# Polynômes

Dans ce chapitre, le corps $\mathbb{K}$ considéré sera $\mathbb{R}$ ou $\mathbb{C}$. On notera $\star$ les notions qui ne seront pas prioritaires dans une première approche de ce chapitre.

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

### 1.1 Définition

Les polynômes à une indéterminée $X$ à coefficients dans $\mathbb{K}$ sont des objets mathématiques de la forme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

où $a_0, a_1, \cdots, a_n \in \mathbb{K}$.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à une indéterminée $X$ à coefficients dans $\mathbb{K}$.

Un terme de la forme $a_k X^k$ est appelé monôme de degré $k$ et $a_k$ est appelé coefficient du monôme de degré $k$.

**Remarques:**

1. Attention, un polynôme n'est pas une fonction. $X$ est un nouveau symbole appelé indéterminée pas une variable.
2. On peut aussi représenter un polynôme $P$ par $P = \sum_{k=0}^{\infty} a_k X^k$, où $(a_k)$ est une suite d'éléments de $\mathbb{K}$ nulles à partir d'un certain rang.

### 1.2 Opérations sur les polynômes et degré

**Définition 1** (Opérations sur les polynômes)**.** *Pour $P = \sum_{k=0}^{\infty} a_k X^k$, $Q = \sum_{k=0}^{\infty} b_k X^k$ polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on définit les polynômes*

- $P + \lambda Q = \sum_{k=0}^{\infty} (a_k + \lambda b_k) X^k$
- $P \cdot Q = \sum_{k=0}^{\infty} c_k X^k, \quad$ où $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

**Remarque:** Ces règles opératoires munissent $\mathbb{K}[X]$ d'un structure d'espace vectoriel et d'anneau (en particulier, la multiplication des polynômes est distributive par rapport à l'addition). On a alors un isomorphisme d'espaces vectoriels entre $\mathbb{K}[X]$ et les suites d'éléments de $\mathbb{K}$ nulles à partir d'un certain rang.

**Définition 2** (Composition des polynômes)**.** *Pour $P = \sum_{k=0}^{\infty} a_k X^k$, $Q = \sum_{k=0}^{\infty} b_k X^k$ polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on définit la composée de $P$ et $Q$ par*

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

**Définition 3.** *Soit* $P = \sum_{k=0}^{\infty} a_k X^k$ *différent du polynôme nul, on appelle degré de* $P$ *noté* $\deg P$ *le plus grand entier* $k$ *tel que* $a_k \neq 0$. *Si* $n = \deg P$, $a_n X^n$ *est appelé monôme dominant et* $a_n$ *coefficient dominant.*

*Un polynôme est dit unitaire si son coefficient dominant est 1.*

*On étend la définition du degré au polynôme nul en posant* $\deg 0 = -\infty$.

**Proposition 1.** *Soient* $P$, $Q$ *deux polynômes non nuls et* $\lambda \in \mathbb{K}^*$, *alors on a*

- $\deg \lambda P = \deg P$.
- $\deg(P+Q) \leq \max(\deg P, \deg Q)$, *une condition suffisante (mais pas nécessaire) pour que ce soit une égalité est* $\deg P \neq \deg Q$.
- $\deg PQ = (\deg P) + (\deg Q)$.
- *Si* $\deg Q > 0$, $\deg P \circ Q = (\deg P)(\deg Q)$.

**Remarque:** Pour calculer le degré d'une somme de polynômes, on calcule le plus souvent une majoration du degré par un entier $p$ puis on explicite les coefficients à partir de celui de degré $p$ en décroissant jusqu'à trouver un coefficient non nul.

**Exemples:**

1. $X^{861} + X^2 + 1$ est un polynôme unitaire de degré 861.
2. $(X^2-1)^n - (X^2+1)^n$ est polynôme de degré $2n-2$ de coefficient dominant $-2n$.

**Corollaire 1.** *L'anneau des polynômes est intègre.*

**Proposition 2** (Division euclidienne)**.** *Soient* $A, B$ *deux polynômes avec* $B$ *non nul, alors il existe un unique couple* $(Q,R) \in \mathbb{K}[X]^2$ *tel que*

$$A = BQ + R \qquad \text{avec} \quad \deg R < \deg B.$$

*Le polynôme* $Q$ *(respectivement* $R$*) est le quotient (respectivement le reste) de la division euclidienne de* $A$ *par* $B$. *On sait que* $B$ *divise* $A$ *si le reste de la division euclidienne est nulle.*

**Exemple:** Pour la division euclidienne de $X^4+3X^2-2X+1$ par $X^2+X+1$, on écrit successivement :

$$\begin{aligned} X^4+3X^2-2X+1 &= X^2(X^2+X+1)+(-X^3+2X^2-2X+1) \\ -X^3+2X^2-2X+1 &= (-X)(X^2+X+1)+3X^2-X+1 \\ 3X^2-X+1 &= 3(X^2+X+1)-4X-2 \end{aligned}$$

