# Algèbre-Premier semestre 2021

# Algèbre-Premier semestre 2021

## Thèmes

- Logique et raisonnement
- Ensembles
- Relations binaires
- Applications
- Nombres complexes
- Polynômes
- Fractions rationnelles

# Polynômes

**Note :** Dans ce chapitre nous travaillerons à la fois sur $\mathbb{R}$ et sur $\mathbb{C}$. Afin d'alléger l'écriture, nous utiliserons la lettre $\mathbb{K}$ pour désigner $\mathbb{R}$ ou $\mathbb{C}$. Ainsi une propriété ou une définition qui est valable à la fois sur $\mathbb{R}$ et sur $\mathbb{C}$ sera énoncée sur $\mathbb{K}$.

## Définition (Scalaire)

*On appelle* **scalaire** *un élément de* $\mathbb{K}$.

# Polynômes

## Définition (Polynôme)

*On appelle* **polynôme** *$P$ d'indéterminée $X$* **à coefficients dans** $\mathbb{K}$ *toute expression de la forme*

$$P = P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

*où*

- $n \in \mathbb{N}$, *et*
- $a_0, a_1, \cdots, a_n$ *sont des éléments de* $\mathbb{K}$. *On les appelle les* **coefficients du polynôme** $P$.

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

**Remarque : $X$ N'EST PAS UN NOMBRE !**
L'objet $X$ est un objet mathématique bien précis que l'on appelle indéterminée. Ce n'est ni une valeur ni une variable.

# Polynômes

Donnons quelques exemples de polynômes.

## Définition

*On appelle :*

- **Polynôme constant :** *Tout polynôme de la forme* $P(X) = a_0$ *avec* $a_0 \in \mathbb{K}$.
- **Polynôme unité** *: Le polynôme* $P(X) = 1$.
- **Polynôme nul** *: Le polynôme* $P(X) = 0$.
- **Monôme :** *Tout polynôme de la forme* $P(X) = a_k X^k,\ a_k \in \mathbb{K}$.

**Remarque :** Tous les coefficients du polynôme nul sont nuls. Réciproquement, tout polynôme ayant tous ses coefficients nuls est le polynôme nul.

# Polynômes

## Théorème (Égalité entre polynômes)

*Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux. C'est-à-dire*

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{m} b_k X^k \quad \Longleftrightarrow \quad m = n \text{ et } a_k = b_k,\ \forall k \in \mathbb{N},\ 0 \leq k \leq n.$$

*En particulier, un polynôme est nul si et seulement si tous ses coefficients sont nuls.*

**Remarque :** Si $P = \sum_{k=0}^{n} a_k X^k$
Si on choisit $m \in \mathbb{N}$.
On convient d'écrire $P = \sum_{k=0}^{m} a_k X^k$ en posant $a_k = 0$ pour $k = n+1, n+2, \cdots, m$.

# Polynômes

Sur l'ensemble de polynômes nous pouvons définir une **addition** et une **multiplication**.

## Définition

*Soient* $P(X) = \sum_{k=0}^{n} a_k X^k$ *et* $Q(X) = \sum_{k=0}^{m} b_k X^k$ *deux polynômes à coefficients dans* $\mathbb{K}$ *et* $\lambda \in \mathbb{K}$.

- **Somme :** *On définit le polynôme* $P + Q$ *par*

$$(P+Q)(X) = \sum_{k=0}^{\max(m,n)} (a_k + b_k) X^k.$$

*en convenant que* $a_k = 0$ *si* $k > n$ *et* $b_k = 0$ *si* $k > m$.

# Polynômes

## Définition

- **Produit :** *On définit le polynôme $P \cdot Q$ par*

$$(P \cdot Q)(X) = \sum_{k=0}^{m+n} c_k X^k \quad \text{où} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

  *en convenant que $a_k = 0$ si $k > n$ et $b_k = 0$ si $k > m$.*
- **Multiplication par $\lambda$ :** *On définit le polynôme $\lambda P$ par*

$$(\lambda P)(X) = \sum_{k=0}^{n} \lambda a_k X^k.$$

# Polynômes

**Exemples :** Considérons les polynômes

$$P(X) = 1 - 2X - X^3 \quad \text{et} \quad Q(X) = 1 + X^2.$$

Alors

$$\begin{aligned} (P+Q)(X) &= 2 - 2X + X^2 - X^3. \\ (P \cdot Q)(X) &= 1 - 2X + X^2 - 3X^3 - X^5. \end{aligned}$$

# Polynômes

Introduisons une dernière opération sur l'ensemble de polynômes.

