XIV Polynômes

3 octobre 2019

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

1 $\mathbb{K}[X]$: définitions et résultats algébriques.

1.1 Premières définitions.

Définition 1.1.1.
On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

Remarque 1.1.2. 1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.

2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse[1] (par exemple la suite $(1/n)$).

Définition 1.1.3 (Anneau des polynômes sur le corps $\mathbb{K}$).
On admet qu'on peut construire un anneau commutatif $(\mathbb{K}[X], +, \times)$ appelé *anneau des polynômes à une indéterminée à coefficients dans* $\mathbb{K}$. Vérifiant les propriétés suivantes :

1. $\mathbb{K}[X]$ étend l'anneau $\mathbb{K}$, c'est-à-dire :
   a) $\mathbb{K} \subset \mathbb{K}[X]$
   b) l'addition et la multiplication de $\mathbb{K}[X]$ coïncident avec celles de $\mathbb{K}$ sur l'ensemble $\mathbb{K}$. Autrement dit : les opérations $+_{\mathbb{K}[X]}$ et $\times_{\mathbb{K}[X]}$ restreintes au sous-ensemble $\mathbb{K}$ sont exactement les opérations $+_{\mathbb{K}}$ et $\times_{\mathbb{K}}$.
   c) le neutre pour l'addition sur $\mathbb{K}$, noté 0, est aussi le neutre pour l'addition sur $\mathbb{K}[X]$ et le neutre pour la multiplication sur $\mathbb{K}$, noté 1, est aussi le neutre pour la multiplication sur $\mathbb{K}[X]$. Le polynôme 0 est appelé *le polynôme nul*.
2. $\mathbb{C}[X]$ étend $\mathbb{R}[X]$.
3. Il existe un polynôme, noté X (appelé l'*indéterminée* de $\mathbb{K}[X]$).
4. Les polynômes de la forme αX^k pour $k \in \mathbb{N}$ et $\alpha \in \mathbb{K}$ sont appelés *monômes*.
5. Tout polynôme P peut s'écrire de façon *unique* sous *forme normale*[2](appelée aussi *forme développée réduite*) :
$$\sum_{k=0}^{+\infty} a_k X^k$$
où $(a_k)_{k\in\mathbb{N}}$ est une suite à support fini, appelée *suite des coefficients de* P (la suite des coefficients de P est donc unique).

Remarque 1.1.4. 1. Si on note φ l'application qui à tout polynôme P associe sa suite des coefficients et ψ l'application qui à toute suite à valeurs dans $\mathbb{K}$ à support fini u associe le polynôme $\sum_{k=0}^{+\infty} u_k X^k$, on constate que pour tout polynôme P, $(\psi \circ \varphi)(P) = P$ et que pour toute suite à support fini u, on a $(\varphi \circ \psi)(u) = u$. Ces deux applications sont donc des bijections réciproques : il y a donc une bijection (canonique) entre les suites à support fini et les polynômes.

2. Il est important de ne pas confondre X et x : $2X^3 + \sqrt{2}X + 7$ est un polynôme, $x \mapsto 2x^3 + \sqrt{2}x + 7$ désigne une fonction polynomiale (allant de $\mathbb{R}$ dans $\mathbb{R}$ ou de $\mathbb{R}$ dans $\mathbb{C}$ ou de $\mathbb{C}$ dans $\mathbb{C}$ selon le contexte). L'expression «$x^3 + \sqrt{2}x + 7$» est une erreur si x n'a pas été introduit ou si c'est une matrice carrée de taille 42. C'est un réel si x est un réel et

---

1. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

2. La somme est une somme finie, prise pour les valeurs de k telle que $a_k \neq 0$. On a donc $P = \sum_{\substack{k\in\mathbb{N}\\ a_k\neq 0}} a_k X^k$ mais aussi $P = \sum_{k=0}^{n} a_k X^k$ si la suite (a_k) est nulle à partir du rang $n+1$.

un complexe si x est un complexe.

Le polynôme 0 a pour suite de coefficients la suite nulle.

Pour tout $\lambda \in \mathbb{K}$, le polynôme λ a pour suite de coefficients la suite nulle partout sauf au rang 0, où elle a pour valeur λ. Les éléments de $\mathbb{K}$ sont appelés les polynômes constants.

Définition 1.1.5 (Degré)**.**
Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$. On appelle degré de P, et note $\deg P$ la valeur

$$\sup \{\, k \in \mathbb{N} \mid a_k \neq 0 \,\},$$

prise dans $\overline{\mathbb{R}}$.

(i) Si P est le polynôme nul, $\deg P = -\infty$.

(ii) Si P n'est pas le polynôme nul, le support de $(a_k)_{k\in\mathbb{N}}$ est un ensemble d'entiers non vide et majoré, donc

$$\deg P = \max \{\, k \in \mathbb{N} \mid a_k \neq 0 \,\}.$$

(iii) Si P est non nul, le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg_P} X^{\deg P}$ est le *monôme dominant* de P.

(iv) Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 1.1.6.
1. $\mathbb{K}_n[X]$ **n'est pas** l'ensemble des polynômes de degré **égal** à n.
2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \cdots \subset \mathbb{K}[X]$.
3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.
4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geqslant d$ (P est de degré *au plus* n), alors P peut s'écrire sous la forme $\sum_{k=0}^{n} a_k X^k$.

1.2 Somme et produit.

Proposition 1.2.1.
Soit P et Q deux polynômes respectivement de la forme $\sum_{k=0}^{+\infty} a_k X^k$ et $\sum_{k=0}^{+\infty} b_k X^k$. Alors on a :

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

Autrement dit, la suite des coefficients de $P+Q$ est la somme de leurs suites de coefficients respectives.

En ce qui concerne le produit, on a

$$P \times Q = \sum_{(i,j)\in\mathbb{N}^2} a_i b_j X^{i+j} = \sum_{k=0}^{+\infty} c_k X^k$$

où $(c_k)_{k\in\mathbb{N}}$ est la suite vérifiant, pour tout $k \in \mathbb{N}$,

$$c_k = \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i.$$

Démonstration.
Il s'agit essentiellement de constater que les sommes sont en fait finies. En notant S et S' les supports respectifs des suites de coefficients de P et Q, on a

$$P = \sum_{k\in S} a_k X^k = \sum_{k\in S\cup S'} a_k X^k,$$

$$Q = \sum_{k\in S'} b_k X^k = \sum_{k\in S\cup S'} b_k X^k,$$

d'où

$$P + Q = \sum_{k\in S\cup S'} (a_k X^k + b_k X^k) = \sum_{k\in S\cup S'} (a_k + b_k) X^k.$$

Or a_k et b_k sont nuls pour tout $k \in \mathbb{N} \setminus (S \cup S')$, donc la somme

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

est finie et vaut la même chose.

Pour le produit, notons, pour tout $k \in \mathbb{N}$,

$$c_k = \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j.$$

Il est clair que c_k est une somme finie (elle comporte $k+1$ termes) et de plus, on a

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i.$$

Il reste à montrer qu'on a bien $P \times Q = \sum_{k=0}^{+\infty} c_k X^k$.

Posons $S'' = \{\, i+j \mid (i,j) \in S \times S' \,\}$, S'' est l'image directe de l'ensemble fini $S \times S'$ par l'application somme, donc S'' est un ensemble fini.

Remarquons tout de suite que pour $k \in \mathbb{N} \setminus S''$ et tout couple $(i,j) \in \mathbb{N}^2$ vérifiant $i+j=k$, on a $(i,j) \notin S \times S'$, donc $a_i = 0$ ou $b_j = 0$. Donc pour tout $k \in \mathbb{N} \setminus S''$, la somme $\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j$ ne comporte que des termes nuls.

En outre

$$\begin{aligned}
PQ &= \left(\sum_{i\in S} a_i X^i\right)\left(\sum_{j\in S'} b_j X^j\right) \\
&= \sum_{(i,j)\in S\times S'} a_i b_j X^{i+j} \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in S\times S' \\ i+j=k}} \left(a_i b_j X^{i+j}\right) \right) \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in S\times S' \\ i+j=k}} a_i b_j \right) X^k \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k \\
&= \sum_{k=0}^{+\infty} \left(\sum_{\substack{(i,j)\in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k.
\end{aligned}$$

d'où le résultat. □

1.3 Composition.

Définition 1.3.1.
Soit P et Q deux polynômes de $\mathbb{K}[X]$. P s'écrit sous la forme

$$\sum_{k=0}^{+\infty} a_k X^k.$$

Alors, la somme

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

est une somme finie, appelée *composée de P et Q* (ou de Q par P) et est notée $P \circ Q$.

Proposition 1.3.2.
La composition est distributive **à droite** par rapport aux lois $+$ et $\times$ et elle est également associative, c'est-à-dire que si P, Q et R désignent trois polynômes, on a :

(i) $(P+Q)\circ R = (P\circ R) + (Q\circ R)$;
(ii) $(PQ)\circ R = (P\circ R)\times(Q\circ R)$;
(iii) $(P\circ Q)\circ R = P\circ(Q\circ R)$.

Démonstration. (i) Direct.
(ii) Traiter d'abord le cas $P = X^n$ et $Q = X^m$, puis le cas P quelconque et $Q = X^m$, puis le cas général.
(iii) Montrer par récurrence que $Q^k \circ R = (Q\circ R)^k$.
□

Attention à la composition à gauche, qui n'est pas distributive. Par exemple :

$$X^2 \circ (X+2) = (X+2)^2 \neq X^2 + 2^2$$
$$(1\circ X) + (1\circ 2) = 2 \neq 1 \circ (X+2)$$
$$(1+X)\circ(X.X) \neq ((1+X)\circ X).((1+X)\circ X).$$

Exemple 1.3.3.
Un polynôme P est dit pair si $P\circ(-X) = P$, impairs si $P\circ(-X) = -P$. Que peut-on dire des coefficients de tels polynômes ?

1.4 Opérations et degré.

Théorème 1.4.1.
Soient $P, Q \in \mathbb{K}[X]$.

(i) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$;
(ii) $\deg(PQ) = \deg P + \deg Q$;

(iii) si Q n'est pas constant, alors $\deg(P \circ Q) = \deg P \times \deg Q$. Si Q est constant, $\deg P \circ Q = 0$ ou $-\infty$.

Remarque 1.4.2.
Méditez les exemples suivants :

(i) $P = X - 1$ et $Q = 2 - X$;

(iii) $P = X^2 - 1$ et $Q = 1$.

Démonstration.
Le théorème est évident si P ou Q est nul. On les supposera donc tous deux non nuls, et on pose $n = \deg P$ et $m = \deg Q$. Les polynômes P, Q et PQ s'écrivent respectivement sous la forme $\sum_{k=0}^{n} a_k X^k$ et $\sum_{k=0}^{m} b_k X^k$ et $\sum_{k=0}^{+\infty} c_k X^k$.

(i) Facile ;

(ii) On a $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.
Soit $k \geqslant m + n$. Si $i > n$, alors $a_i = 0$, et si $i < n$, alors $b_{m+n-i} = 0$.
Ainsi, si $k = m+n$, la somme définissant c_k n'a qu'un terme non nul, et $c_{m+n} = a_n b_m \neq 0$.
Si $k > m + n$, tous les termes de la somme sont nuls, donc $c_k = 0$. Ceci prouve bien le résultat.

(iii) Q non constant équivaut à $\deg Q \geqslant 1$. Donc si k_1 et k_2 sont deux entiers tels que $k_2 > k_1$, on a $\deg Q^{k_2} > \deg Q^{k_1}$. Ainsi $\deg P \circ Q = \deg a_n Q^n = \deg(Q^n)$. Or d'après (ii), $\deg(Q^n) = n \deg Q$.

□

Corollaire 1.4.3.
$\mathbb{K}[X]$ est intègre.

Démonstration.
Il suffit de montrer que pour tout $(P, Q) \in \mathbb{K}[X]^2$, $PQ = 0 \Rightarrow (P = 0$ ou $Q = 0)$. Soit donc $(P, Q) \in \mathbb{K}[X]^2$ vérifiant $PQ = 0$. Alors d'après le point (iii) du théorème **1.4.1**, $-\infty = \deg(PQ) = \deg P + \deg Q$, donc on a nécessairement $\deg P = -\infty$ ou $\deg Q = -\infty$. □

Corollaire 1.4.4.
Soient $P, A, B \in \mathbb{K}[X]$ tel que $P \neq 0$. Alors :

$$PA = PB \Leftrightarrow A = B.$$

Démonstration.
$PA = PB$ si et seulement si $P(A - B) = 0$ si et seulement si ($P = 0$ ou $A - B = 0$) si et seulement si $A - B = 0$ si et seulement si $A = B$. □

Corollaire 1.4.5.
$U(\mathbb{K}[X]) = \mathbb{K}^*$. Autrement dit, les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration.
Soient P un polynôme inversible. Il existe donc un polynôme Q tel $PQ = 1$. P et Q sont non nuls, et donc $\deg P \geqslant 0$ et $\deg Q \geqslant 0$. Mais $0 = \deg 1 = \deg PQ = \deg P + \deg Q$. Nécessairement, $\deg P = \deg Q = 0$. □

Il y a donc peu de polynômes inversibles. L'inversibilité est une propriété fort utile lorsqu'on veut simplifier une égalité de la forme $PA = PB$ (on multiplie alors des deux côtés par l'inverse de P) mais heureusement, elle n'est pas nécessaire pour cela, l'intégrite de $\mathbb{K}[X]$ suffit.

