# Chapitre 15

# Polynômes à une indéterminée

## Sommaire

OBJECTIFS

à la fin du chapitre, vous devrez savoir :

- ▷ effectuer une division euclidienne de polynômes
- ▷ déterminer l'ordre de multiplicité d'une racine d'un polynôme
- ▷ utiliser les liens entre divisibilité et racines d'un polynôme
- ▷ utiliser les liens entre coefficients et racines d'un polynôme scindé
- ▷ déterminer le PGCD et le PPCM de deux polynômes
- ▷ déterminer la décomposition primaire d'un polynôme

## Introduction

Au chapitre Nombres Complexes, nous avons vu quelques exemples de résolutions d'équations polynomiales du type

$$P(z) = 0 \tag{15.1}$$

La tactique générale consiste à faire baisser le degré, en utilisant

— un changement d'inconnue, (par exemple en *posant* $Z = z^2$, etc ...)

— une factorisation $P = Q \times R$ du polynôme $P$.

Dans ce chapitre, nous étudierons particulièrement ce deuxième point de vue en précisant les liens entre racines d'un polynôme et factorisations. Dans cette optique, l'idéal est d'arriver à obtenir une équation "*produit nul*" entièrement scindée, c'est-à-dire une équation du type :

$$(x - \alpha_1)^{r_1} \cdot \cdots \cdot (x - \alpha_p)^{r_p} = 0,$$

où $r_1 + r_2 + \cdots + r_p = n$ puisque dans ce cas, les solutions sont simplement $\alpha_1, \alpha_2, \ldots, \alpha_p$.

## I Structure algébrique de $\mathbf{K}[\mathrm{X}]$

### Motivations

Notons dans tout le chapitre $\mathbf{K}$ pour $\mathbf{R}$ ou $\mathbf{C}$. Nous avons déjà introduit les *fonctions polynomiales* sur $\mathbf{K}$. Pour la convenance du lecteur, j'en rappelle ici la définition :

**Définition :** *Une* ***fonction*** $p : \mathbf{K} \to \mathbf{K}$ *est dite* ***polynomiale*** *s'il existe un entier* $n \in \mathbf{N}$ *et* $(a_0, a_1, \ldots, a_n) \in \mathbf{K}^{n+1}$ *un* $n+1$*-uplet de nombres réels ou complexes tels que :*

$$\forall x \in \mathbf{K}, \quad p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

*Les nombres* $a_0, a_1, \ldots, a_n$ *sont appelés les* ***coefficients*** *de* $p$.

La remarque suivante est le fondement de l'étude des polynômes :

Deux fonctions polynomiales $p$ et $q$ sont égales *si et seulement si*elles ont mêmes coefficients.

Les fonctions polynomiales sont donc très particulières. En général, pour prouver l'égalité de deux fonctions $f$ et $g$ définies sur un intervalle $I$ de $\mathbf{R}$, il faut prouver une infinité d'égalités :

$$\forall x \in I, \qquad f(x) = g(x).$$

Dans le cas de deux fonctions polynomiales $p$ et $q$, l'égalité d'un nombre fini de coefficients suffit.
Cette remarque peut s'interpréter en disant qu'une fonction polynôme est entièrement déterminée par la donnée de ses coefficients. Cela signifie que nous pouvons étudier non pas les *fonctions* polynomiales d'une *variable* $x \in \mathbf{K}$, mais directement la *liste des coefficients* $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$, nulle à partir d'un certain rang.

Une telle suite est appelée un polynôme à coefficients dans $\mathbf{K}$. Cette présentation nous laisse toute liberté de choix en ce qui concerne les ensembles de départ et d'arrivée. Cette définition est donc un peu plus générale que celle des fonctions polynomiales.

# 1 L'ensemble $\mathbf{K}[\mathbf{X}]$

## 1.a Polynômes à une indéterminée

Dans tout le chapitre $\mathbf{K}$ désigne $\mathbf{R}$ ou $\mathbf{C}$.

**Définition : *Polynôme à une indéterminée $X$ et à coefficients dans $\mathbf{K}$***
*On appelle polynôme à une indéterminée $X$ et à coefficients dans $\mathbf{K}$ toute expression de la forme*

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

*dans laquelle*

- *$n$ est un entier naturel,*
- *$a_0, a_1, \ldots, a_n \in \mathbf{K}$ sont des nombres réels ou complexes appelés les **coefficients de $P$**,*
- *$X$ est appelée l'**indéterminée**.*

**Notation :** *$\mathbf{K}[X]$ désigne l'ensemble des polynômes à coefficients dans $\mathbf{K}$ d'indéterminée $X$.*
*On note aussi $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ à la place de $P = a_0 + a_1 X + \cdots + a_n X^n$. Lorsqu'on ne souhaite pas préciser de rang $n$ à partir duquel tous les coefficients sont nuls, on note $P = \sum_{k=0}^{\infty} a_k x^k$.*

**Remarque :** du point de vue formel, un polynôme à coefficients dans $\mathbf{K}$ est une suite $(a_k)_{k\in\mathbf{N}} \in \mathbf{K}^{\mathbf{N}}$ à support fini, c'est-à-dire nulle à partir d'un certain rang.

**Exemples :**

1. Le **polynôme nul** est polynôme de coefficients tous nuls. On le note 0.
2. $P = (1-i)\ X^3 + 4\ X - 7\pi \in \mathbf{C}[X]$ est un polynôme à coefficients dans $\mathbf{C}$.
3. $Q = -e^4\ Y^8 + \sqrt[4]{29}\ Y^2 - Y - 1 \in \mathbf{R}[Y]$ est un polynôme à coefficients dans $\mathbf{R}$.

**Définition : Égalité de deux polynômes**

*Deux polynômes sont égaux s'ils ont mêmes coefficients.*

**Commentaires :** la seule différence entre les notions de polynôme et de fonction polynomiale réside en ceci que la **variable** $x \in \mathbf{K}$ est remplacée par l'**indéterminée** $X$ qui porte bien son nom puisqu'on ne sait même pas de quel ensemble elle est élément. Ainsi, au fil des chapitres, nous considérerons aussi bien des polynômes de nombres réels ou complexes, que des polynômes de *matrices*, ou bien encore d'*endomorphismes* !

## 1.b Degré d'un polynôme

**Définition : Degré d'un polynôme —.** *Soit $P \in \mathbf{K}[X]$ un polynôme. On appelle **degré** de $P$, le plus grand élément $k$ de $\mathbf{N} \cup \{-\infty\}$ tel que $a_k \neq 0$. On note $d^\circ P$ cet entier.*

- *Si $P \neq 0$, il s'écrit $P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$ et $d^\circ(P) = n$.*
- *Si $P = 0$, il a tous ses coefficients nuls et $d^\circ(P) = -\infty$.*

**Vocabulaire :** *Si $P$ est de degré $n \in \mathbf{N}$, $a_n$ est appelé le **coefficient dominant** et $a_n X^n$ est appelé le **monôme dominant**.*
*On dit qu'un polynôme $P$ est **constant** s'il est de degré négatif ou nul. Autrement dit s'il existe $a_0 \in \mathbf{K}$ tel que $P = a_0$.*

**Warning :** Lorsque nous écrivons $P = a_0 + a_1 X + \cdots + a_n X^n$, cela ne signifie pas que $P$ est de degré $n$, mais de **degré inférieur ou égal** à $n$.
Pour garantir que le degré d'un tel polynôme est exactement $n$, il faut s'assurer que $a_n$ est non nul.

**Notation :** *Dans la suite, nous désignerons par $\mathbf{K}_n[X]$ l'ensemble des polynômes de degré **inférieur ou égal à $n$**.*

**Remarque :** Dire que $P \in \mathbf{K}_n[X]$ signifie que tous les coefficients de $P$ de rangs strictement supérieurs à $n$ sont nuls.

### 1.c Fonction polynomiale associée

Comme indiqué plus haut, la différence entre fonction polynomiale et polynôme est subtile voire inutile dans bien des cas. Toutefois, lorsque nous voudrons insister sur cette différence, nous utiliserons la définition suivante :

**Définition :** *Soit $P \in \mathbf{K}[X]$ le polynôme défini par :*

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

*On appelle* ***fonction polynomiale associée*** *à $P$, la fonction $\tilde{P} : \mathbf{K} \to \mathbf{K}$ définie par*

$$\forall x \in \mathbf{K}, \quad \tilde{P}(x) = a_0 + a_1 x + \cdots + a_n x^n$$

**Exemple :** Je considère le polynôme $P(X) = (1-2i)X^3 + 2iX^2 - X + 1$. La fonction polynomiale associée est $\tilde{P} : \mathbf{C} \to \mathbf{C}$ qui à tout nombre complexe $z$ associe $\tilde{P}(z) = (1-2i)z^3 + 2iz^2 - z + 1$. Par exemple $\tilde{P}(1) = 1$.

**En pratique :** vous pouvez laisser tomber la notation $\tilde{}$, et noter également $P$ à la fois le polynôme et la fonction associée. Concrètement, "évaluer le polynôme $P$ au point 1", c'est remplacer l'*indéterminée* $X$ par 1.

## 2 Opérations algébriques dans $\mathbf{K}[X]$

### 2.a Addition des polynômes

L'ensemble $\mathbf{K}[X]$ est muni d'une addition interne, notée + définie par :

**Définition :** *Soit $P = \sum_{k=0}^{n} a_k \ X^k$ et $Q = \sum_{k=0}^{m} b_k \ X^k$ deux polynômes à coefficients dans $\mathbf{K}$. On définit le* ***polynôme somme*** *$P + Q$ par :*

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

**Commentaires :** dans cette définition nous avons posé $a_k = 0$ si $k > n$ et $b_k = 0$ si $k > m$.

**Proposition 15.1.— $\big(\mathbf{K}[X], +\big)$ est un groupe abélien**
Soit $(P, Q, R) \in \mathbf{K}[X]^3\big)$, alors

- L'addition est **commutative** : $P + Q = Q + P$.
- L'addition est **associative** : $(P + Q) + R = P + (Q + R)$.
- 0 est **élément neutre** de l'addition : $P + 0 = 0 + P = P$.
- $P$ possède un **opposé** : si $-P$ désigne le polynôme ayant pour coefficients les opposés de ceux de $P$, $P + (-P) = 0$.

**Exercice :** On considère dans $\mathbf{C}[X]$ les polynômes

$$P = 1 + X + 2X^2 + X^3, \quad Q = 2X^2 - X^3, \quad R = 7 + iX^3 + 2X^4$$

Explicitez $P + Q, P - Q$, $Q + R$ et déterminez leurs degrés.

**Proposition 15.2.— Degré d'une somme**
Soit $(P, Q) \in \mathbf{K}[X]^2$ deux polynômes à coefficients dans $\mathbf{K}$. Alors

- $d^\circ(P + Q) \leq \max\{d^\circ P, d^\circ Q\}$
- Si de plus $d^\circ P \neq d^\circ Q$, alors $d^\circ(P + Q) = \max\{d^\circ P, d^\circ Q\}$

**Commentaires :** la démonstration de cette proposition montre en réalité que le degré de $P + Q$ est **toujours** égal au **maximum** des degrés de $P$ et $Q$ **sauf** dans le cas particulier où les **monômes dominants** de ces deux polynômes sont **opposés**.

**Démonstration** ▽
Supposons sans perte de généralité que $d^\circ P \geq d^\circ Q$ et notons $P = \sum_{k=0}^{n} a_k\ X^k$ et $Q = \sum_{k=0}^{m} b_k\ X^k$ avec $n = d^\circ P$ et $m = d^\circ Q$. Par définition

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

Par conséquent, $d^\circ(P+Q) \leq \max\{d^\circ\ P, d^\circ\ Q\}$. Dans le cas particulier où $n > m$, observons que le dernier terme de cette somme est non nul. En effet, $a_n + b_n = a_n + 0 = a_n$ qui est différent de 0 puisque $n = d^\circ P$. *As a result, we get* $d^\circ(P+Q) = n = \max\{d^\circ\ P, d^\circ\ Q\}$. ▲

### 2.b Multiplication interne dans $\mathbf{K}[\mathbf{X}]$

L'ensemble $\mathbf{K}[X]$ est muni d'une multiplication interne, notée $\times$ définie par :

**Définition :** *Étant donnés deux polynômes* $P = \sum_{k=0}^{n} a_k\ X^k$ *et* $Q = \sum_{k=0}^{m} b_k\ X^k$*, à coefficients dans* $\mathbf{K}$*, on définit le* ***polynôme-produit*** $P \times Q$ *par :*

$$P \times Q = \sum_{k=0}^{n+m} c_k\ X^k, \quad \textit{où} \quad c_k = \sum_{i+j=k} a_i \times b_j = \sum_{i=0}^{k} a_i \times b_{k-i}$$

**Remarque :** l'addition des polynômes correspond simplement à ajouter coefficient par coefficient. La **multiplication des polynômes** est plus compliquée. Toutefois, elle est **parfaitement conforme à la multiplication des fonctions polynomiales associées** comme le montre l'exercice suivant.

**Exercice :** Soit $P(X) = 1 + X^2 + X^3$ et $Q(X) = 4 - 6X$ deux polynômes à coefficients réels. Notons $\tilde{P}$ et $\tilde{Q}$ les fonctions polynomiales associées.

1. Calculez $\tilde{P} \times \tilde{Q}$
2. Explicitez $P \times Q$.

**Proposition 15.3.— $\big(\mathbf{K}[X], +, \times\big)$ est un anneau commutatif**
Soit $(P, Q, R) \in \mathbf{K}[X]^3$.