## Définition (Composition)

*Soient $P(X)=\sum_{k=0}^{n} a_k X^k$ et $Q(X)=\sum_{k=0}^{m} b_k X^k$ deux polynômes à coefficients dans $\mathbb{K}$.*

- **Composée de deux polynômes :** *On définit le polynôme composé $P\circ Q$ par*

$$(P\circ Q)(X)=\sum_{k=0}^{n} a_k Q(X)^k.$$

**Exemple :**

$$\begin{aligned}
(1+X^2)\circ(-2+X) &= 1+(-2+X)^2=5-4X+X^2.\\
(-2+X)\circ(1+X^2) &= -2+(X^2+1)=-1+X^2.\\
(1+X+X^2)\circ(1+X^3) &= 1+(X^3+1)+(X^3+1)^2=3+2X^3+X^6.
\end{aligned}$$

# Polynômes

Étudions quelques propriétés de l'addition :

## Théorème

*L'addition dans* $\mathbb{K}[X]$ *est :*

- **associative** *: Pour tout polynôme* $P,\ Q,\ R \in \mathbb{K}[X]$

$$(P+Q)+R = P+(Q+R);$$

- **commutative** *: Pour tout polynôme* $P,\ Q \in \mathbb{K}[X]$

$$P+Q = Q+P;$$

- **admet pour élément neutre le polynôme nul** *: Pour tout polynôme* $P \in \mathbb{K}[X]$

$$0+P = P+0 = P.$$

## Démonstration.

À vous de vérifier. □

# Polynômes

Étudions quelques propriétés du produit :

## Théorème

*Le produit dans* $\mathbb{K}[X]$ *est :*

- **associative** *: Pour tout polynôme* $P,\ Q,\ R \in \mathbb{K}[X]$

$$(P \cdot Q) \cdot R = P \cdot (Q \cdot R);$$

- **commutative** *: Pour tout polynôme* $P,\ Q \in \mathbb{K}[X]$

$$P \cdot Q = Q \cdot P;$$

- **admet pour élément neutre le polynôme unité** *: Pour tout polynôme* $P \in \mathbb{K}[X]$

$$1 \cdot P = P \cdot 1 = P.$$

## Démonstration.

À vous de vérifier. □

# Degré d'un polynôme

Attaché à chaque polynôme on a l'important notion de degré.

## Définition (Degré d'un polynôme)

*Soit* $P = \sum_{k=0}^{n} a_k X^k$ *un polynôme non nul de* $\mathbb{K}[X]$. *On appelle* **degré du polynôme** $P$ *le plus grand entier* $k$ *tel que*

$$a_k \neq 0.$$

*On note cet entier* $\deg(P)$ *et on dit que :*

- $a_k$ *est le* **coefficient dominant** *de* $P$. *Autrement dit, le coefficient dominant, est le* **coefficient du monôme de plus haut degré** *de* $P(X)$.
- $P$ *est* **unitaire** *(ou normalisé) si son* **coefficient dominant** *est égal à 1.*

**Remarque :** Par convention, le polynôme nul est de degré $-\infty$ :

$$deg(0) = -\infty.$$

**Exemple :**

- $X^{1515} - 1$ est un polynôme unitaire, de degré 1515.
- $3X^5 + 2X^4 - 2x + 1$ est un polynôme de degré 5 , de coefficient dominant 3.
- $5 + 17X + 30X^4 + 6X^7$ est un polynôme de degré 7 , de coefficient dominant 6.

# Degré d'un polynôme

Le degré satisfait les propriétés suivantes.

## Théorème

*Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$. Alors*

- $\deg(P+Q) \leq \max(\deg(P); \deg(Q))$.
- $\deg(P \cdot Q) = deg(P) + deg(Q)$.
- *Pour tout* $\lambda \in \mathbb{K}^*$, $deg(\lambda P) = deg(P)$.
- *Si* $\deg(Q) \geq 1$, $deg(P \circ Q) = \deg(P) \cdot \deg(Q)$.

## Démonstration.

Soient

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

avec $a_n \neq 0$ et $b_m \neq 0$.
Alors $\deg P = n$ et $\deg Q = m$ (on vérifiera sans difficulté que toutes ces propriétés restent vraies dans le cas ou un des 2 polynômes est nul)...

...*à suivre* ...

# Degré d'un polynôme

## Démonstration.

Soient

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

avec $a_n \neq 0$ et $b_m \neq 0$.

Alors $\deg P = n$ et $\deg Q = m$ (on vérifiera sans difficulté que toutes ses propriétés restent vraies dans le cas où l'un des 2 polynômes est nul).

- $\deg(\mathrm{P} + \mathrm{Q}) \leq \max(\deg(\mathrm{P}), \deg(\mathrm{Q}))$ :
  Pour tout $k > \max(m, n)$, on a

$$a_k = b_k = 0 \quad \Longrightarrow \quad a_k + b_k = 0.$$

Ainsi $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.