Définition 1.4.6.
Deux polynômes P et Q de $\mathbb{K}[X]$ sont dits associés s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$.

Remarque 1.4.7.
Ainsi, deux polynômes sont associés si et seulement si on passe de l'un à l'autre en multipliant par un polynôme inversible. On pourra effectuer un rapprochement avec les entiers ainsi qu'avec l'arithmétique sur les entiers : les éléments inversibles de $\mathbb{Z}$ sont 1 et -1, et les objets construits en arithmétique des entiers (PGCD, nombres premiers, etc.) le sont toujours « à un élément inversible près ». Ce sera encore le cas en arithmétique des polynômes.

1.5 Fonctions polynomiales.

Dans cette section, on considère un entier naturel n fixé

Définition 1.5.1.
Soit $P \in \mathbb{K}[X]$ écrit sous forme développée réduite $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\widetilde{P}(x)$ l'élément de $\mathbb{K}$ défini par

$$\widetilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k.$$

Remarque 1.5.2.
Comme précédemment, le symbole $\sum_{k=0}^{+\infty}$ a un sens car la suite (a_k) est à support fini. Cette somme est donc finie.

Exemple 1.5.3.
On pose $P = X^2 + 2X + 3$, que vaut l'évaluation de P en -2 ?

Proposition 1.5.4.
Soit $x \in \mathbb{K}$ fixé. Alors, l'application d'évaluation en x, $\mathsf{eval}_x : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & \widetilde{P}(x) \end{array}$ est un morphisme d'anneaux ; autrement dit pour tout $(P,Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_{\mathbb{K}}$.

De plus, on a

$$\widetilde{P \circ Q}(x) = \tilde{P}(\tilde{Q}(x))$$

On note $\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \widetilde{P}(x) \end{array}$.

Remarque 1.5.5.
D'après ce qui précède, on a donc, pour tous polynômes P et Q :

1. $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$;
2. $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$;
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

Exemple 1.5.6.
Posons $P = X^2 + 2X + 3$.

1. Que vaut $\widetilde{P}$.
2. A t-on $P = \widetilde{P}$?

En pratique, on note en général $P(x)$ la valeur de $\widetilde{P}(x)$. On va même parfois jusqu'à identifier P et $\widetilde{P}$, c'est-à-dire identifier les polynômes et les fonctions polynomiale. Cela se justifie par le résultat suivant :

Théorème 1.5.7.
Soient P et Q deux polynômes de $\mathbb{K}[X]$.

(i) $\widetilde{P}$ est la fonction identiquement nulle si et seulement si $P = 0$;

(ii) $\widetilde{P} = \widetilde{Q}$ si et seulement si $P = Q$.

Cependant, nous ne sommes pas en mesure de montrer tout de suite cette propriété. Nous nous contenterons donc pour l'instant de faire les remarques suivantes :

Remarque 1.5.8.
1. Les implications $P = 0 \Rightarrow \widetilde{P} = 0$ et $P = Q \Rightarrow \widetilde{P} = \widetilde{Q}$ sont évidentes. Il suffit donc de montrer les implications réciproques.
2. Si l'on admet pour tout P l'implication $\widetilde{P} = 0_{\mathbb{K}^{\mathbb{K}}} \Rightarrow P = 0$ alors, pour tout couple (P,Q), l'implication $\widetilde{P} = \widetilde{Q} \Rightarrow P = Q$ s'en déduit. En effet, il suffit de remarquer que $\widetilde{P-Q} = \widetilde{P} - \widetilde{Q}$, donc si $\widetilde{P} = \widetilde{Q}$, alors $\widetilde{P-Q}$ est nul donc $P - Q$ est nul donc $P = Q$.

Remarque 1.5.9 (à caractère culturel)**.**
On verra que la démonstration du résultat exploite le fait que $\mathbb{K}$ est un ensemble infini. Même si seuls les cas $\mathbb{K} = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$ sont au programme, il existe des corps $\mathbb{K}$ finis et on peut définir $\mathbb{K}[X]$ pour de tels corps. Dans le cas où $\mathbb{K}$ est un corps fini, le théorème 1.5.7 n'est plus vrai.

1.6 Division euclidienne.

On peut définir une opération de division dans $\mathbb{K}[X]$ similaire à celle de la division euclidienne dans $\mathbb{Z}$.

Rappelons tout d'abord la définition de la division euclidienne dans $\mathbb{Z}$:

Définition 1.6.1 (Division euclidienne)**.**
Soit P et D deux entiers, avec $D \neq 0$. Alors il existe un unique couple (Q, R) d'entiers vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$
2. et $0 \leqslant R < |D|$.

Q et R sont respectivement appelé le quotient et le reste de la division euclidienne de P par D.

Définition 1.6.2 (Division euclidienne des polynômes)**.**
Soit P et D deux polynômes à coefficients dans $\mathbb{K}$, avec $D \neq 0$. Alors il existe un unique couple (Q, R) de polynômes à coefficients dans $\mathbb{K}$ vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$
2. et $\deg R < \deg D$.

Q et R sont respectivement appelé le quotient et le reste de la division euclidienne de P par D.

Exemple 1.6.3.
La division euclidienne de $3X^4 - 5X^3 + 7X^2 + 8X - 1$ par $X^2 - 3X + 2$ s'écrit :

$$3X^4 - 5X^3 + 7X^2 + 8X - 1$$
$$= (X^2 - 3X + 2)(3X^2 + 4X + 13) + 39X - 27.$$

On la pose comme suit.

$$\begin{array}{rrrrr|l}
3X^4 & -5X^3 & +7X^2 & +8X & -1 & X^2 -3X +2 \\ \cline{6-6}
-(3X^4 & -9X^3 & +6X^2) & & & 3X^2 +4X +13 \\ \cline{1-3}
 & 4X^3 & +X^2 & +8X & -1 & \\
 & -(4X^3 & -12X^2 & +8X) & & \\ \cline{2-4}
 & & 13X^2 & & -1 & \\
 & & -(13X^2 & -39X & +26) & \\ \cline{3-5}
 & & & 39X & -27 &
\end{array}$$

On alignera toujours les monômes de mêmes degrés pour les additionner sans commettre d'erreur.

Remarque 1.6.4.
La preuve du théorème de division euclidienne repose sur l'idée mise en œuvre dans l'algorithme donnant cette division. On cherche en effet chaque fois à annuler le monôme de plus haut degré du dividende en multipliant le diviseur par un monôme convenable.

Démonstration.
• Commençons d'abord par montrer l'unicité.

Soit (Q_1, R_1) et (Q_2, R_2) deux couples convenables. Alors
$$DQ_2 + R_2 = DQ_1 + R_1,$$
donc
$$D(Q_2 - Q_1) = R_1 - R2$$
et donc $D|(R_1 - R_2)$. Si $R_1 - R_2 \neq 0$, alors nécessairement
$$\deg D \leqslant \deg(R_1 - R_2).$$
Or $\deg R_1 < \deg D$ et $\deg R_2 < \deg D$, donc par somme
$$\deg(R_1 - R_2) < \deg D.$$
Par conséquent $R_1 - R_2 = 0$, donc $R_1 = R_2$. Il vient ensuite $D(Q_1 - Q_2) = 0$: puisque $D \neq 0$ et que $\mathbb{K}[X]$ est intègre, alors $Q_1 - Q_2 = 0$, soit finalement $(Q_1, R_1) = (Q_2, R_2)$.

• Montrons maintenant l'existence d'un tel couple, par le principe du minimum. Soit les ensembles
$$E = \{ \, P - DS \mid S \in \mathbb{K}[X] \, \}$$
et
$$\mathscr{E} = \{ \, \deg A \mid A \in E \, \} \, .$$

Si $0 \in E$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = DQ$, et le couple $(Q, 0)$ est donc celui que nous cherchons.

Sinon, si $0 \notin E$, $\mathscr{E}$ est un sous-ensemble de $\mathbb{N}$. Comme il est clairement non vide, il possède un minimum, noté m. Il existe donc $Q \in \mathbb{R}[X]$ tel que $P - DQ \in \mathbb{K}[X]$, et
$$\deg(P - DQ) = m \in \mathbb{N}.$$
La seule chose à montrer est que $m < \deg D$.

Par l'absurde, supposons que $m \geqslant \deg D$. Notons aX^m et bX^d les monômes dominants de R et D respectivement. On sait alors que a et b sont non nuls car R et D sont non nuls, et nous avons supposé que $d \leqslant m$. Posons alors
$$A = R - \frac{a}{b}.D.X^{m-d}.$$
Alors $\deg A < \deg R$, par annulation du monôme dominant aX^m de R. De plus
$$A = P - DQ - \frac{a}{b}.D.X^{m-d} = P - D(Q + \frac{a}{b}X^{m-d}),$$

donc $\deg A \in \mathscr{E}$: ceci contredit la minimalité de m, donc par l'absurde, $m < d$, et le couple (Q, R) est le couple voulu.

• On peut aussi montrer ce résultat d'existence par récurrence forte sur le degré de P. Cela a l'avantage de donner un algorithme de calcul du couple (Q, R). Nous verrons cette méthode sur des exemples, l'idée étant à chaque fois la même : annuler le monôme dominant du dividende. □

Remarque 1.6.5.
Si P et D sont à coefficients dans $\mathbb{R}$, on peut aussi les considérer comme polynômes à coefficients dans $\mathbb{C}$. Remarquer que dans les deux cas, le quotient et le reste de la division euclidienne de P par D sont les mêmes.

Définition 1.6.6.
Soit P et D deux polynômes à coefficients dans $\mathbb{K}$. On dit que D *divise* P ou que P *est un multiple de* D ou que P *est factorisable par* D et on note $D|P$ si et seulement s'il existe un polynôme Q à coefficients dans $\mathbb{K}$ vérifiant $P = D \times Q$.

Remarque 1.6.7.
Le polynôme nul est divisible par tout polynôme.

Remarque 1.6.8.
Le quotient Q, s'il existe, est unique.

Remarque 1.6.9.
P est divisible par D si et seulement si le reste de la division euclidienne de P par D est nul.

Remarque 1.6.10.
En vertu de la remarque sur la division euclidienne, lorsque P et D sont deux polynômes à coefficients dans $\mathbb{R}$, P est divisible par D en tant qu'éléments de $\mathbb{R}[X]$ si et seulement si il l'est en tant qu'éléments de $\mathbb{C}[X]$.

Exemple 1.6.11.
Pour tout $n \in \mathbb{N}$ et tout $a \in \mathbb{K}$, on a

$$X - a | X^n - a^n.$$

Proposition 1.6.12.
Soit $P, Q \in \mathbb{K}[X]$, si $P \mid Q$ et si $Q \neq 0$, alors $\deg(P) \leqslant \deg(Q)$.

Démonstration.
Immédiat à partir de la définition. □

Proposition 1.6.13.
Soit P et Q deux polynômes. $P|Q$ et $Q|P$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$. On dit alors que P et Q sont *associés*.

Tout polynôme P non nul est associé à un unique polynôme unitaire : $\dfrac{1}{c}P$, où c est le coefficient dominant de P.

Démonstration.
Le résultat est évident si P ou Q est nul (et dans ce cas $P = Q = 0$).

Soient donc P et Q deux polynômes non nuls tels que $P|Q$ et $Q|P$. Alors on a à la fois $\deg P \leqslant \deg Q$ et $\deg P \geqslant \deg Q$. Ainsi $\deg P = \deg Q$. Puisque $P|Q$, il existe un polynôme R tel que $PR = Q$, et comme $\deg P = \deg Q$, R est un polynôme constant : P et Q sont bien associés.

Le sens réciproque est évident. □

1.7 L'algorithme de Horner.

Soit $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré au plus n à coefficients dans $\mathbb{K}$ et $x_0 \in \mathbb{K}$.

On a $\widetilde{P}(x_0) = \sum_{k=0}^{\deg P} a_k x_0^k$. Connaissant x_0 et les a_k pour $k \in [\![0, n]\!]$, comment calculer $\widetilde{P}(x_0)$ de façon aussi efficace que possible ?

