# Anneau des polynomes

Dans tout ce chapitre, $\mathbb{K}$ désignera un corps commutatif (ici $K = \mathbb{Q}, \mathbb{R}$, ou $\mathbb{C}$, et pourra être $\mathbb{Z}/p\mathbb{Z}$ en deuxième année). Certains résultats (notamment sur la dérivation) nécessiteront de supposer que la caractéristique du corps $\mathbb{K}$ est nulle. Dans ce cas, $K = \mathbb{Q}, \mathbb{R}$, ou $\mathbb{C}$.

## 1 Construction de $\mathbb{K}[X]$.

### 1.1 Polynôme formel

**Définition 1**

On appelle **polynôme** (à une indéterminée) à coefficients dans $\mathbb{K}$ une suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$, tous nuls à partir d'un certain rang.
Pour $n \in \mathbb{N}$, on dit que le terme $a_n$ est le **$n$-ième coefficient** du polynôme $P$.
L'**ensemble des polynômes** à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[X]$, si on choisit de noter $X$ l'indéterminée.

**Exemple 1**

Par exemple, $P = (1, 0, 2, 3, 0, 0, 0, \ldots)$ est un polynôme, que vous avez l'habitude de noter $P = 1 + 0 \cdot X + 2X^2 + 3X^3$.

**Définition 2**

Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

*Preuve.* C'est la même preuve de deux suites égales. □

### 1.2 Lois et structure

**Définition 3 : Lois de compositions internes et externes sur l'ensemble des polynômes**

Soient $A = (a_n)_{n\in\mathbb{N}}$ et $B = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$.

- On définit $C = A + B$ comme le polynôme dont les coefficients sont définis par
$$\forall n \in \mathbb{N}, \quad c_n = a_n + b_n \ .$$
- On définit $D = A \cdot B$ comme le polynôme dont les coefficients sont définis par
$$\forall n \in \mathbb{N}, \quad d_n = \sum_{k=0}^{n} a_k b_{n-k} \ .$$
- Soit $\lambda \in \mathbb{K}$. On définit le polynôme $P = \lambda A$ comme le polynôme dont les coefficients sont définis par
$$\forall n \in \mathbb{N}, p_n = \lambda a_n \ .$$

On montre (ou vous montrez) que $\mathbb{K}[X]$ est un sous-anneau abélien et un sous espace vectoriel de $\mathbb{K}^{\mathbb{N}}$. On dit que $\mathbb{K}[X]$ est une *algèbre*.

**Définition 4 : Introduction de $X$ et autre écriture**

On appelle indéterminée le polynôme $X = (0, 1, 0, 0, 0, 0, 0, \dots)$ Ainsi, si $P$ est un polynôme, il peut s'écrire

$$\begin{aligned} P =& (a_0, a_1, a_2, \dots, a_p, 0, \dots) = a_0(1, 0, 0, 0, 0, 0 \dots) + a_1(0, 1, 0, 0, 0, 0, \dots) \dots + a_p(0, 0, 0, \dots, 1, 0 \dots) \\ =& a_0 + a_1 X + a_2 X^2 + \dots + a_p X^p \end{aligned}$$

**Vérification des notations**

En utilisant les règles de multiplication sur notre anneau, $X^2 = X \cdot X = (0 \cdot 0, 0 \cdot 1 + 1 \cdot 0, 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0, 0 \dots) = (0, 0, 1, 0, 0 \dots)$ .
De même, $X^3 = (0, 0, 0, 1, 0, 0, 0, 0 \dots)$ et ... $X^n = (0, \dots, 0, \underset{\substack{\uparrow \\ n-\text{ième}}}{1}, 0, 0, 0, 0 \dots)$.

A partir de maintenant, on écrira toujours les polynômes sous la forme

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

car la suite des $(a_k)$ est nulle à partir d'un certain rang.

⚠ Attention $X$ n'est pas un réel ! Malgré son écriture, un polynôme est une suite de coefficients.

**Exemple 2**

Pour tout $n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$. C'est appelé la *Formule de Vandermonde*
Pour le prouver, l'idée est d'utiliser la formule du binôme sur $(X+1)^{2n} = (X+1)^n (X+1)^n$. On obtient

$$\sum_{k=0}^{2n} \binom{2n}{k} X^k = \sum_{i=0}^{n} \binom{n}{i} X^i \times \sum_{j=0}^{n} \binom{n}{j} X^j \ .$$

On identifie alors les coefficients de $X^n$,

$$\binom{2n}{k} = \sum_{i=0}^{n} \binom{n}{i} \binom{n}{n-i} = \sum_{i=0}^{n} \binom{n}{i}^2 ,$$

par symétrie des coefficients binomiaux !

**Définition 5 : Composition**

Soit $P := \displaystyle\sum_{k=0}^{p} a_k X^k$ et $Q$ deux polynômes, tels que $Q$ n'est pas un polynôme constant. On définit

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

**Exemple 3**
Résolvons $P \circ P = P$ d'inconnue $P \in \mathbb{K}[X]$.
Par application directe des définitions,

$$\sum_{k=0}^{p} a_k X^k = \sum_{k=0}^{p} a_k \left( \sum_{k=0}^{p} a_k X^k \right)^k \ .$$

Si $p > 1$, on obtient un coefficient non nul à $X^{p+1}$ à droite, ce qui est absurde.
Si $p = 1$, on obtient $a_0 + a_1 X_k = a_0 + a_1 a_0 + a_1^2 X_k$. Donc $a_1 = 0$.
On a donc montré que $P$ est un polynôme constant. La synthèse est immédiate.

## 2 Degré

**Définition 6**

On ajoute à $\mathbb{N}$ un élément noté $-\infty$ tel que $\forall n \in \mathbb{N} \cup \{-\infty\}, \quad n \geq -\infty \quad$ et $\quad \forall n \in \mathbb{N} \cup \{-\infty\}, \quad n + (-\infty) = -\infty$.

**Définition 7**

Soit $P$ un polynôme de coefficients $(a_n)_{n\in\mathbb{N}}$. On définit son degré, noté $\deg P$ comme

$$\deg P = \begin{cases} -\infty & \text{si } P \text{ est le polynôme nul,} \\ p \in \mathbb{N} & \text{si } a_p \neq 0, \text{ et } \quad \forall n > p, \ a_n = 0 \end{cases}$$

Le **coefficient dominant** de $P$ est le coefficient $a_p$ où $p = \deg(P)$.
Un polynôme est dit **unitaire** si son coefficient dominant vaut 1.

**Proposition 1 : Premières propriétés du degré**

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

(1) $\deg(P+Q) \leq \max\Big(\deg(P), \deg(Q)\Big)$ *, avec égalité si* $\deg P \neq \deg Q$,

(2) $\deg(PQ) = \deg(P) + \deg(Q)$*, et le coefficient dominant de* $PQ$ *est* $a_{\deg P}\, b_{\deg Q}$

(3) $\deg(\lambda P) = \begin{cases} -\infty \text{ si } \lambda = 0 \\ \deg(P) \text{ sinon} \end{cases}$ *, pout tout* $\lambda \in \mathbb{K}$.

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

*Preuve.* Le résultat est évident lorsque $P$ ou $Q$ est nul. Supposons-les donc tous deux non nuls et notons $m$ le degré de $P$ et $n$ celui de $Q$, ainsi que : $\quad P = (a_k)_{k\in\mathbb{N}}, \quad Q = (b_k)_{k\in\mathbb{N}} \quad$ et $\quad PQ = (c_k)_{k\in\mathbb{N}}$.

(1) Pour tout $k > \max\{m, n\}, \quad a_k + b_k = 0, \quad$ donc $\quad \deg(P+Q) \leqslant \max\{m, n\} = \max\{\deg(P), \deg(Q)\}$.

(2) On a d'abord $\quad c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} = \sum_{i=0}^{m-1} a_i \overbrace{b_{m+n-i}}^{=0} + a_m b_n + \sum_{i=m+1}^{m+n} \overbrace{a_i}^{=0} b_{m+n-i} = a_m b_n$, donc comme $a_m \neq 0$ et $b_n \neq 0$, forcément $\quad c_{m+n} \neq 0, \quad$ et donc $\quad \deg(PQ) \geqslant m+n$.
Inversement, pour tout $k > m+n, \quad c_k = \sum_{i=0}^{m} a_i \underbrace{b_{k-i}}_{\substack{=0 \text{ car:} \\ k-i>n}} + \sum_{i=m+1}^{k} \underbrace{a_i}_{=0} b_{k-i} = 0, \quad$ donc $\quad \deg(PQ) \leqslant m+n$.

(3) $\lambda$ ne change pas le degré de $P$.

(4) On suppose $Q$ non constant et on pose $\quad m = \deg(P)$.
Par produit, $\quad \deg\left(Q^k\right) = k \deg(Q)$ pour tout $k \in [\![0, m]\!]$, donc comme $\quad \deg(Q) \geqslant 1, \quad$ la suite $\left(\deg\left(Q^k\right)\right)_{0\leqslant k\leqslant m}$ est strictement croissante.
Finalement, par somme $\quad \deg(P \circ Q) = \deg\left(\sum_{k=0}^{m} a_k Q^k\right) \overset{a_m\neq 0}{=} \deg\left(Q^m\right) = m \deg(Q) = \deg(P) \times \deg(Q)$.

□

On peut obtenir cette conséquence de notre construction du degré.

**Proposition 2 : Intégrité**

*L'anneau* $\mathbb{K}[X]$ *est intègre.*

*Preuve.* Pour tous $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $\deg(P) + \deg(Q) = \deg(PQ) = -\infty$, donc nécessairement $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$, c'est à dire $P = 0$ ou $Q = 0$. □

# 3 Évaluation Polynomiale - Fonction polynomiale

**Définition 8 : Evaluation polynomiale**

Soit $P \in \mathbb{K}[X]$ un polynôme. On écrit $P$ avec ses coefficients

$$\exists p \in \mathbb{N},\ \exists (a_0, \dots, a_p) \in \mathbb{K}^{p+1}, \qquad P = \sum_{k=0}^{p} a_k X^k \ .$$

Pour tout $x \in K$, on appelle **évaluation polynomiale en $x$**, le scalaire $\sum_{k=0}^{p} a_k x^k$ de $\mathbb{K}$.

