{1}$$

il n'est pas optimal de calculer chaque $a_k x^k$ ($k$ opérations) et de les ajouter ($d$ opérations). Au total, il y a donc ici :

$$d + \sum_{k=0}^{d} k = d + \frac{d(d+1)}{2} = \frac{d(d+3)}{2} \text{ opérations nécessaires pour calculer } \tilde{P}(x)$$

L'algorithme suivant permet de calculer efficacement $\tilde{P}(x)$. Supposons par exemple que l'on ait à calculer :

$$f(x) = 5x^4 - 4x^3 + 3x^2 - 2x + 1$$

On remarque que :

$$f(x) = (x(x(x(5x-4)+3)-2)+1)$$

En posant $a = 5$, on calcule alors successivement :

$$b = xa - 4 = 5x - 4, \qquad c = xb + 3 = x(5x-4) + 3 \qquad d = xc - 2 \qquad \text{et} \qquad e = xd + 1 = f(x)$$

Plus généralement, si $\tilde{P}(x)$ s'écrit comme dans (1), alors :

$$\tilde{P}(x) = (\cdots(((a_d x + a_{d-1})x + a_{d-2})x + a_{d-3})\cdots)x + a_0$$

Le calcul nécessitera $d$ multiplications et $d$ additions (soit $2d$ opérations).

```
def horner(P,x) :
    """on code un polynôme par la liste de ses coefficients"""
    d = len(P) #degré de P
    valeur = P[d-1] #coefficient dominant
    for i in range(d-2,-1,-1) :
        valeur = valeur*x+P[i]
    return valeur
```

D'après ce qui précède, la complexité temporelle est donc ici linéaire (alors que pour évaluation classique, la complexité est quadratique).

## 3) Racines d'un polynôme

**Définition (racine d'un polynôme)** Soit $P \in \mathbb{K}[X]$.

- ⋆ On appelle *racine de* $P$ tout élément $a$ de $\mathbb{K}$ tel que $\tilde{P}(a) = 0$, où $\tilde{P}$ est la fonction polynomiale associée à $P$.
- ⋆ On note $\mathrm{Rac}_{\mathbb{K}}(P)$ l'ensemble des racines de $P$ dans $\mathbb{K}$.

**Exemple** ⋆ $\mathrm{Rac}_{\mathbb{C}}(X^2+1) = \{-i, i\}$ et $\mathrm{Rac}_{\mathbb{R}}(X^2+1) = \varnothing$

- ⋆ $\mathrm{Rac}_{\mathbb{C}}(X^n - 1) = \mathbb{U}_n$ pour tout $n \in \mathbb{N} \setminus \{0, 1\}$
- ⋆ $\mathrm{Rac}_{\mathbb{K}}(0_{\mathbb{K}[X]}) = \mathbb{K}$

La connaissance d'une racine d'un polynôme permet de le factoriser.

**Proposition (racine et factorisation)** Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :

$$(a \text{ est racine de } P) \iff (X - a \text{ divise } P)$$

**Démonstration** On raisonne par double implication.

$\boxed{\Longleftarrow}$ Supposons que $X - a$ divise $P$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$. On a alors :

$$\forall x \in \mathbb{K}, \qquad \tilde{P}(x) = (x-a)\tilde{Q}(x)$$

En particulier, $\tilde{P}(a) = (a-a)\tilde{Q}(a) = 0$. Donc $a$ est racine de $P$.

$\boxed{\Longrightarrow}$ Supposons que $a$ soit une racine de $P$. D'après le théorème de la division euclidienne, il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

$$P = (X-a)Q + R \qquad \text{avec} \qquad \deg(R) < 1$$

Le polynôme $R$ est donc constant. En considérant les fonctions polynomiales associées et en évaluant en $a$, on obtient que $\tilde{R}(a) = 0$ et donc $R$ est le polynôme nul. Ainsi, $X - a$ divise $P$. ■

**Corollaire** Soient $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{K}$ des racines de $P$ deux à deux distinctes. Alors $\prod_{k=1}^{n}(X - a_k)$ divise $P$.

**Démonstration** Pour tout $k \in [\![1, n]\!]$, on a $X - a_k \mid P$ et les polynômes $X - a_1, \dots, X - a_n$ sont deux à deux premiers entre eux (puisque les scalaires $a_1, \dots, a_n$ sont deux à deux distincts). On déduit alors le résultat du corollaire 1. ■

Le résultat suivant est central dans l'étude des racines d'un polynôme.

**Proposition (majoration du nombre de racines)**
- ⋆ Soit $P \in \mathbb{K}[X]$ un polynôme de degré $d \in \mathbb{N}$. Alors $P$ admet au plus $d$ racines.
- ⋆ Soient $d \in \mathbb{N}$ et $P \in \mathbb{K}_d[X]$. Si $P$ admet au moins $d+1$ racines distinctes, alors $P = 0_{\mathbb{K}[X]}$.

**Démonstration**
- ⋆ Par l'absurde, supposons que $P$ admette au moins $d+1$ racines (deux à deux distinctes) notées $a_1, \dots, a_{d+1}$. D'après la proposition précédente, on sait que $\prod_{k=1}^{d+1}(X - a_k)$ divise $P$. Comme $P$ n'est pas le polynôme nul, cette relation de divisibilité entraîne la relation sur les degrés suivante :
$$d + 1 = \deg\left(\prod_{k=1}^{d+1}(X - a_k)\right) \leqslant \deg(P) = d,$$
ce qui est absurde.
- ⋆ Si $P \in \mathbb{K}_d[X]$ n'est pas le polynôme nul, alors $\delta = \deg(P) \in [\![0, d]\!]$ et donc $P$ admet au plus $\delta$ racines. En particulier, $P$ admet au plus $d$ racines, d'où le deuxième point par contraposition. ■

**Théorème (identification d'un polynôme et de sa fonction polynomiale associée)**
L'application :
$$i : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[x] \\ P & \longmapsto & \tilde{P} \end{array} \right.$$
est bijective.