On peut évidemment calculer toutes les valeurs x_0^k pour $k \in [\![0, n]\!]$ (cela demande $n-1$ multiplications) puis les produits $a_k x_0^k$ (n multiplications supplémentaires), puis calculer la somme (n additions). Total : $2n-1$ multiplications et n additions.

On peut cependant faire mieux.

L'algorithme de Horner consiste à remarquer qu'on peut écrire $P(x_0)$ sous la forme

$$((\ldots((a_n x_0 + a_{n-1})x_0 + a_{n-2})\ldots)x_0 + a_1)x_0 + a_0$$

Autrement dit, en posant $r_n = a_n$, puis, pour k allant de $n-1$ à 0, $r_k = r_{k+1}x_0 + a_k$, la valeur de $P(x_0)$ est celle de r_0.

Ainsi on a calculé $P(x_0)$ en seulement n multiplications et n additions.

Exemple 1.7.1.
Posons $P = 2X^4 - 4X^3 - 7X^2 + 2X - 1$ par $X - x_0$ et $x_0 = 3$. On exécute parfois l'algorithme de Horner en traçant un tableau. Dans le cas présent, cela donne :

k	4	3	2	1	0
a_k	2	-4	-7	2	-1
r_k	2	2	-1	-1	-4

On a donc $P(x_0) = -4$.

Associé à la proposition suivante, l'algorithme de Horner permet également d'effectuer la division euclidienne d'un polynôme P par un polynôme de degré 1.

Proposition 1.7.2.
Soit $P \in \mathbb{K}[X]$ et $x_0 \in \mathbb{K}$. Alors il existe $Q \in \mathbb{K}[X]$ vérifiant $P = (X - x_0)Q + P(x_0)$.

Démonstration.
Nous donnerons deux démonstrations :

Première méthode Posons la division euclidienne de P par $X - x_0$: il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - x_0)Q + R$, avec $\deg R = 0$ ou $-\infty$. R est donc un polynôme constant, notons-le λ.
Évaluons l'égalité $P = (X - x_0)Q + \lambda$ en x_0 : il reste exactement $P(x_0) = \lambda$, d'où le résultat.

Deuxième méthode Cette deuxième méthode ne fait pas appel à la division euclidienne. Elle consiste à constater, en posant $n = \deg P$ et en écrivant P sous la forme $\sum_{k=0}^{n} a_k X^k$, où $a_k \in \mathbb{K}$ pour $k \in [\![0, n]\!]$, que pour tout $k \in \mathbb{N}$, $X^k - x_0^k$ s'écrit $(X - x_0)Q_k$, où $Q_k = \sum_{i=0}^{k-1} x_0^{k-1-i} X^i$, donc

$$\begin{aligned} P - P(x_0) &= \sum_{k=0}^{n} a_k \left(X^k - x_0^k\right) \\ &= \sum_{k=0}^{n} a_k (X - x_0) Q_k \\ &= (X - x_0) \sum_{k=0}^{n} a_k Q_k \end{aligned}$$

Donc en posant $Q = \sum_{k=0}^{n} a_k Q_k$, on a $P = (X - x_0)Q + P(x_0)$.

□

Calculer le reste de la division est facile par la méthode de Horner. Comment calculer le quotient Q ? Q est de la forme $\sum_{k=0}^{n-1} b_k X^k$. On a alors :

$$\sum_{k=0}^{n} a_k X^k = (X - x_0) \sum_{k=0}^{n-1} b_k X^k + P(x_0)$$

En identifiant les termes de même degré, il vient :

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - x_0 b_{n-1} \\ &\vdots \\ a_2 &= b_1 - x_0 b_2 \\ a_1 &= b_0 - x_0 b_1 \end{aligned}$$

On en déduit :

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + x_0 b_{n-1} \\ &\vdots \\ b_1 &= a_2 + x_0 b_2 \\ b_0 &= a_1 + x_0 b_1 \end{aligned}$$

On peut remarquer que les valeurs des coefficients de Q sont exactement celles calculées pour le calcul de $P(x_0)$: on constate en effet qu'on a

$$\begin{aligned} b_{n-1} &= r_n \\ b_{n-2} &= r_{n-1} \\ &\vdots \\ b_1 &= r_2 \\ b_0 &= r_1 \end{aligned}$$

Exemple 1.7.3.
En reprenant l'exemple 1.7.1, on trouve $P = (X - 3)(2X^3 + 2X^2 - X - 1) - 4$.

2 Décomposition.

2.1 Racines, ordre de multiplicité.

Définition 2.1.1.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est racine de P si $P(a) = 0$.

Proposition 2.1.2.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est racine de P si et seulement si $X - a$ divise P. Autrement dit :

$$P(a) = 0 \iff X - a | P.$$

Démonstration.
Le sens indirect est évident.
Le sens direct découle directement de la proposition 1.7.2 avec $x_0 = a$. □

Corollaire 2.1.3.
Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}$ et $a_1, \ldots, a_n$ n éléments de $\mathbb{K}$ distincts. Alors $a_1, \ldots, a_n$ sont des racines de P si et seulement si $\prod_{k=1}^{n}(X - a_k)$ divise P.

Démonstration.
Là encore le sens indirect est évident.
Le sens direct se fait par récurrence sur le nombre de racines en utilisant la proposition précédente. □

Définition 2.1.4.
Soit $P \in \mathbb{K}[X]$ un polynôme non nul, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. On dit que *a est racine d'ordre de multiplicité r de P* si r est le plus grand entier k tel que $(X - a)^k$ divise P. On dit que a est racine simple (resp. multiple) de P si $r = 1$ (resp. $r > 1$).

Remarque 2.1.5.
L'ensemble des k tel que $(X - a)^k \mid P$ contient 0 et est majoré par le degré de P, donc possède bien un plus grand élément.

Remarque 2.1.6.
Si a est racine d'ordre r, alors pour tout $k \in [\![0, r]\!]$, $(X - a)^k | P$.

Remarque 2.1.7.
a est racine de multiplicité r si et seulement si $(X - a)^r \mid P$ et $(X - a)^{r+1} \nmid P$.

Remarque 2.1.8.
a est racine d'ordre au moins 1 si et seulement si $X - a|P$, c'est-à-dire si et seulement si $P(a) = 0$.

Remarque 2.1.9.
a est racine multiple si et seulement si $(X - a)^2|P$.

Proposition 2.1.10.
Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. a est racine d'ordre r de P si et seulement si P s'écrit sous la forme $(X - a)^r Q$ où $Q(a) \neq 0$.

Démonstration.
Supposons que a est racine d'ordre r de P. Alors P est divisible par $(X - a)^r$, donc s'écrit sous la forme $(X - a)^r Q$. Par l'absurde, supposons $Q(a) = 0$, alors $X - a|Q$, donc $(X - a)^{r+1}|P$, ce qui est absurde. Donc $Q(a) \neq 0$.

Supposons que P s'écrit sous la forme $(X - a)^r Q$ où $Q(a) \neq 0$. Alors l'ordre de multiplicité de a dans P est au moins r. Supposons par l'absurde que cet ordre soit strictement supérieur. Alors $(X - a)^{r+1}$ divise P, donc P s'écrit sous la forme $(X - a)^{r+1}R$, donc $(X - a)^{r+1}R = (X - a)^r Q$, donc $(X - a)R = Q$. Donc $Q(a) = 0$, ce qui est absurde. □

2.2 Nombres de racines.

Proposition 2.2.1.
Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P a au plus $\deg(P)$ racines distinctes.

Démonstration.
Soit P un polynôme non nul de degré n, et $\lambda_1, \ldots, \lambda_{n+1}$ $n + 1$ racines distinctes de P. Alors P est divisible par $\prod_{k=1}^{n+1}(X - \lambda_i)$, qui est un polynôme de degré strictement supérieur au degré de P : c'est absurde. □

Proposition 2.2.2.
Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Si P admet au moins $n + 1$ racines distinctes, alors P est le polynôme nul.

Démonstration.
C'est la contraposée du résultat précédent. □

Corollaire 2.2.3.
On déduit de cette proposition les résultats suivants :

1. Soit $P \in \mathbb{K}[X]$. Si P admet une infinité de racines, alors P est le polynôme nul.
2. Soit $n \in \mathbb{N}$ et $(P, Q) \in \mathbb{K}_n[X]^2$. Si P et Q coïncident sur au moins $n+1$ points, alors $P = Q$.
3. Soit $(P, Q) \in \mathbb{K}[X]^2$. Si P et Q coïncident sur une infinité de valeurs, alors $P = Q$.

Démonstration.
1. Choisir un entier n vérifiant $n \geqslant \deg P$ et appliquer la proposition précédente.
2. Appliquer la proposition précédente au polynôme $P - Q$.
3. Appliquer le premier point à un $n \in \mathbb{N}$ vérifiant $n \geqslant \max(\deg P, \deg Q)$ ou le second à $P - Q$.

□

En particulier, $\mathbb{K}$ étant infini, un polynôme P tel que $\widetilde{P}$ est l'application nulle sur $\mathbb{K}$ est nécessairement nul et deux polynômes P et Q tels que $\widetilde{P} = \widetilde{Q}$ sont nécessairement égaux, ce qui permet de conclure la démonstration du théorème 1.5.7.

Remarque 2.2.4.
(à caractère culturel) Il est essentiel pour ce résultat que $\mathbb{K}$ soit infini. Dans un corps fini $\mathbb{K}$ comportant n éléments k_1, ..., k_n, le polynôme $(X - k_1) \times (X - k_2) \times \cdots \times (X - k_n)$ est non nul (car de degré n) mais a pour racine tous les éléments du corps.

2.3 Polynômes scindés et relations coefficients-racines.

Définition 2.3.1.
Soit $P \in \mathbb{K}[X]$.
On dit que P est *scindé* si P est nul ou peut s'écrire comme produit de polynômes de degré 1, c'est-à-dire s'il existe $n \in \mathbb{N}$, $\lambda \in \mathbb{K}$ et $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ vérifiant

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i).$$

Remarque 2.3.2.
1. Dans cette écriture, si P est non nul :
   — n est le degré de P
   — λ est son coefficent dominant.
   — $(\alpha_1, \ldots \alpha_n)$ sont les racines de P comptées avec ordre de multiplicité.
2. Un polynôme à coefficients réels peut être scindé dans $\mathbb{C}$ sans l'être dans $\mathbb{R}$: $P = X^2 + 1$.

Proposition 2.3.3 (Relations coefficients-racines.)**.**
Soit n un entier et $P = \sum_{i=0}^{n} a_i X^i$ un polynôme scindé de degré n sur $\mathbb{K}$. Alors P est de la forme

$$\lambda \prod_{k=1}^{n} (X - \alpha_k),$$

avec $\lambda = a_n$. Alors P s'écrit

$$\lambda \left(X^n + \sum_{k=1}^{n} (-1)^k \sigma_k X^{n-k} \right),$$

où

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n} \\
\sigma_2 &= \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n} \\
&\vdots \\
\sigma_k &= \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \alpha_{i_1} \ldots \alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n} \\
&\vdots \\
\sigma_n &= \alpha_1 \ldots \alpha_n = (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Démonstration.
Il suffit d'identifier $\sum_{i=0}^{n} a_i X^i$ et $\lambda \prod_{k=1}^{n}(X-\alpha_k)$. □

Définition 2.3.4.
Les scalaires σ_i, pour $i \in [\![1,n]\!]$ sont appelés *fonctions symétriques élémentaires* des racines de P.

Toute expression polynomiale dépendant de variables $\alpha_1, \ldots, \alpha_n$, symétrique en $\alpha_1, \ldots, \alpha_n$ (c'est-à-dire telle que l'échange de deux de ces variables ne change pas sa valeur) est appelée *fonction symétrique* de $\alpha_1, \ldots, \alpha_n$.

Remarque 2.3.5 (à caractère culturel)**.**
Toute fonction symétrique de $\alpha_1, \ldots, \alpha_n$ peut s'écrire à partir des seules fonctions symétriques élémentaires de $\alpha_1, \ldots, \alpha_n$.

Exemple 2.3.6.
Soit $(x_1, x_2) \in \mathbb{C}$. On pose $v = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2 + 49x_1^2x_2^2$.

v est fonction symétrique de x_1 et x_2. Comment l'exprimer à partir des fonctions symétriques élémentaires $\sigma_1 = x_1 + x_2$ et $\sigma_2 = x_1x_2$?