- La loi $\times$ est **commutative** : $P \times Q = Q \times P$.
- La loi $\times$ est **associative** : $(P \times Q) \times R = P \times (Q \times R)$.
- La loi $\times$ est **distributive** sur $+$ : $P \times (Q + R) = P \times Q + P \times R$.
- Le polynôme constant égal à 1 est **élément neutre** pour $\times$ : $1 \times P = P$.

**Démonstration** ▽
Soit $P = \sum_{k=0}^{n} a_k\ X^k$, $Q = \sum_{k=0}^{m} b_k\ X^k$, et $R = \sum_{k=0}^{p} c_k\ X^k$, par définition de la multiplication des polynômes

$$\begin{aligned}
P \times Q &= \sum_{k=0}^{n+m} \gamma_k\ X^k, \quad \text{où} \quad \gamma_k = \sum_{i+j=k} a_i \times b_j \\
Q \times R &= \sum_{k=0}^{m+p} \alpha_k\ X^k, \quad \text{où} \quad \alpha_k = \sum_{i+j=k} b_i \times c_j \\
P \times R &= \sum_{k=0}^{n+p} \beta_k\ X^k, \quad \text{où} \quad \beta_k = \sum_{i+j=k} a_i \times c_j.
\end{aligned}$$

- Il suffit de remarquer que la multiplication dans $\mathbf{K}$ étant commutative,

$$\sum_{i+j=k} a_i \times b_j = \sum_{i+j=k} b_i \times a_j$$

- Notons pour $0 \leq k \leq (n+m)+p$, $\lambda_k = \sum_{s+t=k} \gamma_s c_t$ de sorte que $(P \times Q) \times R = \sum_{k=0}^{(n+m)+p} \lambda_k X^k$. Par construction de $\gamma_s$, il vient :
$$\lambda_k = \sum_{s+t=k} \gamma_s c_t = \sum_{s+t=k} \big( \sum_{i+j=s} a_i b_j \big) c_t = \sum_{i+j+t=k} (a_i b_j) c_t$$
De même $P \times (Q \times R) = \sum_{k=0}^{n+(m+p)} \mu_k X^k$, où
$$\mu_k = \sum_{s+t=k} a_s \alpha_t = \sum_{s+t=k} a_s \big( \sum_{i+j=t} b_i c_j \big) = \sum_{i+j+s=k} a_s (b_i c_j) = \sum_{i+j+t=k} a_i (b_j c_t)$$
La multiplication dans $\mathbf{K}$ étant associative, il en résulte que pour tout $k \in [\![0, n+m+p]\!]$, $\lambda_k = \mu_k$. Par conséquent, $(P \times Q) \times R = P \times (Q \times R)$.
- Il suffit de remarquer que la multiplication dans $\mathbf{K}$ étant distributive sur l'addition, $a_i(b_j + c_j) = a_i b_j + a_i c_j$.
- Notons $U = u_0$ le polynôme constant égal à 1. $U$ étant de degré 0, il vient pour tout $k \in [\![0, n]\!]$ $\sum_{i=0}^{k} u_i \times a_{k-i} = a_k$, ce qui prouve que $U \times P = P$.

▲

**Exercice :** Reprenez les polynômes $P(X) = 1 + X^2 + X^3$ et $Q = 4 - 6X$ de l'***Exercice*** précédent. Calculez $P(X) \times Q(X)$ en utilisant les propriétés de la multiplication interne des polynômes.

**Proposition 15.4.— Degré d'un produit —.** Soit $(P, Q) \in \mathbf{K}[X]^2$ deux polynômes à coefficients dans $\mathbf{K}$. Alors
$$\boxed{d^\circ(P \times Q) = d^\circ P + d^\circ Q}$$

**Commentaires :** il s'agit d'une égalité dans $\mathbf{N} \cup \{-\infty\}$. En particulier, lorsque l'un des polynômes est nul on a
$$\begin{aligned} d^\circ(P) + d^\circ Q &= -\infty \\ d^\circ(P \times Q) &= -\infty \end{aligned}$$

**Démonstration** ▽
Supposons sans perte que $P$ et $Q$ sont non nuls et notons $P = \sum_{k=0}^{n} a_k\, X^k$, $Q = \sum_{k=0}^{m} b_k\, X^k$ avec $n = d^\circ P$ et $m = d^\circ Q$. Soit $k \in \mathbf{N}$, on pose, conformément à la définition du polynôme $P \times Q$, $c_k = \sum_{i+j=k} a_i \times b_j$.
Remarquons tout d'abord que $c_k$ est nul pour $k > n + m$. En effet, si $k > n + m$, il n'existe pas de couple $(i, j) \in [\![0, n]\!] \times [\![0, m]\!]$ tel que $i + j = k$. D'où $\sum_{i+j=k} a_i \times b_j = 0$.
D'autre part, si $k = n + m$, il existe un unique couple $(i, j) \in [\![0, n]\!] \times [\![0, m]\!]$ tel que $i + j = n + m$ : il s'agit du couple $(n, m)$. Par conséquent
$$\sum_{i+j=n+m} a_i \times b_j = a_n \times b_m$$
qui est non nul car par hypothèse $n = d^\circ P$ et $m = d^\circ Q$. ▲

**Exercice :** Déterminez le degré du polynôme $P(X) = \prod_{k=0}^{n} (2X - k)$.

**Théorème 15.5.—** $\big(\mathbf{K}[X], +, \times\big)$ est un anneau commutatif intègre.
Pour tous polynômes $P, Q \in \mathbf{K}[X]$, on a l'équivalence :
$$\boxed{P \times Q = 0 \iff P = 0 \text{ ou } Q = 0}$$

**Démonstration** ▽

- La condition est suffisante :
  Supposons sans perte de généralité que $P$ est le polynôme nul. Montrons que $P \times Q = 0$. Il s'agit donc de démontrer que tous les coefficients de ce polynôme produit sont nuls :
  Soit $k \in \mathbf{N}$, par construction $c_k = \sum_{i+j=k} a_i \times b_j = \sum_{i+j=k} 0 \times b_j = 0$.
- Montrons par contraposée que la condition est nécessaire. Supposons que $P$ et $Q$ sont tous les deux non nuls et montrons qu'il en est de même pour $P \times Q$. Comme $P$ et $Q$ sont non nuls, remarquons que leurs degrés sont positifs ou nuls. Il en résulte, d'après la **Proposition** précédente, que

$$d^\circ(P \times Q) = d^\circ P + d^\circ Q \geq 0$$

  En particulier, $P \times Q$ est non nul. ▲

**Corollaire 15.6.—** Soit $P \in \mathbf{K}[X]$ un polynôme non nul. Alors,

$$\left(\forall (Q, R) \in \mathbf{K}[X]^2\right) \left(P \times Q = P \times R \Rightarrow Q = R\right).$$

**Démonstration** ▽
Soit $Q, R$ deux polynômes à coefficients dans $\mathbf{K}$ tels que $P \times Q = P \times R$. En utilisant la distributivité de $\times$ sur $+$, il vient

$$P \times (Q - R) = 0$$

D'après le **Corollaire** 15.5, il s'ensuit que $P = 0$ ou $Q - R = 0$. Comme par hypothèse $P$ est non nul, nécessairement $Q - R$ est nul. ▲

Un autre corollaire intéressant précise quels polynômes possèdent un inverse pour la multiplication interne. Le résultat est sans surprise :

**Corollaire 15.7.—** Soit $P \in \mathbf{K}[X]$ un polynôme à coefficients dans $\mathbf{K}$. On suppose que $P$ possède un inverse, c'est-à-dire un polynôme $Q \in \mathbf{K}[X]$ tel que

$$P \times Q = 1$$

Alors $P$ est un polynôme constant non nul, *i.e.* $P \in \mathbf{K}^\star$.

**Démonstration** ▽
Soit $P, Q \in \mathbf{K}[X]$ deux polynômes tels que $P \times Q = 1$. En particulier $d^\circ(P \times Q) = d^\circ 1 = 0$. D'après la **Proposition** 15.4 il s'ensuit que $d^\circ P + d^\circ Q = 0$. Comme le degré d'un polynôme est ou bien un entier naturel, ou bien $-\infty$, il en résulte que

$$d^\circ P = d^\circ Q = 0$$

Par conséquent, il existe $a, b \in \mathbf{K}^\star$ tels que $P = a$ et $Q = b$. L'égalité $P \times Q = 1$ se traduit simplement par $a \times b = 1$. Ainsi $P$ est un polynôme constant et non nul. ▲

### 2.c Multiplication externe dans $\mathbf{K}[\mathbf{X}]$

L'ensemble $\mathbf{K}[X]$ est muni d'une multiplication externe, notée $\cdot$ définie par :

**Définition :** *Etant donné un polynôme* $P = \sum_{k=0}^{n} a_k\ X^k$ *à coefficients dans* $\mathbf{K}$ *et un* scalaire $\lambda \in \mathbf{K}$*, on définit le polynôme* $\lambda \cdot P$ *par :*

$$\boxed{\lambda \cdot P = \sum_{k=0}^{n} \lambda\ a_k\ X^k}$$

**Proposition 15.8.— $\big(\mathbf{K}[X],+,\cdot\big)$ est un K-espace vectoriel**

- **Distributivité par rapport à l'addition des scalaires**
$$\forall(\lambda,\mu)\in\mathbf{K}^2,\forall P\in\mathbf{K}[X],\quad (\lambda+\mu)\cdot P=\lambda\cdot P+\mu\cdot P.$$
- **Distributivité par rapport à l'addition des polynômes**
$$\forall\lambda\in\mathbf{K},\forall(P,Q)\in\mathbf{K}[X]^2,\quad \lambda\cdot(P+Q)=\lambda\cdot P+\lambda\cdot Q.$$
- **Associativité mixte**
$$\forall(\lambda,\mu)\in\mathbf{K}^2,\forall P\in\mathbf{K}[X],\quad (\lambda\times\mu)\cdot P=\lambda\cdot\big(\mu\cdot P\big).$$
- **Multiplications par $1$ et $-1$**
$$\forall P\in\mathbf{K}[X],\quad 1\cdot P=P \text{ et } (-1)\cdot P=-P$$

**Démonstration** ▽
Il s'agit de simples vérifications, *left as an exercise for the reader ...* ▲

En ce qui concerne le degré, la situation est simple :

**Proposition 15.9.—** Soit $P\in\mathbf{K}[X]$ un polynôme à coefficients dans $\mathbf{K}$ et $\lambda\in\mathbf{K}^\star$ un scalaire non nul. Alors
$$\boxed{d^\circ\big(\lambda\cdot P\big)=d^\circ P}$$

**Remarque :** Dans le cas où $\lambda$ est nul, le polynôme $0\cdot P$ est le polynôme nul. Il est donc de degré $-\infty$.

**Démonstration** ▽
Soit $P=\sum_{k=0}^{n}a_k\ X^k$ un polynôme de degré $n$ et $\lambda\in\mathbf{K}$ un scalaire non nul. Par construction de $\lambda P$, nous avons :
$$\lambda\cdot P=\sum_{k=0}^{n}\lambda\ a_k\ X^k$$
Comme $\lambda\neq 0$ et $a_n\neq 0$, il en résulte que $\lambda a_n\neq 0$. Ainsi, le polynôme $\lambda\cdot P$ est de degré $n$. ▲

### 2.d Composition de polynômes

Il est aussi possible de composer des polynômes. Si $P=\sum_{k=0}^{n}a_kX^k$ et $Q\in\mathbf{K}[X]$, alors
$$P\circ Q\,(X)=\sum_{k=0}^{n}a_k\big[Q(X)\big]^k$$
En pratique, on note directement $P(X^2)$, $P(X-1)$, à la place de $P\circ Q$ où $Q=X^2$, $Q=(X-1)$.

**Exercice :** Déterminez les polynômes $P\in\mathbf{K}[X]$ tels que
$$P(X^2)=(X^2+1)\times P(X)$$

**Indication :** vous chercherez d'abord une condition nécessaire portant sur le degré de $P$.

*Solution* ▽
*Pour déterminer cet ensemble de polynômes, nous pouvons raisonner par* **analyse-synthèse** *:*
**Analyse :** *Soit $P\in\mathbf{K}[X]$ un polynôme de degré $n$. $P$ s'écrit*
$$\begin{aligned}P(X)&=\sum_{k=0}^{n}a_kX^k=a_nX^n+\cdots\\ P(X^2)&=\sum_{k=0}^{n}a_kX^{2k}=a_nX^{2n}+\cdots\end{aligned}$$
*En identifiant les degrés, on obtient l'équation dans $\mathbf{N}\cup\{-\infty\}$*
$$2\times d^\circ P=2+d^\circ P$$

*D'où l'on tire $d^\circ P = -\infty$ (le polynôme est nul), ou bien $d^\circ P = 2$.*
*Ainsi, un tel polynôme est nécessairement de degré inférieur ou égal à 2.*

**Synthèse :** *soit $P = aX^2 + bX + c$ un polynôme de degré inférieur ou égal à 2. Procédons par identification des coefficients dans l'égalité polynomiale $P(X^2) = (X^2+1)P(X)$, il vient :*

$$P(X^2) = (X^2+1)P(X) \iff \left\{ \begin{array}{rcl} a & = & a \\ b & = & 0 \\ a+c & = & b \\ c & = & c \end{array} \right. \iff \left\{ \begin{array}{rcl} b & = & 0 \\ a+c & = & 0 \end{array} \right.$$

**Conclusion :** *les polynômes solution de l'équation proposée sont les polynômes de la forme $P(X) = a(X^2-1)$, où $a \in \mathbf{K}$.*▲

### 2.e Calculs dans $\mathbf{K}[\mathbf{X}]$

Pour conclure cette partie du chapitre consacrée aux opérations dans $\mathbf{K}[X]$, remarquez que les propriétés de l'addition et de la multiplication internes ainsi que de la multiplication externe, nous permettent d'effectuer les calculs sur les polynômes ne mettant en oeuvre que ces opérations, exactement comme ceux de l'application polynomiale associée ...