□

# Degré d'un polynôme

**Démonstration.**

- $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ : Le terme de plus haut degré de $P \cdot Q$ est

$$(a_n \cdot b_m)X^{n+m}.$$

  Ainsi $\deg(P \cdot Q) = m + n$.
- Si $\deg(Q) \geq 1$, $\deg(P \circ Q) = \deg(P) \cdot \deg(Q)$ : Supposons $\deg(Q) \geq 1$. On a par définition

$$P \circ Q(X) = a_0 + a_1 Q(X) + \cdots + a_n Q(X)^n.$$

  Maintenant, le point précédent nous permet de conclure que pour tout $0 \leq k \leq n$, on a

$$\deg(Q^k) = k \deg(Q).$$

  Ainsi, le terme de plus haut degré de $P \circ Q$ est $a_n Q(X)^n$. D'où on conclut

$$\deg(P \circ Q) = \deg(a_n Q(X)^n) = n \cdot deg(Q) = \deg(P) \cdot \deg(Q).$$

# Degré d'un polynôme

**Exemple d'inégalité stricte :** $\deg(P+Q) < \max(\deg P, \deg Q)$ :
Soit

$$P = X^3 - X + 2 \quad \text{et} \quad Q = -X^3 + X^2.$$

Alors

$$(P+Q)(X) = X^2 - X + 2 \implies \deg(P+Q) = 2 < 3 = \max(\deg P, \deg Q).$$

**Remarque :** Si $\deg(P) \neq \deg(Q)$, alors

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

# Degré d'un polynôme

En utilisant les propriétés du degré, on peut facilement montrer la proposition suivante.

## Proposition

*Le produit de deux polynômes non nuls est non nul. Autrement dit :*

$$\forall\ P,\ Q \in \mathbb{K}[X], \quad P \cdot Q = 0 \implies P = 0 \quad \textit{ou} \quad Q = 0.$$

## Démonstration.

$$\begin{aligned} P \cdot Q = 0 &\implies \deg P + \deg Q = \deg(P \cdot Q) = -\infty \\ &\implies \deg P = -\infty \ \text{ ou } \ \deg Q = -\infty \\ &\implies P = 0 \ \text{ ou } \ Q = 0. \end{aligned}$$

□

# Dérivation de Polynômes

Une autre opération que on peut définir sur l'ensemble des polynômes, c'est la dérivation.

## Définition (Polynôme dérivé)

*Soit* $P = \sum_{k=0}^{n} a_k X^k$ *un polynôme dans* $\mathbb{K}[X]$.
*On appelle* **dérivée (formelle)** *du polynôme* $P$, *le polynôme* $P'$ *défini par*

$$P'(X) = \begin{cases} 0 & \text{si } \deg(P) \leq 0 \\ \sum_{k=1}^{n} k a_k X^{k-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} & \text{si } \deg(P) > 0. \end{cases}$$

*On définit par itération les polynômes dérivés successifs de* $P$ *par*

$$\begin{aligned} P^{(0)} &= P \\ P^{(k)} &= \left(P^{(k-1)}\right)' \text{ pour tout } k \geq 1. \end{aligned}$$

# Dérivation de Polynômes

**Exemple :** Soit $P = 5X^3 + X^2 - 7X + 3$. Alors les dérivées successives de $P$ sont :

$$\begin{aligned} P^{(0)}(X) &= 5X^3 + X^2 - 7X + 3 \\ P^{(1)}(X) &= 15X^2 + 2X - 7 \\ P^{(2)}(X) &= 30X + 2 \\ P^{(3)}(X) &= 30 \\ P^{(k)}(X) &= 0, \quad \forall k \geq 4. \end{aligned}$$

# Dérivation de Polynômes

Étudions quelques propriétés de la dérivation.

## Proposition

*Soit $P$ un polynôme dans $\mathbb{K}[X]$. Alors, si $\deg(P) \geq 1$, on a*

$$\deg(P') = \deg(P) - 1.$$

Cela vient tout simplement de la définition de la dérivée. À vous de vérifier.

## Théorème

*Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$.*

- *On a $P' = 0 \iff P$ est constant.*
- $(P + Q)' = P' + Q'$.
- *Pour tout $\lambda \in \mathbb{K}$, $(\lambda P)' = \lambda P'$.*
- $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$.
- $(P \circ Q)' = Q' \cdot (P' \circ Q)$.

## Démonstration.

Cela vient aussi tout simplement des définitions des sommes et produits. À vous de vérifier. □

# Dérivation de Polynômes

Un raisonnement par récurrence, nous permet de traduire le théorème précédent au cas de dérivées d'ordre supérieur.

## Théorème

*Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$.*

- *Si $\deg(P) = n$, alors $P^{(k)} = 0$ pour tout $k > n$.*
- *Pour tout $\lambda,\ \mu \in \mathbb{K}$ et $n \in \mathbb{N}$*

$$(\lambda P + \mu Q)^{(k)} = \lambda P^{(k)} + \mu Q^{(k)}.$$

- **Formule de Leibniz** *: Pour tout $n \in \mathbb{N}$*

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

# Divisibilité dans $\mathbb{K}[X]$

L'ensemble des polynômes $\mathbb{K}[X]$ dispose des propriétés similaires de celles de l'ensemble des entiers relatifs.
Sur $\mathbb{K}[X]$ on peut parler de la notion importante de divisibilité.

## Définition (Divisibilité)

*Soient* $A, B \in \mathbb{K}[X]$.
*On dit que* $A$ **divise** $B$ *ou que* $B$ *est un* **multiple** *de* $A$ *s'il existe* $Q \in \mathbb{K}[X]$ *tel que :*

$$B = A \cdot Q.$$

*Si* $A$ **divise** $B$ *on note*

$$A|B.$$

*Le polynôme* $A$ *est appelé* **diviseur** *de* $B$ *et* $B$ *un* **multiple** *de* $A$.