**Démonstration** Par définition de l'ensemble des fonctions polynomiales, on a l'égalité :
$$\mathbb{K}[x] = \left\{ \tilde{P} \,\middle|\, P \in \mathbb{K}[X] \right\}$$
Autrement dit, l'application $i$ est surjective. Montrons maintenant que $i$ est injective. Soient $P, Q \in \mathbb{K}[X]$ tels que $i(P) = i(Q)$. Alors :
$$i(P - Q) = i(P) - i(Q) = 0_{\mathbb{K}[x]}$$
c'est-à-dire :
$$\forall a \in \mathbb{K}, \qquad i(P - Q)(a) = 0$$
Donc $P - Q$ a une infinité de racines (puisque $\mathbb{K}$ est infini). La proposition précédente implique que $P - Q = 0_{\mathbb{K}[X]}$, donc $P = Q$, ce qui prouve l'injectivité de $i$. ■

**Remarque :** d'après cette proposition, il nous sera désormais possible d'identifier un polynôme avec sa fonction polynomiale associée.

## 4) Racine et multiplicité

Soient $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ et $a \in \mathbb{K}$. Alors l'ensemble :
$$\left\{ k \in \mathbb{N} \,\middle|\, (X - a)^k \text{ divise } P \right\}$$
est une partie de $\mathbb{N}$ qui est non vide (il contient 0 puisque $1 \mid P$) et majorée (par $d$, par des considérations de degrés). Il admet donc un maximum. Ceci légitime la définition suivante.

**Définition (multiplicité d'une racine)** Soient $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ et $a \in \mathbb{K}$. On appelle *multiplicité de $a$ comme racine de $P$* le nombre :

$$m_P(a) = \max\left\{k \in \mathbb{N} \,\middle|\, (X-a)^k \text{ divise } P\right\}$$

**Vocabulaire :**

- ⋆ si $m_P(a) = 1$, on parle de racine simple ;
- ⋆ si $m_P(a) \geqslant 2$, on parle de racine multiple (double, triple,...).

**Remarques :**

- ⋆ Soient $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ et $a \in \mathbb{K}$. Il est clair que :

$$(a \text{ est racine de } P) \iff m_P(a) \geqslant 1$$

- ⋆ Si $P = aX^2 + bX + c \in \mathbb{C}[X]$ est un polynôme de degré 2, on sait que :
  - — ou bien $P$ possède deux racines distinctes réelles ou complexes $\alpha$ et $\beta$ et :

$$P = a(X-\alpha)(X-\beta)$$

    Ces deux racines sont simples.
  - — ou bien $P$ possède une racine double réelle ou complexe $\gamma$ et :

$$P = a(X-\gamma)^2$$

  Dans $\mathbb{R}[X]$, un polynôme peut n'admettre aucune racine réelle. C'est par exemple le cas de $X^2+1$.

**Définition (polynôme scindé)** Soit $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$. On dit que $P$ est *scindé sur* $\mathbb{K}$ si :

$$\sum_{a \in \mathrm{Rac}_{\mathbb{K}}(P)} m_P(a) = \deg(P)$$

Autrement dit, un polynôme non nul est scindé sur $\mathbb{K}$ si et seulement si le nombre de racines, comptées avec multiplicités, coïncide avec son degré.

**Exemple** Soit $P = X^2(X^2+1) \in \mathbb{R}[X]$. On a $\deg(P) = 4$.

- ⋆ De plus, $\mathrm{Rac}_{\mathbb{R}}(P) = \{0\}$ et 0 est une racine de $P$ de multiplicité 2. Mais $2 \neq \deg(P)$ donc $P$ n'est pas scindé sur $\mathbb{R}$.
- ⋆ Par ailleurs, $\mathrm{Rac}_{\mathbb{C}}(P) = \{0, -i, i\}$ et $-i$ et $i$ sont des racines simples de $P$. Le nombre de racines de $P$, comptées avec multiplicités, est égal à $2+1+1 = 4 = \deg(P)$ donc $P$ est scindé sur $\mathbb{C}$.

**Proposition** Soit $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ de coefficient dominant noté $C_P$. Alors :

$$P \text{ est scindé sur } \mathbb{K} \iff P = C_P \prod_{a \in \mathrm{Rac}_{\mathbb{K}}(P)} (X-a)^{m_P(a)}$$

**Démonstration** $\boxed{\Longleftarrow}$ Si $P = C_P \prod_{a\in \mathrm{Rac}_{\mathbb{K}}(P)} (X-a)^{m_P(a)}$ alors, en prenant les degrés, on a :

$$\sum_{a\in \mathrm{Rac}_{\mathbb{K}}(P)} m_P(a) = \deg(P)$$

et donc $P$ est scindé sur $\mathbb{K}$.

$\boxed{\Longrightarrow}$ Supposons que $P$ soit scindé sur $\mathbb{K}$. Pour tout $a \in \mathrm{Rac}_{\mathbb{K}}(P)$, on sait que $(X-a)^{m_P(a)}$ divise $P$ par définition de $m_P(a)$. De plus les polynômes $(X-a)^{m_P(a)}$, où $a \in \mathrm{Rac}_{\mathbb{K}}(P)$, sont deux à deux premiers entre eux donc, d'après le corollaire 1, on a :

$$\prod_{a\in \mathrm{Rac}_{\mathbb{K}}(P)} (X-a)^{m_P(a)} \mid P$$

Dans cette division, les deux polynômes sont de même degré puisque $P$ est scindé. Donc ces polynômes sont associés. La constante multiplicative manquante est nécessairement $C_P$ par identification des coefficients dominants. ■