**Exemple :** Pour calculer $P \times Q$, où $P = X^2 - 5X + 8$ et $Q = X^4 - 13X^3 + 15X^2 - X - 2$ sont deux polynômes de $\mathbf{R}[X]$, j'utilise la distributivité de $\times$ sur $+$ et je regroupe les termes ainsi obtenus suivant les puissances de $X$ :

$$\begin{aligned} &(X^2 - 5X + 8) \times (X^4 - 13X^3 + 15X^2 - X - 2) \\ =&X^6 - 13X^5 + 15X^4 - X^3 - 2X^2 - 5X^5 + 65X^4 - 75X^3 + 5X^2 + 10X + 8X^4 - 104X^3 + 120X^2 - 8X - 16 \\ =&X^6 + (-13-5)X^5 + (15+65+8)X^4 + (-1-75-104)X^3 + (-2+5+120)X^2 + (+10-8)X - 16 \\ =&X^6 - 18X^5 + 88X^4 - 180X^3 + 123X^2 + 2X - 16. \end{aligned}$$

### 2.f Autres formules célèbres

La **formule du binôme de Newton** et l'**identité géométrique** restent valables dans $\mathbf{K}[X]$. Par exemple,

**Proposition 15.10.—** Pour tout entier naturel $n \in \mathbf{N}$ :

$$\blacksquare \quad (X+1)^n = \sum_{k=0}^{n} \binom{n}{k} X^k$$

$$\blacksquare \quad X^{n+1} - 1 = (X-1) \times \sum_{k=0}^{n} X^k$$

**Exercice :** Soit $n \in \mathbf{N}^\star$. Soit $P(X) = (X+1)^n$ et $Q = (X-1)^n$. Quel est le degré de $P + (-Q)$ ? Quel est son coefficient dominant ?

La différence essentielle entre le calcul dans $\mathbf{K}[X]$ et le calcul dans $\mathbf{K}$ est l'absence d'inverse pour un polynôme quelconque. Rappelez-vous en effet que seuls les polynômes constants égaux à un nombre non nul possèdent un inverse. Il paraît alors délicat d'envisager une division dans $\mathbf{K}[X]$. Pourtant, nous verrons qu'il est possible de définir une division dans $\mathbf{K}[X]$ qui sera étudiée en détail lors d'une prochaine partie.

## 3 Divisibilité dans $\mathbf{K}[\mathbf{X}]$

Du point de vue du calcul dans $\mathbf{K}[X]$, la division est le point délicat. Disons, pour fixer les idées et pour relativiser la difficulté, que la situation est tout à fait comparable à celle rencontrée lors de notre étude de l'anneau $\mathbf{Z}$.

### 3.a Définition

**Définition :** *Soit $(A,B) \in \mathbf{K}[X]^2$ deux polynômes. On dit que $B$ **divise** $A$, ou que $A$ est un multiple de $B$ lorsqu'il existe un polynôme $Q \in \mathbf{K}[X]$ tel que*

$$\boxed{A = B \times Q}$$

*On note $B|A$, et on lit «*B divise A*»cette relation.*

**Exercice :** Montrez que $B$ divise $A$ dans $\mathbf{C}[X]$ lorsque

**1.** $A = X^2 + 1$ et $B = X - i$.

**2.** $A = X^{n+1} - 1$ et $B = 1 + X + \cdots + X^n$.

*Solution* ▽

**1.** $X^2 + 1 = X^2 - i^2 = (X - i) \times (X + i)$. *Par suite,* $X - i \,|\, X^2 + 1$.

**2.** *D'après l'identité géométrique,* $(X - 1) \times (1 + X + X^2 + \cdots + X^n) = X^{n+1} - 1$. *Ainsi,* $1 + X + \cdots + X^n$ *divise* $X^{n+1} - 1$. ▲

### 3.b Polynômes associés

**Définition :** *Deux polynômes non nuls $P$ et $Q$ sont dits* ***associés*** *si $P$ divise $Q$ et $Q$ divise $P$.*

**Proposition 15.11.—** Soit $P$ et $Q$ deux polynômes non nuls.

$$P \text{ et } Q \text{ sont associés } \textit{si et seulement si } \exists a \in \mathbf{K}^\star;\ Q = aP$$

**Démonstration** ▽
Soit $(P, Q)$ un couple de polynômes associés. Par définition, il existe $(A, B) \in \mathbf{K}[X]^2$ tel que $Q = A \times P$ et $P = B \times Q$. Ainsi, $Q = AB \times Q$. Comme $Q$ est non nul, il s'ensuit que $AB = 1$. En particulier, $A$ est inversible : $A = a \in \mathbf{K}^\star$ et donc $Q = aP$. ▲

### 3.c Théorème Fondamental de la division euclidienne dans $\mathbf{K}[\mathbf{X}]$

L'objet de ce paragraphe est de présenter la division dans $\mathbf{K}[X]$, analogue à celle pratiquée dans $\mathbf{Z}$. La division euclidienne dans $\mathbf{K}[X]$ est analogue à celle de $\mathbf{Z}$.

**Théorème 15.12.— Théorème de la division euclidienne**

Soit $(A, B) \in \mathbf{K}[X]^2$ deux polynômes à coefficients dans $\mathbf{K}$. On suppose que $B \neq 0$.

Il existe un couple $(Q, R) \in \mathbf{K}[X]^2$, **unique** tel que
- $A = B \times Q + R$
- $d^\circ R < d^\circ B$

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

**Exemple :** Prenons $A = X^4 - 5X^3 + 6X - 2$ et $B = X^2 - 2$. Il n'est pas difficile de trouver des couples $(Q, R)$ vérifiant $A = B \times Q + R$.

$$\begin{aligned} X^4 - 5X^3 + 6X - 2 &= (X^2 - 2) \times 6 + X^4 - 5X^3 - 12X^2 + 6X + 10 \\ &= (X^2 - 2) \times X + X^4 - 6X^3 + X - 2 \\ &= (X^2 - 2) \times X^3 - X^5 + X^4 - 7X^3 + 6X - 2. \end{aligned}$$

**Commentaires :** il y a donc une infinité de couples $(Q, R)$ tels que $A = B \times Q + R$. La condition sur les degrés force à elle seule l'unicité. Reprenons l'exemple précédent :

**Exemple :** Cherchons à présent un couple $(Q, R)$ tel que $A = B \times Q + R$ et $d^\circ R < d^\circ B$. Pour ce faire, raisonnons sur le monôme dominant de $Q$. Remarquons tout d'abord que si $A = B \times Q + R$, alors $R = A - B \times Q$. Par conséquent, si nous souhaitons faire baisser le degré de $R$, il n'est d'autre solution que de choisir $Q$ de degré

$4-2=2$. De plus les polynômes $A$ et $B\times Q$ doivent avoir le même coefficient dominant, c'est-à-dire 1. Ainsi

$$\begin{aligned} X^4-5X^3+6X-2 &= (X^2-2)\times X^2-\underbrace{5X^3+2X^2+6X-2}_{\text{le 1}^{\text{er}}\text{ reste partiel}} \\ &= (X^2-2)\times X^2-(X^2-2)\times 5X+\underbrace{2X^2-4X-2}_{\text{le 2}^{\text{ème}}\text{ reste partiel}} \\ &= (X^2-2)\times X^2-(X^2-2)\times 5X+(X^2-2)\times 2\underbrace{-4X+2}_{\text{le 3}^{\text{ème}}\text{ reste}} \\ &= (X^2-2)\times \underbrace{(X^2-5X+2)}_{\text{le quotient}}\underbrace{-4X+2}_{\text{le reste}} \end{aligned}$$

**Démonstration** ▽

- **Unicité du couple** $(Q,R)$.
  Supposons que $(Q,R)$ et $(T,U)$ vérifient les conditions de la division euclidienne de $A$ par $B$, c'est-à-dire :

$$\begin{array}{cc} A=B\times Q+R & A=B\times T+U \\ d^\circ R<d^\circ B & d^\circ U<d^\circ B' \end{array}$$

  En retranchant membre nous obtenons tout d'abord $B\times(Q-T)+(R-U)=0$, qui donne

$$B\times(Q-T)=U-R.$$

  Examinons les degrés respectifs de ces deux polynômes.
  - D'après la **Proposition** 15.2, le polynôme $U-R$ est de degré strictement inférieur à $d^\circ B$ ;
  - D'après la **Proposition** 15.4, le polynôme $B\times(Q-T)$ est de degré $d^\circ B+d^\circ(Q-T)$ .

  Par conséquent $d^\circ B+d^\circ(Q-T)<d^\circ B$. Cette inégalité est impossible si $d^\circ B, d^\circ(Q-T)\in\mathbf{N}$. Comme $d^\circ B\in\mathbf{N}$, j'en déduis que nécessairement $d^\circ(Q-T)=-\infty$, c'est-à-dire $Q-T=0$.
  Ainsi $Q=T$. Réinjectons ceci dans l'égalité $B\times(Q-T)=U-R.$, il en résulte que $R=U$.
- **Existence du couple** $(Q,R)$.
  Soit $B=b_mX^m+b_{m-1}X^{m-1}+\cdots+b_1X+b_0$, avec $b_m\neq 0$ un polynôme de degré $m$. On définit pour $n\in\mathbf{N}$ la propriété :
  $\mathcal{P}(n)$ pour tout polynôme $A_n=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$ de degré inférieur ou égal à $n$, il existe un couple $(Q_n,R_n)$ de polynômes tel que

  - $A_n=B\times Q_n+R_n$
  - $d^\circ R_n<d^\circ B$

  Montrons par récurrence que $\forall n\in\mathbf{N}$, $\mathcal{P}(n)$.

  **Initialisation :** lorsque $n<m$, il suffit de remarquer que $A=B\times 0+A$. Comme en ce cas $d^\circ A<d^\circ B$, le couple $(Q,R)=(0,A)$ convient.
  **Hérédité :** soit $n\geq m-1$ tel que $\mathcal{P}(n)$.
  Soit $A_{n+1}=a_{n+1}X^{n+1}+a_nX^n+\cdots+a_1X+a_0$, un polynôme de degré inférieur ou égal à $n+1$. Comme $B\neq 0$, le coefficient dominant $b_m$ de $B$ est non nul, de sorte que le polynôme

$$A_n=A_{n+1}-\frac{a_{n+1}}{b_m}X^{n+1-m}\times B$$

  est bien défini. De plus, comme le montre un examen minutieux du monôme dominant de $\frac{a_{n+1}}{b_m}X^{n+1-m}\times B$, $A_n$ est de degré inférieur ou égal à $n$. Par hypothèse de récurrence, il existe un couple $(Q_n,R_n)$ de polynômes tels que $A_n=B\times Q_n+R_n$ et $d^\circ R_n<d^\circ B$. Par conséquent

$$\begin{aligned} A_{n+1} &= \frac{a_{n+1}}{b_m}X^{n+1-m}\times B+Q_n\times B+R_n \\ &= B\times\left(\frac{a_{n+1}}{b_m}X^{n+1-m}+Q_n\right)+R_n \end{aligned}$$

Par conséquent, le couple $\left(\frac{a_{n+1}}{b_m}X^{n+1-m}+Q_n\ ;\ R_n\right)$ convient.

**Conclusion :** par récurrence, nous avons prouvé que pour tout couple $(A,B)$ de polynômes tels que $B\neq 0$, il existe un couple $(Q,R)$ de polynômes tels que $A=B\times Q+R$ et $d^\circ R<d^\circ B$. ▲

**Exercice :** Soit $n\in\mathbf{N}$ un entier supérieur ou égal à 2 et $A=X^n+2X-2$. Déterminez le reste de la division euclidienne de $A$ par $B$ lorsque

**1.** $B=X-1$.

**2.** $B=(X-1)(X-2)$.

*Solution* ▽

**1.** *Écrivons la division euclidienne de $A$ par $B$ : il existe un couple unique $(Q,R)$ de polynômes tels que $d^\circ R<1$ et*

$$A=(X-1)\times Q+R$$

*La condition sur le degré de $R$ traduit simplement le fait que $R$ est un polynôme constant : $R=a$. Pour déterminer $a$, évaluons l'égalité polynomiale ci-dessus au point 1. Il vient*

$$\tilde{A}(1)=0\times\tilde{Q}(1)+a$$

*D'où je tire $a=1$. Par conséquent le reste dans la division euclidienne de $A$ par $(X-1)$ est 1.*

**2.** *Écrivons la division euclidienne de $A$ par $B$ : il existe un couple unique $(Q,R)$ de polynômes tels que $d^\circ R<2$ et*

$$A=(X-1)(X-2)\times Q+R$$

*La condition sur le degré de $R$ se traduit par l'existence d'un couple $(a,b)\in\mathbf{K}^2$ tel que $R=aX+b$. Pour déterminer $(a,b)$, nous procédons comme précédemment. Cependant, puisque nous avons ici 2 inconnues, il nous faut deux équations. Evaluons l'égalité polynomiale ci-dessus aux points 1 et 2. Il vient*

$$\left\{\begin{array}{rcl}\tilde{A}(1)&=&0\times\tilde{Q}(1)+a+b\\ \tilde{A}(2)&=&0\times\tilde{Q}(2)+2a+b\end{array}\right.$$

*D'où je tire*

$$\left\{\begin{array}{rcl}a&=&2^n+1\\ b&=&-2^n\end{array}\right.$$

*Par conséquent, le reste dans la division euclidienne de $A$ par $(X-1)(X-2)$ est*

$$R=(2^n+1)X-2^n.$$

▲

L'unicité du couple $(Q,R)$ dans la division euclidienne de $A$ par $B$ permet d'obtenir facilement un *critère de divisibilité* dans $\mathbf{K}[X]$ qui ne choquera personne :

**Corollaire 15.13.—** Soit $(A,B)\in\mathbf{K}[X]^2$, $B\neq 0$.

$B$ divise $A$ *si et seulement si* le reste de la division euclidienne de $A$ par $B$ est nul.