De sorte que $X^4+3X^2-2X+1 = (X^2+X+1)(X^2-X+3)+(-4X-2)$. Dans la pratique, on pourra présenter le calcul comme une division euclidienne d'entiers :

$$\begin{array}{r|l} X^4 + 3X^2 - 2X + 1 & X^2+X+1 \\ \cline{2-2} -(X^4+X^3+X^2) & X^2-X+3 \\ \cdots\cdots\cdots & \\ -X^3+2X^2-2X+1 & \\ -(-X^3-X^2-X) & \\ \cdots\cdots\cdots & \\ 3X^2-X+1 & \\ -(3X^2+3X+3) & \\ \cdots\cdots\cdots & \\ -4X-2 & \end{array}$$

## 1.3 Racines

**Définition 4.** *On définit l'application* $\varphi$ :

$$\begin{array}{rccc} \varphi : & \mathbb{K}[X] & \longrightarrow & \mathcal{F}(\mathbb{K},\mathbb{K}) \\ & P = \sum_{k=0}^{\infty} a_k X^k & \longmapsto & \left( t \mapsto \sum_{k=0}^{\infty} a_k t^k \right). \end{array}$$

*La fonction $\varphi(P)$ est appelée fonction polynomiale associée à $P$. On simplifiera $\varphi(P)(t)$ en écrivant $P(t)$.*

**Proposition 3.** *L'application $\varphi$ définie précédemment est un morphisme d'espaces vectoriels*[1] *vérifiant de plus*

$$\forall P, Q \in \mathbb{K}[X], \qquad \varphi(PQ) = \varphi(P)\varphi(Q).$$

**Définition 5.** *Soient $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, $\alpha$ une racine de $P$, si $\varphi(P)(\alpha) = 0$, c'est-à-dire si*

$$P(\alpha) = \sum_{k=0}^{\infty} a_k \alpha^k = 0.$$

**Proposition 4.** *Soient $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, il y a équivalence entre*

*(i)* *$\alpha$ est une racine de $P$.*

*(ii)* *$X - \alpha$ divise $P$.*

**Corollaire 2.** *Soient $(\alpha_1, \cdots, \alpha_n) \in \mathbb{K}^n$ avec les $(\alpha_i)$ 2 à 2 distincts et $P \in \mathbb{K}[X]$, il y a équivalence entre*

*(i)* *$\forall i \in [\![1, n]\!], \quad \alpha_i$ est une racine de $P$.*

*(ii)* *$(X - \alpha_1) \cdots (X - \alpha_n)$ divise $P$.*

**Proposition 5.** *On a*

*(i)* *Soit $P \in \mathbb{K}[X]$ un polynôme non nul, si $P$ a $p$ racines distinctes $(\alpha_1, \cdots, \alpha_p)$, alors $\deg P \geq p$ et si de plus $p = \deg P$, alors*

$$P = \lambda(X - \alpha_1) \cdots (X - \alpha_p), \quad \text{où } \lambda \text{ est le coefficient dominant de } P.$$

*(ii)* *L'application $P \mapsto \varphi(P)$ est une injection de $\mathbb{K}[X]$ dans $\mathcal{F}(\mathbb{K}, \mathbb{K})$.*

*(iii)* *Si un polynôme a une infinité de racines, alors il est nul.*

**Remarques:**

1. La première partie du premier point se traduit par « **Un polynôme $P$ non nul a au plus $\deg P$ racines.** »
2. Le point $(i)$ sert fréquemment pour démontré l'égalité de 2 polynômes $P$ et $Q$. Il faut et il suffit de montrer que $P - Q$ a plus de racines que son degré. On explicitera souvent que ce polynôme a une infinité de racines, ce qui permet d'utiliser le point $(iii)$.

**Exemple :**

On peut montrer l'unicité des polynômes de Tchebychev en utilisant ce corollaire.

