Polynômes

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

I – L'anneau $\mathbb{K}[X]$

1) Polynômes à une indéterminée

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

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

Définition 1 (polynôme) On appelle *polynôme à une indéterminée à coefficients dans* $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telle que :

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

Les termes de cette suite (c'est-à-dire $a_0, a_1, a_2, \dots, a_d, 0, 0, 0, \dots$) sont appelés les coefficients du polynôme.

Vocabulaire. Une telle suite, dont les termes sont nuls à partir d'un certain rang, est dite *presque nulle* (seul un nombre fini de ses termes sont différents de 0).

Notations.

- ⋆ L'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.
- ⋆ 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).
- ⋆ 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 λ.
- ⋆ 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 (où $\delta_{k,n}$ désigne ici le *symbole de Kronecker*, c'est-à-dire $\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases}$).

Il est clair que l'addition $+$ dans $\mathbb{K}^{\mathbb{N}}$ est une loi de composition interne dans $\mathbb{K}[X]$.

Proposition 1 (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).

⋆ Soit $(a_n)_{n\in\mathbb{N}}$ 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 $(\mathbb{K}^{\mathbb{N}}, +)$. ■

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 :

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

où d est un entier naturel tel que les termes de la suite sont nuls à partir du rang $d+1$.

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

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

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

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

où d est un entier naturel tels que les termes des deux suites relatives à P et Q sont nuls à partir du rang $d+1$.

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

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

avec les notations précédentes.

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

Proposition 2 (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 2 (degré) Soit $P \in \mathbb{K}[X]$. On appelle *degré* de P l'entier naturel :

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

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 2 $\deg(1) = 0$, $\deg(X^3 - X^5) = 5$

Définition 3 (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 :

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

Rappelons que 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 3 $1 \in \mathbb{K}_3[X]$, $X - X^2 \in \mathbb{K}_3[X]$, $X^4 \notin \mathbb{K}_3[X]$

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 4 (coefficient dominant) Soit $P \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ un polynôme de degré d. Si $P = (a_0, \dots, a_d, 0, 0, \dots)$, alors a_d est appelé le *coefficient dominant* de P.

Remarque : si $a_d = 1$, on dit que le polynôme P est *unitaire*.

Exemple 4
— 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 3 Soit $(P, Q) \in (\mathbb{K}[X])^2$ 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 Soit $(P, Q) \in (\mathbb{K}[X])^2$ et $\lambda \in \mathbb{K}^*$. Alors :

(i) Notons d le degré de P. Il existe $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ tel que $P = \sum_{k=0}^{d} a_k X^k$. Alors :

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

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 $\mathbb{K}$) et donc le coefficient de plus haut degré de λP est λa_d. Ainsi :

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

(ii) C'est évident si P ou Q est le polynôme nul. Supposons maintenant que P et Q sont non nuls et posons $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{k=0}^{\delta} b_k X^k$ où $d = \deg(P) \in \mathbb{N}$ et $\delta = \deg(Q) \in \mathbb{N}$.
— Si $d \neq \delta$, par exemple si $d < \delta$, alors :

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

où on a posé $a_k = 0$ pour tout $k \in [\![d+1, \delta]\!]$. Le coefficient dominant de $P + Q$ est :

$$a_\delta + b_\delta = b_\delta \neq 0 \qquad \text{(par définition de } \delta)$$

et donc :

$$\deg(P + Q) = \beta = \deg(Q) = \max(\deg(P), \deg(Q))$$

Le cas $d > \delta$ se traite bien sûr de la même manière.

— Supposons maintenant que $d = \delta$. On a $P + Q = \sum_{k=0}^{d} (a_k + b_k)X^k$. Comme les coefficients de $P + Q$ sont nuls à partir de l'indice $d + 1$, on a clairement $\deg(P + Q) \leqslant d$, d'où le résultat. ■

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 1 Soit $(P, Q) \in (\mathbb{K}[X])^2$ de coefficients respectifs $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$. Alors :

(i) en posant

$$\forall n \in \mathbb{N}, \qquad c_n := \sum_{k=0}^{n} a_k b_{n-k}$$

alors la suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle. Il s'agit donc d'un polynôme, appelé produit de P et Q que l'on note PQ.