**Démonstration** ▽
Procédons par équivalences :

$$B\mid A\iff\exists Q\in\mathbf{K}[X];\ A=B\times Q\iff\exists Q\in\mathbf{K}[X];\ A=B\times Q+0.$$

Par unicité du couple $(Q,R)\in\mathbf{K}[X]^2$ dans la division euclidienne de $A$ par $B$, ceci revient à dire que le reste de la division euclidienne de $A$ par $B$ est nul. ▲

**Exercice :** Soit $n\in\mathbf{N}$ un entier supérieur ou égal à 2, $A=X^n+X-1$ et $B=X-1$.

**1.** Déterminez le reste de la division euclidienne de $A$ par $B$.

**2.** Effectuez la division euclidienne de $A=X^n+X-1$ par $B=X-1$.

*Solution* ▽
*Soit $A=X^n+X-1$ et $B=X-1$.*

**1.** *Le reste de la division euclidienne de $A$ par $B$ est un polynôme constant égal à $a$. Pour déterminer $a$ évaluons l'égalité polynomiale*

$$A = (X-1) \times Q + R$$

*au point 1. Il vient $a = \tilde{A}(1) = 1$. Le reste de la division euclidienne de $A$ par $B$ est donc $R = 1$.*

**2.** *Déterminons le quotient. Pour cela remarquons que l'égalité*

$$A = B \times Q + 1$$

*se traduit par fe fait que $A - 1$ est divisible par $(X-1)$. En effet, d'après l'identité géométrique, nous avons :*

$$\begin{aligned} A-1 &= X^n + X - 1 - 1 = X^n - 1 + X - 1 = (X-1) + (X-1) \times \sum_{k=0}^{n-1} X^k \\ &= (X-1)\big(2 + X + \cdots + X^{n-1}\big) \end{aligned}$$

*D'où la division euclidienne de $A$ par $B$ est :*

$$(X^n + X - 1) = (X-1)\big(2 + X + \cdots + X^{n-1}\big) + 1.$$

▲

### 3.d Pratique de la division euclidienne

Pour l'exercice précédent, les coefficients des polynômes $A$ et $B$ ne sont pas explicitement connus. La méthode pour effectuer la division euclidienne a consisté à

- déterminer le reste en évaluant l'égalité $A = B \times Q + R$ en des points bien choisis
- factoriser $A - R$ par $B$.

**Lorsque les polynômes $A$ et $B$ sont parfaitement déterminés**, nous emprunterons la présentation de cette opération à celle de la division vue en sixième. C'est ce qu'on appelle la **division suivant les puissances décroissantes**.

Reprenons l'exemple :

**Exemple :** Nous avions $A = X^4 - 5X^3 + 6X - 2$ et $B = X^2 - 2$.

$$\begin{array}{rrcccc|l} A \rightsquigarrow & X^4 & -5X^3 & & +6X & -2 & X^2-2 \quad \leftsquigarrow B \\ -\big( & X^4 & & -2X^2 & & & \big) \quad X^2 - 5X + 2 \quad \leftsquigarrow Q_1 + Q_2 + Q_3 \\ \hline A_1 \rightsquigarrow & & -5X^3 & +2X^2 & +6X & -2 & \\ -\big( & & -5X^3 & & +10X & & \big) \\ \hline A_2 \rightsquigarrow & & & +2X^2 & -4X & -2 & \\ -\big( & & & 2X^2 & & -4 & \big) \\ \hline A_3 \rightsquigarrow & & & & -4X & +2 & \end{array}$$

Nous retrouvons ainsi le résultat :

$$X^4 - 5X^3 + 6X - 2 = \big(X^2 - 2\big) \times \big(X^2 - 5X + 2\big) - 4X + 2.$$

**Exercice :** Effectuez la division euclidienne de $A = X^3 + iX^2 + X$ par $B = X - i + 1$.

# II Dérivation dans $\mathbf{K}[\mathrm{X}]$

## 1 Polynôme dérivé

### 1.a Définition

**Définition :** *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbf{K}$. On appelle **polynôme dérivé** de $P$, le polynôme défini par*

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

**Commentaires :** concrètement cela revient à dériver *terme à terme* le polynôme $P$ comme vous le feriez pour la fonction polynomiale associée. Par exemple si $P = X^5 + 2X^4 - X^2 + 3X + 12$ le polynôme dérivé de $P$ est $P' = 5X^4 + 8X^3 - 2X + 3$.

**Remarque :** si $P$ est un polynôme constant, alors $P'$ est le polynôme nul.

### 1.b Dérivée d'une combinaison linéaire

**Proposition 15.14.—** Soit $(P, Q) \in \mathbf{K}[X]^2$ et $(\lambda, \mu) \in \mathbf{K}^2$.

- $(P+Q)' = P' + Q'$
- $(\lambda \cdot P + \mu \cdot Q)' = \lambda \cdot P' + \mu \cdot Q'$

**Commentaires :** On dit que la dérivation est une application linéaire de $\mathbf{K}[X]$ dans lui-même.

**Démonstration** ▽
Écrivons

$$\begin{array}{rclcrcl} P & = & \displaystyle\sum_{k=0}^{n} a_k X^k & & Q & = & \displaystyle\sum_{k=0}^{m} b_k X^k \\ P' & = & \displaystyle\sum_{k=1}^{n} k a_k X^{k-1} & & Q' & = & \displaystyle\sum_{k=1}^{m} k b_k X^{k-1} \end{array}$$

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

▲

### 1.c Dérivée d'un produit

**Théorème 15.15.— Leibniz —.** Soit $(P, Q) \in \mathbf{K}[X]^2$, $(P_1, \ldots, P_n) \in \mathbf{K}[X]^n$ un $n$-uplet de polynômes. Alors

- $(P \times Q)' = P' \times Q + P \times Q'$.
- $(P_1 \times \cdots \times P_n)' = \displaystyle\sum_{k=1}^{n} P_k' \times \prod_{\substack{1 \leq \ell \leq n \\ \ell \neq k}} P_\ell$.
- $(P^n)' = nP^{n-1} \times P'$

**Démonstration** ▽

Notons comme précédemment $P=\sum_{k=0}^{n} a_k X^k, Q=\sum_{k=0}^{m} b_k X^k$. Alors

$$\begin{aligned}(P\times Q)' &= \Big(\sum_{k=0}^{n+m}\Big(\sum_{i+j=k} a_i b_j\Big)X^k\Big)' = \sum_{k=1}^{n+m} k\Big(\sum_{i+j=k} a_i b_j\Big)X^{k-1} = \sum_{k=1}^{n+m}\Big(\sum_{i+j=k}(i+j)a_i b_j\Big)X^k\\ &= \sum_{k=1}^{n+m}\Big(\sum_{i+j=k} i a_i b_j\Big)X^{k-1} + \sum_{k=1}^{n+m}\Big(\sum_{i+j=k} j a_i b_j\Big)X^{k-1}\\ &= \sum_{k=1}^{n+m}\Big(\sum_{i+j=k} i a_i b_j\Big)X^{k-1} + \sum_{k=1}^{n+m}\Big(\sum_{i+j=k} j a_i b_j\Big)X^{k-1}\\ &= P'\times Q + P\times Q'.\end{aligned}$$

La deuxième formule s'en déduit par récurrence sur l'entier $n$. ▲

**Proposition 15.16.— Degré du polynôme dérivé —.** Si $P\in\mathbf{K}[X]$ est un polynôme à coefficients dans $\mathbf{K}$.

- si $P$ est de degré négatif ou nul ($P$ constant), alors $P'$ est de degré $-\infty$ ($P'$ est nul)
- si $P$ est de degré $n\in\mathbf{N}^\star$, alors $P'$ est un polynôme de degré $n-1$.

**Démonstration** ▽

Lorsque $P=a_0$ est un polynôme constant, son poynôme dérivé est nul par définition.
Soit donc $P=\sum_{k=0}^{n} a_k X^k$ un polynôme de degré $n\in\mathbf{N}^\star$. Par définition

$$P'=\sum_{k=1}^{n} k.a_k X^{k-1} = n a_n X^{n-1} + \textit{termes de plus bas degré}$$

Comme précisément $n$ et $a_n$ sont non nuls, il en résulte que $P'$ est de degré exactement $n-1$. ▲

## 2 Dérivées successives

**Définition :** *Soit $P\in\mathbf{K}[X]$ un polynôme à coefficients dans $\mathbf{K}$. Les **dérivées successives** de $P$ sont définies par récurrence par*

- $P^{(0)}=P$
- $\forall k\in\mathbf{N},\ P^{(k+1)}=\big(P^{(k)}\big)'$.

**Notation :** *La dérivée $k^{\text{ième}}$ de $P$ est notée $P^{(k)}$. L'exposant entre parenthèses indique l'ordre de dérivation.*

Une récurrence permet d'obtenir l'expression de la dérivée $p^{\text{ième}}$ d'un polynôme :

**Proposition 15.17.—** Soit $P=\sum_{k=0}^{n} a_k X^k$ un polynôme de coefficients $(a_0,a_1,a_2,\dots,a_n)$ dans $\mathbf{K}$ de degré inférieur ou égal à $n$. Alors

- Si $p>n$, $\quad P^{(p)}=0$.
- Si $p\in[\![0,n]\!]$, $\quad P^{(p)}=\displaystyle\sum_{k=p}^{n} a_k\ k(k-1)\dots(k-p+1)\ X^{k-p}=\sum_{k=p}^{n} a_k\ \frac{k!}{(k-p)!}\ X^{k-p}$.

**Démonstration** ▽

Soit $n\in\mathbf{N}^\star$ et $P\in\mathbf{K}_n[X]$ un polynôme de degré $n$ à coefficients dans $\mathbf{K}$.
Montrons tout d'abord la deuxième partie de cette proposition. Comme annoncé, la preuve sera par récurrence sur $p\in[\![0,n]\!]$.
**Initialisation :** Lorsque $p=0$, nous avons d'une part $P^{(0)}=P$ par définition de la suite des dérivées de $P$ et d'autre part

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

**Hérédité :** Soit $p \in [\![0, n-1]\!]$ tel que

$$P^{(p)} = \sum_{k=p}^{n} a_k \ k(k-1)\dots(k-p+1) \ X^{k-p} = \sum_{k=p}^{n} a_k \ \frac{k!}{(k-p)!} \ X^{k-p}$$

Par définition de la dérivée $p+1^{\text{ième}}$, il vient :

$$\begin{aligned} P^{(p+1)} &= \left(P^{(p)}\right)' = \left(\sum_{k=p}^{n} a_k \ \frac{k!}{(k-p)!} \ X^{k-p}\right)' = \sum_{k=p+1}^{n} a_k(k-p) \ \frac{k!}{(k-p)!} \ X^{k-p-1} \\ &= \sum_{k=p+1}^{n} a_k \ \frac{k!}{(k-p-1)!} \ X^{k-p-1}. \end{aligned}$$

**Conclusion :** Pour tout $p \in [\![0, n]\!]$, nous avons

$$P^{(p)} = \sum_{k=p}^{n} a_k \ k(k-1)\dots(k-p+1) \ X^{k-p} = \sum_{k=p}^{n} a_k \ \frac{k!}{(k-p)!} \ X^{k-p}$$

En particulier, remarquons que $P^{(n)} = n!a_n$.
Ainsi, le polynôme $P^{(n)}$ est constant. Par conséquent, les polynômes dérivés d'ordre supérieur ou égal à $n+1$ sont nuls.
Ce qui achève la démonstration de cette proposition. ▲

**Exercice :** Soit $n \in \mathbf{N}$ un entier naturel. Notons $T_n = X^n$.
Utilisez la formule ci-dessus pour calculer les dérivées successives de tous ordres de $T_n$.
En déduire que pour tout $p \in \mathbf{N}$, $p \neq n$, $T_n^{(p)}(0) = 0$ et $T_n^{(n)}(0) = n!$.