Pour tout entier $n \geq 0$, il existe un unique polynôme $T_n$ tel que

$$\forall x \in \mathbb{R}, \quad T_n(\cos(x)) = \cos(nx).$$

**Existence :**

En utilisant la formule de Moivre, on a, pour tout $x \in \mathbb{R}$,

1. C'est-à-dire pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, $\varphi(P + \lambda Q) = \varphi(P) + \lambda\varphi(Q)$

$$\begin{aligned}
\cos(nx) &= \mathrm{Re}(e^{inx}) \\
&= \mathrm{Re}\left((\cos(x)+i\sin(x))^n\right) \\
&= \mathrm{Re}\left(\sum_{k=0}^{n}\binom{n}{k}(i\sin(x))^k(\cos(x))^{n-k}\right) \\
&= \mathrm{Re}\left(\sum_{0\le 2k\le n}\binom{n}{2k}(-1)^k\sin^{2k}(x)\cos^{n-2k}(x)+i\sum_{0\le 2k+1\le n}\binom{n}{2k+1}(-1)^k\sin^{2k+1}(x)\cos^{n-2k-1}(x)\right) \\
&= \sum_{0\le 2k\le n}\binom{n}{2k}(-1)^k\sin^{2k}(x)\cos^{n-2k}(x) \\
&= \sum_{0\le 2k\le n}\binom{n}{2k}(-1)^k(1-\cos^2(x))^k\cos^{n-2k}(x) = T_n(\cos(x))
\end{aligned}$$

où $T_n = \sum_{0\le 2k\le n}\binom{n}{2k}(-1)^k(1-X^2)^kX^{n-2k}$.

**Unicité :**

Supposons qu'il existe $Q_n$ un polynôme tel que

$$\forall x\in\mathbb{R},\quad Q_n(\cos(x)) = \cos(nx).$$

Pour tout $x\in\mathbb{R}$, le polynôme $T_n - Q_n$ admet $\cos(x)$ comme racine, car

$$(T_n-Q_n)(\cos(x)) = T_n(\cos(x)) - Q_n(\cos(x)) = \cos(nx)-\cos(nx) = 0.$$

Tout élément de $[-1,1]$ est donc racine de $T_n - Q_n$, il en résulte que ce polynôme admet une infinité de racines, il est donc nul d'où $Q_n = T_n$.

# 2 Dérivation et racines multiples

## 2.1 Dérivation

### 2.1.1 Définition

On définit la dérivation $D$ comme l'unique endomorphisme de l'espace vectoriel $\mathbb{K}[X]$ tel que

$$D(X) = 1 \qquad \text{et} \qquad \forall P,Q\in\mathbb{K}[X],\quad D(PQ) = D(P)\cdot Q + P\cdot D(Q).$$

**Remarque:** On notera $P'$ pour $D(P)$, mais bien noter que l'opération est algébrique, ce n'est pas une définition analytique (Pas de calcul de la limite d'un taux d'accroissement). D'ailleurs si $\mathbb{K}=\mathbb{C}$, on n'a pas défini de dérivation analytique.

### 2.1.2 Propriétés

**Proposition 6.** *Soit* $P = \sum_{k=0}^{\infty} a_kX^k$, *alors on a* $P' = \sum_{k=0}^{\infty}(k+1)a_{k+1}X^k$.

**Remarque:** Ouf ! On retrouve bien la dérivée usuelle dans le cas des fonctions polynomiales à valeurs réelles, on a bien, pour $P\in\mathbb{R}[X]$, $\varphi\left(P'\right) = \varphi\left(P\right)'$.

**Proposition 7** (Formule de Leibniz)**.** *Soient* $P$, $Q$ *2 polynômes de* $\mathbb{K}[X]$ *et* $n\in\mathbb{N}$, *on a*

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

### 2.1.3 Formule de Taylor polynomiale

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, alors on a

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

**Remarque:** Pas de problème de définition, le polynôme $P^{(k)}$ étant nul dés que $k$ est strictement supèrieur au degré de $P$, la somme est finie.
Cette formule est exacte et ne suppose aucune hypothèse de régularité analytique contrairement aux autres formules de Taylor.

## 2.2 Racines multiples

### 2.2.1 Définition

Soient $P$ un polynôme de $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $n \in \mathbb{N}$, on dit que $\alpha$ est racine d'ordre au moins $n$ si $(X-\alpha)^n$ divise $P$ et que $\alpha$ est racine d'ordre exactement $n$ si $(X-\alpha)^n$, divise $P$ et que $(X-\alpha)^{n+1}$ ne divise pas $P$.

### 2.2.2 Propriétés

**Proposition 8.** *Soient $P$ un polynôme de $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}$, il y a équivalence entre*

*(i) $\alpha$ est racine d'ordre $n$ de $P$.*

*(ii) On a*

$$\forall k \in [0, n-1], \quad P^{(k)}(\alpha) = 0 \qquad et \qquad P^{(n)}(\alpha) \neq 0.$$

**Remarques:**

1. On utilise la formule de Leibniz dans le sens $(i)$ vers $(ii)$ et la formule de Taylor polynomiale dans le sens $(ii)$ vers $(i)$.
2. Si on supprime l'hypothèse $P^{(n)}(\alpha) \neq 0$ dans $(ii)$, on a seulement $\alpha$ est racine d'ordre au moins $n$ de $P$ pour $(i)$.