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

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 (ii) est immédiate (puisque dans ce cas $\deg(PQ) = \deg(0_{\mathbb{K}[X]} = -\infty$ et car $-\infty + (-\infty) = -\infty$ et car $-\infty + d = -\infty$ pour tout entier naturel d).

⋆ 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 $k \in d + \delta$, on a :

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

En effet, pour tout $j \in [\![0, k]\!]$, on a :
— si $j > d$, alors $a_j = 0$;
— si $j \leqslant d$, alors $k - j > \delta$ et alors $b_{k-j} = 0$. ■

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

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

Remarques :

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

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

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

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

Proposition 4 (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) :

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

  donc la loi $\times$ est commutative.

- ⋆ Vérifions maintenant que le produit est associatif. Considérons aussi $R = (c_n)_{n\in\mathbb{N}}$. Montrons que $(PQ)R = P(QR)$. C'est clair si l'un des trois polynômes est nul. Supposons que P, Q et R sont non nuls. En notant θ le degré de R, on a :

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

  où :

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

  Ainsi :

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

- ⋆ 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) :

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

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

Proposition 5 L'anneau $\mathbb{K}[X]$ est intègre. Autrement dit :

$$\forall (P, Q) \in (\mathbb{K}[X])^2, \qquad PQ = 0_{\mathbb{K}[X]} \iff (P = 0_{\mathbb{K}[X]} \text{ ou } Q = 0_{\mathbb{K}[X]})$$

Démonstration Soit $(P, Q) \in (\mathbb{K}[X])^2$. 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 6 Dans l'anneau $\mathbb{K}[X]$, les éléments inversibles (pour la multiplication), sont les polynômes de degré 0 (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 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 $\frac{1}{P}$ est un polynôme de degré 0 et on a clairement $P \times \frac{1}{P} = 1$ don P est inversible. ■

3) Composition de polynômes

Définition 5 (composition) Soit $(P, Q) \in (\mathbb{K}[X])^2$. On pose $P = \sum_{k=0}^{d} a_k X^k$. On appelle *composée de P par Q* le polynôme noté $P \circ Q$ défini par :

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

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

Proposition 7 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). Supposons maintenant que $P \neq 0_{\mathbb{K}[X]}$ et posons :

$$P = \sum_{k=0}^{d} a_k X^k \qquad \text{où} \qquad d = \deg(P) \in \mathbb{N}$$

Alors :

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

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 $\deg(a_d Q^d) = d \deg(Q)$ car $a_d \neq 0$ par définition de d. 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 :

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

II – Arithmétique des polynômes

1) Notion de multiple et de diviseur

Définition 6 (multiple, diviseur) Soit $(A, B) \in (\mathbb{K}[X])^2$. 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 $B = AC$.

Notation. Si $A \in \mathbb{K}[X]$, on notera $\mathscr{D}(A)$ l'ensemble des diviseurs de A et $\mathscr{M}(A)$ l'ensemble de ses multiples.

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 $0_{\mathbb{K}[X]} = A \times 0_{\mathbb{K}[X]}$. De plus, $\mathscr{M}(0_{\mathbb{K}[X]}) = \{0_{\mathbb{K}[X]}\}$.
- ⋆ Soit $(A, B) \in (\mathbb{K}[X])^2$. Alors :
$$A \mid B \iff \mathscr{M}(B) \subset \mathscr{M}(A)$$
- ⋆ Soit $(A, B) \in (\mathbb{K}[X])^2$. Si $A \mid B$, 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 λ un polynôme constant non nul. Alors $P = (\lambda P) \times \frac{1}{\lambda}$ et $\frac{1}{\lambda}$ définit un polynôme donc $\lambda \mid P$.

Proposition 8 (relation $\mid$ dans l'anneau des polynômes) La relation $\mid$ est réflexive et transitive. De plus, pour tout $(A, B) \in (\mathbb{K}[X])^2$, on a l'équivalence :

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

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 Soit $(A, B, C) \in (\mathbb{K}[X])^3$.