# Divisibilité dans $\mathbb{K}[X]$

**Remarques :**

- Un polynôme $P(X)$ non nul est divisible par les polynômes $\lambda$ et $\lambda P(X)$ avec $\lambda \in \mathbb{K}^*$. En effet, pour tout $\lambda \in \mathbb{K}^*$, nous avons

$$P(X) = \lambda \cdot (\lambda^{-1} P(X)) \quad \text{et} \quad P(X) = (\lambda P(X)) \cdot \lambda^{-1}.$$

- Réciproquement, un polynôme de degré 0 (polynôme constant et non nul) divise tous les polynômes. En effet, pour tout $\lambda \in \mathbb{K}^*$ et pour tout $P(X) \in \mathbb{K}[X]$, nous avons

$$P(X) = \lambda \cdot (\lambda^{-1} P(X)).$$

- Tout polynôme divise le polynôme nul. En effet, pour tout $P(X) \in \mathbb{K}[X]$, nous avons $0 = P(X) \cdot 0$.

# Divisibilité dans $\mathbb{K}[X]$

Étudions quelques propriétés de la division.

## Proposition

*Soit $A$, $B$, $C$ et $D$ des polynômes dans $\mathbb{K}[X]$. On a alors :*

- $$\forall\ P, Q \in \mathbb{K}[X] \quad D|A \text{ et } D|B \quad \Longrightarrow \quad D|P \cdot A + Q \cdot B$$
- $$A|B \text{ et } C|D \quad \Longrightarrow \quad A \cdot C|B \cdot D.$$
- $$\forall k \in \mathbb{N}, A|B \quad \Longrightarrow \quad A^k|B^k.$$

## Démonstration.

Appliquer les définitions □

# Divisibilité dans $\mathbb{K}[X]$

**Proposition**

*Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls. Alors :*

$$A|B \text{ et } B|A \iff \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B$$

*On dit alors que $A$ et $B$ sont des* **polynômes associés**.

**Démonstration.**

On raisonne par double implication :

- $\Longleftarrow$: Immédiat
- $\Longrightarrow$:Si $A|B$ et $B|A$, alors il existe $C,\ D \in \mathbb{K}[X]$ tels que :

$$B = A \cdot C \quad \text{et} \quad A = B \cdot D.$$

Ainsi

$$\deg B = \deg A + \deg C \geq \deg A \quad \text{et} \quad \deg A = \deg B + \deg D \geq \deg B.$$

D'où on conclut que $\deg A = \deg B \implies \deg D = \deg C = 0$. Par conséquent, $D$ est un polynôme constant $D = \lambda \in \mathbb{K}^*$ et $A = \lambda B$.

□

# Divisibilité dans $\mathbb{K}[X]$

**Proposition**

*Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$. Alors*

$$P \cdot Q = 1$$

*si et seulement si $P$ et $Q$ sont des constantes inverses l'une de l'autre.*

**Démonstration.**

- $\Longleftarrow$: Immediat.
- $\Longrightarrow$ : Si $P \cdot Q = 1$, alors

$$0 = \deg(P \cdot Q) = \deg(P) + \deg(Q) \quad \Longrightarrow \quad \deg(P) = \deg(Q) = 0.$$

D'où on conclut que

$$P = \lambda \quad \text{et} \quad Q = \lambda'.$$

Or $\lambda\lambda' = 1$. Ce qui implique $\lambda' = \lambda^{-1}$.

□

**Remarque :** Cela veut dire qu'un polynôme non nul n'est pas forcément inversible. Les seuls polynômes inversibles sont les constantes non nulles.

# Divisibilité dans $\mathbb{K}[X]$

**Théorème (Division euclidienne)**

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

$$A = BQ + R, \quad \deg(R) < \deg(B).$$

*Les polynômes $Q$ et $R$ sont appelés le* **quotient** *et le* **reste** *dans la division euclidienne de $A$ par $B$.*

# Divisibilité dans $\mathbb{K}[X]$

## Démonstration.

Soit

$$E = \{A(X) - B(X)Q(X) \in \mathbb{K}[X]\}$$

Soit

$$D = \{deg(R), R \in E\}$$

- Si $B|A$ alors la division euclidenne existe. En effet

$$A = BQ + R \text{ avec } R = 0 \text{ et } deg(R) < deb(B)$$

  car $deg(R) = -\infty$
- Sinon, $min(D) > 0$.
  D étant un sous ensemble de $\mathbb{N}$, il admet un plus petit élément $r$ qui correspond à un polynôme $R$ et un certain polynôme $Q$.