On note $\widetilde{P}(x)$ cet élément de $\mathbb{K}$.

**Sens de l'expression**

L'expression $\sum_{k=0}^{p} a_k x^k$ a bien un sens et est un élément de $\mathbb{K}$ car $\mathbb{K}$ est un corps donc est stable par addition et multiplication.
En fait, si $\mathbb{K}$ n'était qu'un anneau, on pourrait encore le définir.

**Définition 9 : Fonction polynomiale**

L'application $\widetilde{P} : \mathbb{K} \to \mathbb{K}$ qui à un élément $x$ associe $\widetilde{P}(x) = \sum_{k=0}^{p} a_k x^k$ est une fonction de $\mathbb{K}$ dans $\mathbb{K}$ appelée **fonction polynomiale associée au polynôme formel $P$**.

**Proposition 3 : Morphisme d'anneaux**

*Ainsi, l'application $P \mapsto \widetilde{P}$ est un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$.*

*Preuve.* À vous ! □

**En pratique**

Cela veut dire que, pour tous polynôme $P$ et $Q$, on a

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q} \qquad \text{et} \qquad \widetilde{P \cdot Q} = \widetilde{P} \cdot \widetilde{Q} \ .$$

Par abus de notation, on note parfois la fonction $\widetilde{P}$, tout simplement $P$.

# 4 Divisibilité dans $\mathbb{K}[X]$

## 4.1 Division euclidienne

**Théorème 1 : Division euclidienne**

*Soit $A, B$ deux polynômes de $\mathbb{K}[X]$ et $B \neq 0$. Alors il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que*

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

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

*Preuve.* L'existence se fait par récurrence sur le degré de $A$.
L'unicité s'obtient en égalant les degrés. □

**C'est la méthode du "bourrin" pour la décomposition en éléments simples !**

Vous avez déjà fait beaucoup de division euclidienne de polynôme, lors de la décomposition en éléments simples ! Souvenons nous de la première étape de la décomposition en élément simple. On essayait de réduire le degré du polynôme au numérateur jusqu'à ce que son dégré soit strictement inférieur à celui du polynôme au dénominateur. Par exemple,

$$\frac{2X^5-3X^4+3X^3+5X+1}{X^2+2} = 2X^3-3X^2-X+6+\frac{7X-11}{X^2+2}\ .$$

C'est en fait une division euclidienne ! Celle de $A=2X^5-3X^4+3X^3+5X+1$ par $B=X^2+2$ qui a pour quotient $Q=2X^3-3X^2-X+6$ et pour reste $R=7X-11$, que l'on écrit

$$2X^5-3X^4+3X^3+5X+1=\left(X^2+2\right)\cdot\left(2X^3-3X^2-X+6\right)+(7X-11)\ .$$

**Exemple 4**

Poser la division euclidienne de $A=X^5-X^4-3X+1$ par $B=X^3-1$.
Poser la division euclidienne de $A=X^4-2\cos(2\theta)X^2+1$ par $B=X^2-2\cos(\theta)X+1$.

## 4.2 Divisibilité

**Définition 10 : Diviseur, Multiple**

Soit $A, B$ deux polynômes de $\mathbb{K}[X]$.
On dit que $A$ **divise** $B$, et on écrit $A \mid B$, s'il existe un polynôme $Q \in \mathbb{K}[X]$, tel que $B=AQ$
On dit que $B$ est un **multiple** de $A$, si $A$ est un diviseur de $B$.
On dit que $A$ et $B$ sont deux polynômes **associés** si $A \mid B$ et $B \mid A$.

**Division euclidienne**

$A \mid B$ équivaut à dire que le reste de la division euclidienne de $B$ par $A$ (dans le cas où $A$ est non nul) est nul, comme pour les entiers !

**Exemple 5**

Soit $P \in \mathbb{K}[X]$. Montrons que $P(X)-X$ divise $P(P(X))-P(X)$. Notons $P=\sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$.
On a

$$P(P(X))-P(X)=\sum_{k=0}^{n} a_k\left([P(X)]^k-X^k\right)\ .$$

Or $a^k-b^k=(a-b)\sum_{\ell=0}^{k-1} a^\ell b^{k-1-\ell}$ .

$$P(P(X))-P(X)=\sum_{k=0}^{n} a_k\left([P(X)]-X\right)\sum_{\ell=0}^{k-1}[P(X)]^\ell X^{k-1-\ell}\ .$$

Donc $P(X)-X$ divise $[P(X)]^k-X^k$ car

**Proposition 4**

*Deux polynômes $A$ et $B$ sont associées si et seulement s'il existe un scalaire $u \in \mathbb{K}^*$ tel que $A=uB$.*

*Preuve.* Un argument sur les degrés montre que les polynômes diviseurs doivent être constants. □

**On fait la même chose qu'avec les nombres entiers**

Les polynômes associés à un polynôme jouent le même rôle que l'opposé pour un nombre entier. Les diviseurs de $n$ ou $-n$ sont les mêmes et les diviseurs de 2 polynômes associés sont aussi les mêmes.

**Proposition 5 : Propriétés de la relation de divisibilité**

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

1. *La relation de divisibilité $\mid$ est **réflexive et transitive** sur $\mathbb{K}[X]$,*
2. *La relation de divisibilité $\mid$ est **une relation d'ordre** sur l'ensemble des polynômes unitaires ou nuls de $\mathbb{K}[X]$.*
3. *Si $D \mid A$ et $D \mid B$, alors $D \mid (AU + BV)$, pour tous $U, V \in \mathbb{K}[X]$.*
4. *Si $A \mid B$ et $C \mid D$, alors $AC \mid BD$. En particulier, si $A \mid B$, alors $A^k \mid B^k$ pour tout $k \in \mathbb{N}$.*

*Preuve.* A vous ! □

## 4.3 Divisibilité par $(X - a)$ et racines d'un polynôme

**Proposition 6**

*Soit $P \in \mathbb{K}[X]$. Alors le reste de la division de $P$ par $(X - a)$ vaut $P(a)$.*

*Preuve.* On écrit la division euclidienne de $P$ par $B$, $P = (X - a) \cdot Q + R$. Ainsi, $R$ est un polynôme constant. De plus, en prenant les fonctions polynômes associées en $a$, on a $\widetilde{P}(a) = \widetilde{Q}(a)\widetilde{B}(a) + \widetilde{R}(a)$ donc $R = \widetilde{P}(a)$. □

**Algorithme d'Horner**

Les coefficients du quotient $Q$ de la division euclidienne sont donnés par l'**algorithme d'Horner**, qui donne aussi la valeur de $P(a)$. Posons $P = \sum_{k=0}^{n} b_k X^k$ et $Q = \sum_{k=0}^{n-1} q_k X^k$.
L'égalité $P = (X - a)Q + R$ devient

$$\sum_{k=0}^{n} b_k X^k = (X-a)\sum_{k=0}^{n-1} q_k X^k + R = \sum_{k=0}^{n-1} q_k X^{k+1} - \sum_{k=0}^{n-1} a q_k X^k + \widetilde{P}(a) = q_{n-1}X^n + \sum_{k=1}^{n-1} (q_{k-1} - a q_k) X^k + (-a q_0) + \widetilde{P}(a)$$

Deux polynômes sont égaux s'ils ont même coefficients, donc,

$$q_{n-1} = b_n \text{ et } \forall i \in \{1, \dots, n-1\}, q_{i-1} - a q_i = b_i \text{ et } \widetilde{P}(a) - a q_0 = b_0$$

On obtient ainsi l'algorithme d'Hörner permettant de calculer les coefficients $q_i$ et $\widetilde{P}(a)$ :

$$\begin{aligned} q_{n-1} &= b_n \\ q_{n-2} &= b_{n-1} + a b_n, \\ q_{n-3} &= b_{n-2} + a\,(q_{n-2}) \\ &\vdots \\ \widetilde{P}(a) &= b_0 + a q_0 \end{aligned}$$

permet de limiter le nombre de multiplication pour le calcul d'un polynôme en un point.

La méthode de Horner pour l'évaluation polynomiale est explicitement au programme. Elle permet de limiter le nombre de multiplications faites pour évaluer $\tilde{P}(a)$ .

**Définition 11**

On dit qu'un scalaire $a \in \mathbb{K}$ est **racine** (ou zéro) du polynôme $P \in \mathbb{K}[X]$ si $P(a) = 0$.

**Divisibilité et racine**

D'après le proposition précédente, $a$ est une racine de $P$ si et seulement si $(X-a) \mid P$.

**Exemple 6**
Factoriser $A = X^3 - 2X^2 + 1$

**Exemple 7**
Soient $t \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Quel est le reste de la division euclidienne dans $\mathbb{R}[X]$ de $(X\cos t + \sin t)^n$ par $X^2+1$ ?
Ecrivons la division euclidienne : $(X\cos t+\sin t)^n = \left(X^2+1\right)Q + R$ avec $\deg R < 2$, donc permet d'écrire $R = aX+b$ avec $a, b \in \mathbb{R}$.
Cette relation doit être aussi vraie dans $\mathbb{C}[X]$ et peut donc être évaluée en i. On obtient
$(\mathrm{i}\cos t + \sin t)^n = R(\mathrm{i}) = a\mathrm{i} + b$ or $(\mathrm{i}\cos t + \sin t)^n = \mathrm{e}^{\mathrm{i}(n\pi/2 - nt)}$ donc $a = \sin n(\pi/2-t)$ et $b = \cos n(\pi/2-t)$.