## 5) Relations coefficients-racines (formules de Viète)

⋆ Soit $P = a_2X^2+a_1X+a_0 \in \mathbb{K}_2[X]$ un polynôme *scindé* sur $\mathbb{K}$ de degré 2. Il existe alors $\lambda_1, \lambda_2 \in \mathbb{K}$ tels que :

$$P = a_2(X-\lambda_1)(X-\lambda_2)$$

Développons :

$$P = a_2(X^2 - (\lambda_1+\lambda_2)X + \lambda_1\lambda_2)$$

ce qui donne, après identification :

$$\lambda_1+\lambda_2 = -\frac{a_1}{a_2} \qquad \text{et} \qquad \lambda_1\lambda_2 = \frac{a_0}{a_2}$$

⋆ Soit $P = a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{K}[X]$ un polynôme scindé sur $\mathbb{K}$ de racines $\lambda_1, \lambda_2, \lambda_3$ (certaines pouvant éventuellement être confondues). Alors :

$$P = a_3(X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$$

soit, en développant :

$$P = a_3X^3 - a_3(\lambda_1+\lambda_2+\lambda_3)X^2 + a_2(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3)X - a_3\lambda_1\lambda_2\lambda_3$$

En identifiant, on obtient :

$$\lambda_1+\lambda_2+\lambda_3 = -\frac{a_1}{a_3}, \qquad \lambda_1\lambda_2\lambda_3 = -\frac{a_0}{a_3} \qquad \text{et} \qquad \lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3 = \frac{a_1}{a_3}$$

Plus généralement, on a le résultat suivant.

**Théorème (relations coefficients-racines ou formules de Viète)** Soit $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$ (on a donc $a_n \neq 0$) scindé sur $\mathbb{K}$. Notons $\lambda_1, \dots, \lambda_n$ les racines de $P$ (certaines pouvant éventuellement être confondues). Pour tout $k \in [\![1, n]\!]$, on pose :

$$\sigma_k = \sum_{1\leqslant i_1<\dots<i_k\leqslant n} \lambda_{i_1}\dots\lambda_{i_k} \qquad (\textit{fonction symétrique élémentaire})$$

Alors :

$$\forall k \in [\![1,n]\!], \qquad \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}$$

**Remarque :** toutes ces égalités sont équivalentes (par unicité des coefficients d'un polynôme) à l'égalité :

$$P = a_n \prod_{k=1}^{n} (X - \lambda_k) = a_n(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^n \sigma_n) \qquad (*)$$

**Démonstration** Il s'agit essentiellement de se convaincre que $(*)$ est vraie. ■

✎✎✎ **Exercice** Résoudre dans $\mathbb{C}^3$ le système :

$$\mathscr{S} : \begin{cases} x+y+z &= 2 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z} &= \frac{5}{6} \\ xyz &= -6 \end{cases}$$

**Une solution.** Soit $(x,y,z) \in (\mathbb{C}^*)^3$. Alors :

$$\begin{cases} x+y+z &= 2 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z} &= \frac{5}{6} \\ xyz &= -6 \end{cases} \iff \begin{cases} x+y+z &= 2 \\ xy+xz+yz &= -5 \\ xyz &= -6 \end{cases}$$

donc, d'après les relations coefficients-racines, $(x,y,z)$ est solution de $\mathscr{S}$ si et seulement si $x, y$ et $z$ sont racines dans $\mathbb{C}^*$ du polynôme :

$$X^3 - 2X^2 - 5X + 6 = (X-1)(X^2 - X - 6) = (X-1)(X+2)(X-3)$$

L'ensemble des solutions de $\mathscr{S}$ est donc :

$$\big\{(1,-2,3),(1,3,-2),(-2,1,3),(-2,3,1),(1,-2,3),(1,3,-2)\big\}$$

# IV – Dérivation

## 1) Dérivée formelle d'un polynôme

**Définition (dérivée formelle)** Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. On appelle *dérivée formelle de* $P$, notée $P'$, le polynôme :

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

**Remarque :** si $P \in \mathbb{K}_0[X]$, alors $P' = 0_{\mathbb{K}[X]}$.

**Exemple** ⋆ Si $P = X^3 + 2X + 1$, alors $P' = 3X^2 + 2$.

⋆ Si $P = 3X^0 = 3$, alors $P = 0_{\mathbb{K}[X]}$.

**Remarques :**

⋆ On définit par récurrences les dérivées formelles d'ordre supérieur d'un polynôme. Si $P \in \mathbb{K}[X]$, alors on pose $P^{(0)} = P$ et, pour tout $n \in \mathbb{N}$, on pose $P^{(n+1)} = (P^{(n)})'$.

⋆ Soit $P \in \mathbb{R}[X]$. La fonction polynomiale $\tilde{P} \in \mathbb{R}^{\mathbb{R}}$ associée à $P$, est une fonction dérivable sur $\mathbb{R}$ (au sens analytique du terme) et sa dérivée $\tilde{P}'$ correspond à la fonction polynomiale de la dérivée formelle $P'$ de $P$. Autrement dit :

$$\tilde{P}' = \tilde{P'}$$

Les propriétés relatives à la dérivation formelle sont les suivantes.

**Proposition** Soient $P, Q \in \mathbb{K}[X]$.

(*i*) On a $\deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) \geqslant 1 \\ -\infty & \text{si } \deg(P) \in \{-\infty, 0\} \end{cases}$ et, plus généralement,

$$\forall n \in \mathbb{N}, \qquad \deg(P^{(n)}) = \begin{cases} \deg(P) - n & \text{si } \deg(P) \geqslant n \\ -\infty & \text{si } \deg(P) \in \{-\infty, 0, \dots, n-1\} \end{cases}$$

(*ii*) $(P+Q)' = P' + Q'$ et, plus généralement, $(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$ pour tout $n \in \mathbb{N}$

(*iii*) $(PQ)' = P'Q + PQ'$ et, plus généralement :

$$\forall n \in \mathbb{N}, \qquad (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)} \qquad \text{(formule de Leibniz)}$$

(*iv*) $(P \circ Q)' = Q' \times (P' \circ Q)$

**Démonstration**

(*i*) Soit $d = \deg(P) \in \mathbb{N} \cup \{-\infty\}$ le degré de $P$. Si $d \in \{-\infty, 0\}$, alors $P$ est constant et alors $P' = 0_{\mathbb{K}[X]}$ donc $\deg(P') = -\infty$. Supposons maintenant que $d \geqslant 1$. Le monôme de plus haut degré de $P'$ est $da_d X^{d-1}$ (on a bien $da_d \neq 0$) donc $\deg(P) = d - 1$. On généralise par récurrence au cas des dérivées successives.