**Proposition 9.** *Soient $P$ un polynôme de $\mathbb{K}[X]$, $(\alpha_i)_{i\in[1,p]} \in \mathbb{K}^p$ un $n$-uplet de scalaires distincts et $(n_i)_{i\in[1,p]} \in \mathbb{N}^p$ tel que*

$$\forall i \in [1,p], \quad \alpha_i \text{ est racine d'ordre au moins } n_i \text{ de } P,$$

*alors on a*

$$(X-\alpha_1)^{n_1}(X-\alpha_2)^{n_2}\cdots(X-\alpha_p)^{n_p} \text{ divise } P.$$

**Corollaire 3.** *Soient $P$ un polynôme de $\mathbb{K}[X]$, $(\alpha_i)_{i\in[1,p]} \in \mathbb{K}^p$ un $n$-uplet de scalaires distincts et $(n_i)_{i\in[1,p]} \in \mathbb{N}^p$ tel que*

$$\forall i \in [1,p], \quad \alpha_i \text{ est racine d'ordre au moins } n_i \text{ de } P,$$

*alors on a*

$$\sum_{i=1}^{p} n_i \leq \deg P.$$

**Remarque:** Ce corollaire se résume en **« Un polynôme $P$ non nul a au plus** $\deg P$ **racines comptées avec leurs multiplicités. »**

# 3 Arithmétique dans $\mathbb{K}[X]$

## 3.1 Plus grand diviseur commun

### 3.1.1 Définition et premières propriétés

On rappelle qu'un idéal $I$ d'un anneau commutatif $A$ est une sous-groupe de $(A,+)$ vérifiant de plus pour tout $x \in A$ et tout $y \in I$, $xy$ est un élément de $I$.

**Remarque:** Contrairement au cas de l'anneau $\mathbb{Z}$, les sous-groupes additifs de $\mathbb{K}[X]$ ne sont pas tous des idéaux.
Par exemple $G = \left\{aX^2 + b \quad ; \quad a, b \in \mathbb{K}\right\}$ est un sous-groupe additif de $\mathbb{K}[X]$ sans être un idéal, car $1 \in G$ et $X \in \mathbb{K}[X]$, mais $1 \cdot X = X \notin G$.

**Proposition 10.** *Les idéaux de $\mathbb{K}[X]$ sont de la forme $P\mathbb{K}[X] = \{PQ \quad ; \quad Q \in \mathbb{K}[X]\}$, où $P$ un élément de $\mathbb{K}[X]$.*

**Définition 6.** *Soient $A$ et $B$ deux polynômes non tous nuls, on dit que $H$ un plus grand commun diviseur $A$ et $B$ si*

$$A\mathbb{K}[X] + B\mathbb{K}[X] = H\mathbb{K}[X].$$

*Il existe un unique plus grand commun diviseur unitaire, on le note $A \wedge B$.*

**Proposition 11.** *Soient $P, A, B$ 3 polynômes non nuls tel que $P$ divise $A$ et $B$ alors $P$ divise $A \wedge B$.*

**Proposition 12** (Quelques propriétés élémentaires)**.** *Soient $A, B \in \mathbb{K}[X]$ non nuls, on a*

*(i)* $A \wedge A = \tilde{A}$

*(ii)* $A \wedge B = B \wedge A$

*(iii)* $A \wedge 0 = \tilde{A}$

*(iv)* $A \wedge 1 = 1$

*où $\tilde{A}$ est le polynôme unitaire proportionnel à $A$.*

### 3.1.2 Algorithme d'Euclide

**Lemme 1.** *Soient $A$ et $B$ deux polynômes non tous nuls et $Q$ un polynôme quelconque, alors on a*

$$A \wedge B = (A - BQ) \wedge B.$$

**Remarque :** On a en particulier que si $A - BQ = 0$, alors $A \wedge B = \tilde{B}$, où $\tilde{B}$ est le polynôme unitaire proportionnel à $B$.

**Algorithme d'Euclide :**

On construit un suite de polynômes $(R_n)$ de la manière suivante :

On pose $R_0 = A$ et $R_1 = B$

Hérédité :

Pour $n \geq 1$, supposons avoir construite la suite $(R_k)_{k \in [\![0,n]\!]}$, tel que pour tout $k \in [\![1,n]\!]$, $R_k \wedge R_{k-1} = A \wedge B$.

Puis pour $n \geq 1$ tant que $R_n \neq 0$, on effectue la division euclidienne de $R_{n-1}$ par $R_n$, on a donc

$$R_{n-1} = R_n Q_n + R_{n+1}$$

Avec $\deg R_{n+1} < \deg R_n$. Grâce au lemme 1, on a de plus $R_n \wedge R_{n+1} = R_{n-1} \wedge R_n$.