Une méthode systématique est la suivante[3] :

1. On repère tout d'abord le monôme «dominant». Parmi tous les monômes, le monôme dominant fait partie de ceux dont la puissance de la dernière variable est maximale, et parmi ceux-ci, c'est celui dont la puissance de l'avant-dernière variable est maximale, etc. Ici, la puissance maximale pour x_2 est 2, et parmi les monômes x_2^2, $14x_1x_2^2$ et $49x_1^2x_2^2$, celui dont la puissance de x_1 est maximale est $49x_1^2x_2^2$.
2. Pour éliminer un monôme $\alpha x_1^{k_1} \ldots x_n^{k_n}$, on soustrait $\alpha\sigma_1^{k_n-k_{n-1}} \ldots \sigma_{n-1}^{k_2-k_1}\sigma_n^{k_1}$. Autrement dit, ici on soustrait $49\sigma_1^{2-2}\sigma_2^2$. On obtient donc $v - 49\sigma_2^2 = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2$.
3. On itère. Ici il convient donc d'éliminer le monôme $14x_1x_2^2$ et pour cela de soustraire $14\sigma_1^{2-1}\sigma_2$, ce qui donne $v - 49\sigma_2^2 - 14\sigma_1\sigma_2 = x_1^2 + 2x_1x_2 + x_2^2$.
   Le plus grand monôme est alors x_2^2 ; on soustrait donc σ_1^2, ce qui donne $v - 49\sigma_2^2 - 14\sigma_1\sigma_2 - \sigma_1^2 = 0$.
   On a donc $v = 49\sigma_2^2 + 14\sigma_1\sigma_2 + \sigma_1^2$.

On remarque cependant qu'on pouvait aller beaucoup plus vite en remarquant dès le début $v = (x_1 + 7x_1x_2 + x_2)^2 = (\sigma_1 + 7\sigma_2)^2$.

NB : selon le programme officiel «Aucune connaissance spécifique sur le calcul des fonctions symétriques des racines n'est exigible».

3. Source : article *Elementary symmetric polynomial* sur Wikipedia (`en.wikipedia.org`).

Exercice 2.3.7.
Résoudre le système d'inconnues (x, y, z)

$$\begin{cases} x + y + z = 3 \\ x^2 + y^2 + z^2 = 11 \\ x^3 + y^3 + z^3 = 27 \end{cases}$$

2.4 Le théorème fondamental de l'algèbre.

Définition 2.4.1 (Polynômes irréductibles)**.**
Soit $P \in \mathbb{K}[X]$, avec $\deg P \geqslant 1$. On dit que P est réductible dans $\mathbb{K}[X]$ s'il existe deux polynômes Q et R dans $\mathbb{K}[X]$ vérifiant

1. $\deg Q \geqslant 1$
2. et $\deg R \geqslant 1$
3. et $P = Q \times R$.

On dit que P est irréductible dans $\mathbb{K}[X]$ dans le cas contraire.

Remarque 2.4.2.
1. La notion de polynôme irréductible est comparable à celle de primalité dans $\mathbb{Z}$: un polynôme est irréductible si et seulement s'il est de degré au moins 1 et que ses seuls diviseurs sont les éléments de $\mathbb{K}$ et ses associés.
2. Attention : un polynôme peut être irréductible dans $\mathbb{R}[X]$ sans l'être dans $\mathbb{C}[X]$. Par exemple $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais se factorise en $(X - i)(X + i)$ dans $\mathbb{C}[X]$.

3. Tout polynôme à coefficients réels irréductible dans $\mathbb{C}[X]$ est irréductible dans $\mathbb{R}[X]$.
4. Tout polynôme de degré 1 est irréductible.
5. Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 2 admettant une racine dans $\mathbb{K}$ est réductible dans $\mathbb{K}[X]$.
6. Il existe des polynômes sans racines qui ne sont pas irréductibles. Par exemple $X^4 + 2X^2 + 1$ n'admet pas de racines réelles alors qu'il se décompose comme produit de deux polynômes de degré 2.

Proposition 2.4.3.
Tout polynôme non constant se décompose comme produit de polynômes irréductibles.

Démonstration.
Par récurrence forte sur le degré du polynôme. □

Reste au moins deux questions :

1. Cette décomposition est-elle unique ?
2. Quels sont les polynômes irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$?

On verra plus loin comment répondre au premier point. Pour le second, la réponse nous est fournie par le théorème de d'Alembert-Gauss, aussi appelé théorème fondamental de l'algèbre : comme ce dernier nom l'indique, ce résultat est effectivement d'une importance capitale en algèbre.

Théorème 2.4.4 (d'Alembert-Gauss)**.**
Tout polynôme non constant à coefficients dans $\mathbb{C}$ admet au moins une racine dans $\mathbb{C}$.

Démonstration.
Ce résultat est admis. Pour mémoire, une démonstration possible est de considérer un polynôme P et de montrer successivement :

1. Il existe $R > 0$ tel que pour tout z vérifiant $|z| > R$, $|P(z)| \geqslant |P(0)|$;
2. $z \mapsto |P(z)|$ admet un minimum sur le pavé des complexes de parties réelles et imaginaires appartenant à $[-R, R]$ en un point a (montrer que la borne inférieure de $|P(z)|$ est un minimimun en exploitant la compacité de ce pavé).
3. $z \mapsto |P(z)|$ admet donc un minimum sur $\mathbb{C}$ au point a.
4. Par l'absurde, on suppose $P(a) \neq 0$ et on pose $Q = \frac{1}{P(a)}(P \circ (X + a))$. Alors $Q(0)$ vaut 1 et $z \mapsto |Q(z)|$ admet un minimum (global) en 0.
5. En explicitant Q, on constate que son coefficient constant est égal à 1 et on montre qu'il existe z vérifiant $|Q(z)| < 1$, ce qui est absurde, donc $P(a) = 0$.

□

Corollaire 2.4.5.
Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration.
On sait déjà que tous les polynômes de degré 1 sont irréductibles. De plus, pour tout $n \geqslant 2$, tout polynôme P de degré n admet une racine complexe a, donc est le produit de $X - a$ par un polynôme de degré $n - 1$. Or $n - 1 \geqslant 1$, donc P est réductible. □

Remarque 2.4.6.
Ce corollaire est en fait équivalent au théorème de d'Alembert-Gauss. En effet, si l'on admet ce corollaire, on peut démontrer le théorème de d'Alembert-Gauss par une récurrence forte sur le degré du polynôme.

Corollaire 2.4.7.
Tout polynôme non constant est scindé dans $\mathbb{C}[X]$.

Démonstration.
Il suffit d'utiliser les résultats 2.4.3 et 2.4.5. □

Pour les polynômes à coefficients réels, il est intéressant de noter le résultat suivant :

Proposition 2.4.8.
Soit P un polynôme à coefficients réels et $z \in \mathbb{C}$.

Alors z et $\overline{z}$ sont des racines de P de même multiplicité.

En particulier, z est racine de P si et seulement si $\overline{z}$ est racine de P.

Les racines de P non réelles sont donc deux à deux conjuguées.

Démonstration.
On note $\overline{P}$ le polynôme conjugué de P, c'est-à-dire le polynôme dont les coefficients sont les conjugués de ceux de P. On peut alors démontrer plusieurs résultats simples :

1. Si $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, alors $\overline{P(\lambda)} = \overline{P}\left(\overline{\lambda}\right)$;
2. Si $P, Q \in \mathbb{K}[X]$, $\overline{PQ} = \overline{P}\,\overline{Q}$;
3. P est à coefficients réels si et seulement si $\overline{P} = P$.

Soit donc P un polynôme à coefficients réels, et z une racine complexe de P, de multiplicité exactement r. Alors il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - z)^r Q$, avec $Q(z) \neq 0$. Mais alors $P = \overline{P} = \overline{(X - z)^r Q} = (X - \overline{z})^r \overline{Q}$. Donc $\overline{z}$ est racine de P multiplicité au moins r. Mais $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$, donc $\overline{z}$ est racine de P multiplicité exactement r.

On peut également démontrer ce résultat de la manière suivante, en utilisant le résultat 3.2.7 qui vient un peu plus loin.

Soit $z \in \mathbb{C}$. On sait que z est racine d'ordre r de P si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(z) \neq 0 \right\}$ si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; \overline{P^{(k)}(z)} \neq 0 \right\}$.

Or pour tout k, $\overline{P^{(k)}(z)} = \overline{P^{(k)}}(\overline{z})$ et pour P à coefficients réels, $\overline{P^{(k)}} = P^{(k)}$, donc

$$\left\{ k \in \mathbb{N} \;\middle|\; \overline{P^{(k)}(z)} \neq 0 \right\} = \left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(\overline{z}) \neq 0 \right\}$$

Par conséquent z est racine d'ordre r de P si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(\overline{z}) \neq 0 \right\}$ si et seulement si z est racine d'ordre r de $\overline{P}$. □

On en déduit la proposition suivante

Proposition 2.4.9.
Soit P un polynôme à coefficients réels non constant n'admettant pas de racine réelle. Alors il est divisible par un polynôme à coefficients réels de degré 2.

Démonstration.
Notons a une racine complexe de P. D'après ce qui précède $\overline{a}$ est également une racine de P.

Or, $a \notin \mathbb{R}$ donc $a \neq \overline{a}$, donc $(X - a)(X - \overline{a}) \mid P$.

On voit alors que

$$(X - a)(X - \overline{a}) = X^2 - 2\operatorname{Re}(a)X + |a|^2 \in \mathbb{R}[X].$$

□

On obtient alors le résultat suivant.

Proposition 2.4.10.
Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Démonstration.
Montrons déjà que les polynômes réels de degré deux sans racine réelle sont irréductibles. Soit P un tel polynôme, et Q, R deux polynômes réels tels que $P = QR$. Supposons que $\deg Q = 1$. Alors Q est de la forme $aX + b$, où a et b sont des réels, avec $a \neq 0$. Il admet donc $-\dfrac{b}{a}$ comme récine réelle, et donc P a une récine réelle, ce qui est absurde. Ainsi $\deg Q = 0$ ou 2, et P est irréductible.
Soit P un polynôme réel irréductible, de degré strictement supérieur à 1. S'il admet une racine réelle a, il est divisible par $X - a$ et n'est donc pas irréductible. S'il n'admet pas de racine réelle, il est divisible par un polynôme réel de degré 2. Donc si P est de degré strictement supérieur à 2, il est réductible. S'il est de degré 2, il est bien de la forme annoncée. □

2.5 Décomposition en produit de facteurs irréductibles.

Le théorème de d'Alembert-Gauss a pour corollaires immédiats les résultats suivants.

Corollaire 2.5.1.
Soit $n \in \mathbb{N}$, P un polynôme de degré n et de coefficient dominant c. Alors il existe $z_1, \dots, z_n$ des complexes vérifiant :

$$P = c \prod_{k=1}^{n} (X - z_k),$$

où les z_k, pour $k \in [\![1, n]\!]$ sont les racines de P, éventuellement répétées.

Remarque 2.5.2.
Dans une telle écriture, c est forcément le coefficient dominant de P, n est le degré de P et les z_i sont les racines de P, répétées autant de fois que leurs multiplicités.

Une telle écriture est donc unique. On retrouvera l'unicité de cette décomposition ultérieurement, et de manière plus abstraite (et semblable à la démonstration donnée sur les entiers).

Corollaire 2.5.3.
Soit $n \in \mathbb{N}$, $P \in \mathbb{C}[X]$ de degré n et de coefficient dominant c. Alors, en notant p le nombre de racines distinctes de P, $z_1, \dots, z_p$ les racines

distinctes de P, et $n_1, \ldots, n_p$ leurs multiplicités respectives, on a :

$$P = c \prod_{k=1}^{p} (X - z_k)^{n_k},$$
$$n = \sum_{k=1}^{p} n_k.$$

Démonstration.
La première égalité découle directement du corollaire précédent, et la seconde est l'égalité des degrés dans l'égalité polynomiale précédente. □

Théorème 2.5.4.
Soit P un polynôme à coefficients réels, alors on peut écrire P sous la forme

$$P = c \prod_{k=1}^{n} (X - a_k) \prod_{k=1}^{m} (X - z_k)(X - \overline{z}_k)$$

où $a_1, \ldots, a_n$ sont les racines réelles de P (répétées avec leur multiplicité), $z_1, \ldots, z_m, \overline{z}_1, \ldots, \overline{z}_m$ les racines complexes non réelles (répétées avec leur multiplicité), c le coefficient dominant de P, et $n + 2m = \deg(P)$.

On a donc

$$P = c \prod_{k=1}^{n} (X - a_k) \prod_{k=1}^{m} \left(X^2 - 2\,\mathrm{Re}(z_k)X + |z_k|^2\right)$$

Remarque 2.5.5.
On obtiendrait une décomposition semblable à celle obtenue au corollaire 2.5.3 en faisant apparaître des multiplicités.

Corollaire 2.5.6.
Tout polynôme à coefficients réels de degré impair a au moins une racine réelle.

Démonstration.
Par contraposition : un polynôme à coefficients réels n'ayant pas de racine réelle s'écrit sous la forme $c \prod_{k=1}^{m} \left(X^2 - 2\,\mathrm{Re}(z_k)X + |z_k|^2\right)$ et est donc de degré pair. □

Exercice 2.5.7.
Factoriser sur $\mathbb{R}$ les polynômes $X^5 + 1$ et $X^4 + 1$.