(*ii*) & Co La formule de Leibniz se démontre par récurrence, la preuve est la même que dans $\mathbb{C}$ (l'argument clé est la commutativité du produit dans l'anneau des polynômes). Pour les autres identités, il faut revenir à la définition de la somme, d'un produit et de la composée de deux polynômes. ■

## 2) Formule de Taylor polynomiale

**Théorème (formule de Taylor polynomiale)** Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :

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

En particulier (en prenant $a = 0$) :

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

**Remarques :**

- ⋆ La notation $P^{(k)}(a)$ est ici abusive : on a identifié polynôme et fonction polynomiale associée.
- ⋆ Les coefficients du polynôme $P$ s'expriment donc en fonction des dérivées successives en 0.

**Démonstration** Posons $P = \sum_{k=0}^{+\infty} a_k X^k$.

⋆ Soit $\ell \in \mathbb{N}$. En dérivant $\ell$ fois le polynôme $P$, on obtient :

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

En évaluant en 0, il vient $P^{(\ell)}(0) = a_\ell \ell\,!$. Ainsi, $a_\ell = \dfrac{P^{(\ell)}(0)}{\ell\,!}$ et donc $P = \sum_{k=0}^{+\infty} \dfrac{P^{(k)}(0)}{k\,!} X^k$.

⋆ On étudie maintenant le cas général. Soit $a \in \mathbb{K}$. Posons $Q = P(X+a) \in \mathbb{K}[X]$. Alors, pour tout $k \in \mathbb{N}$, on a $Q^{(k)}(X) = P^{(k)}(X+a)$ (dérivation d'une composée). Alors :

$$Q = \sum_{k=0}^{+\infty} \frac{Q^{(k)}(0)}{k\,!} X^k = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k\,!} X^k$$

On obtient le polynôme $P$ en composant à droite par le polynôme $X - a$. ■

✎✎✎ **Exercice** Montrer qu'il existe un unique polynôme $P$ de degré inférieur ou égal à 2 tel que $P(0) = 0$, $P'(0) = 2$ et $P'(0) = 3$.

Le résultat qui suit est très pratique pour étudier les racines multiples d'un polynôme et pour déterminer la multiplicité de celles-ci.

**Corollaire (étude pratique de la multiplicité)** Soient $a \in \mathbb{K}$, $k \in \mathbb{N}$ et $P \in \mathbb{K}[X]$. Alors :

$$m_P(a) = k \iff \begin{cases} \forall \ell \in [\![0, k-1]\!],\ P^{(\ell)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}$$

**Démonstration** On raisonne par double implication.

⟸ Supposons que pour tout $\ell \in [\![0, k-1]\!]$, on a $P^{(\ell)}(a) = 0$ et que $P^{(k)}(a) \neq 0$. D'après la formule de Taylor polynomiale :

$$P = \sum_{\ell=k}^{+\infty} \frac{P^{(\ell)}(a)}{\ell\,!}(X-a)^\ell = \frac{P^{(k)}(a)}{k\,!}(X-a)^k + \underbrace{(X-a)^{k+1} \sum_{\ell=k+1}^{+\infty} \frac{P^{(\ell)}(a)}{\ell\,!}(X-a)^{\ell-k-1}}_{:=Q}$$

Ainsi $(X-a)^k \mid P$ donc $m_P(a) \geqslant k$. Par l'absurde, si $m_P(a) \geqslant k+1$, alors $(X-a)^{k+1} \mid P - Q$ *i.e.* :

$$(X-a)^{k+1} \mid \frac{P^{(k)}(a)}{k\,!}(X-a)^k$$

ce qui est absurde car $P^{(k)}(a) \neq 0$.

⟹ Supposons que $m_P(a) = k$.

⋆ En particulier, $(X-a)^k \mid P$ donc, d'après la formule de Taylor polynômiale, on a :

$$(X-a)^k \mid \sum_{\ell=0}^{k-1} \frac{P^{(\ell)}(a)}{\ell\,!}(X-a)^\ell =: Q$$

Si $Q$ n'est pas le polynôme nul, alors on obtient une absurdité en considérant les degrés (le polynôme de gauche est de degré $k$, celui de droite est de degré au plus $k-1$). Ainsi, $Q = 0_{\mathbb{K}[X]}$. Par conséquent :

$$Q \circ (X+a) = \sum_{\ell=0}^{k-1} \frac{P^{(\ell)}(a)}{\ell\,!} X^\ell = 0_{\mathbb{K}[X]}$$

Par unicité des coefficients du polynôme nul, on en déduit que :

$$\forall \ell \in [\![0, k-1]\!], \qquad P^{(\ell)}(a) = 0$$

⋆ Si $P^{(k)}(a) \neq 0$, alors (d'après la formule de Taylor polynomiale et le point précédent), on a :

$$P = \sum_{\ell=k+1}^{+\infty} \frac{P^{(\ell)}(a)}{\ell\,!}(X-a)^\ell,$$

ce qui prouve que $P$ est divisible par $(X-a)^{k+1}$. Ceci contredit la définition de $k$.

Le corollaire est démontré. ■

**Exemple** Le polynôme $P = X^4 + 3X^3 - 3X^2 - 7X + 6$ admet 1 pour racine double. Il suffit en effet de vérifier que $P(1) = P'(1) = 0$ et que $P''(1) \neq 0$.