- ⋆ 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 $(Q, R) \in (\mathbb{K}[X])^2$ tel 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.
- ⋆ 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 λ et $\frac{1}{\lambda}$ sont des polynômes). Réciproquement, supposons que $A \mid B$ et $B \mid A$. Il existe alors $(P, Q) \in (\mathbb{K}[X])^2$ 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 $\lambda = 1$ convient) ou $PQ = 1$, ce qui est possible que si P et Q sont des constantes non nulles. ■

Le résultat suivant est fondamental.

Théorème 1 (de la division euclidienne dans l'anneau des polynômes) Soit $(A, B) \in (\mathbb{K}[X])^2$ 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) $\deg(R) < \deg(B)$.

Vocabulaire. Comme dans le cas de la division euclidienne dans $\mathbb{Z}$, on dit que :

— l'on a effectué la division euclidienne de A par B (dans $\mathbb{K}[X]$) ;

— que R est le reste dans cette division euclidienne ;
— que Q est le quotient ;
— que A est le dividende ;
— et B le diviseur.

Exemple 6 $X^2+X+1=X(X+1)+1$ 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 non vide (car contient $\deg(A)$ qui est un entier car $A \neq 0_{\mathbb{K}[X]}$ puisque B ne divise pas A) de $\mathbb{N}$ (en effet, la valeur $-\infty$ est exclue puisque B est non nul). Donc cet ensemble admet un plus petit élément que nous notons $r \in \mathbb{N}$. Considérons un polynôme $Q \in \mathbb{K}[X]$ pour lequel $\deg(A-BQ) = r$ et posons $R = A-BQ$. La propriété (i) est alors clairement vérifiée. Il reste à montrer que $\deg(R) < \deg(B)$. Notons ρ le coefficient dominant de R et supposons par l'absurde que $r \geqslant b$. Alors :

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

Or, $\deg\left(R - \frac{\rho}{\beta}X^{r-b}B\right) = \deg(A-BK) \in \mathscr{D}$, où l'on a posé $K = Q + \frac{\rho}{\beta}X^{r-b}$. 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 :

$$\deg\big(B(Q_1 - Q_2)\big) = \deg(B) + \deg(Q_1 - Q_2) \geqslant \deg(B) \qquad \text{alors que} \qquad \deg(R_2 - R_1) < \deg(B)$$

par définition de R_1 et R_2. On obtient donc une absurdité. Ainsi, $Q_1 = Q_2$ et alors $R_1 = R_2$, d'où l'unicité. ■

2) PGCD

Proposition/définition 2 (PGCD de deux polynômes) Soit $(A, B) \in (\mathbb{K}[X])^2$ tel 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 On sait que $\mathscr{D}(A) \cap \mathscr{D}(B)$ est non vide (en effet, cet ensemble contient $\mathbb{K}^*$) donc :

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

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 $\max(\deg(A), \deg(B))$. La notion de PGCD est donc bien définie. ■

Remarque : 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 λD où $\lambda \in \mathbb{K}^*$ est un PGCD de A et B.

Proposition 9 Soient $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$ et $\Delta \in \mathbb{K}[X]$. Alors :

$$\Delta \text{ est un PGCD de } A \text{ et } B \iff \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta)$$

Démonstration La démonstration est analogue à celle vu dans $\mathbb{Z}$. ■

Corollaire 1 Soient $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$ et Δ, Δ' deux PGCD de A et B. Alors Δ et Δ' sont associés, c'est-à-dire :

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

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

Remarque : si Δ est un PGCD de A et B, alors l'ensemble des PGCD de A et B est :

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

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

Définition 7 Soit $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$. Le PGCD de A et B est l'unique PGCD unitaire de A et B. On le note $A \wedge B$.

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

$$\Delta = A \wedge B \iff \begin{cases} \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta) \\ \text{coefficient dominant de } \Delta = 1 \end{cases}$$

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 7
— $(X^2 + 3X + 1) \wedge (X + 1) = 1$;
— $(X^2 - 3X + 2) \wedge (X^3 - 2X^2 + X - 2) = X - 2$.

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

Proposition 10 Soit $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$. Alors il existe $(U, V) \in (\mathbb{K}[X])^2$ tel que :

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

Démonstration analogue au cas entier ■

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

Exemple 8 Reprendre l'un des deux exemples précédents.