3 Dérivation des polynômes.

On introduit maintenant la notion de dérivation formelle de polynômes. Le mot « formel » est à prendre au sens suivant : on effectue des opérations *algébriques*, qui n'ont pas forcément de sens *analytique* (même si la dérivation formelle de polynômes coïncide avec la dérivation de fonctions polynomiales).

3.1 Définition.

Définition 3.1.1.
Soit $P \in \mathbb{K}[X]$, que l'on écrit $P = \sum_{k=0}^{+\infty} a_k X^k$. Son polynôme dérivé est

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

Remarque 3.1.2.
- La somme ne commence qu'à l'indice 1 :

 en effet, pour $k = 0$, X^{k-1} n'existe pas.
- On a également, après changement d'indice :

$$P' = \sum_{k=0}^{+\infty} a_{k+1}(k+1)X^k.$$

Cette formule est intéressante lorsqu'il s'agit de manipuler plusieurs polynômes, tous exprimés comme sommes commençant à l'indice 0.
- Sur $\mathbb{R}[X]$, cette opération coïncide avec la dérivation des applications à valeurs réelles :

$$\forall P \in \mathbb{R}[X] \qquad \widetilde{(P')} = \left(\widetilde{P}\right)'.$$

- Si P est de degré 0 ou $-\infty$, alors $P' = 0$. Sinon $\deg(P') = \deg(P) - 1$.

• P est un polynôme vérifiant $P' = \sum_{k=0}^{+\infty} a_k X^k$ si et seulement s'il existe $C \in \mathbb{K}$ vérifiant

$$P = C + \sum_{k=0}^{+\infty} \frac{a_k}{k+1} X^{k+1}$$

(donner un nom aux coefficients de P, calculer P' et utiliser l'unicité de la forme développée réduite).
• Si $P' = 0$, alors P est constant.

Définition 3.1.3.
Soit $P \in \mathbb{K}[X]$. On définit, pour $n \in \mathbb{N}$, le n-ième dérivé de P, noté $P^{(n)}$ par

$$\begin{aligned} & P^{(0)} = P \\ \text{et } \forall n \in \mathbb{N} \qquad & P^{(n+1)} = \left(P^{(n)}\right)' \end{aligned}$$

Exercice 3.1.4.
Soit $p \in \mathbb{N}$, dériver successivement X^p.

3.2 Propriétés.

Proposition 3.2.1.
Soit $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q', \tag{1}$$
$$(PQ)' = P'Q + PQ', \tag{2}$$
$$(P \circ Q)' = Q' \times (P' \circ Q). \tag{3}$$

Démonstration.
Écrivons P sous la forme $\sum_{k=0}^{+\infty} a_k X^k$ et Q sous la forme $\sum_{k=0}^{+\infty} b_k X^k$.

Alors on a

$$\begin{aligned} (\lambda P + \mu Q)' &= \left(\sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) X^k\right)' \\ &= \sum_{k=1}^{+\infty} k(\lambda a_k + \mu b_k) X^{k-1} \\ &= \lambda \left(\sum_{k=1}^{+\infty} k a_k X^{k-1}\right) + \mu \left(\sum_{k=1}^{+\infty} k b_k X^{k-1}\right) \\ &= \lambda P' + \mu Q'. \end{aligned}$$

Le premier point est donc assuré. Il se généralise évidemment par récurrence à toute combinaison linéaire finie de polynômes.

Montrons alors le second. Notons, pour tout $i \in \mathbb{N}$, A_i le monôme X_i et remarquons que pour tout $(i, j) \in \mathbb{N}^2$, on a $(A_i A_j)' = A_i' A_j + A_i A_j'$.

En effet, c'est évidemment vrai si $i = 0$ (auquel cas $A_i = 1$ et $A_i' = 0$) ou symétriquement si $j = 0$. Si ni i ni j n'est nul, on a $i \geqslant 1$ et $j \geqslant 1$, d'où

$$\begin{aligned} (A_i A_j)' &= (X^{i+j})' \\ &= (i+j) X^{i+j-1} \\ &= i X^{i-1} X^j + X^i \times j X^{j-1} \\ &= A_i' A_j + A_i A_j'. \end{aligned}$$

On a alors successivement :

$$\begin{aligned} (PQ)' &= \left(\left(\sum_{i \in \mathbb{N}} a_i A_i\right)\left(\sum_{j \in \mathbb{N}} b_j A_j\right)\right)' \\ &= \left(\sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A_j\right)' \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j (A_i A_j)' \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j \left(A_i' A_j + A_i A_j'\right) \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i' A_j + \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A_j'. \end{aligned}$$

Or on a

$$\begin{aligned} \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i' A_j &= \left(\sum_{i \in \mathbb{N}} a_i A_i'\right)\left(\sum_{j \in \mathbb{N}} b_j A_j\right) \\ &= P'Q \\ \text{et } \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A_j' &= \left(\sum_{i \in \mathbb{N}} a_i A_i\right)\left(\sum_{j \in \mathbb{N}} b_j A_j'\right) \\ &= PQ', \end{aligned}$$

donc $(PQ)' = P'Q + PQ'$.

On en déduit par récurrence que pour tout entier $k \in \mathbb{N}^*$, on a $\left(Q^k\right)' = kQ' \times Q^{k-1}$. En outre, on a évidemment $\left(Q^0\right)' = \left(1_{\mathbb{K}[X]}\right)' = 0$.

On a alors successivement

$$\begin{aligned}(P \circ Q)' &= \left(\sum_{k=0}^{+\infty} a_k Q^k\right)' \\ &= \sum_{k=1}^{+\infty} a_k k Q' \times Q^{k-1} \\ &= Q' \times \sum_{k=1}^{+\infty} a_k k Q^{k-1} \\ &= Q' \times \left(\left(\sum_{k=1}^{+\infty} k a_k X^{k-1}\right) \circ Q\right) \\ &= Q' \times \left(P' \circ Q\right).\end{aligned}$$

□

Remarque 3.2.2.
Notamment, $P' = Q'$ si et seulement si il existe $C \in \mathbb{K}$ tel que $P = Q + C$.

Proposition 3.2.3 (Formule de Leibniz)**.**
Soit $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$. Alors

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

Démonstration.
Elle se démontre par récurrence et est laissée en exercice au lecteur, qui remarquera une très très forte ressemblance avec la démonstration d'une formule de début d'année. □

Lemme 3.2.4 (Formule de Taylor Mac-Laurin)**.**
Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Alors

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

Démonstration.
Démontrons-la par récurrence :
pour tout $n \in \mathbb{N}$, soit (H_n) : pour tout $P \in \mathbb{K}_n[X]$, $P = \displaystyle\sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$.

• Pour $n = 0$, la propriété est évidente.

• Soit $n \in \mathbb{N}$ tel que la propriété soit vraie, et soit $P \in \mathbb{K}_{n+1}[X]$. Puisque $P' \in \mathbb{K}_n[X]$, on peut lui appliquer l'hypothèse de récurrence : $P' = \displaystyle\sum_{k=0}^{n} \frac{(P')^{(k)}(0)}{k!} X^k = \sum_{k=0}^{n} \frac{P^{(k+1)}(0)}{k!} X^k$. Il existe donc une constante $C \in \mathbb{K}$ telle que $P = \displaystyle\sum_{k=0}^{n} \frac{P^{(k+1)}(0)}{(k+1)!} X^{k+1} + C = \sum_{k=1}^{n+1} \frac{P^{(k)}(0)}{k!} X^k + C$ après un changement d'indice. Pour calculer C, on peut étudier les fonctions polynomiales associés aux polynômes de l'égalité précédente, et les évaluer en 0 : on trouve alors $C = P(0) = \dfrac{P^{(k)}(0)}{k!} X^k$ avec $k = 0$, et donc H_{n+1} est bien vérifiée. □

Proposition 3.2.5 (Formule de Taylor)**.**
Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors

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

Corollaire 3.2.6.
On en déduit immédiatement

$$P \circ (a + X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k$$

Démonstration.
Il suffit d'effectuer une "translation" à partir du théorème précédent : posons $Q = P \circ (X + a)$.
Alors $Q = \displaystyle\sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k$. Mais on vérifie facilement que pour tout k, $Q^{(k)} = P^{(k)} \circ (X + a)$ et donc $Q^{(k)}(0) = P^{(k)}(a)$.
Finalement, on a

$$\begin{aligned}P &= Q \circ (X - a) \\ &= \left(\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k\right) \circ (X - a) \\ &= \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X - a)^k\end{aligned}$$

□

Proposition 3.2.7.
Soit $P \in \mathbb{K}[X]$ non nul, $r \in \mathbb{N}$ et $a \in \mathbb{K}$.

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

Démonstration.
On écrit
$$P = \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!}(X-a)^k + \sum_{k=r}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$
Si
$$P(a) = P'(a) = \cdots = P^{r-1}(a) = 0,$$
alors directement $(X-a)^r \mid P$.

Réciproqueemnt, si $(X-a)^r \mid P$, alors
$$(X-a)^r \mid \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$
Comme
$$\deg\left(\sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!}(X-a)^k\right) \leqslant r-1,$$
on obtient
$$\sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!}(X-a)^k = 0.$$
On écrit alors
$$\begin{aligned} 0 &= 0 \circ (X+a) \\ &= \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!}(X)^k. \end{aligned}$$
Par unicité des coefficients d'un polynôme, on a alors
$$P(a) = P'(a) = \cdots = P^{r-1}(a) = 0,$$
On a donc bien $(X-a)^r \mid P$ et $(X-a)^{r+1} \nmid P$ si et seulement si $P^{(r)}(a) \neq 0$ et pour tout $k \in [\![0, r-1]\!]$, $P^{(k)}(a) = 0$. □

Exercice 3.2.8.
Déterminer les multiplicités de -2 et de i en tant que racines de
$$\begin{aligned} P = X^8 + 9X^7 + 32X^6 + 62X^5 \\ + 85X^4 + 97X^3 + 78X^2 + 44X + 24. \end{aligned}$$

Corollaire 3.2.9.
Soit $P \in \mathbb{K}[X]$, $r \in \mathbb{N}^*$ et $a \in \mathbb{K}$.

Si a est racine d'ordre r de P, alors a est racine d'ordre $r-1$ de P'.

La réciproque est fausse ! Par exemple si $P = X^2 - 1$, alors 0 est racine de multiplicité 1 de P', mais n'est pas racine de multiplicité 2 de P (ce n'est même pas une racine de P).

On peut cependant énoncer le résultat suivant : si a est racine d'ordre $r-1$ de P' et si a est racine, de P, alors a est racine d'ordre r de P.

4 Arithmétique de $\mathbb{K}[X]$.

4.1 PGCD.

Dans cette partie, pour tout $a \in \mathbb{K}[X]$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs de a et pour tout couple $(a,b) \in \mathbb{K}[X]$, $\mathscr{D}(a,b)$ l'ensemble des diviseurs communs à a et b. On remarquera que $\mathscr{D}(a,b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Remarque 4.1.1.
1. Soit d et d' deux polynômes. $\mathscr{D}(d) = \mathscr{D}(d')$ si et seulement si d et d' sont associés.
2. En particulier, si on a $\mathscr{D}(d) = \mathscr{D}(d')$ et que d et d' sont unitaires, alors $d = d'$ et pour tout polynôme d, il existe d' unitaire vérifiant $\mathscr{D}(d') = \mathscr{D}(d)$.

Lemme 4.1.2 (lemme d'Euclide)**.**
Soient $(a,b) \in \mathbb{K}[X]^2$, avec $b \neq 0$. Notons r le reste de la division euclidienne de a par b. Alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$.

Démonstration.
Soit $d \in \mathscr{D}(a,b)$. Alors a s'écrit sous la forme $bq + r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise bq, donc divise r. Donc $\mathscr{D}(a,b) \subset \mathscr{D}(b,r)$.

Réciproquement, soit $d \in \mathscr{D}(b,r)$, alors a s'écrit sous la forme $bq + r$ or $d|b$ et $d|r$ donc d divise a. Donc $\mathscr{D}(b,r) \subset \mathscr{D}(a,b)$. □

Théorème 4.1.3.
Soit $(a,b) \in \mathbb{K}[X]^2$ avec $(a,b) \neq (0,0)$. Alors, il existe $d \in \mathbb{K}[X]$ tel que $\mathscr{D}(a,b) = \mathscr{D}(d)$.