La suite de polynômes $(R_n)$ est de degré strictement décroissante à partir du rang 1, donc par propriété des entiers naturels, l'algorithme termine avec $R_n = 0$ et alors $A \wedge B = R_{n-1} \wedge R_n = \tilde{R}_{n-1}$, où $\tilde{R}_{n-1}$ est le polynôme unitaire proportionnel à $R_{n-1}$.

**Proposition 13** (Identité de Bezout). *Soient $A, B \in \mathbb{K}[X]$, il existe $U, V \in \mathbb{K}[X]$ tel que*

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

L'existence découle directement de la définition du PGCD, il n'y a pas unicité et on a un algorithme pour déterminer un couple solution.

Algorithme d'Euclide étendu :

Pour déterminer un couple $(U, V) \in \mathbb{K}[X]$, tel que $AU + BV = A \wedge B$, on utilise l'algorithme d'Euclide étendu.

On initialise toujours la suite $(R_n)$ par $R_0 = A$ et $R_1 = B$. On construit de plus par récurrence la suite de couple de polynômes $(U_n, V_n)$ tel que pour tout $n$ tel que $R_n \neq 0$, $R_n = U_n A + V_n B$.

**Initialisation :**

Pour $n = 0$, comme $R_0 = A$, il suffit de prendre $U_0 = 1$ et $V_0 = 0$.

Pour $n = 1$, comme $R_1 = B$, il suffit de prendre $U_1 = 0$ et $V_1 = 1$.

**Hérédité :** On suppose avoir construit les suites $(R_n)$, $(U_n, V_n)$ jusqu'au rang $n \geq 1$ $R_n \neq 0$.

Tel que pour tout $k \in [\![0, n]\!]$,

$$R_k = U_k A + V_k B.$$

On a alors

$$R_{n-1} = R_n Q_n + R_{n+1}.$$

Si $R_{n+1} = 0$, on a alors $\tilde{R}_n = \frac{1}{\lambda} U_n A + B \frac{1}{\lambda} V_n = A \wedge B$, où $\lambda$ est le coefficient dominant de $R_n$, donc $(U, V) = (\frac{1}{\lambda} U_n, \frac{1}{\lambda} V_n)$ est une solution.

Si $R_{n+1} \neq 0$, on a alors

$$R_{n+1} = R_{n-1} - R_n Q_n = (U_{n-1} A + V_{n-1} B) - (U_n A + V_n B) Q_n = (U_{n-1} - U_n Q_n) A + (V_{n-1} - V_n Q_n) B$$

On pose alors $U_{n+1} = U_{n-1} - U_n Q_n$ et $V_{n+1} = V_{n-1} - V_n Q_n$.

Comme l'algorithme d'Euclide termine, on a explicitement une solution par cette méthode.

## 3.2 Polynômes premiers entre eux, Bezout et Gauss

**Définition 7.** *Soient $A, B \in \mathbb{K}[X]$, on dit que $A$ et $B$ sont premiers entre eux si $A \wedge B = 1$.*

**Proposition 14** (Théorème de Bezout ). *Soient $A, B \in \mathbb{K}[X]$, il y a équivalence entre*

*(i) $A$ et $B$ sont premiers entre eux.*

*(ii) Il existe $U, V \in \mathbb{K}[X]$ tel que $AU + BV = 1$.*

**Remarque :** Dans le cas de deux polynômes quelconques $A$ et $B$ non tous nuls, on a bien l'existence de $U, V \in \mathbb{K}[X]$ tel que $AU + BV = A \wedge B$, mais pas de réciproque. Que peut-on dire de $A \wedge B$, si $AU + BV = Q$ ?

**Proposition 15** (Lemme de Gauss). *Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$ tel que $A \wedge B = 1$ et $A$ divise $BC$, alors $A$ divise $C$.*

**Proposition 16.** *Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$ tel que $A \wedge B = 1$ et $B \wedge C = 1$ alors $A \wedge BC$.*

On généralise le PGCD à $n$ polynômes $A_1, \cdots, A_n$ en utilisant les idéaux

$$A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = (A_1 \wedge A_2 \wedge \cdots \wedge A_n)\mathbb{K}[X],$$

où $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ est l'unique polynôme unitaire générateur de l'idéal.

On peut calculer le PGCG de $A_1, \cdots, A_n$ par récurrence, grâce à la formule

$$A\mathbb{K}[X] + B\mathbb{K}[X] = A \wedge B\mathbb{K}[X].$$

On dit que $A_1, \cdots A_n$ sont premiers dans leurs ensembles si $A_1 \wedge A_2 \wedge \cdots \wedge A_n = 1$.

Si $A_1, \cdots A_n$ sont premiers deux à deux, alors ils sont premiers dans leur ensemble, mais pas de réciproque.