# V – Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$

## 1) Notion de polynôme irréductible sur $\mathbb{K}$

**Définition (polynôme irréductible)** Soit $P \in \mathbb{K}[X]$. On dit que $P$ est *irréductible sur* $\mathbb{K}$ si :

- ⋆ $P$ est non constant ;
- ⋆ et si :

$$\forall Q, R \in \mathbb{K}[X], \qquad P = QR \implies Q \in \mathbb{K}_0[X] \text{ ou } R \in \mathbb{K}_0[X]$$

**Exemple**

- ⋆ Tout polynôme $P \in \mathbb{K}[X]$ de degré 1 est irréductible sur $\mathbb{K}$.
- ⋆ Un polynôme $P \in \mathbb{R}[X]$ de degré 2 et de discriminant strictement négatif est irréductible sur $\mathbb{R}$ ; par contre, nous allons voir qu'il est toujours *réductible* sur $\mathbb{C}$. Par exemple, $P = X^2 + 1 \in \mathbb{R}[X]$ est irréductible sur $\mathbb{R}$ et on a la factorisation $P = (X - i)(X + i)$ dans $\mathbb{C}[X]$.

**Théorème** Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Alors $P$ peut se décomposer comme produit de polynômes irréductibles sur $\mathbb{K}$.

**Démonstration** On utilise une récurrence forte sur le degré. Pour tout entier naturel $n$ non nul, on considère la propriété $\mathscr{P}_n$ : « tout polynôme $P \in \mathbb{K}[X]$ non constant de degré $n$ se décompose comme produit de polynômes irréductibles sur $\mathbb{K}$ ».

- Tout polynôme de degré 1 étant irréductible sur $\mathbb{K}$, la proposition $\mathscr{P}_1$ est vrai.
- Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$ un polynôme de degré $n+1$. Si $P$ est irréductible sur $\mathbb{K}$, alors il n'y a rien à démontrer. Supposons maintenant que $P$ ne soit pas irréductible. Comme $P$ est non constant, il existe deux polynômes $Q$ et $R$ à coefficients dans $\mathbb{K}$ non constants tels que $P = QR$. On a alors $\deg(Q) \leqslant n$ et $\deg(R) \leqslant n$ et, par hypothèse de récurrence, $Q$ et $R$ se décomposent en produits de polynômes irréductibles sur $\mathbb{K}$, ce qui démontre la propriété pour le polynôme $P$. La propriété est donc héréditaire. ■

**Exemple** Soit $n \in \mathbb{N}^*$. Le polynôme $X^n - 1$ admet exactement $n$ racines qui sont les racines $n^{\text{e}}$ de l'unité. Ce polynôme est donc scindé et on a la décomposition de $X^n - 1$ sur $\mathbb{C}$ en produit de facteurs irréductibles suivante :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{i\frac{2k\pi}{n}}\right)$$

puisque le coefficient dominant de $X^n - 1$ est égal à 1.

✎✎✎ **Exercice** Décomposer le polynôme $P = X^3 + 27$ en produit de facteurs irréductibles sur $\mathbb{C}$.

## 2) Factorisation dans $\mathbb{C}[X]$

La question essentielle à laquelle nous n'avons pas encore répondue est la suivante :

*Tout polynôme non constant possède-t-il une racine ?*

La réponse affirmative suivante est un théorème majeur en mathématiques que l'on admettra. On l'appelle aussi *théorème fondamental de l'algèbre*.

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

**Démonstration** admis ■

On en déduit immédiatement les polynômes irréductibles sur $\mathbb{C}$.

**Corollaire** Les polynômes irréductibles sur $\mathbb{C}$ sont les polynômes de degré 1.

**Démonstration**
- ⋆ Il est clair que tout polynôme de degré 1 est irréductible sur $\mathbb{C}$.
- ⋆ Réciproquement, si $P \in \mathbb{K}[X]$ est irréductible sur $\mathbb{C}$, alors il est de degré supérieur ou égal à 1. Donc il admet une racine $a \in \mathbb{C}$ (d'après le théorème de D'Alembert-Gauss) ; il existe donc $R \in \mathbb{C}[X]$ tel que $P = (X-a)R$. Mais $P$ est irréductible sur $\mathbb{C}$ donc (par définition de l'irréductibilité), le polynôme $R$ est constant (non nul). Donc $P$ est de degré 1. ■

**Remarque :** si $P \in \mathbb{K}[X]$ est non constant et si $\alpha$ est une racine de $P$, alors on peut écrire $P = (X-\alpha)Q$ où $\deg(Q) = \deg(P) - 1$. Si $Q$ est non constant, alors il admet une racine dans $\mathbb{C}$ (qui est aussi une racine de $P$), *etc.* On en déduit le résultat suivant.

**Corollaire** Soit $P \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$. Alors $P$ est scindé sur $\mathbb{C}$ :

$$P = C_P \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)} (X-\alpha)^{m_P(\alpha)},$$

où $C_P$ est le coefficient dominant de $P$.

### 3) D'autres conséquences du théorème de D'Alembert-Gauss

**Corollaire (critère de divisibilité)** Soient $A, B \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$. Alors :

$$A \mid B \iff (*) \begin{cases} \mathrm{Rac}_{\mathbb{C}}(A) \subset \mathrm{Rac}_{\mathbb{C}}(B) \\ \forall a \in \mathrm{Rac}_{\mathbb{C}}(A),\ m_A(a) \leqslant m_B(a) \end{cases}$$

**Démonstration** On raisonne par double implication.

$\boxed{\Longrightarrow}$ Supposons que $A \mid B$. Il existe alors $Q \in \mathbb{C}[X]$ tel que $B = AQ$. Soit $a \in \mathrm{Rac}_{\mathbb{C}}(A)$. Alors $A(a) = 0$ donc $B(a) = A(a)Q(a) = 0$. Ainsi, $a \in \mathrm{Rac}_{\mathbb{C}}(B)$ ce qui prouve l'inclusion $\mathrm{Rac}_{\mathbb{C}}(A) \subset \mathrm{Rac}_{\mathbb{C}}(B)$. De plus, pour tout $a \in \mathrm{Rac}_{\mathbb{C}}(A)$, on a $(X-a)^{m_A(a)} \mid A$ (par définition de la multiplicité) et comme $A \mid B$, on a $(X-a)^{m_A(a)} \mid B$ (par transitivité de la relation $\mid$). Ainsi, $m_A(a) \leqslant m_B(a)$ (par définition de la multiplicité).