Démonstration.
Ce résultat repose sur un algorithme, appelé algorithme d'Euclide. En utilisant les objets «polynômes» fournis par la bibliothèque python `numpy`, cet algorithme s'écrit :

```
# utilise les polynômes fournis par numpy
# / retourne le couple (quotient, reste)
from numpy import poly1d

# p.order retourne le degré de p.
# Mais attention : si p == 0, p.order == 0.
# d'où cette définition
def degre(p):
    """Retourne le degré de p.
    Par convention degre(0) == -1."""
    if p == poly1d([]):
      return -1
    else
      return p.order

def diveuclide(p, q):
    return p / q

def euclide (a,b) :
    """Calcule le PGCD des polynômes a,b
       Précondition (a,b) != (0,0)"""
    R0 = a
    R1 = b
    while degre(R1) >= 0 :
        # Invariant : D(R0,R1) = D(a,b)
        # et (R0, R1) != (0,0)
        # Variant : degre(R1)
        (q, R2) = diveuclide (R0,R1)
        R0 = R1
        R1 = R2
    # R1 == 0
    return R0
```

Soit a et b deux polynômes non tous les deux nuls. Il est clair que l'appel `euclide(`a`,`b`)` termine. La valeur d retournée vérifie $\mathscr{D}(a,b) = \mathscr{D}(d,0)$ et $(d,0) \neq (0,0)$. Or $\mathscr{D}(d,0)$ est l'ensemble des diviseurs de d donc $\mathscr{D}(a,b)$ est bien l'ensemble des diviseurs d'un polynôme d.

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante :

$$\begin{cases} r_0 = a \\ r_1 = b \\ \forall n \in \mathbb{N},\ r_{n+2} = \begin{cases} \texttt{diveuclide}(r_n, r_{n+1}) & \text{si } r_{n+1} \neq 0 \\ 0 & \texttt{sinon} \end{cases} \end{cases}$$

À partir d'un certain rang, cette suite est nulle, sinon la suite $(\deg(r_n))_{n\in\mathbb{N}}$ serait strictement décroissante (du moins, à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0,0)$, on a $\mathscr{D}(r_n, r_{n+1}) = \mathscr{D}(a,b)$. En particulier, pour la dernière valeur non nulle r_n, on a $\mathscr{D}(r_n, 0) = \mathscr{D}(a,b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au $n$ème tour de boucle, R_0 contient la valeur de r_n, et R_1 celle de r_{n+1}. □

Remarque 4.1.4.
D'après la remarque 4.1.1, il existe donc un unique d unitaire tel que $\mathscr{D}(a,b) = \mathscr{D}(d)$.

Définition 4.1.5.
Soit a et b deux polynômes avec $(a,b) \neq (0,0)$, alors on appelle plus grands diviseurs communs de a et b (pgcd de a et b) **les** polynômes d vérifiant $\mathscr{D}(d) = \mathscr{D}(a,b)$. L'unique polynôme unitaire parmi ceux-ci est appelé **le** pgcd de a et b et noté $\mathrm{PGCD}(a,b)$ ou $a \wedge b$.

On convient que $\mathrm{PGCD}(0,0) = 0$.

Remarque 4.1.6.
1. L'existence des pgcd assurée par le théorème 4.1.3. D'après la remarque 4.1.1, il y en a donc un nombre infini.
2. L'existence et l'unicité du pgcd unitaire est assurée par la remarque 4.1.4.
3. Les pgcd de a et b sont les polynômes de degré maximum de $\mathscr{D}(a,b)$.
4. Si a et b sont deux polynômes de $\mathbb{R}[X]$, nous avons déjà vu que leurs divisoions euclidiennes dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$ sont les mêmes. Le lemme d'Euclide assure donc que le PGCD de a et b dans $\mathbb{C}[X]$ est le même que leur PGCD dans $\mathbb{R}[X]$. L'unicité du PGCD permet également de s'en assurer.
5. La relation de divisibilité $|$ n'est pas une relation d'ordre sur $\mathbb{K}[X]$, mais induit une relation d'ordre sur l'ensemble des polynômes unitaires. Le pgcd de deux polynômes unitaire a et b est alors le maximum des polynômes unitaires de $\mathscr{D}(a,b)$ pour $|$ et est donc la borne inférieure de a et b pour $|$.

On peut donner la caractérisation suivante :

Proposition 4.1.7.
Soient $(a, b, d) \in \mathbb{K}[X]^3$. d est un pgcd de a et b si et seulement si $d|a$ et $d|b$ et pour tout $n \in \mathbb{K}[X]$ vérifiant $n|a$ et $n|b$, on a $n|d$.

Démonstration.
Remarquons successivement :

1. $d|a$ et $d|b \Leftrightarrow d \in \mathscr{D}(a, b) \Leftrightarrow \mathscr{D}(d) \subset \mathscr{D}(a, b)$. La dernière équivalence peut se démontrer comme suit : le sens direct provient de la transitivité de la relation de divisibilité (si d est un diviseur de a, tout diviseur de d est un diviseur de a ; idem avec b) ; le sens indirect vient du fait que $\mathscr{D}(d)$ contient d.
2. $\left[\forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d\right] \Leftrightarrow \mathscr{D}(d) \supset \mathscr{D}(a, b)$ découle directement de la définition de $\mathscr{D}(d)$ et $\mathscr{D}(a, b)$.
3. Par conséquent, on a $\left[d|a \text{ et } d|b \text{ et } \forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d\right]$ si et seulement si $\mathscr{D}(d) = \mathscr{D}(a, b)$, si et seulement si d est un pgcd de a et b.

$\square$

On a également :

Proposition 4.1.8.
Soient $(a, b, c) \in \mathbb{K}[X]^3$. Alors $(ac) \wedge (bc) = \frac{1}{\lambda} c(a \wedge b)$, où λ est le coefficient dominant de c.

Démonstration.
Soit $\delta = a \wedge b$ et $\Delta = (ac) \wedge (bc)$. Il suffit de montrer que $c\delta$ et Δ sont associés, et pour cela nous allons montrer que $c\delta|\Delta$ et $\Delta|c\delta$.

1. $\delta|a$ et $\delta|b$, donc $c\delta|ac$ et $c\delta|bc$. Par suite $c\delta|\Delta$.
2. $c|ac$ et $c|bc$, donc $c|\Delta$. Ainsi il existe $p \in \mathbb{R}[X]$ tel que $\Delta = pc$. Donc $pc = \Delta|ac$ et $pc = \Delta|bc$. Le polynôme c étant non nul, on en déduit $p|a$ et $p|b$, et donc $p|\delta$. Finalement $\Delta = pc|\delta c$.

On a donc le résultat. $\square$

Théorème 4.1.9 (Théorème de Bézout, première partie)**.**
Soient $(a, b) \in \mathbb{K}[X]^2$. Il existe deux polynômes u et v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b.

Démonstration.
L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires (à coefficients polynomiaux) de a et b. À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b.

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0 a + V_0 b$ et $R_1 = U_1 a + V_1 b$. En python, en supposant[4] que l'existence d'un type des polynômes, et à condition que les notation `+` et `*` soient autorisées pour la somme et le produit de polynômes (et pour le produit d'un polynôme par un scalaire), cet algorithme s'écrit :

```
def euclide_etendu (a, b) :
    """Donne une relation de Bézout sur a,b
       Précondition : (a,b) != (0,0)"""
    R0 = a
    U0 = 1
    V0 = 0
    # R0 == U0*a + V0*b
    R1 = b
    U1 = 0
    V1 = 1
    # R1 == U1*a + V1*b
    while degre(R1) >= 0 :
        # Invariant : D(R0,R1) == D(a,b)
        # et R1>=0 et R2>=0 et
        # (R1,R2)!= (0,0)
        # et R0 == U0*a + V0*b
        # et R1 == U1*a + V1*b
        # Variant : deg(R1)
        (q,R2) = diveuclide(R0,R1)
        # donc R2 = R0 - q*R1
        U2 = U0 - q*U1
        V2 = V0 - q*V1
        # R2 = U2*a + V2*b
        R0, U0, V0 = R1, U1, V1
        R1, U1, V1 = R2, U2, V2
    # R1 == 0
    return (R0,U0,V0)
```

(attention cependant, l'algorithme ci-dessus ne retourne pas *le* pgcd mais *un* pgcd avec les coefficients de Bézout associés).

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r, u et v, où r est la suite considérée précédemment, où u et v vérifient $r_i = u_i a + v_i b$ pour $i = 0, 1$ et pour n tel que r_{n+1} soit non nul, $u_{n+2} = u_n - aq_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$, où q est le quotient de la division euclidienne de r_n par r_{n+1}. Là encore, il n'est pas difficile de montrer par récurrence double que tant que $(r_n, r_{n+1}) \neq (0, 0)$, on a $r_n = u_n a + v_n b$. $\square$

Le couple des coefficients de Bézout n'est

4. Il existe des bibliothèques pour cela (`numpy` par ex.) !

pas unique. Par exemple on a

$$\begin{array}{rlrl} 1\times & (2X^2+X) & -2X\times & X = X \\ (X+1)\times & (2X^2+X) & -(2X^2+3X)\times & X = X \end{array}$$

Exemple 4.1.10.
Calcul d'un couple de Bézout pour

$$P = 2X^6 - 5X^5 + 8X^4 - 6X^3 + 3X - 2$$

et

$$Q = 2X^5 - 7X^4 + 14X^3 - 17X^2 + 12X - 4$$

4.2 Polynômes premiers entre eux.

Définition 4.2.1.
Deux polynômes a et b sont dit premiers entre eux si et seulement si $(a, b) \neq (0, 0)$ et $a \wedge b = 1$.

Remarque 4.2.2.

1. Le PGCD de deux polynômes réels étant le même dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$, alors deux polynômes réeles sont premiers dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.
2. a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont les éléments inversibles de $\mathbb{K}[X]$, en d'autres termes si et seulement si $\mathscr{D}(a, b) \subset \mathbb{K}^*$ (ce qui est équivalent à $\mathscr{D}(a, b) = \mathbb{K}^*$).
3. si a et b sont irréductibles, alors ils sont soit premiers entre eux, soit associés. En particulier, si a et b sont irréductibles et unitaires, alors ils sont soit premiers entre eux, soit égaux.

Théorème 4.2.3 (Théorème de Bézout, seconde partie)**.**
Soient $a, b \in \mathbb{K}[X]$. a et b sont premiers entre eux si et seulement s'il existe deux polynômes u et v tels que $au + bv = 1$.

Démonstration.
Le cas $(a, b) = (0, 0)$ est trivial (dans ce cas, a et b ne sont pas premiers entre eux et il n'existe pas de couple de Bézout).

Considérons donc $(a, b) \in \mathbb{K}[X]^2 \setminus \{ (0, 0) \}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout première partie, on a le résultat.

Réciproquement, supposons qu'il existe deux polynômes u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathscr{D}(a, b)$. On a $d|a$ et $d|b$, donc $d|(au + bv)$, donc $d|1$, donc $d \in \mathbb{K}^*$. Donc $\mathscr{D}(a, b) \subset \mathbb{K}^*$. □

$au+bv = 1$ implique $a \wedge b = 1$, mais $au+bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b)|d$.

Corollaire 4.2.4.
Soit $a, b \in \mathbb{K}[X] \setminus \{ (0, 0) \}$. Alors en posant $d = a \wedge b$, a et b s'écrivent respectivement sous la forme $a' \times d$ et $b' \times d$ où $(a', b') \in \mathbb{K}[X]^2$. On a alors $a' \wedge b' = 1$

Démonstration.
On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a'u + b'v$, d'où a' et b' sont premiers entre eux. □

Remarque 4.2.5.
Ce corollaire est très fréquemment utilisé.

Corollaire 4.2.6.

(i) Soient a premier avec k polynômes $b_1, b_2, \dots, b_k$. Alors a est premier avec $b_1.b_2.\dots.b_k$.

(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}^*$, a^m et b^n sont également premiers entre eux.

Démonstration.

(i) On traite le cas $k = 2$, le cas général s'en déduit immédiatement par récurrence. Il existe a_i et b_i vérifiant $au_i + b_iv_i = 1$ pour $i = 1, 2$. En multipliant ces deux relations, il vient successivement

$$1 = (au_1 + b_1v_1)(au_2 + b_2v_2)$$
$$1 = a^2u_1u_2 + au_1b_2v_2 + b_1v_1au_2 + b_1v_1b_2v_2$$
$$1 = a(au_1u_2 + u_1b_2v_2 + b_1v_1u_2) + b_1b_2(v_1v_2)$$

D'où le résultat.

(ii) On applique (i) à a et $b.b.b.\dots.b$, puis (i) à b^n et $a.a.a.\dots.a$. Plus proprement, la résultat se démontre par récurrence.

□

Théorème 4.2.7 (Théorème de Gauss)**.**
Soient $(a,b,c) \in \mathbb{K}[X]^3$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.
On a $a \wedge b = 1$ donc 1 s'écrit sous la forme $au + bv$ avec $(u,v) \in \mathbb{K}[X]^2$. Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire à coefficients dans $\mathbb{K}[X]$ de a et bc. Or bc est un multiple de a donc c est un multiple de a. $\square$

Théorème 4.2.8 (Unicité de la décomposition en facteurs irréductibles)**.**
Tout polynôme non nul se décompose de façon unique comme produit d'un scalaire par des irréductibles unitaires, à l'ordre près des facteurs.