# Divisibilité dans $\mathbb{K}[X]$

**Démonstration.**

Montrons que $deg(R) < deg(B)$
**Par l'absurde :** supposons $deg(B) \geq deg(R)$
Soit $a_r X^r$ le monôme dominant de R et $b_m X^m$ le monôme dominant de B.
On a

$$R(X) = a_r X^r + \sum_{i=0}^{r-1} a_i X^i \text{ et } B(X) = b_m X^m + \sum_{i=0}^{m-1} b_i X^i$$

On pose

$$\begin{aligned} R'(X) &= R(X) - \frac{a_r}{b_m} X^{r-m} B(X) \\ &= a_r X^r + \sum_{i=0}^{r-1} a_i X^i - \frac{a_r}{b_m} X^{r-m} \left( b_m X^m + \sum_{i=0}^{m-1} b_i X^i \right). \\ &= \sum_{i=0}^{r-1} a_i X^i - \sum_{i=0}^{m-1} \frac{a_r b_i}{b_m} X^{i+r-m} \end{aligned}$$

Donc $deg(R') < r$ on a donc $A(X) - B(X)\left(Q(X) + \frac{a_r}{b_m} X^{r-m}\right) = R'(X)$
ce qui **contredit** le fait que $r$ était le minimum de D.
On a bien $deg(B) < deg(R)$

□

# Divisibilité dans $\mathbb{K}[X]$

Démonstration.

**Unicité**

- Si $deg(B) = 0$ alors $\exists \lambda \in \mathbb{K}, B(X) = \lambda$ et donc

$$A = B(X)Q(X) + R(X) \text{ avec } Q = \frac{1}{\lambda}A \text{ et } R = 0$$

- Si $deg(B) > 0$, supposons que

$$A(X) = B(X)Q(X) + R(X) = B(X)Q'(X) + R'(X)$$

avec $deg(R) < deg(B)$ et $deg(R') < deg(B)$.
Alors

$$B(X)(Q(X) - Q'(X)) = R(X) - R'(X)$$

donc

$$deg(R - R') = deg(B) + deg(Q - Q')$$

or $deg(R - R') \leq max(deg(R), deg(R')) < deg(B)$
L'égalité n'est possible que si $R = R'$ et $Q = Q'$

Il y donc bien unicité dans les deux cas. □

# Divisibilité dans $\mathbb{K}[X]$

**Exemple :** Faisons la division euclidienne de $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ par $B = X^2 - X + 1$. Notons que on pose une division de polynômes comme on pose une division euclidienne de deux entiers. En effet

$$\begin{array}{rrrrrrrrrrr|l}
 & 2X^4 & - & X^3 & - & 2X^2 & + & 3X & - & 1 & X^2 - X + 1 \\
\cline{11-11}
- & 2X^4 & - & 2X^3 & + & 2X^2 & & & & & 2X^2{+}X\ {-}3 \\
\cline{1-9}
 & & & X^3 & - & 4X^2 & + & 3X & - & 1 & \\
 & & - & X^3 & - & X^2 & + & X & & & \\
\cline{3-9}
 & & & & & -3X^2 & + & 2X & - & 1 & \\
 & & & & - & -3X^2 & + & 3X & - & 3 & \\
\cline{5-9}
 & & & & & & & -X & + & 2 &
\end{array}$$

Alors on trouve

$$Q = 2X^2 + X - 3 \text{ (Quotient)} \quad \text{et} \quad R = -X + 2 \text{ (Reste)}.$$

On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.

# Divisibilité dans $\mathbb{K}[X]$

## Proposition

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

$A$ *divise* $B \iff$ *le reste de la division euclidienne de* $A$ *par* $B$ *est nul.*

## Démonstration.

- $\Longrightarrow$ : Si $A|B$, alors il existe $Q$ tel que $B = AQ$. Alors le couple $(Q, 0)$ satisfait la définition de la division euclidienne. Par unicité du reste de la division euclidienne pour les polynômes, on en déduit que ce reste est nul.
- $\Longleftarrow$ : Si le reste de la division euclidienne de $A$ par $B$ est nul, on obtient qu'il existe $Q \in \mathbb{K}[X]$ tel que

$$B = AQ + 0 = BQ.$$

Donc on a bien $A|B$.

# Évaluation polynomiale

## Définition (Fonction polynomiale)

*Soit* $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$. *Alors on définit*

$$P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k \qquad \textbf{(on évalue P en } \lambda\textbf{)}.$$

*La fonction*

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x) \end{array}$$

*est appelée* **fonction polynomiale** *associée au polynôme* $P$.

# Évaluation polynomiale

L'évaluation polynomiale nous permet d'exprimer les coefficients d'un polynôme à l'aide des dérivées successives.

## Théorème (Formule de Taylor en 0)

*Pour tout polynôme* $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ *de degré* $n \in \mathbb{N}$, *on a*

$$P(X) = P(0) + P^{(1)}(0)X + \frac{P^{(2)}(0)}{2!}X^2 + \cdots + \frac{P^{(n)}(0)}{n!}X^n$$

*Ce qui revient à*

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

*C'est-à-dire*

$$a_k = \frac{P^{(k)}(0)}{k!}.$$

# Racines d'un polynôme

Nous pouvons généraliser la formule de Taylor à tout $a \in \mathbb{K}$.