## 4.4 Divisibilité par $\prod_{i=1}^{n}(X-a_i)$, où les $a_i$ sont deux à deux distincts

**Proposition 7**
*Soit $P \in \mathbb{K}[X]$ et $a_1, \dots, a_n$ $n$ scalaires deux à deux distincts. Alors*

$$P \text{ est divisible par } \prod_{i=1}^{n}(X-a_i) \quad \text{si et seulement si} \quad \forall k \in \{1,\dots,n\},\ \widetilde{P}(a_k) = 0.$$

*Preuve.* Montrons par récurrence que pour tout $k \in [\![1, r]\!]$, $(X-a_1)^{m_1}\dots(X-a_k)^{m_k}$ divise $P$.
**Initialisation** $a_1$ est racine de $P$ de multiplicité $m_1$, donc $(X-a_1)^{m_1}$ divise $P$.
**Hérédité** Soit $k \in [\![1, r-1]\!]$. Faisons l'hypothèse que $(X-a_1)^{m_1}\dots(X-a_k)^{m_k}$ divise $P$.

Dans ces conditions, $P = (X-a_1)^{m_1}\dots(X-a_k)^{m_k} A$ pour un certain $A \in \mathbb{K}[X]$.

Si $\alpha$ désigne la multiplicité de $a_{k+1}$ dans $A$, $A = (X-a_{k+1})^{\alpha} B$ pour un certain $B \in \mathbb{K}[X]$ avec $B(a_{k+1}) \neq 0$.
En outre $(X-a_{k+1})^{\alpha}$ divise $A$, donc $P$, donc $\alpha \leqslant m_{k+1}$.

Enfin, $P = (X-a_{k+1})^{m_{k+1}} C$ pour un certain $C \in \mathbb{K}[X]$ avec $C(a_{k+1}) \neq 0$.

Il découle de ces trois points que $(X-a_1)^{m_1}\dots(X-a_k)^{m_k}(X-a_{k+1})^{\alpha} B = (X-a_{k+1})^{m_{k+1}} C$. Divisons cette égalité par $(X-a_{k+1})^{\alpha}$ grâce à l'intégrité de $\mathbb{K}[X]$, $(X-a_1)^{m_1}\dots(X-a_k)^{m_k} B = (X-a_{k+1})^{m_{k+1}-\alpha} C$. Le polynôme de gauche n'admet pas $a_{k+1}$ pour racine, donc celui de droite non plus, donc $\alpha = m_{k+1}$.
Donc $(X-a_{k+1})^{m_{k+1}}$ divise $A$, donc $(X-a_1)^{m_1}\dots(X-a_{k+1})^{m_{k+1}}$ divise $P$. □

**Corollaire 7.1**

1. *Un polynôme de degré $n$ a au plus $n$ racines distinctes.*
2. *Un polynôme de degré $\leq n$ qui s'annule en au moins $n+1$ points distincts est le polynôme nul.*
3. *Deux polynômes de degré $\leq n$ qui coincident en au moins $n+1$ points distincts sont égaux.*
4. *Si deux polynômes coincident en une infinité de points, alors ils sont égaux.*

On rappelle que 2 polynômes sont égaux s'ils ont les mêmes coefficients.

*Preuve.* (1) (2) Application directe de la proposition précédente.
(3) Soient $P, Q$ deux polynômes de degré inférieur ou égal à $n$, tels que $P(a_i) = Q(a_i)$, où $i \in [\![1, n]\!]$. Alors le polynôme $P-Q$ vérifie (2) et est donc nul, donc $P = Q$.
(4) Application de (3). □

**Divisibilité par $(X-a)^k$**

L'ensemble $\{k \in \mathbb{N} \mid (X-a)^k \text{ divise } P\}$ possède un plus grand élément $m$ appelé la multiplicité de $a$ dans $P$. On dit souvent pour résumer que $m$ est la plus grande puissance de $X-a$ qui divise $P$.
En particulier, dire que $a$ n'est pas racine de $P$, c'est dire que $a$ a pour multiplicité 0 dans $P$. Une racine est dite simple si elle est de multiplicité 1 , double si elle est de multiplicité 2 , etc.

Plus concrètement, $m$ est caractérisé par les deux propositions suivantes, équivalentes :

- $P$ est divisible par $(X-a)^m$ mais pas par $(X-a)^{m+1}$.
- Il existe $Q \in \mathbb{K}[X]$ pour lequel $P = (X-a)^m Q$ et $Q(a) \neq 0$.

**Exemple 8**
Déterminons les polynômes $P \in \mathbb{R}[X]$ tels que $P(k) = k^{1789}$ pour tout $k \in \mathbb{N}$.
Pour un tel polynôme $P$, le polynôme $P - X^{1789}$ admet une infinité de racines donc est nul: d'où $P = X^{1789}$ est la seule solution !

# 5 Dérivation et racines multiples

## 5.1 Dérivation formelle

**Définition 12 : Dérivation d'un polynôme formelle**
Soit $P = \sum_{k\geq 0} a_k X^k$ un polynôme
On définit le **polynôme dérivé** par la formule

$$P' = \sum_{k\geq 1} a_k k X^{k-1} = \sum_{j\geq 0} a_{j+1}(j+1)X^j$$

**C'est bien encore un polynôme ?**

Comme $P = \sum_{k\geq 0} a_k X^k$ est un polynôme, $(a_n)_{n\in\mathbb{N}}$ est une suite nulle à partir d'un certain rang.
Les coefficients de $P'$ étant bien une suite à support fini, $P'$ est bien un polynôme.

Ainsi, si le corps de référence est $\mathbb{R}$, on a $\widetilde{P'} = \widetilde{P}\,'$, c'est à dire que la fonction polynomiale de $P'$ est la dérivée de la fonction polynômiale de $P$. On peut définir par récurrence la **dérivée $m$ ième** par

$$P^{(0)} = P \text{ et } P^{(m+1)} = \left(P^{(m)}\right)'.$$

**Proposition 8 : Propriétés de la dérivation formelle**
*Soient $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.*

1. ***Linéarité*** $\forall \lambda, \mu \in \mathbb{K}, \quad (\lambda P + \mu Q)' = \lambda P' + \mu Q'$
2. ***Degré*** $\begin{cases} \deg\left(P^{(n)}\right) = \deg(P) - n & \text{si } \deg(P) \geqslant n \\ P^{(n)} = 0 & \text{sinon.} \end{cases}$
3. ***Produit*** $(PQ)' = P'Q + PQ'$. *Et on a encore la formule de Leibniz* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$
4. ***Composition*** $(P \circ Q)' = Q' \times P' \circ Q$.

**Cas particulier de $(X-a)^n$**

On a
$$((X-a)^n)^{(k)} = \begin{cases} n(n-1)(n-2)\dots(n-k+1)(X-a)^{n-k} & \text{si} \quad n \geq k \\ 0 & \text{si} \quad n < k \\ n! & \text{si} \quad n = k \end{cases}$$
Vous retrouvez vos ancien calculs de dérivée $n$-ièmes !

*Preuve.*

(1) Si $P = \sum_{k\geq 0} a_k X^k$ et $Q = \sum_{k\geq 0} b_k X^k$, alors $\lambda P + \mu Q = \sum_{k\geq 0} (\lambda a_k + \mu b_k) X^k$.
Par définition, on a $(\lambda P + \mu Q)' = \sum_{k\geq 1} (\lambda a_k + \mu b_k) kX^{k-1} = \lambda \sum_{k\geq 1} a_k kX^{k-1} + \mu \sum_{k\geq 1} b_k kX^{k-1}$ d'où le résultat.

(2) Immédiat avec la formule.

(3) Si $P = \sum_{k\geq 0} a_k X^k$ et $Q = \sum_{k\geq 0} b_k X^k$, alors

- $P'Q$ a pour coefficient $d_n = \sum_{k=0}^{n} (k+1)a_{k+1}b_{n-k} = \sum_{j=1}^{n+1} j\ a_j b_{n+1-j} = \sum_{j=0}^{n+1} j\ a_j b_{n+1-j}$
- $PQ'$ a pour coefficient $e_n = \sum_{k=0}^{n} a_k(n-k+1)b_{n-k+1}$.

Ainsi, $P'Q + PQ'$ a pour coefficient
$$e_n + d_n = (n+1)a_{n+1}b_0 + \sum_{k=0}^{n} a_k(k+1+n-k)b_{n+1-k} = (n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k} = (n+1)c_{n+1}\ ,$$
où $c_n$ sont les coefficients de $PQ$.

(4) - premier cas, si $P = X^k$. Montrons par récurrence sur $k$ que $\left(Q^k\right)' = kQ'Q^{k-1}$. Si $k = 1$, c'est la définition. Soit $k \in \mathbb{N}^*$. Supposons la propriété vraie au rang $k$. Alors $\left(Q^{k+1}\right)' = \left(Q^k Q\right)' = \left(Q^k\right)' Q + Q^k Q'$ par dérivation d'un produit. Puis par hypohtèse de récurrence : $\left(Q^{k+1}\right)' = kQ'Q^{k-1}Q + Q^k Q' = (k+1)Q'Q^k$ : conclusion de récurrence. Si $P = \sum_{k=0}^{n} a_k X^k$, alors $(P\circ Q)' = \sum_{k=0}^{n} a_k \left(Q^k\right)' = \sum_{k=1}^{n} a_k kQ'Q^{k-1} = Q'P'\circ Q$.