Démonstration.
On a déjà vu l'existence. Il reste donc à montrer l'unicité. Par l'absurde, supposons qu'il existe un polynôme admettant deux décompositions. Alors il existe un polynôme P de degré minimal admettant deux décompositions distinctes $\lambda \prod_{k=1}^{a} A_k$ et $\mu \prod_{k=1}^{b} B_k$, où $(a,b) \in \mathbb{N}^2$, $(\lambda,\mu) \in \mathbb{K}^2$ et les A_k et les B_k sont irréductibles pour k appartenant respectivement à $[\![1,a]\!]$ et $[\![1,b]\!]$.

Alors λ et μ sont le coefficient dominant de P, donc sont égaux.

Donc $\prod_{k=1}^{a} A_k = \prod_{k=1}^{b} B_k$.

On a $a \neq 0$. En effet, sinon on aurait $b = 0$ et on aurait dans les deux cas à un produit vide, il aurait donc unicité.

De même $b \neq 0$.

Remarquons que pour tout $k \in [\![1,b]\!]$, A_a est premier avec B_k. En effet, sinon il existerait $k_0 \in [\![1,b]\!]$ tel que A_a et B_{k_0} ne soient pas premiers entre eux. Or ils sont irréductibles, donc ils sont égaux. Donc on a

$$\prod_{k=1}^{a-1} A_k = \prod_{\substack{k \in [\![1,b]\!] \\ k \neq k_0}} B_k$$

Il existe donc un polynôme de degré strictement plus petit que $\deg P$, admettant deux décompositions distinctes, ce qui est absurde.

Donc A_a est donc premier avec $\prod_{k=1}^{b} B_k$, donc avec P. Or A_a divise P et n'est pas un polynôme constant.

C'est donc absurde. $\square$

Remarque 4.2.9.
Comme pour les entiers, nous pouvons donner les résultats suivants :

— Deux polynômes sont premiers entre eux si et seulement s'ils n'ont aucun facteur irréductible en commun ;

— Deux polynômes sont premiers entre eux si et seulement s'ils n'ont aucune racine complexe en commun ;

— la notion de *valuation* d'un polynôme irréductible dans un polynôme peut se définir, et permet de calculer le PGCD de deux polynômes A et B, en considérant le minimum des valuations d'un même facteur irréductible dans A et B. En anticipant sur les paragraphes qui suivent, la valuation est également utilisée pour le PPCM de deux polynômes, mais aussi les PGCD et PPCM d'une famille de polynômes.

4.3 PGCD de n polynômes.

Comme dans le cas de l'arithmétique sur les entiers, on introduit la notion de PGCD de plusieurs polynômes et de polynômes premiers entre eux dans leur ensemble.

Définition 4.3.1.
Soit $(A_1,\dots,A_n) \in \mathbb{K}[X]^n$, on note $\mathscr{D}(A_1,\dots,A_n) = \bigcap_{i=1}^{n} \mathscr{D}(A_i)$ l'ensemble des diviseurs communs à tous ces polynômes.

Proposition 4.3.2.
Soit $(A_1,\dots,A_n) \in \mathbb{K}[X]^n$, il existe un polynôme D unique à association près tel que $\mathscr{D}(A_1,\dots,A_n) = \mathscr{D}(D)$.

Démonstration.
L'unicité à association près est évidente. On montre par récurrence que $\forall n \in \mathbb{N}^*, \mathscr{H}_n : \forall (A_1,\dots,A_n) \in \mathbb{K}[X]^n, \exists D \in \mathbb{K}[X], \mathscr{D}(A_1,\dots,A_n) = \mathscr{D}(D)$.

Initialisation : OK.

Hérédité : Soit $n \in \mathbb{N}^*$, supposons $\mathscr{H}_n$ et montrons $\mathscr{H}_{n+1}$. Soit $(A_1,\dots,A_{n+1}) \in \mathbb{K}[X]^{n+1}$. D'après $\mathscr{H}_n$, il existe D_1 tel que $\mathscr{D}(A_1,\dots,A_n) = \mathscr{D}(D_1)$. On a alors

$$\begin{aligned}
\mathscr{D}(A_1,\dots,A_{n+1}) &= \bigcap_{i=1}^{n+1} \mathscr{D}(A_i) \\
&= \mathscr{D}(A_1,\dots,A_n) \cap \mathscr{D}(A_{n+1}) \\
&= \mathscr{D}(D_1) \cap \mathscr{D}(A_{n+1}) \\
&= \mathscr{D}(D_1 \wedge A_{n+1}),
\end{aligned}$$

d'où $\mathscr{H}_{n+1}$.

□

Remarque 4.3.3.
On a toujours $\mathscr{D}(A_1,\dots,A_n,0)=\mathscr{D}(A_1,\dots,A_n)$.

Définition 4.3.4.
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls. On note alors $A_1\wedge\dots\wedge A_n=\mathrm{PGCD}(A_1,\dots,A_n)$ l'unique polynôme unitaire D vérifiant $\mathscr{D}(A_1,\dots,A_n)=\mathscr{D}(D)$ (un polynôme non unitaire vérifiant ceci est *un* PGCD).

On convient que $\mathrm{PGCD}(0,\dots,0)=0$.

Corollaire 4.3.5.
Soit $A_1,\dots,A_n\in\mathbb{K}[X]$, tels que les $A_1,\dots,A_{n-1}$ soient non tous nuls. On a alors $A_1\wedge\dots\wedge A_n=(A_1\wedge\dots\wedge A_{n-1})\wedge A_n$.

Corollaire 4.3.6.
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls, soit $D\in\mathbb{K}[X]$ unitaire. Alors $D=A_1\wedge\dots\wedge A_n$ si et seulement si

1. $\forall i\in\{1,\dots,n\},\ D|A_i$;
2. $\forall P\in\mathbb{K}[X],\ (\forall i\in\{1,\dots,n\},\ P|A_i)\Rightarrow P|D$.

Définition 4.3.7.
Des polynômes $A_1,\dots,A_n$ sont dits premiers entre eux *dans leur ensemble* si $A_1\wedge\dots\wedge A_n=1$, c'est-à-dire si $\mathscr{D}(A_1,\dots,A_n)=\mathbb{K}^*$.

Théorème 4.3.8 (Théorème de Bézout.)**.**
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls.

1. Il existe $(U_1,\dots,U_n)\in\mathbb{K}[X]^n$ tel que
$$\sum_{i=1}^n A_iU_i=A_1\wedge\dots\wedge A_n.$$
2. S'il existe $(U_1,\dots,U_n)\in\mathbb{K}[X]^n$ tel que $\sum_{i=1}^n A_iU_i=1$, alors les $(A_i)_{i=1}^n$ sont premiers entre eux dans leur ensemble.

Démonstration.
Exactement comme pour les entiers, en remarquant que s'il existe D et $U_1,\dots,U_n$ vérifiant $\sum_{i=1}^n A_iU_i=D$, alors $A_1\wedge\dots\wedge A_n|D$. □

Remarque 4.3.9.
Si une famille finie de polynômes contient deux polynômes premiers entre eux, alors les polynômes de cette famille sont premiers entre eux dans leur ensemble.

Exemple 4.3.10.
Comme dans le cas des entiers, des polynômes qui ne sont pas premiers entre eux deux à deux peuvent être premiers entre eux dans leur ensemble. Exhiber une telle famille.

4.4 PPCM.

Pour tout polynôme a, b, l'ensemble des multiples de a est noté $a\mathbb{K}[X]$. L'ensemble des multiples communes à a et b est donc $a\mathbb{K}[X]\cap b\mathbb{K}[X]$.

Remarque 4.4.1.
1. Soit d et d' deux polynômes. $d\mathbb{K}[X]=d'\mathbb{K}[X]$ si et seulement d et d' sont associés.
2. En particulier, si on a $d\mathbb{K}[X]=d'\mathbb{K}[X]$ et que d et d' sont unitaires, alors $d=d'$ et pour tout polynôme d, il existe d' unitaire vérifiant $d'\mathbb{K}[X]=d\mathbb{K}[X]$.

Théorème 4.4.2.
Soit $(a,b)\in\mathbb{K}[X]^2$. Alors il existe $m\in\mathbb{K}[X]$ tel que $a\mathbb{K}[X]\cap b\mathbb{K}[X]=m\mathbb{K}[X]$.

Démonstration.
Dans le cas où a ou b est nul, on a évidemment $a\mathbb{K}[X]\cap b\mathbb{K}[X]=0\mathbb{K}[X]$. On suppose donc par la suite que a et b sont tous deux non nuls.

Posons $d=a\wedge b$. Alors a (resp. b) est de la forme $a'd$ (resp. $b'd$) et a' et b' sont premiers entre eux.

Posons $m = a'b'd$. m est un multiple de a et de b, donc $m\mathbb{K}[X] \subset a\mathbb{K}[X]$ et $m\mathbb{K}[X] \subset b\mathbb{K}[X]$. Donc $m\mathbb{K}[X] \subset a\mathbb{K}[X] \cap b\mathbb{K}[X]$.

Réciproquement, soit $c \in a\mathbb{K}[X] \cap b\mathbb{K}[X]$. Comme c est multiple de a, il existe $u \in \mathbb{K}[X]$ tel que $c = ua = ua'd$. De même, c est multiple de b, il existe $v \in \mathbb{K}[X]$ tel que $c = vb = vb'd$.

On a donc, comme $d \neq 0$, $ua' = vb'$. Ainsi, $b'|ua'$. Or, a' et b' sont premiers entre eux, donc d'après le lemme de Gauss $b'|u$. Ainsi, $b'a'd|ua'd$, or $m = b'a'd$ et $c = ua'd$. donc $c \in m\mathbb{K}[X]$. □

Définition 4.4.3.
Soit a et b deux polynômes. Alors on appelle plus petits communs multiples de a et b (ppcm de a et b) **les** polynômes d tels que l'ensemble $a\mathbb{K}[X] \cap b\mathbb{K}[X]$ des multiples communs à a et b soit l'ensemble $d\mathbb{K}[X]$ des multiples de d.

On appelle **le** ppcm de a et b le seul de ces ppcm qui soit unitaire ou nul. Il est noté $\mathrm{PPCM}(a, b)$ ou $a \vee b$.

Remarque 4.4.4.
1. Cette définition est justifiée par la remarque 4.4.1 et le théorème 4.4.2.
2. $a \vee b = 0$ si et seulement si a ou b est nul.

Remarque 4.4.5.
Sur l'ensemble des polynômes unitaires, le ppcm de deux polynômes a et b est donc la borne supérieure de a et b pour l'ordre $|$.

On peut donner la caractérisation suivante :

Proposition 4.4.6.
Soient $a, b, m \in \mathbb{K}[X]$. m est un ppcm de a et b si et seulement si on a
1. $a|m$;
2. et $b|m$;
3. et pour tout $n \in \mathbb{K}[X]$, $a|n$ et $b|n \Rightarrow m|n$.

On a également :

Proposition 4.4.7.
Soient $a, b, c \in \mathbb{K}[X]$, avec $c \neq 0$.
(i) $(ac) \vee (bc)$ et $c(a \vee b)$ sont associés.
(ii) ab et $(a \wedge b).(a \vee b)$ sont associés.

Exemple 4.4.8.
Calculer $X^2 - 4X + 3 \vee X^2 + X - 2$.

5 Formule d'interpolation de Lagrange.

Dans cette partie, on considère un entier n et (x_0, y_0), ..., (x_n, y_n) des couples d'éléments de $\mathbb{K}$.

On aimerait savoir s'il existe un polynôme P vérifiant

$$\forall i \in [\![0, n]\!] \quad P(x_i) = y_i, \tag{4}$$

dit autrement, on cherche s'il existe une fonction polynomiale dont le graphe passe par tous les points (x_i, y_i) pour $i \in [\![0, n]\!]$.

Il est bien évident que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i = y_j$, on peut supprimer le couple (x_j, y_j) de la liste des couples considérés sans changer le problème.

Il est évident également que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i \neq y_j$, il n'existe pas de solution.

C'est pourquoi, par la suite, **on suppose que** x_0**, ..., **x_n **sont deux à deux distincts**.

Définition 5.0.1.
On appelle *base de Lagrange associée aux points* x_0, ..., x_n le $(n+1)$-uplet $(L_0, \dots, L_n)$ vérifiant pour tout $i \in [\![0, n]\!]$:

$$L_i = \frac{1}{\alpha_i} \prod_{\substack{j \in [\![0,n]\!] \\ j \neq i}} (X - x_j)$$

où

$$\alpha_i = \prod_{\substack{j \in [\![0,n]\!] \\ j \neq i}} (x_i - x_j).$$

Proposition 5.0.2.
Pour tout $(i, j) \in [\![0, n]\!]^2$, on a $L_i(x_i) = 1$ et $L_i(x_j) = 0$ si $j \neq i$.