## Théorème (Formule de Taylor en $a \in \mathbb{K}$)

*Pour tout polynôme $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$ et $a \in \mathbb{K}$, nous avons :*

$$P(X) = P(a) + P^{(1)}(a)(X-a) + \frac{P^{(2)}(a)}{2!}(X-a)^2 + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n$$

*Ce qui revient à*

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

# Racines d'un polynôme

Étudions les points où un polynôme s'annule.

## Définition (Racines)

*Soit $P \in \mathbb{K}[X]$. On dit que $a \in \mathbb{K}$ est une* **racine** *(ou un* **zéro***) de $P$ si*

$$P(a) = 0.$$

**Exemple :**

- Tout polynôme de degré 1 a une racine :
  la racine de
  $$aX + b \texttt{ est } -\frac{b}{a}$$
  En effet
  $$a \cdot \left(-\frac{b}{a}\right) + b = 0$$
- L'existence de racines dépend de $\mathbb{K}$ :
  par exemple $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$,
  il a les racines $+i$ et $-i$ dans $\mathbb{C}$.

# Racines d'un polynôme

Donnons une characterization des racines d'un polynôme.

## Proposition

*Soit* $\alpha \in \mathbb{K}$ *et* $P \in K[X]$. *Alors*

$$\alpha \text{ est racine de } P \iff (X-\alpha)|P.$$

## Démonstration.

On raisonne par double implication :

- $\Longleftarrow$ : Supposons que $(X-\alpha)|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)Q(X)$. Alors on obtient :

$$P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0.$$

□

# Racines d'un polynôme

## Démonstration.

- $\Longrightarrow$: Supposons que $\alpha$ soit racine de $P$, et écrivons la division euclidienne de $P$ par $X-\alpha$ :

  il existe $Q,\ R \in \mathbb{K}[X]$ tels que :

  $$P(X) = (X-\alpha)Q(X) + R(X), \qquad \deg(R) < \deg(X-a) = 1.$$

  Ainsi $\deg(R) \leq 0$, et $R(X) = r \in \mathbb{K}$.

  On évalue alors l'égalité précédente en $\alpha$ :

  $$0 = P(\alpha) = (\alpha-\alpha)Q(\alpha) + r = r \quad \Longrightarrow \quad r = 0.$$

  Ainsi $P(X) = (X-\alpha)Q(X)$ et $(X-\alpha)$ divise $P$.

# Racines d'un polynôme

**Exemple :** Considérons le polynôme $P = X^3 - X + 6$.
On voit que $-2$ est racine de $P$ :

$$(-2)^3 + 2 + 6 = 0$$

Par la proposition précédente, $P$ se factorise par $(X + 2)$. Pour obtenir sa factorisation, on peut :

- soit écrire $P = (X + 2)(aX^2 + bX + c)$ et développer :

  $$aX^3 + (2a + b)X^2 + (2b + c)X + 2c$$

  et procéder par identification des coefficients

  $$1 = a \quad ; \quad 0 = 2a + b \quad ; \quad -1 = 2b + c \quad ; \quad 6 = 2c$$

- soit faire la division euclidienne de $P$ par $(X + 2)$ : le quotient correspond à l'autre facteur de la factorisation.

# Racines d'un polynôme

## Définition (Ordre de multiplicité)

*Soit $P(X) \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$.*
*On dit que $\alpha$ est une racine* **d'ordre** *$m$ (ou de* **multiplicité** *$m$) de $P$ si :*

- *$P$* **est divisible** *par $(X-\alpha)^m$, et*
- *$P$* **n'est pas divisible** *par $(X-\alpha)^{m+1}$.*

**Remarque** : Puisque $(X-\alpha)^m$ divise $P(X)$ nous avons $m \leq deg(P)$.
Donc $1 \leq m \leq \deg(P)$.

# Racines d'un polynôme

Donnons une caractérisation de l'ordre de multiplicité à l'aide de la dérivation.

## Proposition

*Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a l'équivalence entre :*

- $(X-\alpha)^m$ *divise* $P$,
- $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$.

*Si l'une de ces conditions est satisfaite, on dit alors que $\alpha$ est racine de $P$ de* **multiplicité au moins** *$m$.*

## Démonstration.

C'est une conséquence directe de la formule de Taylor. À vérifier. □

**Exemple :** Considérons $P = X^5 - 7X^4 + 19X^3 - 25X2 + 16X - 4$.
On a

$$P(1) = P'(1) = P''(1) = 0.$$

Donc 1 est racine de $P$ de multiplicité au moins 3. Ainsi

$$(X-1)^3 \quad \text{divise} \quad X^5 - 7X^4 + 19X^3 - 25X2 + 16X - 4.$$

# Racines d'un polynôme

Comme corollaire du résultat précédent on a :

**Théorème**

*Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors $\alpha$ est une racine* **de multiplicité** *$m$ de $P(X)$ si et seulement si*

$$P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \quad \textit{et} \quad P^{(m)}(\alpha) \neq 0.$$

**Démonstration.**

Cela découle tout simplement de la définition de la multiplicité d'une racine et de la proposition précédente. □

**Vocabulaire :**

- Lorsque $m \geq 2$, on parle de racine multiple.
- Les racines d'ordre 1,2,3 de $P$ sont respectivement appelés racines simples, doubles, triples de $P$.