□

**Théorème 2 : Formule de Taylor**

*Soit $n$ un entier naturel, et $\mathbb{K}$ un sous-corps de $\mathbb{C}$.*
*Pour tout polynôme $P$ de degré inférieur à $n$, pour tout scalaire $a \in \mathbb{K}$,*
$$P(X) = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^k$$

*Preuve.* Soit $Q(X) = P(X+a)$. Alors $Q$ est de degré au plus $n$, avec $Q = \sum_{k=0}^{n} b_k X^k$. Alors $P(X) = Q(X-a)\dots$ puis on dérive $j$ fois et on égalise en $a$. □

## 5.2 Ordre de multiplicité d'une racine

**Définition 13**

On dit que $a \in \mathbb{K}$ est **racine d'ordre $\alpha \in \mathbb{N}$** d'un polynôme $P \in \mathbb{K}[X]\backslash\{0\}$, si
$$(X-a)^\alpha \mid P \qquad \text{et} \qquad (X-a)^{\alpha+1} \nmid P$$

**Proposition 9 : Caractérisations d'une racine multiple**

*Supposons $\mathbb{K} \subset \mathbb{C}$. Dire que $a$ est racine d'ordre $\alpha > 1$ d'un polynôme non nul $P$ est équivalent à dire*

- $\exists Q \in \mathbb{K}[X], \quad P(X) = (X-a)^\alpha Q(X) \quad ET \quad \widetilde{Q}(a) \neq 0$
- $P(a) = 0$ *et* $a$ *est racine d'ordre* $\alpha - 1$ *de* $P'$
- $a$ *est racine d'ordre* $\alpha$ *de* $P \iff \begin{cases} \widetilde{P}(a) = 0 = \widetilde{P}'(a) = \widetilde{P}''(a) = \ldots = \widetilde{P}^{(\alpha-1)}(a) = 0 \\ \text{ET } \widetilde{P}^{(\alpha)}(a) \neq 0 \end{cases}$

*Preuve.*

- Sens direct par récurrence sur $\alpha$. Initialisation : cas $\alpha = 1$, on utilise la première caractérisation pour avoir $\widetilde{P}(a) = 0$ et $\widetilde{P}'(a) \neq 0$.
  Soit $\alpha \in \mathbb{N}^*$ fixé. On suppose l'implication vraie pour tout polynôme $P$ et toute racine $a$ d'ordre $\alpha$. Soit $P$ un polynôme tel que $a$ soit racine d'ordre $\alpha + 1$ de $P$. Par la première caractérisation, $a$ est racine d'ordre $\alpha$ de $P'$ et $\widetilde{P}(a) = 0$.
  On applique alors l'hypothèse de récurrence au polynôme $P'$ : $\widetilde{P'}(a) = 0 = \widetilde{P}'(a) = \widetilde{P}''(a) = \ldots = \widetilde{P}^{(\alpha-1)}(a) = 0$ et $\widetilde{P}^{(\alpha)}(a) \neq 0$ d'où le résultat.
- Sens réciproque : On applique la formule de Taylor ; si $n = \deg(P)$ :

$$P = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!}(X-a)^k = \sum_{k=\alpha}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!}(X-a)^k = (X-a)^\alpha \underbrace{\left( \sum_{k=\alpha}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!}(X-a)^{k-\alpha} \right)}_{\text{polynôme } Q}$$

et $\widetilde{Q}(a) = \frac{\widetilde{P}^{(\alpha)}(a)}{\alpha!} \neq 0$ par hypothèse.
Conclusion : $a$ est racine d'ordre $\alpha$ de $P$. □

# 6 Relation coefficients-racines

## 6.1 Fonctions symétriques élémentaires

**Définition 14**

Soit $n \in \mathbb{N}^*$. On appelle fonctions symétriques élémentaires les $n$ fonctions des $n$ variables $x_1, \ldots, x_n$,

$$\begin{aligned}
\sigma_1 : &\quad (x_1, x_2, \ldots, x_n) \mapsto \sum_{i=1}^{n} x_i \\
\sigma_2 : &\quad (x_1, x_2, \ldots, x_n) \mapsto \sum_{1 \leq i < j \leq n} x_i x_j \\
&\quad \vdots \\
\sigma_k : &\quad (x_1, x_2, \ldots, x_n) \mapsto \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} \prod_{j=1}^{k} x_{i_j} = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k} \\
\sigma_n : &\quad (x_1, x_2, \ldots, x_n) \mapsto \prod_{i=1}^{n} x_i
\end{aligned}$$

**Exemple 9**

Si $n = 4$, alors
$\sigma_1 = x_1 + x_2 + x_3 + x_4$,
$\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$,
$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$,
$\sigma_4 = x_1x_2x_3x_4$.

## 6.2 Développement de $\prod_{k=1}^{n}(X-x_k)$

On pourrait le montrer par récurrence ; on se contentera de l'intuition. Soit $P=\prod_{k=1}^{n}(X-x_k)$. Lorsque l'on développe $P$, on obtient $2^n$ termes, obtenus faisant le produit de $n$ termes $b_1b_2\dots b_n$, où $b_i$ vaut soit $X$ soit $-x_i$ (distributivité de la multiplication).

- Alors le terme de plus haut degré de $P$ est obtenu en ne prenant que les termes $b_i$ valant $X$ : on obtient $X^n$.
- Le terme de degré $n-1$ est obtenu en prenant dans le produit $b_1b_2\dots b_n$ le terme $Xn-1$ fois ; et le dernier terme valant $-x_j$. Il y a $n$ termes ainsi, pour $j$ valant $1,2,\dots n$.
  Ainsi, ce terme vaut : $(-x_1-x_2-\dots-x_n)\,X^{n-1}=-\sigma_1X^{n-1}$
- De même, le terme en $X^{n-2}$ est la somme des termes obtenus en prenant $n-2$ fois le termes $X$ et il reste le produit $(-a_i)\,(-a_j)$, pour $i<j$. Ainsi ce terme vaut: $(x_1x_2+\dots x_1x_n+\dots x_{n-1}x_n)\,X^{n-2}=\sigma_2X^{n-2}$
- De même, Le terme en $X^{n-k}$ a pour coefficient la somme des possibilité des produits de $k$ éléments de $(-x_i)_{i\in[\![1,n]\!]}$, soit : $(-1)^k\sigma_kX^{n-k}$

**Proposition 10**

*On a l'égalité suivante, en posant $\sigma_0=1$*

$$\prod_{k=1}^{n}(X-x_k)=X^n-\sigma_1X^{n-1}+\dots+(-1)^n\sigma_n=\sum_{k=0}^{n}(-1)^k\sigma_kX^{n-k}=\sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}X^k$$

## 6.3 Polynômes scindés

**Définition 15**

On dit qu'un polynôme est **scindé** sur $\mathbb{K}$
s'il s'écrit sous la forme suivante

$$\exists\lambda\in\mathbb{K}^*,\exists\,(x_1,\dots,x_n)\in\mathbb{K}^n,P=\lambda\prod_{k=1}^{n}(X-x_k)$$

⚠ Attention La précision "*scindé sur* $\mathbb{K}$" n'est pas superflue, car un polynôme peut avoir des racines complexes, mais aucune réelle. Le polynôme $X^2+1=(X+i)(X-i)$ est ainsi scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

⚠ Attention Les $(x_i)$ ne sont pas forcément deux à deux distincts. La définition d'un polynôme scindé est que le polynôme a autant de racines comptées avec multiplicité que son degré. Cela ne signifie pas que les racines sont simples. En fait, $\lambda$ est le coefficient dominant de $P$.

**Exemple 10**

$6X^3-3X+2$ est scindé sur $\mathbb{R}$
$X^2+1$ n'est pas scindé sur $\mathbb{R}$ mais est scindé sur $\mathbb{C}$.

**Exemple 11**

Montrons que si $P$ est scindé, alors $P'$ est aussi scindé.
Posons $n=\deg P\geq 2, a_1<a_2<\dots<a_p$ les racines réelles distinctes de $P$ et $\alpha_1,\alpha_2,\dots,\alpha_p$ leurs ordres respectifs. On a $\alpha_1+\alpha_2+\dots+\alpha_p=n$ car $P$ est supposé scindé. En appliquant le théorème de Rolle à $x\mapsto\tilde{P}(x)$ sur chaque $[a_i;a_{i+1}\,[$ on justifie l'existence de racines distinctes $b_1,b_2,\dots,b_{p-1}$ disposée de sorte que

$$a_1 < b_1 < a_2 < b_2 < \ldots < b_{p-1} < a_p$$

Comme les $a_1, a_2, \ldots, a_p$ sont des racines d'ordres $\alpha_1 - 1, \alpha_2 - 1, \ldots, \alpha_p - 1$ de $P'$ et que $b_1, b_2, \ldots, b_{p-1}$ sont des racines au moins simples de $P'$, on vient de déterminer $(n-1) = \deg P'$ racines de $P'$ comptées avec leur multiplicité. Finalement $P'$ est scindé.

**Théorème 3 : Relations coefficents-racines**

*Soit $P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{k=1}^{n} (X - x_k)$ un polynôme de degré $n$, de coefficients $(a_k)_{k\in\mathbb{N}}$, scindé sur $\mathbb{K}$, dont les $n$ racines écrites avec multiplicité sont $(x_1, x_2 \ldots, x_n)$. Alors on a les relations coefficients racines*

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots x_n &&= \frac{-a_{n-1}}{a_n} \\
\sigma_2 &= \sum_{1\le i<j\le n} x_i x_j &&= \frac{a_{n-2}}{a_n} \\
&\vdots \\
\sigma_k &= \sum_{1\le i_1<i_2<\ldots<i_k\le n} \prod_{j=1}^{k} x_{i_j} &&= \frac{(-1)^k a_{n-k}}{a_n} \\
&\vdots \\
\sigma_n &= x_1 \cdot x_2 \cdot \ldots x_n &&= \frac{(-1)^n a_0}{a_n}
\end{aligned}$$

**En pratique**

Les plus utiles sont celle de $\sigma_1$ et $\sigma_n$.

*Preuve.* D'après la partie précédente,

$$P = a_n \prod_{k=1}^{n} (X - x_k) = a_n \left( \sum_{k=0}^{n} (-1)^{n-k} \sigma_{n-k} X^k \right) .$$

Par unicité des coefficients d'un polynômes, pour tout $k \in [\![0, n]\!]$, $a_k = a_n (-1)^{n-k} \sigma_{n-k}$. □

**Exemple 12**

On retrouve le cas des équations de degré 2.