$\boxed{\Longleftarrow}$ Supposons que la condition $(*)$ soit vérifiée. D'après le corollaire 5, on a :

$$\begin{aligned} B &= C_B \prod_{b\in \mathrm{Rac}_{\mathbb{C}}(B)} (X-b)^{m_B(b)} \\ &= \underbrace{\left(C_A \prod_{b\in \mathrm{Rac}_{\mathbb{C}}(A)} (X-b)^{m_A(b)}\right)}_{=A} \left(\frac{C_A}{C_B} \prod_{b\in \mathrm{Rac}_{\mathbb{C}}(A)} (X-b)^{m_B(b)-m_A(b)}\right) \\ &\qquad \times \left(\prod_{b\in \mathrm{Rac}_{\mathbb{C}}(B)\setminus \mathrm{Rac}_{\mathbb{C}}(A)} (X-b)^{m_B(b)}\right) \end{aligned}$$

Ainsi, $A \mid B$. ■

**Exemple** Pour tout entier naturel $n$, le polynôme $P_n = X^{3n+2} + X^{3n+1} + X^{3n}$ est divisible par $X^2 + X + 1$.

**Corollaire (critère de primalité)** Soient $A, B \in \mathbb{C}[X]$. Alors :

$$A \wedge B = 1 \iff \mathrm{Rac}_{\mathbb{C}}(A) \cap \mathrm{Rac}_{\mathbb{C}}(B) = \varnothing$$

**Démonstration** On raisonne par double implication.

$\boxed{\Longrightarrow}$ Supposons que $A$ et $B$ soient premiers entre eux. D'après le théorème de Bézout, il existe $U, V \in \mathbb{C}[X]$ tels que $AU + BV = 1$. Par l'absurde, supposons que $A$ et $B$ admette une racine complexe commune notée $\alpha$. En évaluant en $\alpha$ dans la relation de Bézout, on obtient $A(\alpha)U(\alpha) + B(\alpha)V(\alpha) = 1$, ce qui fournit l'absurdité $0 = 1$. Donc $\mathrm{Rac}_{\mathbb{C}}(A) \cap \mathrm{Rac}_{\mathbb{C}}(B) = \varnothing$.

$\boxed{\Longrightarrow}$ Supposons que $\mathrm{Rac}_{\mathbb{C}}(A) \cap \mathrm{Rac}_{\mathbb{C}}(B) = \varnothing$. Par l'absurde, si $D := A \wedge B \neq 1$, alors $\deg(D) \geqslant 1$. D'après le théorème de D'Alembert-Gauss, $D$ admet une racine complexe $\alpha$. Comme $D \mid A$ et $D \mid B$, le nombre $\alpha$ est aussi une racine de $A$ et de $B$, ce qui contredit l'hypothèse. Donc $A \wedge B = 1$. ■

**Exemple** Les polynômes $X(X+1)(X+2)^2$ et $(X-1)(X+4)^3$ sont premiers entre eux.

### 4) Factorisation dans $\mathbb{R}[X]$

On sait qu'un polynôme à coefficient réel peut ne pas être scindé sur $\mathbb{R}$ ; c'est par exemple le cas du polynôme $X^2 + 1$.

**Proposition**

- ⋆ Soient $P \in \mathbb{R}[X]$ et $\lambda \in \mathbb{C}$ une racine de $P$. Alors $\bar{\lambda}$ est racine de $P$ et $m_P(\bar{\lambda}) = m_P(\lambda)$.
- ⋆ Les polynômes irréductibles sur $\mathbb{R}$ sont :
  - — les polynômes de degré 1 à coefficients réels ;
  - — et les polynômes de la forme $aX^2 + bX + c$ $((a,b,c) \in \mathbb{R}^* \times \mathbb{R}^2)$ tels que $b^2 - 4ac < 0$.
- ⋆ Pour tout $P \in \mathbb{R}[X] \setminus \mathbb{R}_0[X]$, on a la décomposition suivante (en notant $C_P$ le coefficient dominant de $P$) :

$$P = C_P \prod_{\alpha\in \mathrm{Rac}_{\mathbb{R}}(P)} (X-\alpha)^{m_P(\alpha)} \prod_{\substack{\alpha\in \mathrm{Rac}_{\mathbb{C}}(P)\setminus \mathrm{Rac}_{\mathbb{R}}(P) \\ \mathrm{Im}(\alpha)>0}} (X - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2)$$

**Démonstration** ⋆ Soient $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{R}[X]$ et $\lambda \in \mathrm{Rac}_{\mathbb{C}}(P)$. Alors $P(\lambda) = 0$, *i.e.* $\sum_{k=0}^{+\infty} a_k \lambda^k = 0$.
En considérant le conjugué de ce nombre complexe et en utilisant les propriétés de la conjugaison, on a :

$$0 = \bar{0} = \overline{\sum_{k=0}^{+\infty} a_k \lambda^k} = \sum_{k=0}^{+\infty} \overline{a_k \lambda^k} = \sum_{k=0}^{+\infty} a_k \left(\overline{\lambda}\right)^k \qquad (\text{car } a_k \in \mathbb{R})$$
$$= P(\bar{\lambda})$$

donc $\bar{\lambda} \in \mathrm{Rac}_{\mathbb{C}}(P)$. De plus, pour tout $d \in \mathbb{N}$, on a :

$$\begin{aligned} m_P(\lambda) = d &\iff \begin{cases} \forall k \in [\![0, d-1]\!],\ P^{(k)}(\lambda) = 0 \\ P^{(d)}(\lambda) \neq 0 \end{cases} \\ &\iff \begin{cases} \forall k \in [\![0, d-1]\!],\ P^{(k)}(\bar{\lambda}) = 0 \\ P^{(d)}(\bar{\lambda}) \neq 0 \end{cases} \qquad (\text{d'après ce qui précède}) \\ &\iff m_P(\bar{\lambda}) = d \end{aligned}$$

donc $m_P(\lambda) = m_P(\bar{\lambda})$.