3) Théorème de Bézout et lemme de Gauss

Définition 8 (polynômes premiers entre eux) Soit $(A, B) \in (\mathbb{K}[X])^2$. On dit que A et B sont premiers entre eux si $A \wedge B = 1$.

Exemple 9
— 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 ($X \wedge (X^2 + X) = X$).

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

Théorème 2 (de Bézout) Soit $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$. Alors :

$$(A \text{ et } B \text{ sont premiers entre eux}) \iff (\exists\,(U,V) \in (\mathbb{K}[X])^2,\ AU + BV = 1)$$

Démonstration analogue au cas entier ■

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

Théorème 3 (Lemme de Gauss) Soit $(A, B, C) \in (\mathbb{K}[X])^3$ tel que $B \neq 0_{\mathbb{K}[X]}$. Si :

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

alors A divise C.

Démonstration analogue au cas entier ■

✎✎✎ **Exercice 1** 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 $C \in \mathbb{K}[X]$.

4) PPCM de deux polynômes

De la même manière, on peut définir le PPCM de deux polynômes A et B.

Proposition/définition 3 (PPCM) Soit $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0_{\mathbb{K}[X]}$. 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.

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 maximal de $\mathscr{M}(A) \cap \mathscr{M}(B)$.
- ⋆ 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 10 $(3X^2(X + 1)) \vee (X^4(X + 2)^2) = X^4(X + 1)(X + 2)^2$

5) Généralisations

Définition 9 (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 $A_1 \wedge \cdots \wedge A_n$.

Proposition 11 (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 analogue au cas entier ■

Définition 10 (polynômes premiers entre eux dans leur ensemble, deux à deux 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 :
$$\forall (i,j) \in [\![1,n]\!]^2, \qquad i \neq j \Leftrightarrow A_i \wedge A_j = 1$$

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 11 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 12 Soit $n \in \mathbb{N} \setminus \{0,1\}$, $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$ et $P \in \mathbb{K}[X]$. On suppose que :

- ⋆ les polynômes $A_1, \dots, A_n$ sont deux à deux premiers entre eux ;
- ⋆ pour tout $k \in [\![1,n]\!]$, le polynôme A_k divise P.

Alors le produit $A_1 \dots A_n$ divise P.

Démonstration la faire ■

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

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

Notation. L'ensemble des fonctions polynomiales sur $\mathbb{K}$ 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 $P(x)$ est bien défini. On dit qu'on a évalué le polynôme P en x.

Exemple 12 La fonction polynomiale associé à $P(X) = X^2 + 1 \in \mathbb{R}[X]$ est la fonction :

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

Remarques :