On déduit aisément de cette proposition que la dérivée $p^{\text{ième}}$ d'une somme de deux polynômes est simplement la somme des dérivées $p^{\text{ièmes}}$. Pour calculer les dérivées successives d'un produit de polynômes, nous disposons de la

**Proposition 15.18.— Formule de Leibniz —.** Soit $(P, Q) \in \mathbf{K}[X]^2$, $n \in \mathbf{N}$. Alors

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

**Démonstration** ▽
La preuve est par récurrence sur $n \in \mathbf{N}$.
**Initialisation :** lorsque $n = 0$, c'est immédiat !
**Hérédité :** Soit $n \geq 0$ tel que $(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$. La **relation de Pascal** permet de conclure :

$$\begin{aligned} (P \times Q)^{(n+1)} &= \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} \times Q^{(n-k)}\right)' = \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k)} \times Q^{(n-k)}\right)' \\ &= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k+1)} \times Q^{(n-k)} + P^{(k)} \times Q^{(n+1-k)}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} \times Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} \times Q^{(n+1-k)} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)} \times Q^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} \times Q^{(n+1-k)} \\ &= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) P^{(k)} \times Q^{(n+1-k)} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} \times Q^{(n+1-k)} \end{aligned}$$

**Conclusion :** par récurrence sur $n$, nous avons prouvé que la formule de Leibniz est vraie pour tout entier $n \in \mathbf{N}$. ▲

**Exercice :** Exprimez en fonction des dérivées successives de $P$ celles de $(X^2 - 2X + 3) \times P$.

## 3 Formules de Taylor et Taylor Mac Laurin

### 3.a Formule de Taylor-Mac Laurin

En appliquant la formule (cf **Proposition** 15.17) pour les dérivées $p^{\text{ièmes}}$ d'un polynôme $P = \sum_{k=0}^{n} a_k X^k$, nous obtenons :

$$P^{(p)} = \sum_{k=p}^{n} a_k \frac{k!}{(k-p)!} X^{k-p} = p!\, a_p + \sum_{k=p+1}^{n} a_k \frac{k!}{(k-p)!} X^{k-p}$$

En évaluant ce polynôme au point 0, nous constatons que tous les termes s'annulent à l'exception du premier, de sorte que :

$$\forall p \in [\![0, n]\!], \quad a_p = \frac{P^{(p)}(0)}{p!}$$

Réinjectant ceci dans l'expression du polynôme $P$, nous obtenons la

**Théorème 15.19.— Formule de Taylor - Mac Laurin pour les polynômes —.** Soit $P \in \mathbf{K}_n[X]$ un polynôme de degré inférieur ou égal à $n$

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

**Exercice :** Soit $P = 1 + 2X + 4X^2 - 6X^3 + X^4$. Quelles sont les dérivées successives de $P$ en 0 ?

*Solution* ▽

*D'après la* **formule de Taylor-Mac Laurin**

$$P = 1 + 2X + 4X^2 - 6X^3 + X^4 = P(0) + P'(0)X + \frac{1}{2}P''(0)X^2 + \frac{1}{6}P^{(3)}(0)X^3 + \frac{1}{24}P^{(4)}(0)X^4$$

*En identifiant les coefficients, il vient :*

$$P(0) = 1,\ P'(0) = 2,\ P''(0) = 8,\ P^{(3)}(0) = -36,\ P^{(4)}(0) = 24.$$

▲

### 3.b Formule de Taylor

Comme le montre clairement la **formule deTaylor - Mac Laurin**, la définition des polynômes accorde une place centrale aux puissances de $X$. Il est parfois intéressant de pouvoir travailler en utilisant un développement en puissances de $(X - \alpha)$ où $\alpha \in \mathbf{K}$ est un nombre quelconque. Dans ce contexte, le théorème ci-dessus se généralise de la façon suivante :

**Théorème 15.20.— Formule de Taylor pour les polynômes —.** Soit $P \in \mathbf{K}_n[X]$ un polynôme de degré inférieur ou égal à $n$ et $\alpha \in \mathbf{K}$ un scalaire. Alors

$$\boxed{P = P(\alpha) + P'(\alpha)\ (X - \alpha) + \cdots + \frac{P^{(n)}(\alpha)}{n!}\ (X - \alpha)^n = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k}$$

**Remarque :** les coefficients du développement de $P$ en puissances de $X - \alpha$ sont uniquement déterminés. En effet, si $P = \sum_{k=0}^{n} c_k (X - \alpha)^k$, on a pour tout $p \in [\![0, n]\!]$ l'expression de la dérivée $p^{\text{ième}}$ de $P$ :

$$P = \sum_{k=p}^{n} c_k \frac{k!}{(k-p)!} (X - \alpha)^{k-p}$$

En particulier, en évaluant en $\alpha$, on obtient $p!\, c_p = \widetilde{P^{(p)}}(\alpha)$.

**Démonstration** ▽
L'idée est en quelque sorte de *centrer* les monômes $X^k$ au point $\alpha$. Pour cela, nous utilisons l'astuce $X^k = (X-\alpha+\alpha)^k$. Il ne reste plus dès lors qu'à utiliser la **formule du binôme de Newton** ... Voici les détails :

$$\begin{aligned} P &= \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} a_k (X-\alpha+\alpha)^k = \sum_{k=0}^{n} a_k \sum_{p=0}^{k} \binom{k}{p} (X-\alpha)^p \alpha^{k-p} \\ &= \sum_{p=0}^{n} (X-\alpha)^p \sum_{k=p}^{n} \binom{k}{p} a_k \alpha^{k-p} = \sum_{p=0}^{n} \frac{1}{p!}(X-\alpha)^p \sum_{k=p}^{n} \frac{k!}{(p-k)!} a_k \alpha^{k-p} = \sum_{p=0}^{n} \frac{P^{(p)}(\alpha)}{p!}(X-\alpha)^p. \end{aligned}$$

▲

La **formule de Taylor** permet de développer un polynôme *au voisinage* de n'importe quel point $\alpha \in \mathbf{K}$, c'est-à-dire de développer $P$ en puissances de $X-\alpha$.

**Exercice :** Soit $P = X^4 + 10X^3 - 6X^2 + 18X - 3$. Développez $P$ suivant les puissances de $(X-1)$.

*Solution* ▽
*Calculons les dérivées successives de $P$ évaluées au point 1, il vient :*

$$P(1) = 20,\ P'(1) = 40,\ P''(1) = 60,\ P^{(3)}(1) = 84,\ P^{(4)} = 24$$

*D'après la* **Formule de Taylor**, *il s'ensuit que*

$$P = 20 + 40(X-1) + 30(X-1)^2 + 14(X-1)^3 + (X-1)^4$$

▲

Comme corollaire, nous déduisons qu'un polynôme est entièrement déterminé par la donnée de la suite de ses dérivées en **un** point :

**Corollaire 15.21.—** Soit $P \in \mathbf{K}_n[X]$. On suppose qu'il existe un point $\alpha \in \mathbf{K}$ tel que

$$P(\alpha) = P'(\alpha) = \cdots = P^{(n)}(\alpha) = 0$$

Alors $P$ est le polynôme nul.

**En pratique :** pour démontrer que deux polynômes sont égaux vous pouvez prouver qu'ils ont la même suite de dérivées successives en un point $\alpha \in \mathbf{K}$.

**Démonstration** ▽
Écrivons le développement de $P$ en puissances de $X-\alpha$ grâce à la **formule de Taylor**.

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

Comme toutes les dérivées successives de $P$ s'annulent au point $\alpha$, il en résulte que $P$ est le polynôme nul. ▲

# III Fonctions polynomiales et racines d'un polynôme

## 1 Caractérisation des racines d'un polynôme

**Définition :** *Soit $P \in \mathbf{K}[X]$ un polynôme à coefficients dans $\mathbf{K}$ et $\alpha \in \mathbf{K}$ un nombre réel ou complexe. On dit que $\alpha$ est **racine** de $P$, ou bien que $\alpha$ est un **zéro** de $P$ si*

$$\boxed{P(\alpha) = 0}$$

**Commentaires :** dans la définition ci-dessus, $P(\alpha)$ désigne bien entendu $\tilde{P}(\alpha)$, la valeur en $\alpha$ de la fonction polynomiale $\tilde{P}$. Ainsi lorsqu'on dit que $\alpha$ est racine du **polynôme** $P$, cela signifie que la **fonction** polynomiale associée $\tilde{P}$ s'annule en $\alpha$.

Grâce au **Théorème** 15.12, il est possible de caractériser les racines d'un **polynôme** sans recourir à la fonction polynomiale associée[1] :

**Théorème 15.22.— Caractérisation des racines d'un polynôme**
Soit $P \in \mathbf{K}[X]$ un polynôme et $\alpha \in \mathbf{K}$ un nombre réel ou complexe.

$$\boxed{\alpha \text{ est une racine de } P \textit{ si et seulement si } (X-\alpha) \text{ divise } P}$$

**Démonstration** ▽

- Montrons que la condition est suffisante :
  Supposons que $X-\alpha$ divise $P$. Il existe par conséquent un polynôme $Q \in \mathbf{K}[X]$ tel que $P(X) = (X-\alpha) \times Q(X)$. Il en résulte immédiatement que
  $$P(\alpha) = (\alpha - \alpha) \times Q(\alpha) = 0.$$
- Montrons que la condition est nécessaire :
  Supposons que $\alpha$ soit une racine de $P$ et montrons que $(X-\alpha)$ divise $P$. Pour cela faisons la division euclidienne de $P$ par $X-\alpha$. Il existe un couple $(Q,R) \in \mathbf{K}[X]^2$ unique tel que :
  $$P(X) = (X-\alpha) \times Q(X) + R(X) \quad \text{et} \quad d^\circ R < 1$$
  La condition $d^\circ R < 1$ se traduit par $R \in \mathbf{K}$ est un polynôme constant. Montrons que $R$ est nul. Pour cela *évaluons* les fonctions polynomiales associées à $P$ et à $(X-\alpha) \times Q(X) + R(X)$ en $\alpha$, il vient
  $$0 = P(\alpha) = 0 + R(\alpha)$$
  Par conséquent, $R(\alpha) = 0$. Comme $R$ est un polynôme constant, il en résulte que $R$ est le polynôme nul. Autrement dit $P(X) = (X-\alpha) \times Q(X)$. ▲

Plus généralement, nous montrons par récurrence que :

**Proposition 15.23.—** Soit $P \in \mathbf{K}[X]$ un polynôme et $(\alpha_1, \dots, \alpha_p) \in \mathbf{K}^p$, un $p$-uplet d'éléments **distincts** de $\mathbf{K}$. Alors

$$\boxed{\alpha_1, \dots, \alpha_p \quad \text{sont racines de } P \textit{ si et seulement si } \prod_{k=1}^{p}(X-\alpha_k) \text{ divise } P}$$

**Démonstration** ▽
Il est clair que la condition est suffisante. Démontrons qu'elle est nécessaire. Comme indiqué plus haut la preuve sera par récurrence sur $p \in \mathbf{N}^\star$.
Plus précisément, démontrons sur $p \in \mathbf{N}^\star$ que :

$\boldsymbol{\mathcal{P}(p)}$ pour tout $p$-uplet $(a_1, \dots, a_p) \in \mathbf{K}^p$, **de $p$ racines distinctes de $P$,** $\prod_{k=1}^{p}(X-\alpha_k)$ divise $P$

**Initialisation :** lorsque $p=1$, c'est le **Théorème** 15.22.
**Hérédité :** soit $p \in \mathbf{N}^\star$ tel que $\mathcal{P}(p)$ et considérons une famille $(\alpha_1, \dots, \alpha_p, \alpha_{p+1}) \in \mathbf{K}^{p+1}$ de racines deux à deux distinctes de $P$. Par hypothèse de récurrence, appliquée à la famille $(\alpha_1, \dots, \alpha_p)$, le polynôme $\prod_{k=1}^{p}(X-\alpha_k)$ divise $P$. Par conséquent, il existe un polynôme $Q \in \mathbf{K}[X]$ tel que

$$P(X) = Q(X) \times \prod_{k=1}^{p}(X-\alpha_k) \tag{15.2}$$

*Evaluons* cette égalité au point $\alpha_{p+1}$, il vient $Q(\alpha) \times \prod_{k=1}^{p}(\alpha_{p+1}-\alpha_k) = 0$. Ainsi, ce produit de $p+1$ facteurs étant nul, l'un (au moins) de ces facteurs doit être nul. Or, par hypothèse, les $\alpha_1, \dots, \alpha_{p+1}$ sont *deux à deux distincts*, par suite, aucun

1. traduisez : la notion de racine d'un polynôme est une notion *intrinsèque*

des facteurs $(\alpha_{p+1}-\alpha_k)_{1\leq k\leq p}$ n'est nul. Il en résulte que $Q(\alpha_{p+1})$ doit être nul. D'après le **Théorème** 15.22, il existe un polynôme $Q_1$ tel que $Q(X)=(X-\alpha_{p+1})\times Q_1(X)$. Réinjectons ceci dans l'égalité (15.2), il en résulte finalement que

$$P(X)=Q_1(X)\times\prod_{k=1}^{p+1}(X-\alpha_k).$$

Ce qui prouve que $\prod_{k=1}^{p+1}(X-\alpha_k)$ divise $P$.

**Conclusion :** Par récurrence, nous avons démontré que pour tout $p\in\mathbf{N}^\star$

pour tout $p$-uplet $(\alpha_1,\ldots,\alpha_p)\in\mathbf{K}^p$, **de p racines distinctes de** $P$, $\prod_{k=1}^{p}(X-\alpha_k)$ divise $P$. ▲

Ce théorème possède un corollaire très efficace pour démontrer qu'un polynôme est nul :

**Corollaire 15.24.—** Soit $P\in\mathbf{K}_n[X]$ un polynôme de degré inférieur ou égal à $n\in\mathbf{N}$.

- Si $P$ possède au moins $n+1$ racines distinctes, $P$ est le polynôme nul.
- Si $P$ est de degré $n$, alors $P$ possède au plus $n$ racines distinctes.

**En pratique :** pour démontrer qu'un polynôme est nul, il suffit de prouver qu'il admet ≪trop de racines pour son degré≫. En particulier, si $P\in\mathbf{K}[X]$ possède une infinité de racines, alors $P$ est le polynôme nul.