**Exemple 13**

Résoudre le système $\begin{cases} x + y + z = 1 \\ xy + xz + yz = 1 \\ xyz = 1 \end{cases}$

**Exemple 14**

On considère l'équation $(E) : x^4 + 12x - 5 = 0$.
Résolvons $(E)$ dans $\mathbb{C}$ sachant que la somme de deux des solutions vaut 2 .
Comme le coefficient en $X^3$ est nul, la somme des quatre racines vaut 0 ; si la somme de deux racines vaut 2 , la somme des deux autres vaut -2 et le polynôme s'écrit sous la forme

$$X^4 + 12X - 5 = \left(X^2 + 2X + a\right)\left(X^2 - 2X + b\right)$$

Par identification, on trouve $a = -1$ et $b = 5$. Il reste ensuite deux équations du second degré à résoudre.
On trouve finalement quatre racines distinctes : $-1 + \sqrt{2}, -1 - \sqrt{2}, 1 + 2i$ et $1 - 2i$.

# 7 Polynômes d'interpolation de Lagrange

Le but est d'approcher une fonction par un polynôme en ne connaissant que certains points de la fonction. En fait, on chercher un polynôme qui passe par les mêmes $n$ points que la fonction.

**Théorème 4 : Polynômes de Lagrange**

*Soit $n \in \mathbb{N}^*$, et $n$ éléments $x_1, \dots, x_n \in \mathbb{K}$ distincts. Alors*

$$\forall y_1, y_2, \dots, y_n \in \mathbb{K}, \quad \exists! P \in \mathbb{K}_{n-1}[X], \quad \forall i \in [\![1, n]\!], \quad \widetilde{P}(x_i) = y_i \quad \text{et } \deg(P) \leq n-1 \ .$$

*Preuve.* **Unicité** Si $P$ et $Q$ sont deux polynômes solution, alors $P - Q$ admet $n$ racines deux à deux distinctes et est de degré au plus $n-1$, donc est le polynôme nul.
**Existence** On pose pour tout $j \in [\![1, n]\!]$, le polynôme :

$$L_j = \prod_{\substack{k=1 \\ k \neq j}}^{n} \left( \frac{X - x_k}{x_j - x_k} \right)$$

C'est un polynôme de degré $n-1$ (Pour comprendre les polynômes, prendre $n = 3$, et écrivez $L_1, L_2, L_3$.)
Alors pour tout $i \in [\![1, n]\!]$, $\widetilde{L_j}(x_i) = \delta_{i,j}$.
On pose $P = \sum_{j=1}^{n} y_j L_j$. Alors $\forall i \in [\![1, n]\!], \widetilde{P}(x_i) = y_i$ et son degré est inférieur à $n-1$ □

**Vocabulaire** Ces polynômes sont appelés les **polynômes de Lagrange**, et sont trop importants pour ne pas être très bien connus !

**Exemple 15**

Notons $f$ la fonction $x \longmapsto \sin \frac{x\pi}{2}$ sur$[0, 4]$, pour laquelle $f(0) = f(2) = f(4) = 0$, $f(1) = 1$ et $f(3) = -1$. Notons ensuite $L_0, \dots, L_4$ les cinq polynômes de Lagrange de $0, \dots, 4$.
Le polynôme d'interpolation de Lagrange de $f$ aux points $0, \dots, 4$ est alors en vertu du théorème précédent le polynôme $\sum_{i=0}^{4} f(i) L_i = L_1 - L_3$. Or

$$L_1 = -\frac{X(X-2)(X-3)(X-4)}{6} \quad \text{et} \quad L_3 = -\frac{X(X-1)(X-2)(X-4)}{6}$$
$$\text{donc } L_1 - L_3 = -\frac{X(X-2)(X-3)(X-4)}{6} + \frac{X(X-1)(X-2)(X-4)}{6} = \frac{X(X-2)(X-4)}{3}$$

**Corollaire 4.1**

*Soit $n \in \mathbb{N}^*$, et $n$ éléments $x_1, \dots, x_n \in \mathbb{K}$ distincts. On se fixe $y_1, y_2, \dots, y_n \in \mathbb{K}$.*
*Soit $P_0$ le polynôme de Lagrange définit comme dans le théorème précédent, tel que $\forall i \in [\![1, n]\!]$, $\widetilde{P_0}(x_i) = y_i$.*
*Alors l'ensemble $S$ des polynômes $P$ de $\mathbb{K}[X]$ vérifiant, $\forall i \in [\![1, n]\!], \widetilde{P}(x_i) = y_i$ est*

$$S = \left\{ P_0 + \left( \prod_{k=1}^{n} (X - x_k) \right) Q \;\middle|\; Q \in \mathbb{K}[X] \right\} \ .$$

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

On a donné l'écriture d'un polynôme scindé lorsque l'on a des informations sur ses racines et leurs ordres de multiplicité. Se pose maintenant le problème de l'existence de ces racines.

**Théorème 5 : Théorème de d'Alembert-Gauss**

*Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.*

*Preuve.* [**Hors-programme**] Soit $A$ un polynôme à coefficients complexes de degré $p \geqslant 1$. Pour montrer que $A$ possède une racine complexe, considérons la borne inférieure $\alpha = \inf_{z\in\mathbb{C}} |A(z)|$, qui existe puisque $\{|A(z)| \mid z \in \mathbb{C}\}$ est une partie non vide de $\mathbb{R}_+$, et montrons que cette borne inférieure est atteinte, puis qu'elle est nulle.

Notons $A = \sum_{k=0}^{p} a_k X^k$, avec $a_p \neq 0$. Pour $|z| = r$, on a, par inégalité triangulaire

$$|A(z)| \geqslant |a_p z^p| - \left|\sum_{k=0}^{p-1} a_k z^k\right| \geqslant |a_p|\, r^p - \sum_{k=0}^{p-1} |a_k|\, r^k$$

Ce minorant définit une fonction réelle polynomiale de $r$ équivalente à $r \mapsto |a_p|\, r^p$ et qui tend donc vers $+\infty$ quand $r$ tend vers $+\infty$. Elle est donc plus grande que $\alpha + 1$ au voisinage de $+\infty$, ce qui prouve qu'il existe un disque $D$ centré en 0, en dehors duquel on a $|A(z)| \geqslant \alpha + 1$. Puisque $\alpha = \inf_{z\in\mathbf{C}} |A(z)|$, on peut trouver une suite de nombres complexes $(u_n)_{n\in\mathbb{N}}$ telle que $\lim_{n\to+\infty} |A(u_n)| = \alpha$.

D'après ce qui précède, cette suite est dans le disque $D$ à partir d'un certain rang et est donc bornée. D'après le théorème de Bolzano-Weierstrass, on peut donc en extraire une sous-suite $\left(u_{\varphi(n)}\right)_{n\in\mathbb{N}}$ convergeant vers un complexe $z_0$. Comme

$$A\left(u_{\varphi(n)}\right) = \sum_{k=0}^{p} a_k u_{\psi(n)}^k$$

on en déduit $\lim_{n\to+\infty} A\left(u_{\varphi(n)}\right) = A(z_0)$, ce qui donne

$$\alpha = \lim_{n\to+\infty} \left|A\left(u_{\psi(n)}\right)\right| = |A(z_0)|$$

Montrons par l'absurde que $A(z_0) = 0$. On suppose $A(z_0) \neq 0$. Quitte à considérer le polynôme $\frac{A(z_0+X)}{A(z_0)}$, on peut supposer $z_0 = 0$ et $A(z_0) = A(0) = 1$. Le polynôme non constant $A$ s'écrit donc

$$A = 1 - a_q X^q + \sum_{k=q+1}^{p} a_k X^k \quad \text{avec} \quad a_q \neq 0 \quad \text{et} \quad 1 \leqslant q \leqslant p$$

Posons $a_q = \rho e^{-i\theta}$ avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$. Pour $z = re^{i\theta/q}$, avec $r > 0$, on a

$$A(z) = 1 - \rho r^q + \sum_{k=q+1}^{p} a_k r^k e^{ik\theta/q} \quad \text{et donc} \quad |A(z)| \leqslant |1 - \rho r^q| + \sum_{k=q+1}^{p} |a_k|\, r^k$$

Si l'on suppose $r \leqslant (1/\rho)^{1/q}$, on a $|1 - \rho r^q| = 1 - \rho r^q$ et alors

$$|A(z)| - 1 \leqslant -\rho r^q + \sum_{k=q+1}^{p} |a_k|\, r^k$$

Ce majorant définissant une fonction polynomiale de $r$, équivalente en 0 à $r \mapsto -\rho r^q$, il est strictement négatif au voisinage de $0^+$. Par conséquent, pour $r > 0$ assez petit et $z = re^{i\theta/q}$, on a $|A(z)| < 1 = \alpha$, ce qui est contradictoire. □

**Proposition 11 : Factorisation des polynômes à coefficients complexes**

*Soit $P$ un polynôme non nul à coefficients complexes, de coefficient dominant $\lambda \in \mathbb{C}$. Soit $\alpha_1, \ldots, \alpha_p$ les racines complexes distinctes de $P$ et $r_1, \ldots, r_p$ leurs ordres de multiplicité respectifs. On a alors*

$$A = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{r_k}$$

*Autrement dit,* *Tout polynôme non nul de $\mathbb{C}[X]$ est scindé.*

*Preuve.* Notons $\alpha_1, \ldots, \alpha_p$ les racines (complexes) distinctes de $A$ et $r_1, \ldots, r_p$ leurs ordres respectifs. Il existe un polynôme $Q$ tel que $A = Q \prod_{k=1}^{p} (X - \alpha_k)^{r_k}$.

Si $Q$ est de degré non nul, il admet au moins une racine complexe qui est alors aussi une racine de $A$. Il existe donc $j \in [\![1,p]\!]$ tel que $\alpha_j$ soit aussi racine de $Q$. On a alors $(X-\alpha_j)^{r_j+1}$ divise $A$, ce qui contredit la définition de $r_j$. Par suite, $Q$ est une constante $\lambda$ et l'on a alors le résultat. □

⚠ Attention Ce résultat est évidemment faux dans $\mathbb{R}[X]$, puisque, par exemple, $X^2+1$ n'est pas scindé sur $\mathbb{R}$. Cependant, On peut toujours voir un polynôme à coefficients réels comme un polynôme à coefficients complexes. Donc ce polynôme est scindé sur $\mathbb{C}$.