**Exemple :** Considérons toujours $P = X^5 - 7X^4 + 19X^3 - 25X2 + 16X - 4$. On a

$$P(1) = P'(1) = P''(1) = 0 \quad \text{et} \quad P^{(3)}(1) = 6$$

Donc 1 est racine de $P$ de multiplicité 3 exactement.

# Racines d'un polynôme

Étudions le nombre possible de racines d'un polynôme.

## Proposition

*Soit $P \in \mathbb{K}[X]$, et $\alpha_1,\ \alpha_2\ \cdots,\ \alpha_p$, $p$ racines distincts de $P$. Alors*

$$(X-\alpha_1)\cdot(X-\alpha_2)\cdot\ \cdots\ \cdot(X-\alpha_p) \quad \textit{divise} \quad P.$$

# Racines d'un polynôme

Comme conséquence de cette proposition, on obtient les deux théorèmes suivants.

**Théorème**

*Un polynôme de degré $n \in \mathbb{N}$ a au plus $n$ racines distinctes.*

**Démonstration.**

Soit $P$ un polynôme et supposons que $P$ admette $p$ racines distinctes $\alpha_1, \cdots, \alpha_p$.
D'après la proposition précédente, il existe alors $Q \in \mathbb{K}[X]$ tel que :

$$P(X) = (X - \alpha_1) \cdot \cdots \cdot (X - \alpha_p) Q(X).$$

En prenant les degrés dans cette égalité, on en déduit que

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

et donc $p \leq \deg(P) = n$. □

# Racines d'un polynôme

**Théorème**

*Le seul polynôme qui possède une infinité de racines est le polynôme nul.*

**Démonstration.**

C'est une conséquence directe de la proposition précédente :
si $P$ est non nul, il n'a qu'un nombre fini de racines. □

**Remarque** :

- Un polynôme de degré $n$, ayant au moins $n+1$ racines est le polynôme nul.

# Racines d'un polynôme

Si on compte les racines avec leur multiplicité alors on a :

**Théorème**

*Soit $P \in \mathbb{K}[X]$, et $\alpha_1,\ \alpha_2\ \cdots,\ \alpha_p$, $p$ racines distincts de $P$ de multipicité respectives $m_1,\ m_2, \cdots,\ m_p$. Alors*

$$(X-\alpha_1)^{m_1} \cdot (X-\alpha_2)^{m_2} \cdot \ \cdots\ \cdot (X-\alpha_p)^{m_p} \quad \textit{divise} \quad P.$$

Comme conséquence de cette proposition, on a le résultat suivant.

**Corollaire**

*Un polynôme de degré $n$ a au plus $n$ racines comptées avec leurs ordres de multiplicité.*

# Décomposition en facteurs irréductibles

Étudions comme un polynôme se décompose en produit de polynômes plus simples (i.e. de dégre inférieur)

## Définition (Polynôme irréductible)

*Soit* $P(X) \in \mathbb{K}[X]$.
*On dit que* $P(X)$ *est* **irréductible** *s'il satisfait :*

- $\deg P \geq 1$.
- *les seuls diviseurs de* $P$ *sont les polynômes :*

$$\lambda \quad \text{et} \quad \lambda P(X), \quad \text{avec } \lambda \in \mathbb{K}^*.$$

*C'est-à-dire les polynômes constants non nuls et les polynômes associés à* $P(X)$.

*Autrement dit,* $P(X)$ *est* **irréductible** *sur* $\mathbb{K}$ *s'il satisfait :*

$$A,\ B \in \mathbb{K}[X],\ P(X) = A(X)B(X) \implies \deg(A) = 0 \ \text{ ou } \ \deg(B) = 0.$$

**Remarque :** Les polynômes de degré 1 sont irréductibles.

# Racines d'un polynôme

**Théorème**

*Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 se décompose de manière unique en produit d'une constante non nulle et de polynômes irréductibles unitaires à l'ordre des facteurs près.*

**Définition (Polynôme Scindé)**

*On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré supérieur ou égal à 1 est* **scindé** *s'il peut être écrit comme un produit de polynômes de degré 1 de $\mathbb{K}[X]$.*

# Décomposition en facteurs irréductibles

**Remarque :**

- Les polynômes de degré 1 sont irréductibles.
- Un polynôme $P \in \mathbb{K}[X]$ est scindé et irréductible sur $\mathbb{K}$ si et seulement si $\deg(P) = 1$.
- Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$ puisqu'il peut s'écrire :

$$X^2 + 1 = (X - i)(X + i).$$

La décomposition d'un polynôme dépend de $\mathbb{K}$. Nous allons donc distinguer les décompositions sur $\mathbb{C}[X]$ et sur $\mathbb{R}[X]$.

# Décomposition dans $\mathbb{C}[X]$

**Théorème (Théorème de d'Alembert-Gauss)**

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

La démonstration est difficile. Le théorème sera admis dans ce cours.