**Démonstration** ▽

- Supposons que $P\in\mathbf{K}_n[X]$ possède au moins $n+1$ zéros notés $\alpha_0,\ldots,\alpha_n$. Montrons que $P=0$. D'après le **Théorème** précédent, il existe $Q\in\mathbf{K}[X]$ tel que :

$$P(X)=Q(X)\times\prod_{k=0}^{n}(X-\alpha_k) \tag{15.3}$$

  Identifions les degrés des deux membres de cette égalité, il vient par la **Proposition** 15.4 :

$$d^\circ P=d^\circ Q+n+1$$

  Par hypothèse, $P\in\mathbf{K}_n[X]$, c'est-à-dire $d^\circ P\leq n$. Par conséquent, le degré de $Q$ satisfait l'inégalité $n\geq d^\circ Q+n+1$ c'est-à-dire $d^\circ Q\leq -1$. Il s'ensuit que nécessairement $d^\circ Q=-\infty$. Ainsi $Q$ est le polynôme nul. Il suffit alors de se rappeler de (15.3), pour conclure $P=0$.
- Supposons que $P$ soit exactement de degré $n$, alors $P$ n'est pas le polynôme nul. Par conséquent il admet au plus $n$ racines distinctes d'après le premier ■. ▲

**Exercice :** Soit $n\in\mathbf{N}^\star$, on note $\omega=e^{2i\pi/n}$. Démontrez la factorisation suivante :

$$X^n-1=\prod_{k=0}^{n-1}(X-\omega^k)$$

*Solution* ▽

*Soit $P(X)=X^n-1$. Les racines de $P$ sont les nombres complexes qui vérifient l'équation polynomiale $P(z)=0$, soit :*

$$z^n=1.$$

*Ainsi, les racines de $P$ sont les racines $n^{\text{ièmes}}$ de 1. D'après le* **Théorème** *2.31, il s'agit de $1$, $\omega$, $\omega^2$, ... , $\omega^{n-1}$. D'après la* **Proposition** *15.23, il en résulte immédiatement que*

$$\prod_{k=0}^{n-1}(X-\omega^k)\ \textit{divise}\ P=X^n-1$$

*Comme de plus ces deux polynômes ont visiblement le même degré $n$, il en résulte l'existence d'une constante $c\in\mathbf{C}^\star$ telle que*

$$P=c\cdot\prod_{k=0}^{n-1}(X-\omega^k).$$

*Enfin, un simple examen des coefficients dominants de ces polynômes permet d'en conclure que $c=1$, comme annoncé dans l'énoncé.* ▲

## 2 Racines multiples

### 2.a Définition

Supposons que $\alpha$ soit une racine d'un polynôme $P \in \mathbf{K}[X]$. D'après le **Théorème** 15.22, il existe un polynôme $Q_1 \in \mathbf{K}[X]$ tel que

$$P(X) = (X-\alpha) \times Q_1(X)$$

Il se peut très bien que $\alpha$ soit aussi racine de $Q_1$. Il existe alors un polynôme $Q_2$ tel que $Q_1(X) = (X-\alpha)\times Q_2(X)$. En ce cas, nous pouvons écrire

$$P(X) = (X-\alpha)^2 \times Q_2(X)$$

Bien entendu, il peut arriver que $\alpha$ soit aussi racine de $Q_2$, auquel cas il existe un polynôme $Q_3 \in \mathbf{K}[X]$ tel que

$$P(X) = (X-\alpha)^3 \times Q_3(X)$$

$$\vdots$$

Ainsi de suite, jusqu'à ce que l'on obtienne une expression

$$P(X) = (X-\alpha)^k \times Q_k(X)$$

où $Q_k(\alpha) \neq 0$, ce qui revient à dire que l'on ne peut plus factoriser par $(X-\alpha)$.

Au vu de cette remarque, il est intéressant de **quantifier** la notion de racine. Nous adoptons la définition suivante :

**Définition :** *Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$ une racine de $P$.*
*On appelle **ordre de multiplicité** de la racine $\alpha$ de $P$, le plus grand entier $k \in \mathbf{N}^\star$ tel que $P$ soit divisible par $(X-\alpha)^k$.*

- *Lorsque $k=1$ (resp. $k=2$, $k=3$), on dit que $\alpha$ est **racine simple** (resp. **double**, **triple**) de $P$.*
- *De manière générale, lorsque $k>1$, on dit que $\alpha$ est **racine multiple** de $P$.*

### 2.b Une première caractérisation

La proposition qui suit est une simple traduction quantifiée de la notion de racine de multiplicité $k$ :

**Proposition 15.25.—** Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$.

$$\alpha \text{ est racine d'ordre } k \in \mathbf{N}^\star \text{ de } P \iff \text{il existe } Q \in \mathbf{K}[X] \text{ tel que } \begin{cases} \bullet & P = (X-\alpha)^k \times Q \\ \bullet & Q(\alpha) \neq 0 \end{cases}$$

**Démonstration** ▽
Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$, et $k \in \mathbf{N}^\star$. Formons la division euclidienne de $P$ par $(X-\alpha)^k$ : il vient

$$P = (X-\alpha)^k \times Q + R \qquad , \text{ où } d^\circ R < k$$

- Supposons que $\alpha$ soit racine d'ordre $k$ de $P$, alors d'après la définition ci dessus, $P$ est divisible par $(X-\alpha)^k$, mais non par $(X-\alpha)^{k+1}$. Par conséquent, le reste dans la division euclidienne de $P$ par $(X-\alpha)^k$ est nul, de sorte que $P = (X-\alpha)^k \times Q$. Montrons par l'*absurde* que $Q(\alpha)$ est non nul. Supposons *au contraire* que $Q(\alpha)=0$, *i.e.* $\alpha$ est racine de $Q$. D'après la caractérisation des racines (**Théorème** 15.22), il s'en suivrait que $(X-\alpha)$ divise $Q$. Mais en ce cas, $(X-\alpha)\times(X-\alpha)^k = (X-\alpha)^{k+1}$ diviserait $P$, ce qui *contredit* notre hypothèse.
  Ainsi $P = (X-\alpha)^k \times Q$ et $Q(\alpha) \neq 0$.
- Réciproquement, supposons que $P$ s'écrive $P = (X-\alpha)^k \times Q$ avec $Q(\alpha) \neq 0$. Dès lors, il est clair que $(X-\alpha)^k$ divise $P$. D'autre part, Montrons par l'absurde que $(X-\alpha)^{k+1}$ ne divise pas $P$. Supposons au contraire que $P$ s'écrive $P = (X-\alpha)^{k+1} \times Q_1 = (X-\alpha)^k \times \big((X-\alpha)\times Q_1\big)$. Par unicité du quotient dans la division euclidienne de $P$ par $(X-\alpha)^k$, il en résulte que $Q = (X-\alpha)\times Q_1$. Par la caractérisation des racines, il s'en suivrait que $\alpha$ est racine de $Q$, ce qui *contredit* le fait que $Q(\alpha) \neq 0$. ▲

**Exercice :** En effectuant la division euclidienne de $P = X^5 - X^4 - 2X^3 + 2X^2 + X - 1$ par $(X-1)^3$, démontrez que 1 est racine d'ordre de multiplicité 3 de $P$.

*Solution* ▽
*En posant la division suivant les puissances décroissantes, j'obtiens :*

$$X^5 - X^4 - 2X^3 + 2X^2 + X - 1 = (X^3 - 3X^2 + 3X - 1) \times (X^2 + 2X + 1) = (X-1)^3 \times (X+1)^2$$

*Ainsi,* $P(X) = (X-1)^3 Q_3(X)$, *où* $\tilde{Q}_3(1) = 4 \neq 0$. *D'après* **Proposition** *15.25 ceci garantit que* 1 *est une racine d'ordre 3 de* $P$. ▲

### 2.c Caratérisation des racines multiples

Nous disposons d'un critère **fondamental** pour déterminer l'ordre de multiplicité des racines d'un polynôme :

**Exemple introductif**
Soit $P = X^4 - 4X^3 + 3X^2 + 2X - 2 \in \mathbf{R}_4[X]$.

**1.** Montrez que $P(1) = P'(1) = 0$ et $P''(1) \neq 0$.

**2.** Déterminez son ordre de multiplicité.

**3.** En déduire une factorisation de $P$.

**Théorème 15.26.— Caractérisation des racines multiples —.** Soit $P \in \mathbf{K}[X]$ un polynôme, $\alpha \in \mathbf{K}$ un nombre réel ou complexe, et $k \in \mathbf{N}^\star$. Les assertions suivantes sont équivalentes :

$$\alpha \text{ est racine d'ordre } k \text{ de } P \quad \textit{si et seulement si} \quad \begin{cases} \bullet & P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \\ \bullet & P^{(k)}(\alpha) \neq 0 \end{cases}$$

**En pratique :** avant de donner la preuve de ce résultat fondamental, voyons quelles en sont les principales applications

- pour démontrer qu'**un nombre** $\alpha$ est **racine d'ordre 2** d'un polynôme $P$ vous calculez simplement $\tilde{P}(\alpha)$, $\tilde{P}'(\alpha)$ et $\tilde{P}''(\alpha)$.
- pour démontrer qu'**un polynôme** $P$ est **divisible** par $(X-\alpha)^r$ , il vous suffit de vérifier que $P(\alpha) = P'(\alpha) = \cdots = P^{(r-1)}(\alpha) = 0$.

**Démonstration** ▽
Pour démontrer l'équivalence proposée dans le **Théorème** 15.26, remarquons tout d'abord que la **formule de Taylor** en $\alpha$ donne :

$$\begin{aligned} P &= \sum_{j=0}^{n} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j = \sum_{j=0}^{k-1} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j + \sum_{j=k}^{n} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j \\ &= \underbrace{\sum_{j=0}^{k-1} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j} + (X-\alpha)^k \times \underbrace{\sum_{j=k}^{n} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^{j-k}} \\ &= R + (X-\alpha)^k \times Q, \end{aligned}$$

avec les notations évidentes pour $Q$ et $R$. Il est clair que $R$ est de degré au plus égal à $k-1$, par conséquent l'égalité :

$$P = R + (X-\alpha)^k \times Q \tag{15.4}$$

n'est autre que la *division euclidienne* de $P$ par $(X-\alpha)^k$.

Par définition, $\alpha$ est racine d'ordre $k$ de $P$ *ssi* $\begin{cases} \bullet & P \text{ est divisible par } (X-\alpha)^k \\ \bullet & P \text{ n'est pas divisible par } (X-\alpha)^{k+1} \end{cases}$.

Autrement dit, $\alpha$ est racine d'ordre $k$ de $P$ *si et seulement si* le *reste* de la division euclidienne de $P$ par $(X-\alpha)^k$ est nul, tandis que le *quotient* de la division euclidienne de $P$ par $(X-\alpha)^k$ ne s'annule pas en $\alpha$.

D'après (15.4) nous connaissons **le** *reste* et **le** *quotient* de la division euclidienne de $P$ par $(X-\alpha)^k$ : il s'agit respectivement des polynômes $R$ et $Q$ définis dans la remarque préliminaire. Par conséquent :

$$\alpha \text{ est racine d'ordre } k \text{ de } P \iff \begin{cases} R & = & 0 \\ Q(\alpha) & \neq & 0 \end{cases} \tag{15.5}$$

Or l'unicité des coefficients dans le développement d'un polynôme en puissances de $(X-\alpha)$ (**Corollaire** 15.21), permet d'affirmer que $R$ est nul si et seulement si toutes les dérivées d'ordre inférieur ou égal à $k-1$ s'annulent en $\alpha$. D'autre part, un calcul élémentaire montre que $Q(\alpha) = (1/k!)\,P^{(k)}(\alpha)$. Par conséquent , $Q(\alpha)$ est non nul *si et seulement si* $P^{(k)}(\alpha)$ est non nul. Réinjectons ces équivalences dans (15.5), nous obtenons finalement :

$$\alpha \text{ est racine d'ordre } k \text{ de } P \iff \begin{cases} P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \\ P^{(k)}(\alpha) \neq 0 \end{cases}$$

▲

## 3 Nombre de racines et degré d'un polynôme

Nous pouvons à présent généraliser la **Proposition** 15.23 au cas des racines *répétées* :

**Théorème 15.27.—** Soit $(\alpha_1, \ldots, \alpha_p) \in \mathbf{K}^p$ un $p$-uplet d'éléments **distincts** de $\mathbf{K}$.

Pour tout $k \in [\![1, p]\!]$, $\alpha_k$ est racine de multiplicité supérieure à $r_k \in \mathbf{N}^\star$ de $P$

*si et seulement si*

$$\prod_{k=1}^{p} (X-\alpha_k)^{r_k} \text{ divise } P$$

**Démonstration** ▽

- Supposons que $P$ se factorise sous la forme $P = \left(\prod_{k=1}^{p} (X-\alpha_k)^{r_k}\right) \times Q$.

  En ce cas, pour tout entier $k \in [\![1, p]\!]$, l'ordre de multiplicité de $\alpha_k$ est au moins égal à $r_k$.

- Réciproquement, montrons par récurrence sur $p \in \mathbf{N}^\star$ que si pour tout $k \in [\![1, p]\!]$, $\alpha_k$ est une racine de $P$ de multiplicité supérieure à $r_k \in \mathbf{N}^\star$ de $P$ alors $P$ est divisible par $\prod_{k=1}^{p} (X-\alpha_k)^{r_k}$.