⋆ On raisonne par analyse-synthèse.

— **Analyse :** supposons que $P \in \mathbb{R}[X] \backslash \mathbb{R}_0[X]$ soit un polynôme irréductible sur $\mathbb{R}$. D'après le théorème de D'Alembert-Gauss, $P$ admet une racine complexe notée $\alpha \in \mathbb{C}$. Si $\alpha \in \mathbb{R}$, alors il existe $Q \in \mathbb{R}[X]$ tel que $P = (X - \alpha)Q$. Or $P$ est irréductible sur $\mathbb{R}$ donc $Q$ est constant. Si $\alpha \in \mathbb{C} \setminus \mathbb{R}$, alors $\bar{\alpha}$ est racine de $P$. Comme $\alpha \neq \bar{\alpha}$, le polynôme $P$ est divisible par $(X - \alpha)(X - \bar{\alpha})$ dans $\mathbb{C}[X]$. Il existe donc $Q \in \mathbb{C}[X]$ tel que :

$$P = (X - \alpha)(X - \bar{\alpha})Q \tag{2}$$

Justifions maintenant que $Q$ est à coefficients réels. Comme $(X - \alpha)(X - \bar{\alpha})$ est un polynôme non nul à coefficients réels, on peut effectuer la division euclidienne de $P$ par ce polynôme dans $\mathbb{R}[X]$ : il existe donc $\tilde{Q}, R \in \mathbb{R}[X]$ tels que :

$$P = (X - \alpha)(X - \bar{\alpha})\tilde{Q} + R \qquad \text{avec} \qquad \deg(R) < 2 \tag{3}$$

En soustrayant (3) à (2), on obtient :

$$(X - \alpha)(X - \bar{\alpha})(Q - \tilde{Q}) = R$$

Si $Q \neq \tilde{Q}$, alors $R$ serait de degré supérieur ou égal à 2, ce qui est absurde. On en déduit que $Q = \tilde{Q} \in \mathbb{R}[X]$ (et $R = 0_{\mathbb{R}[X]}$). Finalement, $P = (X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2)Q$ et $P$ est irréductible sur $\mathbb{R}$ donc $Q$ est un polynôme constant. Ainsi, si $P$ est irréductible sur $\mathbb{R}$, alors il est bien de l'une des deux formes annoncée.

— **Synthèse :** si $P$ est un polynôme de degré 1 à coefficients réels, alors il est clairement irréductible sur $\mathbb{R}$. Supposons maintenant qu'il est de degré 2 à coefficients réels et de discriminant strictement négatif. S'il était réductible sur $\mathbb{R}$, il existerait deux polynômes non constants $Q$ et $R$ à coefficients réels tels que $P = QR$. Les polynômes $Q$ et $R$ sont alors de degré 1 et donc $P$ admet une racine réelle, ce qui contredit l'hypothèse sur le discriminant.

⋆ Soit $P \in \mathbb{R}[X] \setminus \mathbb{R}_0[X]$. Alors $P$ est scindé sur $\mathbb{C}$ et, en notant $C_P$ le coefficient dominant de $P$, on a :

$$\begin{aligned} P &= C_P \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)} (X - \alpha)^{m_P(\alpha)} \\ &= C_P \prod_{\alpha \in \mathrm{Rac}_{\mathbb{R}}(P)} (X - \alpha)^{m_P(\alpha)} \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \backslash \mathrm{Rac}_{\mathbb{R}}(P)} (X - \alpha)^{m_P(\alpha)} \\ &= C_P \prod_{\alpha \in \mathrm{Rac}_{\mathbb{R}}(P)} (X - \alpha)^{m_P(\alpha)} \prod_{\substack{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \backslash \mathrm{Rac}_{\mathbb{R}}(P) \\ \mathrm{Im}(\alpha) > 0}} (X - \alpha)^{m_P(\alpha)} (X - \bar{\alpha})^{m_P(\alpha)} \end{aligned}$$

en utilisant le premier point. Ceci achève la démonstration. ■

## VI – Interpolation de Lagrange

On considère le problème suivant. Considérons un entier $n$ supérieur ou égal à 2 et $x_1, \dots, x_n \in \mathbb{R}$ tels que $x_1 < \cdots < x_n$. Soit encore $y_1, \dots, y_n \in \mathbb{R}$. Le problème de l'*interpolation* consiste à trouver une fonction $f \in \mathbb{R}^{[x_1,x_n]}$ telle que :

$$\forall k \in [\![1,n]\!], \qquad f(x_k) = y_k$$

Il est aisé d'en trouver au moins une : il suffit de relier les points de manière linéaire (on obtient alors une fonction affine par morceaux). Ici, on cherche des solutions polynomiales.