# Décomposition dans $\mathbb{C}[X]$

**Proposition**

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

**Démonstration.**

Montrons par récurrence la propriété $\mathscr{P}(n)$ pour $n \in \mathbb{N}$ :

Tout polynôme de $\mathbb{C}[X]$ de degré $n$ est scindé

- **Initialisation** : Si $\deg P = 1$, alors $P$ est scindé par définition, donc $\mathscr{P}(1)$ est vraie.

# Décomposition dans $\mathbb{C}[X]$

## Démonstration.

- **Hérédité** : Soit $n \in \mathbb{N}$ et supposons $\mathscr{P}(n)$ vraie.
  Soit $P$ de degré $n+1$. D'après le **Théorème de d'Alembert Gauss**, $P$ admet au moins une racine $\alpha \in \mathbb{C}$. Alors $(X-\alpha)$ divise $P$ et il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-\alpha)Q(X)$. Or $\deg(Q) = n$ et par hypothèse de récurrence, $Q$ est scindé :

$$Q = \lambda(X-\alpha_1)\cdot\cdots\cdot(X-\alpha_n).$$

  Ainsi $P = \lambda(X-\alpha)(X-\alpha_1)\cdot\cdots\cdot(X-\alpha_n)$ est scindé, et $\mathscr{P}(n+1)$ est vraie. On conclut par principe de récurrence.

□

# Décomposition dans $\mathbb{C}[X]$

## Proposition

1. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
2. *Tout polynôme $P$ de $\mathbb{C}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{C}[X]$ sous la forme :*

$$P(X) = \lambda(X-\alpha_1)^{m_1} \cdot (X-\alpha_2)^{m_2} \cdot \ \cdots \ \cdot (X-\alpha_k)^{m_k}.$$

## Démonstration.

1. On a déjà vu que les polynômes de degré 1 sont irréductibles. Réciproquement, soit $P$ un polynôme irréductible. Par le **Théorème de d'Alembert Gauss**, il existe $\alpha$ tel que $P(\alpha) = 0$. Il existe donc $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$. Comme de plus $P$ est irréductible, on en déduit que $Q \in \mathbb{K}^*$ et que $P$ est de degré 1.
2. Soit $P$ un polynôme de degré supérieur ou égal à 1 de $\mathbb{C}[X]$. D'après la proposition précédente, $P$ est **scindé** sur $\mathbb{C}[X]$, d'où l'existence d'une telle factorisation.

# Décomposition dans $\mathbb{R}[X]$

Passons maintenant à la décomposition dans $\mathbb{R}[X]$. Commençons introduite le résultat suivant :

**Lemme**

*Soit $P(X) \in \mathbb{R}[X]$. Si on considère $P(X)$ comme un polynôme de $\mathbb{C}[X]$ et que $\alpha \in \mathbb{C} \setminus \mathbb{R}$ est une racine de $P(X)$ alors $\overline{\alpha}$ est aussi une racine complexe de $P(X)$ avec même multiplicité.*

**Démonstration.**

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$. Puisque les coefficients de $P$ sont réels, nous pouvons écrire

$$0 = P(\alpha) \quad \Longrightarrow \quad 0 = \overline{P(\alpha)}$$

On a donc

$$\begin{aligned} P(\overline{\alpha}) &= \sum_{k=0}^{n} a_k \overline{\alpha}^k = \sum_{k=0}^{n} \overline{a_k} \cdot \overline{\alpha}^k \\ &= \overline{\left( \sum_{k=0}^{n} a_k \alpha^k \right)} = 0 \end{aligned}$$

Donc $\overline{\alpha}$ est une racine. □

# Décomposition dans $\mathbb{R}[X]$

À l'aide du lemme précédent nous pouvons donner la décomposition dans $\mathbb{R}[X]$.

## Théorème

1. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont*
   - *les polynômes de degré 1 ;*
   - *les polynômes de degré 2 à* **discriminant strictement négatif**.
2. *Tout polynôme $P$ de $\mathbb{R}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{R}[X]$ sous la forme :*

$$P(X) = \lambda \left( \prod_{k=1}^{p} (X - \alpha_k)^{m_k} \right) \left( \prod_{k=1}^{q} (X^2 + \beta_k X + \gamma_k)^{n_k} \right).$$

# Somme et produit des racines d'un polynôme

On finit le chapitre avec le résultat suivant.

## Proposition (Somme et produit des racines d'un polynôme scindé)

*Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme scindé, $\alpha_1,\ \alpha_2\ \cdots,\ \alpha_n$, ses racines (distinctes ou non). Alors*

$$\begin{aligned} \alpha_1 + \alpha_2 + \cdots + \alpha_n &= -\frac{a_{n-1}}{a_n}. \\ \alpha_1 \cdot \alpha_2 \cdot\ \cdots\ \cdot \alpha_n &= (-1)^n \frac{a_0}{a_n}. \end{aligned}$$

**Remarque :** En particulier, pour $n = 2$ et $P(X) = c + bX + aX^2$, nous avons :

$$\begin{aligned} \alpha_1 + \alpha_2 &= -\frac{b}{a} \\ \alpha_1 \cdot \alpha_2 &= \frac{c}{a} \end{aligned}$$