  **Initialisation :** lorsque $p = 1$, ceci découle immédiatement de la définition de racine d'ordre $r_1$.

  **Hérédité :** soit $p \geq 1$ tel que la propriété est vérifiée pour tout polynôme $P$ et pour tout $p$-uplet de racines distinctes de $P$.
  Soit $P \in \mathbf{K}[X]$ un polynôme et $\alpha_0, \alpha_1, \ldots, \alpha_p$, $p+1$ racines distinctes de $P$ de multiplicités supérieures à $r_0, r_1, \ldots, r_p$.
  Par hypothèse de récurrence, on sait que $\prod_{k=1}^{p} (X-\alpha_k)^{r_k}$ divise $P$ : il existe donc $Q_1 \in \mathbf{K}[X]$ tel que

  $$P = Q_1 \times \prod_{k=1}^{p} (X-\alpha_k)^{r_k}$$

  De plus, en évaluant en $\alpha_0$, il vient $0 = P(\alpha_0) = Q_1(\alpha_0) \times \prod_{k=1}^{p} (\alpha_0 - \alpha_k)^{r_k}$. Comme par hypothèse les $(\alpha_k)$ sont deux à deux dictinctes, il en résulte que $\alpha_0$ est racine de $Q_1$.
  Notons $r$ l'ordre de multiplicité de $\alpha_0$ comme racine de $Q_1$ D'après la **petite caractérisation**, (**Proposition** 15.25), il existe $Q_2 \in \mathbf{K}[X]$ tel que

  $$Q_1 = Q_2 \times (X-\alpha_0)^r \text{ avec } \; Q_2(\alpha_0) \neq 0$$

  Réinjectons ceci dans l'expression de $P$, il s'ensuit que

  $$P = (X-\alpha_0)^r \times \underbrace{Q_2 \times \prod_{k=1}^{p} (X-\alpha_k)^{r_k}}_{Q(X)} = (X-\alpha_0)^r \times Q(X)$$

  Comme $Q(\alpha_0) \neq 0$, $r$ est l'ordre de multiplicité de $\alpha_0$ comme racine de $P$, en particulier, $r \geq r_0$. Ainsi,

  $$\prod_{k=0}^{p} (X-\alpha_k)^{r_k} \text{ divise } P$$

**Conclusion :** La propriété est vraie pour $p = 1$, elle est héréditaire à partir de la première génération. Elle est vraie pour tout entier $p \in \mathbf{N}^\star$.

▲

Comme conséquence, nous en déduisons le

**Corollaire 15.28.—** Soit $(n, p) \in \mathbf{N}^2$, $P \in \mathbf{K}_n[X]$ un polynôme de degré inférieur ou égal à $n$, $\alpha_1, \ldots, \alpha_p$ des racines distinctes de $P$. Notons pour chaque $k \in [\![1, p]\!]$, $r_k \in \mathbf{N}^\star$ l'ordre de multiplicité de $\alpha_k$. Alors

- si $\displaystyle\sum_{k=1}^{p} r_k \geq n+1$ alors $P = 0$.
- si $d^\circ P = n$, alors $\displaystyle\sum_{k=1}^{p} r_k \leq d^\circ P$ avec égalité *si et seulement si* $P = a_n \prod_{k=1}^{p} (X - \alpha_k)$

**Commentaires :** En français, ≪*la somme des ordres de multiplicité des racines de $P$ est inférieure au degré de $P$*≫.

**Exercice :** Déterminez le reste de la division euclidienne de $A = X^n + 2X - 2$ par $B = (X-1)^2$

**Exercice :** Soit $P \in \mathbf{K}[X]$ le polynôme défini pour $n \in \mathbf{N}^\star$ par
$$P = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n.$$

**1.** Montrez que $(X-1)^3 | P$.

**2.** Déterminez le quotient de la division euclidienne de $P$ par $(X-1)^3$.
**Indication :** vous pourrez développer $P$ en puissances de $(X-1)$ à l'aide de la **formule de Taylor**.

## 4 Polynômes scindés

### 4.a Définition

**Définition :** *Un polynôme $P \in \mathbf{K}[X]$ est dit **scindé** sur $\mathbf{K}$ s'il existe $a \in \mathbf{K}^\star$, $(x_1, \ldots, x_n) \in \mathbf{K}^n$ tels que*
$$P = a(X - x_1) \times \cdots \times (X - x_n)$$

**Exemple :** Dans $\mathbf{C}[X]$ nous verrons que tout polynôme est scindé d'après le **Théorème de factorisation** dans $\mathbf{C}[X]$. En revanche, ce n'est pas le cas dans $\mathbf{R}[X]$. Par exemple, le polynôme $P = X^2 + 2X + 2 \in \mathbf{R}[X]$ n'est pas scindé, il possède deux racines complexes conjuguées.

### 4.b Caractérisation à l'aide de ses racines d'un polynôme scindé

**Proposition 15.29.—** Soit $P \in \mathbf{K}[X]$ un polynôme de degré $n \in \mathbf{N}$. On note $(\alpha_1, \ldots, \alpha_p) \in \mathbf{K}^p$ ses racines distinctes de multiplicités respectives $(r_1, \ldots, r_p)$. Alors

$$P \text{ est scindé sur } \mathbf{K} \textit{ si et seulement si } \sum_{k=1}^{p} r_k = n$$

**Commentaires :** un polynôme $P$ de degré $n$ est scindé s'il possède $n$ racines distinctes ou confondues.

**Démonstration** ▽
Dans $\mathbf{C}[X]$ tout polynôme est scindé. Dans $\mathbf{R}[X]$, la condition $\sum_{k=1}^{p} r_k = n$ garantit qu'il n'existe pas de racines complexes conjuguées. Ainsi, d'après le théorème de factorisation dans $\mathbf{R}[X]$, $P$ est scindé.

### 4.c Relations coefficients et racines d'un polynôme scindé

Soit $P = X^2 + \sigma_1 X + \sigma_2$ un polynôme de degré 2. Nous avons déjà observé que $x_1$ et $x_2$ sont racines de $P$ si et seulement si $(x_1, x_2)$ est solution du système

$$\begin{cases} x_1 + x_2 &= -\sigma_1 \\ x_1 \times x_2 &= \sigma_2 \end{cases}$$

Cette propriété se généralise aux polynômes de degré quelconque, à l'aide des fonctions symétriques élémentaires.

**Définition :** *Soit $n \in \mathbf{N}^\star$, $(x_1, \dots, x_n) \in \mathbf{K}^n$. On appelle* ***fonctions symétriques élémentaires*** *des $x_1, \dots x_n$ les quantités suivantes :*

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{n} x_i \\
\sigma_2 &= \sum_{1\leq i_1<i_2\leq n} x_{i_1}x_{i_2} \\
\sigma_3 &= \sum_{1\leq i_1<i_2<i_3\leq n} x_{i_1}x_{i_2}x_{i_3} \\
\sigma_k &= \sum_{1\leq i_1<i_2<\cdot<i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k} \\
\sigma_n &= x_1x_2\cdots x_n
\end{aligned}$$

**Commentaires :** en clair, $\sigma_k$ est la somme de tous les produits possibles de $k$ facteurs d'indice distincts parmi $x_1, x_2, \dots, x_n$. $\sigma_k$ est donc une somme de $\binom{n}{k}$ termes !

**Exemple :**

- pour $n = 2$, $\sigma_1 = x_1 + x_2$, $\sigma_2 = x_1x_2$ ;
- pour $n = 3$, $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.

Si $P$ est un polynôme scindé, ses coefficients s'expriment à l'aide des fonctions symétriques élémentaires :

**Proposition 15.30.—** Soit $n \in \mathbf{N}^\star$, $(x_1, \dots, x_n) \in \mathbf{K}^n$ et $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires de $x_1, \dots, x_n$. Alors

$$(X - x_1) \times \cdots \times (X - x_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_n$$

**Démonstration** ▽

Commençons par $n = 3$. On obtient en développant

$$\begin{aligned}
(X - x_1)(X - x_2)(X - x_3) &= (X - x_1) \times \left[X^2 - (x_2 + x_3)X + x_2x_3\right] \\
&= X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_1x_3 + x_2x_3)X - x_1x_2x_3 \\
&= X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3
\end{aligned}$$

Le cas général s'obtient de la même manière, par identification des coefficients. ▲

On en déduit

**Théorème 15.31.—** Soit $P = a_nX^n + \cdots + a_1X + a_0$ un polynôme scindé de degré $n \in \mathbf{N}^\star$. Pour tout $(x_1, \dots, x_n) \in \mathbf{K}^n$,

$x_1, \dots, x_n$ sont les racines distinctes ou confondues de $P$ *si et seulement si* $\forall k \in [\![1, n]\!],\ \sigma_k = (-1)^k \dfrac{a_{n-k}}{a_n}$

**Commentaires :** Dans le cas particulier $n = 2$, nous retrouvons :

$$x_1 \text{ et } x_2 \text{ sont les racines de } P = aX^2 + bX + c \ \textit{ si et seulement si } \begin{cases} x_1 + x_2 &= -b/a \\ x_1 \times x_2 &= c/a \end{cases}$$

Si $P = aX^3 + bX^2 + cX + d$, avec $a \neq 0$, nous obtenons $x_1, x_2, x_3$ sont les racines distinctes ou confondues de $P$ *si et seulement si* $(x_1, x_2, x_3)$ est solution du système

$$\begin{cases} x_1 + x_2 + x_3 &= -b/a \\ x_1x_2 + x_1x_3 + x_2x_3 &= c/a \\ x_1x_2x_3 &= -d/a \end{cases}$$

**Exercice :** Déterminez les racines complexes de $P = X^3 - 4X^2 + 6X - 4$ sachant que la somme de deux de ses racines est égale à la troisième.

*Solution* ▽

*Notons $a$, $b$ et $c$ les racines complexes distinctes ou confondues de $P$. Supposons que $c = a+b$. D'après le théorème précédent, $P$ s'écrit*

$$P = X^3 - 4X^2 + 6X - 4 = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$$

*Par identification des coefficients, nous en déduisons que les racines $a$, $b$ et $c$ vérifient le système d'équations suivant :*

$$\left\{\begin{array}{rcl} a+b & = & c \\ a+b+c & = & 4 \\ ab+ac+bc & = & 6 \\ abc & = & 4 \end{array}\right. \iff \left\{\begin{array}{rcl} a+b & = & c \\ 2c & = & 4 \\ ab+c^2 & = & 6 \\ abc & = & 4 \end{array}\right. \iff \left\{\begin{array}{rcl} c & = & 2 \\ a+b & = & 2 \\ a\times b & = & 2 \end{array}\right.$$

*Ainsi, $(a,b)$ est solution du système $\left\{\begin{array}{rcl} a+b & = & 2 \\ a\times b & = & 2 \end{array}\right.$. Ce sont donc les racines du polynôme $X^2 - 2X + 2$.*

*Le discriminant de ce polynôme est $\Delta = 4-8 = -4 = (2i)^2$. Ses racines sont donc $a = \dfrac{2+2i}{2} = 1+i$ et $b = \dfrac{2-2i}{2} = 1-i$.*

*Finalement, les racines de $P$ sont $a = 1+i, b = 1-i$ et $c = 2$.* ▲

**Exercice :** Résolvez les systèmes suivants d'inconnues $(x,y,z) \in \mathbf{C}^3$

$$\left\{\begin{array}{rcl} x+y+z & = & 2 \\ xy+xz+yz & = & -5 \\ xyz & = & -6 \end{array}\right. \qquad \left\{\begin{array}{rcl} x+y+z & = & 1 \\ x^2+y^2+z^2 & = & 9 \\ x^3+y^3+z^3 & = & 1 \end{array}\right.$$

*Solution* ▽

- *Notons $\sigma_1, \sigma_2, \sigma_3$ les fonctions symétriques élémentaires de $x, y$ et $z$. D'après le théorème précédent, $x, y$ et $z$ sont les racines du polynôme $P = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$. En identifiant, on obtient*

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

  *1 et racine évidente. Donc $P$ est divisible par $(X-1)$ : $P = (X-1)(X^2 - X - 6)$. 3 et $-2$ sont racines évidentes de $X^2 - X - 6$. Par conséquent, les racines de $P$ sont $1, -2$ et $3$. Les solutions du système symétrique proposé sont les permutations de $(1,-2,3)$.*
- *Notons comme précédemment $\sigma_1, \sigma_2, \sigma_3$ les fonctions symétriques élémentaires de $x, y$ et $z$. Introduisons en outre les quantités*

  $$\begin{array}{rcl} S_1 & = & x+y+z \\ S_2 & = & x^2+y^2+z^2 \\ S_3 & = & x^3+y^3+z^3 \end{array}$$

  *Nous pouvons exprimer ces quantités symétriques en $x$, $y$ et $z$ à l'aide des fonctions symétriques élémentaires grâce aux relations,*

  $$\begin{array}{rcl} \sigma_1 & = & S_1 \\ \sigma_1^2 & = & S_2 + 2\sigma_2 \\ \sigma_1^3 & = & S_3 + 3\big[x^2y + x^2z + y^2x + y^2z + z^2x + z^2y + \big] + 6xyz = S_3 + 3\big[S_2S_1 - S_3\big] + 6\sigma_3 \end{array}$$

  *Supposons que $(x,y,z)$ est solution du système $\left\{\begin{array}{rcl} S_1 & = & 1 \\ S_2 & = & 9 \\ S_3 & = & 1 \end{array}\right.$ Il vient $\left\{\begin{array}{rcl} \sigma_1 & = & 1 \\ 9+2\sigma_2 & = & 1 \\ 1+3(S_2S_1 - S_3) + 6\sigma_3 & = & 1 \end{array}\right.$. D'où l'on tire $\left\{\begin{array}{rcl} \sigma_1 & = & 1 \\ \sigma_2 & = & -4 \\ \sigma_3 & = & -4 \end{array}\right.$*

  *Ainsi, $x, y, z$ sont les racines de $P = X^3 - X^2 - 4X + 4$. 1 est racine évidente de $P$. Donc $P = (X-1)(X^2-4) = (X-1)(X-2)(X+2)$.*

  *Par conséquent, $(x,y,z)$ est une permutation de $(1,2,-2)$.*
  *Réciproquement, on vérifie aisément que toute permutation de $(1,2,-2)$ est solution du système proposé.*

  ▲

**Remarque :** toute expression symétrique par rapport à $x_1, \dots, x_n$ peut être exprimée à l'aide de $\sigma_1, \dots, \sigma_n$.