**Exemple :**

Les polynômes $(X^2-1), (X-1)(X-2)$ et $(X+1)(X-2)$ sont premiers entre eux, mais pas 2 à 2.

### 3.3 Plus petit commun multiple

De manière similaire à l'arithmétique dans $\mathbb{Z}$, on définit le plus petit commun multiple de deux polynômes non nuls $A$ et $B$ comme l'unique polynôme unitaire noté $A \vee B$ tel que

$$(A \vee B)\,\mathbb{K}[X] = A\mathbb{K}[\![X] \cap B\mathbb{K}[X].$$

## 4 Polynômes irréductibles, polynômes scindés, sommes et produits des racines, relations de Viète

### 4.1 Définitions

Soit $P$ un polynôme non nul de $\mathbb{K}[X]$, on dit que

(a) $P$ de $\mathbb{K}[X]$ est un polynôme irréductible, si pour toute factorisation de $P$ sous la forme $P_1P_2$ avec $P_1$ et $P_2$ élément de $\mathbb{K}[X]$, on a $\deg P_1 = 0$ ou $\deg P_2 = 0$. Les polynômes irréductibles sont pour l'arithmétique dans $\mathbb{K}[X]$, l'équivalent des nombres premiers pour l'arithmétique dans $Z$.
Attention, cela dépend du choix du corps $\mathbb{K}$, le polynôme $X^2+1$ est irréductible comme polynôme de $\mathbb{R}[X]$ mais pas comme polynôme de $\mathbb{C}[X]$ $(X^2+1 = (X+i)(X-i))$.
Un polynôme de degré 1 est irréductible quelque soit le choix du corps.
**Remarque:** Un polynôme irréductible sur $\mathbb{K}$ de degré supérieur ou égal à 2 ne possède aucun racine dans $\mathbb{K}$. La réciproque n'est pas vraie en général, le polynôme $(X^2+1)^2$ n'a pas de racine réelle, mais il n'est pas irréductible sur $\mathbb{R}$.
**Exemples:**
   (a) Un polynôme de degré 2 ou 3 est irréductible sur $\mathbb{K}$ si et seulement si il n'a pas de racine dans $\mathbb{K}$.
   (b) Un polynôme de degré 2 à coefficients réels est irréductible sur $\mathbb{R}$, si et seulement si son discriminant est strictement négatif.

(b) $P$ est scindé sur $\mathbb{K}$, si il existe $(\alpha_1, \cdots, \alpha_n) \in \mathbb{K}^n$ et $\lambda \in \mathbb{K}$, tel que

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

ce qui est équivalent à ce que le nombre de racines dans $\mathbb{K}$ de $P$ comptées avec leur multiplicité est égal au degré de $P$.

## 4.2 Sommes et produits des racines d'un polynôme

**Proposition 17.** *Soit $P$ un polynôme de $\mathbb{K}[X]$ scindé de degré $n$ avec $P = \sum_{k=0}^{n} a_k X^n = \lambda \prod_{k=1}^{n}(X-\alpha_k)$, alors on a*

$$\sum_{k=1}^{n} \alpha_k = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{k=1}^{n} \alpha_k = (-1)^n \frac{a_0}{a_n}.$$

**Exemples:**

1. Calcul de
$$A = \prod_{k=0}^{n-1} \sin\left(\frac{k\pi}{n} + a\right) \qquad \text{et} \qquad B = \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right).$$
On utilise le polynôme $P_n = (X+1)^n - e^{2ina}$.
On calcule les racines sur $\mathbb{C}$ et on obtient $\alpha_k = e^{i\left(2a+\frac{2\pi}{n}\right)} - 1 = 2i\sin\left(a+\frac{\pi}{n}\right)e^{i\left(a+\frac{\pi}{n}\right)}$ avec $k \in [\![0, n-1]\!]$.
La relation sur le produit des racines nous donne directement
$$\prod_{k=0}^{n-1} 2i\sin\left(a+\frac{\pi}{n}\right)e^{i\left(a+\frac{\pi}{n}\right)} = (-1)^n(1-e^{2ina}).$$
En simplifiant, on obtient
$$A = \frac{(-1)^n(1-e^{2ina})}{\prod_{k=0}^{n-1} 2ie^{i\left(a+\frac{\pi}{n}\right)}} = \frac{\sin(na)}{2^{n-1}}.$$
Par passage à la limite en $a=0$, on obtient
$$B = \frac{n}{2^{n-1}}.$$