**Corollaire 11.1**

*Soit $P = \lambda \prod_{k=1}^{p} (X-\alpha_k)^{r_k}$ un polynôme non nul de $\mathbb{C}[X]$ de coefficient dominant $\lambda$, et de racines $\alpha_1, \dots, \alpha_p$, d'ordres de multiplicité respectifs $r_1, \dots, r_p$.*

*Les diviseurs de $A$ sont exactement les polynômes $\mu \prod_{k=1}^{p} (X-\alpha_k)^{s_k}$ où $\mu \in \mathbb{C}^*$ et, pour tout $k \in [\![1,p]\!]$, $s_k \in [\![0, r_k]\!]$.*

*Preuve.* C'est clair que ces polynômes sont des diviseurs de $A$. Montrons que tout diviseur $B$ de $A$ est cette forme. On a alors $A = BQ$, avec $Q \in \mathbb{C}[X]$. Les racines de $B$ sont alors les racines de $A$ et donc $B$ s'écrit comme dans le corollaire. □

**Proposition 12 : Factorisation des polynômes à coefficients réels**

*Tout polynôme non nul $P$ de $\mathbb{R}[X]$ peut s'écrire sous la forme*

$$P = \lambda \prod_{j=1}^{p} (X-\alpha_j)^{r_j} \prod_{k=1}^{q} \left(X^2+\beta_k X+\gamma_k\right)^{s_k}$$

*où $p$ et $q$ sont deux entiers naturels, $\lambda$ un réel non nul et*

- *pour tout $j \in [\![1,p]\!]$, $r_j$ est un entier naturel non nul et $\alpha_j$ est un nombre réel,*
- *pour tout $k \in [\![1,q]\!]$, $s_k$ est un entier naturel non nul et $\beta_k$ et $\gamma_k$ sont des nombres réels vérifiant $\beta_k^2 - 4\gamma_k < 0$.*

**Exemple 16**

Pour factoriser $X^4+1$ dans $\mathbb{R}[X]$, on peut utiliser les racines quatrièmes de -1

$$\begin{aligned} X^4+1 &= \left(X-e^{i\pi/4}\right)\left(X-e^{-i\pi/4}\right)\left(X-e^{3i\pi/4}\right)\left(X-e^{-3i\pi/4}\right) \\ &= \left(X^2-2\cos\frac{\pi}{4}X+1\right)\left(X^2-2\cos\frac{3\pi}{4}X+1\right) \\ &= \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right) \end{aligned}$$

Une autre méthode consiste plus simplement à écrire :

$$X^4+1 = \left(X^2+1\right)^2 - 2X^2 = \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$$

Comme $X^4+1$ n'a pas de racines réelles, ces deux polynômes du second degré n'ont pas de racines réelles, et donc leur discriminant est strictement négatif.

# 9 Arithmétique dans $\mathbb{K}[X]$

**Notation** L'ensemble des diviseurs d'un polynôme $A$ est noté $\mathrm{div}(A)$.

## 9.1 Plus grands diviseurs communs

**Proposition 13 : Division euclidienne**

*Soit $A, B, Q$ et $R$ quatre polynômes tels que $A = BQ + R$. Alors*

$$\mathrm{div}(A) \cap \mathrm{div}(B) = \mathrm{div}(B) \cap \mathrm{div}(R)$$

*Preuve.* En effet, la relation $A = BQ + R$ montre que tout diviseur commun à $B$ et $R$ est aussi un diviseur de $A$, et aussi de $B$ ! L'inclusion réciproque provient de même de la relation $R = A - BQ$. □

**Définition 16 : Plus grands diviseurs communs**

Soit $A$ et $B$ deux polynômes, l'un au moins étant non nul. Tout diviseur commun à $A$ et $B$ de degré maximal est appelé le PGCD de $A$ et $B$.

**Pourquoi il existe un PGCD ?**

Soit $A$ et $B$ deux polynômes, l'un au moins étant non nul.
L'ensemble des diviseurs communs à $A$ et $B$ est une partie de $\mathbb{K}[X]$ non vide (puisqu'elle contient 1) et ne contenant pas le polynôme nul, puisque $A$ ou $B$ est non nul.
Donc $\mathrm{div}(A) \cap \mathrm{div}(B)$ est donc une partie de $\mathbb{N}$ non vide, majorée par $\deg A$ ou $\deg B$. Elle possède donc un plus grand élément $r$ dans $\mathbb{N}$.
Donc il existe un polynôme $D$ de degré $r$ tel que $D$ soit un diviseur commun à $A$ et $B$.

**Proposition 14**

*Soit $A, B \in \mathbb{K}[X]$, avec $A \neq 0$. Soit $D$ un PGCD de $A$ et $B$. On a alors $\mathrm{div}(D) = \mathrm{div}(A) \cap \mathrm{div}(B)$, c'est-à-dire*

$$\forall P \in \mathbb{K}[X] \quad (P \mid A \quad \text{et} \quad P \mid B) \iff P \mid D.$$

*Preuve.* On démontre par récurrence sur $n$ la propriété

"Si $A, B \in \mathbb{K}[X]$, avec $A \neq 0$, vérifiant $\min(\deg A, \deg B) < n$, et si $D$ en est un PGCD, alors $\mathrm{div}(A) \cap \mathrm{div}(B) = \mathrm{div}(D)$ "

en utilisant la division euclidienne. □

**Théorème 6 : Plus grand diviseur commun**

*Soit $A, B \in \mathbb{K}[X]$, avec $A \neq 0$. Il existe un unique polynôme $D$ unitaire qui soit un PGCD de $A$ et $B$.*
*On l'appelle* **le** *PGCD de $A$ et $B$, et on le note $A \wedge B$.*

*Preuve.* Deux PGCDs $D_1$ et $D_2$ de $A$ et $B$ vérifient $\mathrm{div}(D_1) = \mathrm{div}(D_2) = \mathrm{div}(A) \cap \mathrm{div}(B)$ donc $D_1$ et $D_2$ ont les mêmes diviseurs, donc ils sont associés, car non nuls.
De plus, deux polynômes unitaires et associés sont égaux, donc $A \wedge B$ est unique, obtenu en divisant n'importe quel PGCD par son coefficient dominant. □

**Quelques propriétés en pratique**

- Le polynôme $A \wedge B$ est donc l'unique polynôme $D$ unitaire tel que

$$\forall P \in \mathbb{K}[X] \quad (P \mid A \quad \text{et} \quad P \mid B) \iff P \mid D$$

- Si $A$ et $B$ sont dans $\mathbb{R}[X]$, on déduit de l'unicité du quotient et du reste de la division euclidienne que le PGCD de $A$ et $B$ dans $\mathbb{R}[X]$ est égal au PGCD de $A$ et $B$ dans $\mathbb{C}[X]$. Comme pour les entiers, on a évidemment $A \wedge B = B \wedge A$
- Comme pour les entiers, on a évidemment $A \wedge B = B \wedge A$.
- Comme deux polynômes associés ont exactement les mêmes diviseurs, on peut remplacer $A$ et $B$ par les polynômes unitaires qui leur sont associés avant de calculer leur PGCD.

## 9.2 Algorithme d'Euclide et coefficients de Bézout

La Proposition 13 montre que si $R$ est le reste de la division euclidienne de $A$ par $B$, alors $A \wedge B = B \wedge R$. Comme le degré de $R$ est strictement inférieur à celui de $B$, cela simplifie le calcul à effectuer, et l'on peut répéter le procédé tant que $R \neq 0$. C'est le même principe de l'algorithme d'Euclide des entiers !

**Exemple 17**
Calculons le PGCD de $A = X^4 + X^3 - 5X^2 - 5X + 6$ et $B = X^3 - 6X + 4$. On effectuera les divisions euclidiennes à gauche, et l'on en tirera à droite les conséquences sur $A \wedge B$. On a

$$\begin{aligned} A &= B(X+1) + X^2 - 3X + 2 \\ B &= \left(X^2 - 3X + 2\right)(X+3) + X - 2 \\ X^2 - 3X + 2 &= (X-2)(X-1) + 0. \end{aligned}$$

Donc

$$A \wedge B = B \wedge \left(X^2 - 3X + 2\right) = \left(X^2 - 3X + 2\right) \wedge (X-2) = (X-2) \wedge 0 = X - 2\ .$$

Ainsi, $A \wedge B = X - 2$. On voit que, concrètement, le dernier reste non nul dans notre suite de divisions euclidiennes est un PGCD de $A$ et $B$, si bien que la seule colonne de gauche suffisait dans notre calcul.

**Proposition 15 : Coefficients de Bézout**
*Soit $A, B \in \mathbb{K}[X]$, avec $A \neq 0$. Il existe deux polynômes $U$ et $V$ tels que $AU + BV = A \wedge B$.*
*Un tel couple $(U, V)$ est un couple de* ***coefficients de Bézout*** *de $A$ et $B$.*

*Preuve.* On montre par récurrence sur $n \in \mathbb{N}$, l'assertion

"Si $A, B \in \mathbb{K}[X]$, avec $A \neq 0$, vérifiant $\min(\deg A, \deg B) < n$, alors $\exists U, V$ tels que $AU + BV = A \wedge B$."

□

⚠ Attention L'existence de deux polynômes $U$ et $V$ tels que $AU + BV = D$, n'implique pas que $D = A \wedge B$ mais seulement que $A \wedge B \mid D$.

**Infinité du nombre de couples de coefficients de Bézout et Algorithme d'Euclide étendu**

- Dans la proposition précédente, il n'y a pas unicité du couple $(U, V)$, puisque si $(U_0, V_0)$ est un couple de coefficients de Bézout de $A$ et $B$, alors il en est de même du couple $(U_0 + QB, V_0 - QA)$ pour tout polynôme $Q$.
- Comme dans le cas des entiers, le calcul du PGCD est fondé sur l'algorithme d'Euclide. En remontant l'algorithme on peut alors trouver un couple de coefficients de Bézout. On parle d'algorithme d'Euclide étendu.