**Proposition/définition (polynômes de Lagrange)** Soient $x_1, \dots, x_n \in \mathbb{K}$ des scalaires deux à deux distincts. Pour tout $i \in [\![1,n]\!]$, on pose :

$$L_i = \prod_{\substack{k=1 \\ k\neq i}}^{n} \frac{X - x_k}{x_i - x_k}$$

Les polynômes $L_1, \dots, L_n$ sont appelés *polynômes de Lagrange associés* aux scalaires $x_1, \dots, x_n$. On a alors :

$$\forall i,j \in [\![1,n]\!], \qquad L_i(x_j) = \delta_{i,j}$$

Pour tout $i \in [\![1,n]\!]$, on a de plus :

$$\deg(L_i) = n \qquad \text{et} \qquad \mathrm{Rac}_{\mathbb{K}}(L_i) = \left\{ x_k \,\middle|\, k \in [\![1,n]\!] \setminus \{i\} \right\}$$

**Démonstration** Soient $i,j \in [\![1,n]\!]$. On a :

- ⋆ Si $j = i$, alors :
$$L_i(x_i) = \prod_{\substack{k=1 \\ k\neq i}}^{n} \frac{x_i - x_k}{x_i - x_k} = 1 = \delta_{i,i}$$
- ⋆ Si $j \neq i$, alors :
$$L_i(x_j) = \frac{x_j - x_j}{x_i - x_j} \prod_{\substack{k=1 \\ k\notin\{i,j\}}}^{n} \frac{x_i - x_k}{x_i - x_k} = 0 = \delta_{i,j}$$

Les autres propriétés du polynôme $L_i$ sont immédiates. ■

**Exemple** Pour $n = 3$, les polynômes de Lagrange associés aux scalaires deux à deux distincts $x_1$, $x_2$ et $x_3$ sont :

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

Le résultat central est le suivant.

**Théorème (polynôme d'interpolation de Lagrange de degré minimal)** Soient $x_1, \dots, x_n \in \mathbb{K}$ des scalaires deux à deux distincts et $y_1, \dots, y_n \in \mathbb{K}$ (quelconques). Il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que :

$$\forall k \in [\![1,n]\!], \qquad P(x_k) = y_k$$

Il s'agit du polynôme :

$$P = \sum_{i=1}^{n} y_i L_i,$$

où $L_1, \dots, L_n$ sont les polynômes de Lagrange associés aux scalaires $x_1, \dots, x_n$. On dit que $P$ est le *polynôme interpolateur de Lagrange de degré minimal* du nuage de points $\left\{ (x_k, y_k) \,\middle|\, k \in [\![1,n]\!] \right\}$.

**Démonstration** On démontre séparément l'existence et l'unicité.

⋆ **Existence.**
Posons $P = \sum_{i=1}^{n} y_i L_i$. Les polynômes $L_1, \dots, L_n$ sont de degré $n-1$ donc $\deg(P) \leqslant n-1$ (d'après les propriétés sur le degré). De plus :

$$\forall j \in [\![1,n]\!], \qquad P(x_j) = \sum_{i=1}^{n} y_i L_i(x_j) = \sum_{i=1}^{n} y_i \delta_{i,j} = y_j,$$

ce qui démontre l'existence.

⋆ **Unicité.**
Soient $P, Q \in \mathbb{K}_{n-1}[X]$ tels que :

$$\forall i \in [\![1,n]\!], \qquad P(x_i) = Q(x_i) = y_i$$

On a alors :

$$\forall i \in [\![1,n]\!], \qquad (P-Q)(x_i) = 0$$

Le polynôme $P-Q$ est de degré inférieur ou égal à $n-1$ (puisque les polynômes $P$ et $Q$ le sont, et d'après les propriétés sur le degré) et admet au moins $n$ racines deux à deux distinctes (les scalaires $x_1, \dots, x_n$). On en déduit que $P - Q = 0_{\mathbb{K}[X]}$, c'est-à-dire que $P = Q$. ■

✎✎✎ **Exercice** Déterminer un polynôme $P \in \mathbb{R}[X]$ tel que $P(1) = 3$, $P(-1) = 2$ et $P(2) = -1$.

**Solution.** On a ici $x_1 = 1$, $x_2 = -1$, $x_3 = 2$, $y_1 = 3$, $y_2 = 2$ et $y_3 = -1$. Les polynômes de Lagrange associés à $x_1, x_2, x_3$ sont :

$$L_1 = \frac{(X+1)(X-2)}{(1+1)(1-2)} = \frac{-1}{2}(X^2 - X - 2), \qquad L_2 = \frac{(X-1)(X-2)}{(-1-1)(-1-2)} = \frac{1}{6}(X^2 - 3X + 2)$$

et :

$$L_3 = \frac{(X-1)(X+1)}{(2-1)(2+1)} = \frac{1}{3}(X^2 - 1)$$

D'après le théorème précédent, le polynôme (d'interpolation de Lagrange) $P$ suivant répond à la question :

$$P = 3L_1 + 2L_2 - L_3 = -\frac{3}{2}X^2 + \frac{X}{2} + 4$$

**Théorème (polynômes d'interpolation de Lagrange, cas général)** Avec les mêmes notations qu'au théorème précédent, posons $Y = \sum_{i=1}^{n} y_i L_i$. L'ensemble des polynômes $P \in \mathbb{K}[X]$ tels que :

$$\forall i \in [\![1,n]\!], \qquad P(x_i) = y_i$$

est :

$$\left\{ Y + Q \prod_{k=1}^{n} (X - x_k) \;\middle|\; Q \in \mathbb{K}[X] \right\}$$

**Démonstration** Soit $P \in \mathbb{K}[X]$. Alors :

$$\begin{aligned}
(\forall i \in [\![1,n]\!],\ P(x_i) = y_i) &\iff (\forall i \in [\![1,n]\!],\ P(x_i) = Y(x_i)) \\
&\iff (P - Y \text{ admet pour racines } x_1, \dots, x_n) \\
&\iff \prod_{k=1}^{n} (X - x_k) \text{ divise } P - Y \qquad \text{(d'après le corollaire 1)} \\
&\iff \exists Q \in \mathbb{K}[X],\ P - Y = Q \prod_{k=1}^{n} (X - x_k),
\end{aligned}$$

ce qui démontre le théorème. ■