2. Soit $P = X^5 + 3X^2 + X + 1$ et $\alpha_1, \cdots, \alpha_5$ ses 5 racines dans $\mathbb{C}$ (on admet que $P$ est scindé sur $\mathbb{C}$). Calculer de manière réduite
$$\sum_{k=1}^{5} \frac{1}{2+\alpha_k}.$$
Si on pose $\beta_k = \frac{1}{2+\alpha_k}$, on remarque que $\frac{1}{\beta_k} - 2$ est racine du polynôme $P$, d'où
$$\left(\frac{1}{\beta_k}-2\right)^5 + 3\left(\frac{1}{\beta_k}-2\right)^2 + \frac{1}{\beta_k} - 2 + 1 = 0,$$
soit
$$(1-2\beta_k)^5 + 3\beta_k^3(1-2\beta_k)^2 + 2\beta_k^4 - \beta_k^5 = 0.$$
On en déduit que les $(\beta_k)$ sont les racines du polynôme
$$Q = (1-2X)^5 + 3X^3(1-2X)^2 + X^4 - X^5 = -21X^5 + 69X^4 - 77X^3 + 40X^2 - 10X + 1.$$
Le développement complet de l'expression n'était pas ici nécessaire, on a seulement besoin des coefficients des monômes de degré 4 et 5. En utilisant la relation sur le somme des racines, on obtient
$$\sum_{k=1}^{5} \frac{1}{2+\alpha_k} = -\frac{-69}{21} = \frac{23}{7}.$$

### 4.3 Relations coefficients-racines (Relations de Viète), cas général

Les formules générales ne sont pas à apprendre par coeur, mais à savoir retrouver rapidement si nécessaire.

**Exemple:**

Soit $P$ un polynôme de degré 3 scindé sur $\mathbb{K}$, on a donc

$$P = \lambda(X-\alpha)(X-\beta)(X-\gamma) = a_3X^3 + a_2X^2 + a_1X + a_0,$$

avec $a_3 \in \mathbb{K}^*$ et avec $\alpha, \beta, \gamma \in \mathbb{K}$ non forcément distincts (cas des racines multiples).

En développant, on obtient

$$\begin{cases} \lambda = a_3 \\ \alpha+\beta+\gamma = -\dfrac{a_2}{a_3} \\ \alpha\beta+\alpha\gamma+\beta\gamma = \dfrac{a_1}{a_3} \\ \alpha\beta\gamma = -\dfrac{a_0}{a_3}. \end{cases}$$

**Proposition 18.** *Soit $P$ un polynôme de degré $n$ scindé sur $\mathbb{K}$, on a donc*

$$P = \lambda\prod_{k=1}^{n}(X-x_k) = \sum_{k=0}^{n} a_kX^k,$$

*avec $a_n \in \mathbb{K}^*$ et avec $x_1, \cdots, x \in \mathbb{K}^*$ non forcément distincts (cas des racines multiples).*

$$\begin{cases} \lambda = a_n \\ \sigma_1 = \displaystyle\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \\ \sigma_2 = \displaystyle\sum_{1\le i_1<i_2\le n} x_{i_1}x_{i_2} = \frac{a_{n-2}}{a_n} \\ \sigma_3 = \displaystyle\sum_{1\le i_1<i_2<i_3\le n} x_{i_1}x_{i_2}x_{i_3} = -\frac{a_{n-3}}{a_n} \\ \quad\vdots \\ \sigma_n = \displaystyle\prod_{i=1}^{n} x_i = (-1)^n\frac{a_0}{a_n}. \end{cases}$$

*Par cohérence, on pose $\sigma_0 = 1$.*

**Exercice 1.** Si $P$ un polynôme réel de degré $n$ scindé, $P = \displaystyle\sum_{k=0}^{n} a_kX^k$, alors

$$\left(\frac{a_{n-1}}{a_n}\right)^2 - 2\frac{a_{n-2}}{a_n} \ge 0.$$

Pour $x_1, \cdots x_n$ les racines réelles de $P$, calculer $\displaystyle\sum_{k=1}^{n} x_k^2$ en fonction de $\sigma_1$ et $\sigma_2$.

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

Les deux premiers paragraphes de cette partie présentent la théorie. Le plus important est de savoir factoriser rapidement les polynômes, le troisième paragraphe donne quelques exemples et méthodes.

## 5.1 Dans $\mathbb{C}[X]$

### 5.1.1 Théorème de D'Alembert-Gauss

Tout polynôme $P$ de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 admet une racine sur $\mathbb{C}$.