**Exemple 18**
On reprend l'exemple de $A = X^4 + X^3 - 5X^2 - 5X + 6$ et $B = X^3 - 6X + 4$. On avait obtenu :

$$\begin{aligned} A &= B(X+1) + X^2 - 3X + 2 \\ B &= \left(X^2 - 3X + 2\right)(X+3) + X - 2 \\ X^2 - 3X + 2 &= (X-2)(X-1) + 0, \end{aligned}$$

ce qui donnait $A \wedge B = B \wedge \left(X^2 - 3X + 2\right) = \left(X^2 - 3X + 2\right) \wedge (X-2) = (X-2) \wedge 0 = X - 2$. On trouve immédiatement des coefficients de Bézout pour l'avant-dernier couple de polynômes en "renversant" la dernière division euclidienne qui ne tombait pas juste :

$$X - 2 = 1B - (X+3)\left(X^2 - 3X + 2\right)$$

On remonte ensuite les calculs, chaque division euclidienne $C = DQ + R$ permettant de remplacer $R$ par $C - DQ$, et d'obtenir des coefficients de Bézout pour $C$ et $D$ à partir de ceux pour $D$ et $R$. Dans notre exemple, la première division euclidienne donne $X^2 - 3X + 2 = A - (X+1)B$, d'où l'on tire

$$\begin{aligned} X - 2 &= 1B - (X+3)\left(X^2 - 3X + 2\right) \\ &= 1B - (X+3)(A - (X+1)B) \\ &= -(X+3)A + (1 + (X+3)(X+1))B \\ &= -(X+3)A + \left(X^2 + 4X + 4\right)B, \end{aligned}$$

ce qui donne des coefficients de Bézout pour $A$ et $B$.

## 9.3 Polynômes premiers entre eux

**Définition 17**

Deux polynômes $A$ et $B$ sont **premiers entre eux** s'ils vérifient l'une des deux propriétés équivalentes

1. $A$ et $B$ n'ont que les polynômes de degré 0 comme diviseurs communs,
2. $(A,B) \neq (0,0)$ et $A \wedge B = 1$.

On dit aussi que **$A$ est premier avec $B$.**

**Proposition 16 : Identité de Bézout**

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

$$A \text{ et } B \text{ sont premiers entre eux} \quad \text{si, et seulement si} \quad \exists U, V \in \mathbb{K}[X] \text{ tel que } AU + BV = 1.$$

*Preuve.* Découle de la proposition sur les coefficients de Bézout. □

**Proposition 17 : Propriétés**

*Soient $A, B, C, B_1, \dots, B_n \in \mathbb{K}[X]$.*

1. $\exists A_1, B_1 \in \mathbb{K}[X]$ *tels que* $A = DA_1$ *et* $B = DB_1$ *avec* $A_1 \wedge B_1 = 1$ .
2. *$A$ est premier avec $B_1 \cdots B_n$ si, et seulement si, $A$ est premier avec chacun des $B_i$.*
3. *Si $A$ est premier avec $B$, allors $\forall m, n \in \mathbb{N}$,* $A^m \wedge B^n = 1$
4. ***Lemme de Gauss*** *Si $A$ divise $BC$ et si $A$ est premier avec $B$, alors $A$ divise $C$.*

*Preuve.* On montre seulement le Lemme de Gauss.
Supposons $A \wedge B = 1$ et $A \mid BC$. D'après l'identité de Bézout, il existe des polynômes $U$ et $V$ tels que $AU + BV = 1$, ce qui implique $ACU + BCV = C$.
Comme $A$ divise $ACU$ et $BCV$, on a $A \mid ACU + BCV$ et donc $A \mid C$. □

**En pratique**

Pour utiliser des hypothèses sur le PGCD de deux polynômes $A$ et $B$, on utilise, comme pour l'arithmétique des entiers, cette propriété !

$$A \wedge B = D \iff \exists A_1, B_1 \in \mathbb{K}[X], \begin{cases} A_1 \wedge B_1 = 1 \\ A = A_1 D \\ B = B_1 D \end{cases}$$

**Proposition 18 : Primalité entre eux et racines communes**

*Soient $A, B \in \mathbb{C}[X]$, avec $A \neq 0$. Alors $A$ et $B$ sont premiers entre eux si, et seulement s'ils n'ont pas de racine commune.*

*Preuve.*

($\Rightarrow$) Si $A$ et $B$ possèdent une racine commune $z \in \mathbb{C}$, ils sont tous les deux divisibles par $X - z$ et donc non premiers entre eux, ce qui prouve le résultat par contraposée.

($\Leftarrow$) Réciproquement, supposons que $A$ et $B$ n'aient aucune racine commune et montrons qu'ils sont premiers entre eux. Soit $D$ un diviseur commun à $A$ et $B$, on a donc $D \neq 0$, car $A$ et $B$ ne sont pas tous les deux nuls.
Si $\deg D \geqslant 1$, le polynôme $D$ est non constant. Il admet alors une racine $z \in \mathbb{C}$, et est donc divisible par $X - z$. On

en déduit que $A$ et $B$ sont tous deux divisibles par $X-z$, et donc que $A$ et $B$ possèdent $z$ comme racine commune, ce qui contredit l'hypothèse. On en déduit donc $\deg D = 0$, ce qui montre que $A$ et $B$ sont premiers entre eux.

□

**Exemple 19**
Soit $A$ un polynôme non nul de $\mathbb{C}[X]$. Une racine commune à $A$ et $A'$ est la même chose qu'une racine multiple de $A$. Les polynômes $A$ et $A'$ sont donc premiers entre eux si, et seulement si, $A$ ne possède pas de racine multiple.

⚠ Attention Se cantonner aux racines réelles ne suffit pas !
Les polynômes $X^2+1$ et $\left(X^2+1\right)^2$ n'ont pas de racine réelle commune, mais ils ne sont pas premiers entre eux !
Dans $\mathbb{R}$, on "ne voit pas" toutes les racines.
Par contre, on a vu que le PGCD est le même, qu'on le calcule dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. En particulier, on peut appliquer la proposition précédente, c'est à dire deux polynômes de $\mathbb{R}[X]$ sont premiers entre eux si, et seulement s'ils n'ont pas de racine complexe commune.

## Extension à un nombre fini de polynômes

Comme dans le cas de l'arithmétique des entiers, on généralise la notion de PGCD de deux polynômes à un nombre fini de polynômes.
Soit $k \in \mathbb{N}^*$ et $A_1, \dots, A_k$ des polynômes non tous nuls de $\mathbb{IK}[X]$. Il existe un unique polynôme unitaire $D$ dont les diviseurs sont exactement les diviseurs communs à tous les $A_i$, c'est-à-dire qui vérifie

$$\forall P \in \mathbb{K}[X], \quad (\forall i \in [\![1,k]\!], \quad P \mid A_i) \iff P \mid D.$$

On l'appelle le **PGCD de $A_1, \dots, A_k$** et on le note $A_1 \wedge \cdots \wedge A_k$ ou $\bigwedge_{i=1}^k A_i$. On garde une identité de Bézout

$$\exists (U_1, \dots, U_k) \in \mathbb{K}[X]^k, \quad D = A_1U_1 + \cdots + A_kU_k = \sum_{i=1}^k A_iU_i$$

On peut alors définir,

- des polynômes non tous nuls $A_1, \dots, A_k$ **premiers entre eux dans leur ensemble**, si $\bigwedge_{i=1}^k A_i = 1$.
- des polynômes $A_1, \dots, A_k$ **premiers entre eux deux à deux**, si $\forall (i,j) \in [\![1,k]\!]^2 \quad i \neq j \Rightarrow A_i \wedge A_j = 1$.

⚠ Ne pas confondre les deux définition !
Il est clair que, si les $A_i$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble, mais la réciproque est fausse.

La même preuve de l'identité de Bézout pour deux polynômes, nous donne par contre que des polynômes $A_1, \dots, A_k$ de $\mathbb{K}[X]$ sont premiers entre eux dans leur ensemble si, et seulement s'il existe des polynômes $U_1, \dots, U_k$ tels que

$$\sum_{i=1}^k A_iU_i = 1 \ .$$

**Exemple 20**
Considérons $A = (X-1)(X+2), B = (X+2)(X-3)$ et $C = (X-1)(X-3)$. Les polynômes $A$ et $B$ ne sont pas associés, mais ils ont un diviseur commun de degré 1 , à savoir $X+2$. On en déduit $A \wedge B = X+2$, donc $A$ et $B$ ne sont pas premiers entre eux. On voit de même que $A$ et $C$ ne sont pas premiers entre eux, et $B$ et $C$ non plus. En revanche, comme $X+2$ ne divise pas $C$, on voit que les seuls diviseurs communs à $A, B$ et $C$ sont de degré 0 , c'est-à-dire que ces polynômes sont premiers entre eux dans leur ensemble.

## 9.4 Plus Petit Commun Multiple

Soient $A, b \in \mathbb{K}[X]$. L'ensemble des multiples non nuls communs à $A$ et $B$ est une partie de $\mathbb{K}[X]$, non vide car elle contient $AB$. L'ensemble des degrés de ces polynômes est donc une partie non vide de $\mathbb{N}$. Elle possède ainsi un plus petit élément $q$. Il existe alors un polynôme $M$ de degré $q$ tel que $M$ soit un multiple commun à $A$ et $B$.

**Définition 18**

Soit $A$ et $B$ deux polynômes non nuls de $\mathbb{K}[X]$. Tout multiple non nul commun à $A$ et $B$ de degré minimal est appelé un PPCM de $A$ et $B$.