- ⋆ On montre facilement que $(\mathbb{K}[x], +, \times)$ est un sous-anneau de $\mathbb{K}^{\mathbb{K}}$.
- ⋆ On peut démontrer que, pour tout $(P, Q) \in (\mathbb{K}[X])^2$, 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
```

3) Racines d'un polynôme

Définition 12 (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).

Notation. On notera $\mathrm{Rac}_{\mathbb{K}}(P)$ l'ensemble des racines de P.

Exemple 13
- $\mathrm{Rac}_{\mathbb{C}}(X^2+1) = \{-i, i\}$ 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 permet de factoriser un polynôme.

Proposition 13 (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.

($\Leftarrow$) 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.

($\Rightarrow$) Supposons que a soit 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 2 Soient $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $(a_1, \ldots, a_n) \in \mathbb{K}^n$ des racines de P deux à deux distinctes. Alors $\prod_{k=1}^{n}(X - a_k)$ divise P.

Démonstration On utilise un raisonnement par récurrence (ou utiliser 12). Pour tout entier n, considérons la propriété $\mathscr{P}_n$: « pour tout $P \in \mathbb{K}[X]$ et pour tout n-uplet $(a_1, \ldots, a_n) \in \mathbb{K}^n$ de racines deux à deux distinctes de P, le produit $\prod_{k=1}^{n}(X - a_k)$ divise P ».

⋆ La proposition $\mathscr{P}_1$ est vraie d'après la proposition 13.

⋆ Soit $n \in \mathbb{N}^*$ la propriété $\mathscr{P}_n$ soit vraie et montrons que $\mathscr{P}_{n+1}$ est vraie. Soit $P \in \mathbb{K}[X]$ et $a_1, \ldots, a_{n+1}$ des racines deux à deux distinctes de P. Par hypothèse de récurrence, il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = \left(\prod_{k=1}^{n} (X - a_k) \right) Q$$

Or $\tilde{P}(a_{n+1}) = 0$ et $\prod_{k=1}^{n} (a_{n+1} - a_k) \neq 0$ donc a_{n+1} est racine de Q. D'après la proposition 13, il existe $R \in \mathbb{K}[X]$ tel que $Q = (X - a_{n+1})R$. On a alors :

$$P = \left(\prod_{k=1}^{n+1} (X - a_k) \right) R$$

et donc $\prod_{k=1}^{n+1} (X - a_k)$ divise P. La proposition $\mathscr{P}_{n+1}$ est donc vraie. ■

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

Proposition 14 (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 ⋆ Soient $k \in \mathbb{N}^*$ et $a_1, \ldots, a_k$ des racines deux à deux distinctes de P. D'après le corollaire précédent, on sait que $\prod_{\ell=1}^{k} (X - a_\ell)$ divise P. Alors :

$$k = \deg \left(\prod_{\ell=1}^{k} (X - a_\ell) \right) \leqslant \deg(P) = d$$

d'où le premier point.

⋆ 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 δ racines. En particulier, P admet au plus d racines, d'où le deuxième point par contraposition. ■

Théorème 4 (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 :

$$\mathbb{K}[x] = \left\{ \tilde{P} \,\middle|\, P \in \mathbb{K}[X] \right\}$$

donc l'application i est surjective. Montrons maintenant que i est injective. Soit $(P, Q) \in (\mathbb{K}[X])^2$ tel 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). Par conséquent, $P - Q = 0_{\mathbb{K}[X]}$ et 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 13 (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 a deux racines distinctes réelles ou complexes α et β et :

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

    Ces deux racines sont simples.
  - — ou une racine double (réelle) γ et :

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

    Cette racine est double.

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

Définition 14 (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 14 Soit $P = X^2(X^2+1) \in \mathbb{R}[X]$. On a $\deg(P) = 4$.

- — On a $\mathrm{Rac}_{\mathbb{R}}(P) = \{0\}$ 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 15 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 ($\Leftarrow$) Si $P = C_P \prod_{a \in \mathrm{Rac}_{\mathbb{K}}(P)} (X-a)^{m_P(a)}$ alors, en prenant les degré, on a :

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

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

($\Rightarrow$) 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 la proposition 12, 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 donc $(\lambda_1, \lambda_2) \in \mathbb{K}^2$ tel 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 5 (relations coefficients-racines ou formules de Viète) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ un polynôme non constant de degré $n \in \mathbb{N}^*$ (on a donc $a_n \neq 0$). Notons $\lambda_1, \ldots, \lambda_n$ les racines de P comptées avec multiplicité. Pour tout $k \in [\![1, n]\!]$, on pose :

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \lambda_{i_1} \ldots \lambda_{i_k}$$

et alors :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

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

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

Démonstration Il s'agit essentiellement de se convaincre que (2) est vraie. ■

✎✎✎ **Exercice 2** 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. On a :

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

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 :

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

IV – Dérivation

1) Dérivée formelle d'un polynôme

Définition 15 (dérivée formelle) Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$. On appelle *dérivée formelle de P*, notée P', le polynôme :

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

avec $P' = 0_{\mathbb{K}[X]}$ si P est un polynôme constant.