### 5.1.2 Conséquences

**Corollaire 4.** *Tout polynôme $P$ de $\mathbb{C}[X]$ est scindés sur $\mathbb{C}$ et se factorise de manière unique à l'ordre près des facteurs sous la forme*

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

*où les $\alpha_k$ sont des nombres complexes 2 à 2 distincts et les $n_k$ des entiers naturels.*

**Corollaire 5.** *Un polynôme de $\mathbb{C}[X]$ est irréductible si et seulement si il est de degré 1.*

**Corollaire 6.** *Soit $A, B \in \mathbb{K}[X]$ (avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), il y a équivalence entre :*

1. *$A \wedge B = 1$*
2. *$A$ et $B$ n'ont pas de racine commune dans $\mathbb{C}$.*

### 5.1.3 Polynôme conjugué

**Définition 8.** *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, on définit le polynôme conjugué de $P$ noté de $\overline{P}$ par*

$$\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k.$$

**Proposition 19.** *L'application $P \mapsto \overline{P}$ est une application $\mathbb{R}$-linéaire de $\mathbb{C}[X]$ dans $\mathbb{C}[X]$ vérifiant*

$$\forall P, Q \in \mathbb{C}[X], \qquad \overline{(PQ)} = \overline{P}\,\overline{Q}.$$

**Corollaire 7.** *Soient $P \in \mathbb{C}[X]$, $\alpha \in \mathbb{C}$ et $p \in \mathbb{N}$, il y a équivalence entre*

*(i) $\alpha$ est racine d'ordre $p$ de $P$.*

*(ii) $\overline{\alpha}$ est racine d'ordre $p$ de $\overline{P}$.*

## 5.2 Dans $\mathbb{R}[X]$

**Proposition 20.** *Tout polynôme $P$ de $\mathbb{R}[X]$ se factorise de manière unique à l'ordre près des facteurs sous la forme*

$$P = \lambda \prod_{k=1}^{m} (X - \alpha_k)^{n_k} \prod_{k=1}^{p} (X^2 + \beta_k X + \gamma_k)^{q_k},$$

*où les $\alpha_k$ sont des nombres réels 2 à 2 distincts, les $n_k$ des entiers naturels, les $(\beta_k, \gamma_k)$ sont des couples de nombres réels 2 à 2 distincts tel que $\beta_k^2 - 4\gamma_k < 0$, les $q_k$ des entiers naturels.*

**Corollaire 8.** *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.*

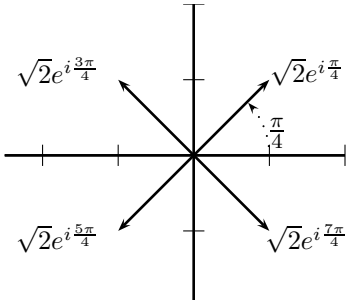
## 5.3 Méthode et exemples de factorisation

On factorisera le plus souvent d'abord sur $\mathbb{C}$, pour ensuite regrouper les racines conjugués pour obtenir.

**Exemples:**

1. Factorisons $Q = X^4 + 4$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

   On détermine les racines de $Q$ $\alpha^4 = -4 = 4e^{i\pi}$, soit $\alpha = \sqrt{2}e^{i\left(\frac{\pi}{4}+k\frac{\pi}{2}\right)}$ avec $k \in [\![0,3]\!]$.




   La factorisation dans $\mathbb{C}[X]$ est donc

$$X^4 + 4 = \left(X - \sqrt{2}e^{i\frac{\pi}{4}}\right)\left(X - \sqrt{2}e^{i\frac{3\pi}{4}}\right)\left(X - \sqrt{2}e^{i\frac{5\pi}{4}}\right)\left(X - \sqrt{2}e^{i\frac{7\pi}{4}}\right).$$

   En regroupant les racines conjuguées (le premier et le quatrième facteur, puis le deuxième et le troisième facteur), la factorisation dans $\mathbb{R}[X]$ est

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

2. Factorisons $Q_n = X^n - 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$, déduisons en la factorisation de $P_n = \sum_{k=0}^{n} X^k$.

   Les racines de $Q_n$ sont $e^{i\frac{2k\pi}{n}}$ avec $k \in [\![0, n-1]\!]$. On en déduit donc

$$Q_n = \prod_{k=0}^{n-1}\left(X - e^{i\frac{2k\pi}{n}}\right).$$

   Si $n(= 2p+1)$ est un nombre impair, il y a une seule racine réelle et on obtient en regroupant les racines conjugués :

$$Q_{2p+1} = (X-1)\prod_{k=1}^{p}\left(X^2 - 2\cos\left(\frac{2k\pi}{2p+1}\right)X + 1\right).$$

   Si $n(= 2p)$ est un nombre pair, il y a deux racines réelles et on obtient en regroupant les racines conjugués :

$$Q_{2p} = (X-1)(X+1)\prod_{k=1}^{p-1}\left(X^2 - 2\cos\left(\frac{k\pi}{p}\right)X + 1\right).$$

   Pour $P_n$ on remarque que $(X-1)P_n = Q_{n+1}$ et on en déduit que

$$P_n = \prod_{k=1}^{n}\left(X - e^{i\frac{2k\pi}{n+1}}\right).$$