Autrement dit, dans tous les cas, on a

$$L_i(x_j) = \delta_{i,j}.$$

Corollaire 5.0.3.
Soit $(\lambda_0, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$. Alors, en posant

$$P = \sum_{i=0}^{n} \lambda_i L_i,$$

on a pour tout $i \in [\![0, n]\!]$:

$$P(x_i) = \lambda_i.$$

Théorème 5.0.4.
Il existe un unique polynôme P de degré au plus n vérifiant l'équation (4). Il s'agit du polynôme

$$\sum_{i=0}^{n} y_i L_i.$$

Démonstration. **Unicité sous réserve d'existence** Soit P et Q deux polynômes de degré au plus n vérifiant la propriété demandée. Alors P et Q coïncident en $n+1$ points distincts et sont de degré au plus n donc P et Q sont égaux.

Existence Le polynôme donné dans l'énoncé vérifie évidemment l'équation (4). Par ailleurs, il s'agit d'une combinaison linéaire de polynômes qui sont tous de degré n. Il est donc de degré au plus n.

□

Exercice 5.0.5.
Montrer que pour tout $P \in \mathbb{K}_n[X]$, il existe un existe un unique $(\lambda_0, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que $P = \sum_{i=0}^{n} \lambda_i L_i$.

Exercice 5.0.6.
Déterminer l'unique polynôme P de degré au plus 3 vérifiant $P(-1) = -9$, $P(0) = -1$, $P(1) = 5$ et $P(2) = 21$.

Corollaire 5.0.7.
L'ensemble des polynômes vérifiant l'équation (4) est

$$\{ P \times D + P_0 \mid P \in \mathbb{K}[X] \}$$

où

$$D = \prod_{i=0}^{n} (X - x_i),$$
$$P_0 = \sum_{i=0}^{n} y_i L_i.$$

Démonstration.
Remarquons tout d'abord que pour tout $i \in [\![0, n]\!]$, on a $D(x_i) = 0$.

Analyse Soit Q un polynôme vérifiant l'équation (4). En effectuant la division euclidienne de Q par D, on peut écrire Q sous la forme $P \times D + R$ où $P \in \mathbb{K}[X]$ et $R \in \mathbb{K}[X]$ avec $\deg R < n+1$. On a donc $\deg R \leqslant n$. De plus, pour tout $i \in [\![0, n]\!]$, on a $R(x_i) = Q(x_i) - P(x_i)D(x_i) = y_i - P(x_i) \times 0 = y_i$. Donc R est nécessairement le polynôme P_0 et P s'écrit sous la forme $P \times D + P_0$.

Synthèse Réciproquement, soit P un polynôme. Posons $Q = P \times D + P_0$. Alors pour tout $i \in [\![0, n]\!]$, on a $Q(x_i) = P(x_i) \times 0 + P_0(x_i) = y_i$. Donc Q vérifie l'équation (4).

Conclusion L'ensemble des polynômes vérifiant l'équation (4) est

$$\{ P \times D + P_0 \mid P \in \mathbb{K}[X] \}.$$

□

Remarque 5.0.8.
En exprimant l'équation (4) sous la forme

$$(P(x_0), \ldots, P(x_n)) = (y_0, \ldots, y_n),$$

cet ensemble de solutions est encore un ensemble de la forme solution particulière plus l'ensemble des solutions de l'équation homogène associée.

6 Annexe : construction de $\mathbb{K}[X]$

La construction de $\mathbb{K}[X]$ n'est pas exigible, cette partie est une version alternative aux parties 1.1 et 1.2.

Définition 6.0.1.
On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

Remarque 6.0.2.
1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.
2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse [5].

On peut alors construire l'anneau des polynômes à coefficients dans $\mathbb{K}$ comme suit.

Définition 6.0.3.
On note $\mathbb{K}[X]$ l'ensemble des suites à support fini à valeurs dans $\mathbb{K}$.

Définition 6.0.4.
Soit $P = (P_n)_{n\in\mathbb{N}}$ un polynôme. Si P n'est pas la suite nulle, le *degré* de P est le plus grand rang d pour lequel $P_d \neq 0$. Si P est la suite nulle, on considère que c'est $-\infty$.

Dans tous les cas, on peut écrire :

$$\deg P = \sup \{d \in \mathbb{N},\ P_d \neq 0\}.$$

Définition 6.0.5.
L'addition sur $\mathbb{K}[X]$ est celle de $\mathbb{K}^{\mathbb{N}}$, on la notera $+$. $(\mathbb{K}[X], +)$ est alors un groupe abélien.

Remarque 6.0.6.
$\mathbb{K}[X]$ hérite aussi de la multiplication scalaire de $\mathbb{K}^{\mathbb{N}}$. On dira plus tard que c'en est un *sous-espace vectoriel*.

5. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

Remarque 6.0.7.
Par l'injection $\mathbb{K} \to \mathbb{K}[X], x \mapsto (x, 0, \dots)$, on voit $\mathbb{K}$ comme étant inclus dans $\mathbb{K}[X]$. C'en est aussi un sous-groupe (et un sous-espace vectoriel). On identifiera par exemple le réel 1 au polynôme $(1, 0, \dots)$.

Démonstration.
On montre que c'est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. La suite nulle est bien entendu à support fini. Il suffit donc de montrer que la différence de deux polynômes est un polynôme. Soit P et Q deux polynômes de degrés p et q respectivement. Si $n \geqslant \max(p, q)$, alors $P_n - Q_n = 0$ donc $P - Q$ est un polynôme. □

Définition 6.0.8.
Soit $P = (P_n)$ et $Q = (Q_n)$ deux polynômes, on définit le polynôme $P \times Q$ par :

$$PQ = \left(\sum_{k=0}^{n} P_k Q_{n-k}\right)_{n\in\mathbb{N}}.$$

Proposition 6.0.9.
Si P et Q sont deux polynômes, PQ est un polynôme de degré $\deg P + \deg Q$.

Démonstration.
Si P ou Q sont nuls, il est évident que $PQ = 0$. Sinon, notons p et q les degrés respectifs de P et de Q. Soit $n > p + q$, soit $k \in [\![0, n]\!]$. Si $k > p$, alors $P_k = 0$ et si $k \leqslant p$, $n - k \geqslant n - p > q$, donc $Q_{n-k} = 0$. Ainsi, si $n > p + q$, $\sum_{k=0}^{n} P_k Q_{n-k} = 0$ et PQ est donc bien un polynôme, de degré au plus $p + q$. Il suffit ensuite de voir que $(PQ)_{p+q} = P_p Q_q \neq 0$ pour obtenir le degré de PQ. □

Théorème 6.0.10.
$(\mathbb{K}[X], +, \times)$ est un anneau.

Remarque 6.0.11.
La structure multiplicative de $\mathbb{K}[X]$ est différente de celle de $\mathbb{K}^{\mathbb{N}}$, $\mathbb{K}[X]$ n'est pas un sous-anneau (notion HP) de $\mathbb{K}^{\mathbb{N}}$.

Démonstration.
Le caractère de groupe abélien a déjà été vu, le reste des propriétés se montre de manière élémentaire, mais fastidieuse. L'écriture canonique introduite plus bas permet un peu d'alléger les notations. □

Définition 6.0.12.
On note X la suite toujours nulle, sauf pour le terme de rang 1 qui vaut 1 : $X = (0, 1, 0, 0, \dots)$.

Proposition 6.0.13.
Par convention, $X^0 = 1$. De plus, si $n \geqslant 1$,

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ fois}}, \underbrace{1}_{(n+1)^{\text{e}} \text{ position}}, 0, \dots).$$

Plus formellement, si $k \in \mathbb{N}$,

$$(X^n)_k = \begin{cases} 1 & \text{si } k = n+1 \ ; \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.
On le montre aisément par récurrence sur n, en remarquant que pour tout polynôme P le k^{e} coefficient de PX est le $(k-1)^{\text{e}}$ coefficient de P. □

On obtient donc la représentation usuelle des polynômes.

Corollaire 6.0.14.
Soit $P = (P_n)_{n \in \mathbb{N}}$ un polynôme de degré d. On a alors

$$P = \sum_{n=0}^{d} P_n X^n.$$

De plus, pour tout entier $d' \geqslant d$,

$$P = \sum_{n=0}^{d'} P_n X^n.$$

On s'autorise donc à écrire

$$P = \sum_{n=0}^{+\infty} P_n X^n$$

et, pour tout polynôme $Q = \sum_{n=0}^{d} P_n X^n$, on a bien

$$P + Q = \sum_{n=0}^{+\infty} (P_n + Q_n) X^n$$

ainsi que

$$P \times Q = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} P_k Q_{n-k} \right) X^n.$$

Enfin, on retrouve les mêmes notations que classiquement.

Définition 6.0.15.
Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$, non nul.

Le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg_P} X^{\deg P}$ est le *monôme dominant* de P.

Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 6.0.16.
1. $\mathbb{K}_n[X]$ **n'est pas** l'ensemble des polynômes de degré **égal** à n.
2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \dots \subset \mathbb{K}[X]$.
3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.
4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geqslant d$ alors P peut s'écrire sous la forme $\sum_{k=0}^{n} a_k X^k$.

7 Annexe : fonctions polynomiales à valeurs dans un anneau

Dans cette section, on considère un entier naturel n fixé et on pose $A = \mathbb{K}$ ou $A = \mathscr{M}_n(\mathbb{K})$.

Dans tous les cas, A, muni de l'addition et de la multiplication usuelle est un anneau. Notons 0_A et 1_A les neutres respectifs pour l'addition et la multiplication dans A. Il s'agit de 0 et 1 si $A = \mathbb{K}$ et de $0_{M_n(\mathbb{K})}$ et I_n si $A = \mathscr{M}_n(\mathbb{K})$.

Dans les deux cas, on dispose d'une loi de composition externe, que nous noterons $\cdot : \mathbb{K} \times A \to A$. C'est la multiplication usuelle dans $\mathbb{K}$ si $A = \mathbb{K}$ et la multiplication d'une matrice par un scalaire si $A = \mathscr{M}_n(\mathbb{K})$.

Dans les deux cas, on a d'une part les propriétés suivantes [6] :

1. La loi $\cdot$ est distributive à gauche par rapport à l'addition dans A et à droite par rapport à l'addition dans $\mathbb{K}$.
2. Elle vérifie la propriété d'associativité mixte par rapport à la multiplication dans $\mathbb{K}$.
3. l'élément neutre de $\mathbb{K}$ est neutre à gauche pour $\cdot$.

Autrement dit, pour tout $(\lambda, \mu) \in \mathbb{K}^2$ et tout $(x, y) \in A^2$:

1. $\lambda \cdot (x +_A y) = \lambda \cdot x +_A \lambda \cdot y$ et $(\lambda +_{\mathbb{K}} \mu) \cdot x = \lambda \cdot x +_A \mu \cdot x$.
2. $(\lambda \times_{\mathbb{K}} \mu) \cdot x = \lambda \cdot (\mu \cdot x)$.
3. $1 \cdot x = x$.

Dans les deux cas, on a de plus la propriété additionnelle [7] que pour tout (λ, μ) et tout (x, y), on a :

$$(\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_{\mathbb{K}} \mu) \cdot (x \times_A y)$$

Si on met l'accent sur ces seules propriétés, c'est parce qu'elles sont suffisantes pour montrer tout ce dont nous aurons besoin dans cette partie, sans plus avoir besoin de distinguer le cas $A = \mathbb{K}$ du cas $A = \mathscr{M}_n(\mathbb{K})$. Par exemple, le fait que pour élément x de A on a $0 \cdot x$ peut se montrer en remarquant qu'on a $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$.

6. On dit que $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
7. Un anneau $(A, +, \times)$ tel que $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et qui vérifie cette propriété est appelé une $\mathbb{K}$-algèbre.

Définition 7.0.1.
Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\widetilde{P}(x)$ l'élément de A défini par

$$\widetilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k$$

Exemple 7.0.2.
On pose $P = X^2 + 2X + 3$

1. Que vaut l'évaluation de P en -2 ?
2. Que vaut l'évaluation de P en $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$?

Proposition 7.0.3.
Soit $x \in A$ fixé. Alors l'application d'évaluation en x, $\mathsf{eval}_x : \begin{array}{ccc} \mathbb{K}[X] & \to & A \\ P & \mapsto & \widetilde{P}(x) \end{array}$ est un morphisme d'anneau ; autrement dit pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_A$.

De plus, on a

$$\widetilde{P \circ Q}(x) = P(Q(x))$$

La suite du cours considère uniquement le cas $A = \mathbb{K}$, le cas $A = \mathscr{M}_n(\mathbb{K})$ fera l'objet d'une étude plus approfondie en spé.