Exemple 15
— 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 $\tilde{P} : \mathbb{R} \longrightarrow \mathbb{R}$ 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 16 Soit $(P, Q) \in (\mathbb{K}[X])^2$.

(*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,

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

(*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.

(suite) Les formules donnant $(P+Q)'$, $(PQ)'$ et $(P \circ Q)'$ proviennent des formules :

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

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). ■

✎✎✎ **Exercice 3** Soit $P = (X-2)(X-7)(X-18)(X-\pi)$. Montrer que P' admet une racine dans $]2, \pi[$.

2) Formule de Taylor polynomiale

Proposition 17 Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :

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

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

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

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 ℓ fois la somme finie, on a :

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

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

⋆ On étudie maintenant le cas général. Soit $a \in \mathbb{K}$. Posons $Q = P(X+\lambda) \in \mathbb{K}[X]$. Alors, pour tout $k \in \mathbb{N}$, on a $Q^{(k)}(X) = P^{(k)}(X+\lambda)$ (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 4** 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 3 (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.

(⇐) Dans ce cas, on a d'après la formule de Taylor polynomiale :

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

Le polynôme Q est divisible par $(X-a)^{k+1}$ tandis que $\dfrac{P^{(k)}(a)}{k\,!}(X-a)^k$ est divisible par $(X-a)^k$ mais pas par $(X-a)^{k+1}$ (puisque $P^{(k)}(a) \neq 0$). On en déduit que $m_P(a) = k$.

(⇒) Pour la réciproque, on peut raisonner par récurrence sur l'entier k. Si $m_P(a) = 0$, alors on sait que $P^{(a)} \neq 0$. Supposons que la propriété soit vérifiée au rang k et supposons que $m_P(a) = k+1$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^{k+1}Q$ avec $Q(a) \neq 0$ (car si $Q(a) = 0$, alors Q est divisible par $X - a$ et alors $m_P(a) \geqslant k+2$). Alors :

$$P' = (k+1)(X-a)^k Q + (X-a)^{k+1}Q' = (X-a)^k \underbrace{((k+1)Q + (X-a)Q')}_{:=R}$$

Comme $R(a) = (k+1)Q(a) \neq 0$, on a $m_{P'}(a) = k$. Donc, par hypothèse de récurrence,

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

c'est-à-dire :

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

d'où le résultat car $P(a) = 0$ (d'après l'égalité $P = (X-a)^{k+1}Q$). ■

Exemple 16 La multiplicité de 1 comme racine de $P = X^4 + 3X^3 - 3X^2 - 7X + 6$ est égale à 2.

V – Polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$

1) Notion d'irréductibilité

Définition 16 (polynôme irréductible) Soit $P \in \mathbb{K}[X]$. On dit que P est *irréductible sur* $\mathbb{K}$ si :

- ⋆ P est non constant ;
- ⋆ s'il existe $(Q, R) \in (\mathbb{K}[X])^2$ tel que $P = QR$, alors Q ou R est un polynôme constant.

Exemple 17
- — 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, il est *réductible* sur $\mathbb{C}$. Par exemple, si $P = X^2 + 1 \in \mathbb{R}[X]$, alors $P = (X - i)(X + i)$ dans $\mathbb{C}[X]$.

Théorème 6 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 18 Soit $n \in \mathbb{N}^*$. Le polynôme $X^n - 1$ admet exactement n racines qui sont les racines n^{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 5** Décomposer le polynôme $P = X^3 + 27$ en produit de facteurs irréductibles sur $\mathbb{C}$.

2) Décomposition sur $\mathbb{C}$

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 7 (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 4 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 $a \in C$; il existe alors $R \in \mathbb{C}[X]$ 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 α 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 on peut en déterminer une racine (qui est aussi une racine de P). En itérant le procédé, on obtient la factorisation :

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

où C est le coefficient dominant de P. La factorisation de P en produit de facteurs irréductibles correspond donc à sa forme scindée sur $\mathbb{C}$.

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 construire des fonctions $f : [x_1, x_n]$ telles 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. Ici, on cherche des solutions polynomiales.

Proposition/définition 4 (polynômes de Lagrange) Soit $x_1, \dots, x_n \in \mathbb{K}$ 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 $i \in [\![1, n]\!]$, le polynôme L_i est de degré $n-1$ et ses racines sont $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$.

Démonstration évident ■

Exemple 19 Pour $n = 3$, les polynômes de Lagrange 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 8 (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 $x_1, \dots, x_n$.

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 $\deg(P) \leqslant n-1$. 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 $n-1$ et admet au moins n racines deux à deux distinctes (les scalaires $x_1, \dots, x_n$). On en déduit que $P - Q = 0$, c'est-à-dire que $P = Q$. ■

✎✎✎ **Exercice 6** 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 9 (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 :

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

ce qui démontre le théorème. ■