**Proposition 19 : Propriétés**

*Soit $A, B \in \mathbb{K}[X]$, $A, B \neq 0$. Soit $M$ un PPCM de $A$ et $B$. On a alors*

$$\forall P \in \mathbb{K}[X] \quad (A \mid P \quad \text{et} \quad B \mid P) \iff M \mid P.$$

*Preuve.* Immédiat par définition. □

**Le PPCM**

On a déjà prouvé l'existence. Pour l'unicité, de même que pour le PGCD,

Il existe un polynôme unitaire dans l'ensemble des PPCM de $A$ et $B$. En fait, ce polynôme est unique. En effet, si $M_1$ et $M_2$ sont deux PPCM de $A$ et de $B$ alors ils se divisent l'un l'autre et sont donc associés. Comme ils sont non nuls, il existe un et un seul PPCM unitaire de $A$ et $B$.

Ce polynôme est appelé **le PPCM** de $A$ et de $B$. On le note $A \vee B$.

**Proposition 20 : Relation PGCD/PPCM**

*Si $A$ et $B$ sont des polynômes premiers entre eux, alors $A \vee B$ et $AB$ sont des polynômes associés.*

*Plus généralement,* *les polynômes $AB$ et $(A \wedge B)(A \vee B)$ sont associés*.

*Preuve.*

- D'abord le cas où $A$ et $B$ sont premiers entre eux. Les multiples de $AB$ sont des multiples communs à $A$ et $B$. Réciproquement, supposons que $A \mid P$ et $B \mid P$. Il existe donc un polynôme $Q$ tel que $P = BQ$. Comme $A$ divise $P$ et qu'il est premier avec $B$, le lemme de Gauss nous dit que $A$ divise $Q$. Il existe donc un polynôme $R$ tel que $Q = AR$, et par suite, $P = ABR$. Les multiples communs à $A$ et à $B$ sont donc les multiples de $AB$, ce qui prouve le résultat.
- Montrons maintenant le cas général. On peut supposer $A$ et $B$ unitaires quitte à les diviser par leurs coefficients dominants. On va alors montrer que $AB = (A \wedge B)(A \vee B)$ dans ce cas. Soit $D = A \wedge B$. Prenons $A_1$ et $B_1$ tels que $A = DA_1$ et $B = DB_1$. Alors $A_1 \wedge B_1 = 1$. On va montrer que $A \vee B = DA_1B_1$.
  Il suffit de montrer que les multiples communs à $A$ et $B$ sont exactement les multiples du polynôme unitaire $DA_1B_1$.
  D'abord, tout multiple de $DA_1B_1$ est un multiple de $DA_1 = A$ et $DB_1 = B$.
  Réciproquement, soit $P$ un multiple commun à $A$ et $B$. Un tel polynôme est donc nécessairement multiple de $D$, donc on peut trouver $P_1 \in \mathbb{K}[X]$ tel que $P = DP_1$.
  Les relations de divisibilité $A \mid P$ et $B \mid P$ entraînent alors l'existence de $(U, V) \in \mathbb{K}[X]^2$ tel que $DP_1 = UDA_1 = VDB_1$.
  Puisque $D$ est unitaire, il est non nul, et l'on en déduit que $P_1 = UA_1 = VB_1$. Les polynômes premiers entre eux $A_1$ et $B_1$ divisent donc $P_1$, et, comme au point précédent, le lemme de Gauss entraîne $A_1B_1 \mid P_1$, d'où $DA_1B_1 \mid P$.
  On a ainsi montré $A \vee B = DA_1B_1$, d'où $(A \wedge B)(A \vee B) = D^2A_1B_1 = AB$.

□

## 9.5 Polynômes irréductibles de $\mathbb{K}[X]$

**Définition 19**

On appelle polynôme irréductible de $\mathbb{K}[X]$ tout polynôme $P$ vérifiant

$$\deg P \geqslant 1 \qquad \text{et} \qquad \text{les seuls diviseurs de } P \text{ sont les éléments de } \mathbb{K}^* \text{ et les associés de } P.$$

Ainsi un polynôme irréductible est un polynôme $P \in \mathbb{K}[X]$ non constant tel que

$$\forall (A, B) \in \mathbb{K}[X]^2 \quad P = AB \quad \Rightarrow \quad (\deg A = 0 \quad \text{ou} \quad \deg B = 0)$$

**Polynômes irréductibles $\sim$ nombres premiers !**

On rappelle que, pour les nombres premiers dans $\mathbb{N}$, un entier $p$ est premier si $p \geqslant 2$ et si

$$\forall (a,b) \in \mathbb{N}^2 \quad p = ab \Rightarrow (a = 1 \text{ ou } b = 1).$$

Un polynôme $P$ est non irréductible s'il est constant ou s'il peut s'écrire comme produit de deux polynômes non constants.

**Seulement les polynômes de degré 1 ?**

Tout polynôme de degré 1 est irréductible. En effet, si $A$ est un polynôme de degré 1 , considérons des polynômes $B$ et $C$ tels que $A = BC$. On a alors $\deg B + \deg C = \deg A = 1$. Comme $\deg B$ et $\deg C$ sont des entiers positifs, on en déduit $\deg B = 0$ ou $\deg C = 0$, ce qui prouve que $A$ est irréductible.
À l'exception des polynômes de degré 1, irréductibles d'après l'exemple précédent, les polynômes irréductibles ne peuvent pas avoir de racines. En effet, si $\deg P \geqslant 2$ et que $P$ possède une racine $\alpha$, on peut trouver $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$ et $\deg Q = \deg P - 1 \geqslant 1$, ce qui montre que $P$ n'est pas irréductible.

**Exemple 21**
Le polynôme $X^2 + 1$ n'est pas irréductible dans $\mathbb{C}[X]$ puisqu'il est divisible par $X - i$. En revanche, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$. En effet, n'ayant pas de racine réelle, il n'est divisible par aucun polynôme de degré 1 et ses seuls diviseurs sont donc les polynômes constants non nuls et ses associés.

⚠ Attention L'exemple précédent montre qu'un polynôme non constant peut ne pas être irréductible sans pour autant avoir de racine, au moins quand $\mathbb{K} = \mathbb{R}$.
Par exemple, le polynôme $\left(X^2 + 1\right)^2$ n'est pas irréductible dans $\mathbb{R}[X]$, puisque divisible par $X^2 + 1$.

**Proposition 21**
*Un polynôme $P$ irréductible est premier avec tous les polynômes qu'il ne divise pas.*

*Preuve.* Soit $P$ un polynôme irréductible. Les diviseurs communs à $P$ et à un polynôme $A$ sont des diviseurs de $P$, donc sont soit constants, soit associés à $P$. Ainsi, si $P$ ne divise pas $A$, les seuls diviseurs communs à $P$ et $A$ sont les constantes. Donc $A \wedge P = 1$. □

**Proposition 22 : Polynômes à coefficients complexes irréductibles**
*Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

*Preuve.* Dans un sens, on a vu que les polynômes de degré 1 sont irréductibles. Réciproquement, un polynôme irréductible $P$ est non constant par définition et possède donc une racine $\alpha \in \mathbb{C}$ d'après le théorème de d'Alembert-Gauss. On peut donc trouver un polynôme $Q \in \mathbb{C}[X]$ tel que $P = (X - \alpha)Q$. Par irréductibilité de $P$, on doit avoir $\deg Q = 0$, et donc $\deg P = 1$. □

**Exemple 22**
Un polynôme de $\mathbb{R}[X]$ de degré 2 est irréductible si, et seulement s'il n'a pas de racine dans $\mathbb{R}$. En effet, si il a une racine, il n'est pas irréductible par définition. S'il na pas de racine, donc il est divisible seulement par des polynômes de degré 2, donc par tous les polynômes qui lui sont associés.

**Proposition 23 : Polynômes à coefficients réels irréductibles**
*Les polynômes irréductibles de $\mathbb{R}[X]$ sont*

- *les polynômes de degré 1,*
- *les polynômes de degré 2 dont le discriminant est strictement négatif.*

*Preuve.* A vous ! □

**Théorème 7 : Décomposition en polynômes irréductibles**

*Tout polynôme de $\mathbb{K}[X]$ non nul est le produit d'un élément de $\mathbb{K}^*$ et d'un produit de polynômes unitaires irréductibles dans $\mathbb{K}[X]$.*
*L'écriture est unique à l'ordre près des facteurs.*

**C'est une décomposition en "facteurs premiers"**

Si $A$ est un polynôme non constant, cette décomposition en produit de polynômes irréductibles peut encore s'écrire

$$A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k} \ ,$$

où $\lambda$ est un scalaire non nul, les $P_i$ des irréductibles unitaires distincts et les $\alpha_i$ des entiers naturels non nuls. Cela ressemble beaucoup à la décomposition en facteurs premiers.

*Preuve.*

- Soit $A = \lambda \prod_{k=1}^{p} (X - a_k)^{\alpha_k}$ un polynôme $A$ non constant, où les $a_k$ sont des nombres complexes distincts, les $\alpha_k$ des entiers naturels non nuls et $\lambda \in \mathbb{C}^*$. Il y a unicité d'une telle factorisation, à l'ordre près des facteurs, puisque $\lambda$ est le coefficient dominant de $A$, les $a_k$ sont ses racines et les $\alpha_k$ leurs ordres de multiplicité.
- De même, dans une factorisation dans $\mathbb{R}[X]$,

$$A = \lambda \prod_{j=1}^{p} (X - \alpha_j)^{r_j} \prod_{k=1}^{q} \left(X^2 + \beta_k X + \gamma_k\right)^{s_k} \ ,$$

où les $\alpha_j$ d'une part et les $(\beta_k, \gamma_k)$ vérifiant $\beta_k^2 - 4\gamma_k < 0$ d'autre part sont distincts, les $r_j$ et $s_k$ des entiers naturels non nuls et $\lambda$ un réel non nul,

  - ▷ les racines réelles de $A$ sont les $\alpha_j$ avec l'ordre de multiplicité $r_j$,
  - ▷ les racines non réelles sont, pour chaque $k \in [\![1, q]\!]$, les deux racines complexes du polynôme $X^2 + \beta_k X + \gamma_k$ à l'ordre de multiplicité $s_k$,
  - ▷ $\lambda$ est le coefficient dominant de $A$, ce qui donne l'unicité, à l'ordre près des facteurs, de la factorisation.

□