## 5 Formule d'interpolation de Lagrange

**Théorème 15.32.— Interpolation de Lagrange —.** Soit $x_1, \dots, x_n$ des nombres distincts, $y_1, \dots, y_n$ quelconques. Il existe un polynôme $P \in \mathbf{K}_{n-1}[X]$, unique tel que $\forall i \in [\![1, n]\!]$, $P(x_i) = y_i$. $P$ est donné par $P(X) = \sum_{i=1}^{n} y_i \Big[ \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{X - x_j}{x_i - x_j} \Big]$.

# IV Arithmétique dans $\mathbf{K}[\mathrm{X}]$

Comme nous l'avons vu, la structure algébrique de $\mathbf{K}[X]$ est très proche de celle de $\mathbf{Z}$. En particulier, nous disposons encore de l'outil fondamental qu'est la division euclidienne.

## 1 PGCD de deux polynômes

### 1.a Diviseurs communs à deux polynômes

**Définition :** *Soit $(A, B) \in \mathbf{K}[X]^2$. On note $\mathcal{D}(A)$ l'ensemble des diviseurs de $A$. On note $\mathcal{D}(A, B)$ l'ensemble des diviseurs communs à $A$ et à $B$ :*

$$\mathcal{D}(A, B) = \mathcal{D}(A) \cap \mathcal{D}(B)$$

**Exemple :**

1. $X^2 - 1$ est un diviseur commun à $X^3 - X$ et $X^4 - 1$,
2. $\mathcal{D}(0) = \mathbf{K}[X]$, et pour tout polynôme $A \in \mathbf{K}[X]$, $\mathcal{D}(A, 0) = \mathcal{D}(A)$.

**Remarque :** Si $P \in \mathcal{D}(A, B)$, tout diviseur associé à $P$ est aussi un diviseur commun à $A$ et $B$.

### 1.b Plus grand diviseur commun à deux polynômes

**Théorème 15.33.— plus grand commun diviseur de deux polynômes —.** Soit $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ un couple de polynômes non nuls. Il existe un unique polynôme $\Delta \in \mathbf{K}[X]$ tel que

- $\Delta$ est unitaire
- $\mathcal{D}(A, B) = \mathcal{D}(\Delta)$

**Définition :** *Ce polynôme $\Delta$ est appelé le **plus grand diviseur commun** de $A$ et de $B$, on note*

$$\Delta = PGCD(A, B) \text{ ou } \Delta = A \wedge B.$$

On déduit immédiatement de la définition de PGCD la propriété suivante :

**Corollaire 15.34.—** Soit $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ un couple de polynômes non nuls. On note $\Delta = A \wedge B$. Pour tout polynôme $P \in \mathbf{K}[X]$, on a l'équivalence :

$$P \mid A \text{ et } P \mid B \iff P \mid \Delta$$

**Commentaires :** tout diviseur commun à $A$ et $B$ est un diviseur de $A \wedge B$.

**Démonstration** ▽

- **Unicité :** soit $(\Delta_1, \Delta_2)$ un couple de polynômes unitaires tels que $\mathcal{D}(\Delta_1) = \mathcal{D}(\Delta_2)$. En ce cas, $\Delta_1$ et $\Delta_2$ sont associés. Comme de plus ils sont unitaires, ils sont égaux.

- **Existence :** la preuve sera par récurrence sur $n \in \mathbf{N}$, où $B \in \mathbf{K}_n[X]$ est un polynôme non nul de degré inférieur ou égal à $n$.
- **Initialisation :** si $d^\circ B = 0$, $B$ est une constante non nulle, donc $\Delta = 1$ convient.
- **Hérédité :** soit $n \in \mathbf{N}$. Supposons le résultat établi pour tout polynôme $B$ de degré inférieur ou égal à $n$.
  Soit $B \in \mathbf{K}[X]$ un polynôme non nul de degré inférieur ou égal à $n+1$. Effectuons la division euclidienne de $A$ par $B$ : il existe un couple $(Q, R) \in \mathbf{K}[X]$, unique tel que $A = BQ + R$ avec $d^\circ R \leq n$.
  Montrons que
  $$\mathcal{D}(A, B) = \mathcal{D}(B, R)$$
  - Soit $P$ un diviseur commun à $B$ et $R$. En ce cas $P$ divise aussi $A = BQ + R$. Ceci étant vrai pour tout polynôme $P \in \mathcal{D}(B, R)$, il en résulte que $\mathcal{D}(B, R) \subset \mathcal{D}(A, B)$.
  - Soit $P$ un diviseur commun à $A$ et $B$. En ce cas, $P$ divise aussi $R = A - BQ$. Ceci étant vrai pour tout polynôme $P \in \mathcal{D}(A, B)$, il s'ensuit que $\mathcal{D}(A, B) \subset \mathcal{D}(B, R)$.
  - par double-inclusion, nous avons prouvé que $\mathcal{D}(A, B) = \mathcal{D}(B, R)$.

  Comme de plus $d^\circ R \leq n$, l'hypothèse de récurrence s'applique : il existe un polynôme $\Delta$, unitaire tel que
  $$\mathcal{D}(A, B) = \mathcal{D}(B, R) = \mathcal{D}(\Delta)$$
- **Conclusion :** OK

▲

### 1.c Algorithme d'Euclide

Dans la démonstration ci-dessus, nous avons établi, la propriété suivante :

**Théorème 15.35.—** Soit $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ un couple de polynômes non nuls. Soit $(Q, R) \in \mathbf{K}[X] \times \mathbf{K}[X]$ le quotient et le reste de la division euclidienne de $A$ par $B$. Alors

$$\boxed{\mathcal{D}(A, B) = \mathcal{D}(B, R)}$$

En particulier, si $R$ est non nul

$$\boxed{PGCD(A, B) = PGCD(B, R)}$$

**Remarque :** lorsque $R$ est nul, $PGCD(A, B) = PGCD(B, 0)$ est le polynôme unitaire associé à $B$.

**En pratique :** pour déterminer le PGCD de deux polynômes, vous utilisez de façon répétée la **Proposition** 15.35.

**Mise en œuvre** :
On souhaite calculer $\Delta = A \wedge B$. Si $d^\circ A \geq d^\circ B$, on note $A_0 = A$, $A_1 = B$, sinon, on note $A_0 = B$ et $A_1 = A$.

- **Etape 1** on effectue la division euclidienne de $A_0$ par $A_1$.
  $$A_0 = A_1 Q_1 + A_2, \text{ avec } d^\circ A_2 < d^\circ A_1$$
  D'après la proposition précédente, on a
  $$\mathcal{D}(A_0, A_1) = \mathcal{D}(A_1, A_2)$$
  ►Si $A_2$ est nul, alors on peut conclure : $\mathcal{D}(A_0, A_1) = \mathcal{D}(A_1)$. $\Delta$ est donc le polynôme unitaire associé à $A_1$.
  ►si $A_2$ est non nul, on passe à l'
- **Etape 2**on effectue la division euclidienne de $A_1$ par $A_2$.
  $$A_1 = A_2 Q_2 + A_3, \text{ avec } d^\circ A_3 < d^\circ A_2$$
  D'après la proposition précédente, on a
  $$\mathcal{D}(A_1, A_2) = \mathcal{D}(A_2, A_3)$$

►Si $A_3$ est nul, alors on peut conclure : $\mathcal{D}(A_0, A_1) = \mathcal{D}(A_1, A_2) = \mathcal{D}(A_2, A_3)\mathcal{D}(A_2)$. $\Delta$ est donc le polynôme unitaire associé à $A_2$.
►si $A_3$ est non nul, on passe à l'étape suivante ...

- **ainsi de suite ...**
  Comme les degrés des polynômes $A_2$, $A_3$, *etc.* forment une suite strictement décroissante d'entiers naturels, après un nombre fini $m$ d'étapes, on obtient nécessairement un reste nul. A la fin :
- **Etape** $m$on effectue la division euclidienne de $A_{m-1}$ par $A_m$.

$$A_{m-1} = A_m Q_m + 0$$

D'après la proposition précédente, on a

$$\mathcal{D}(A_0, A_1) = \mathcal{D}(A_1, A_2) = \cdots = \mathcal{D}(A_m, 0) = \mathcal{D}(A_m)$$

Retenez que :

**Proposition 15.36.—** Soit $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ un couple de polynômes non nuls.

$\boxed{A \wedge B \text{ est le polynôme unitaire associé au dernier reste non nul de l'algorithme d'Euclide.}}$

**Exercice :** Déterminez le PGCD de $A = X^3 + X^2 - 2$ et $B = X^3 + X - 2$

*Solution* ▽

$$\begin{aligned} X^3 + X^2 - 2 &= (X^3 + X - 2) \times 1 + (X^2 - X) \\ X^3 + X - 2 &= (X^2 - X) \times (X + 1) + \boxed{2X - 2} \\ X^2 - X &= (2X - 2) \times \frac{1}{2}X + 0 \end{aligned}$$

*Par conséquent,* $A \wedge B = X - 1$. ▲

### 1.d Égalité de Bézout

**Théorème 15.37.— Égalités de Bézout —.** Soit $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ et $D = A \wedge B$ leur PGCD. Alors, il existe $(U, V) \in \mathbf{K}[X] \times \mathbf{K}[X]$ tel que

$$\boxed{A \times U + B \times V = D}$$

**Démonstration** ▽
il s'agit comme dans $\mathbf{Z}$ de remonter dans l'algorithme d'Euclide. Après $m$ étapes l'algorithme d'Euclide donne

$$\begin{aligned} A_0 &= A_1 Q_1 + A_2 \\ A_1 &= A_2 Q_2 + A_3 \\ A_2 &= A_3 Q_3 + A_4 \\ &\vdots \\ A_{m-2} &= A_{m-1} Q_{m-1} + \boxed{A_m} \end{aligned}$$

La dernière équation permet d'obtenir $A_m$ en fonction de $A_{m-2}$ et de $A_{m-1}$. En remontant, on arrive finalement à $A_m$ en fonction de $A_0$ et $A_1$. ▲

**Exercice :** Déterminez une relation de Bézout entre $A = X^3 + X^2 - 2$ et $B = X^3 + X - 2$

*Solution* ▽
*On a*

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

*Par conséquent,*

$$X-1=\frac{1}{2}(X+2)\times B-\frac{1}{2}(X+1)A$$

▲

**Corollaire 15.38.—** Soit $C\in\mathbf{K}[X]$ un polynôme unitaire. Alors

$$PGCD(AC,BC)=PGCD(A,B)\times C$$

**Démonstration** ▽
Notons $\Delta=A\wedge B$ et $D=(AC)\wedge(BC)$.

- comme $\Delta$ divise $A$ et $B$, $\Delta C$ divise $AC$ et $BC$. Par conséquent $\Delta C$ divise $D$.
- comme $\Delta=A\wedge B$, il existe $(U,V)\in\mathbf{K}[X]^2$ tel que $\Delta=AU+BV$.
  Ainsi, $\Delta C=ACU+BCV$. Comme $D$ divise $AC$ et $BC$, il divise en particulier $\Delta C$.
- Ainsi $\Delta C\mid D$ et $D\mid\Delta C$. Ces deux polynômes sont donc associés. Comme de plus, ils sont unitaires, ils sont égaux.

▲

**Généralisation :** Soit $A_1,\dots,A_n$ des polynômes non nuls. Parmi les diviseurs communs de $A_1,\dots,A_n$, il existe un unique polynôme $\Delta$, unitaire et de degré maximal, appelé **plus grand diviseur commun** de $A_1,\dots,A_n$. On le note $\Delta=PGCD(A_1,\dots,A_n)$ ou $\Delta=A_1\wedge\cdots\wedge A_n$.

**Proposition 15.39.— Relation de Bézout —.** Soit $(A_1,\dots,A_n)\in(\mathbf{K}[X]\setminus\{0\})^n$, $\Delta=A_1\wedge\cdots\wedge A_n$. Alors il existe $(U,\dots,U_n)\in\mathbf{K}[X]^n$ tel que $\Delta=A_1U_1+\cdots+A_nU_n$.

## 2 PPCM de deux polynômes

**Définition :** *Soit $(A,B)\in\mathbf{K}[X]^2$. On note $A\mathbf{K}[X]$ l'ensemble des multiples de $A$. L'ensemble des diviseurs communs à $A$ et à $B$ est $A\mathbf{K}[X]\cap B\mathbf{K}[X]$.*

**Théorème 15.40.— Plus petit multiple commun de deux polynômes —.** Soit $(A,B)\in\mathbf{K}[X]$ un couple de polynômes non nuls. Il existe un unique polynôme $M$ tel que

- $M$ est unitaire
- $A\mathbf{K}[X]\cap B\mathbf{K}[X]=M\mathbf{K}[X]$

**Définition :** *$M$ est appelé le **plus grand multiple commun** de $A$ et $B$. On le note $M=PPCM(A,B)$ ou $M=A\vee B$.*

On déduit immédiatement de la définition

**Corollaire 15.41.—** Soit $(A,B)\in\mathbf{K}[X]$ un couple de polynômes non nuls. On note $M=A\vee B$. Pour tout polynôme $P\in\mathbf{K}[X]$, on a l'équivalence :

$$\boxed{A\mid P \text{ et } B\mid P \iff P\mid M}$$

**Commentaires :** tout multiple commun de $A$ et $B$ est en fait multiple de $A\vee B$.

**Démonstration** ▽

- **Unicité :** soit $(M_1,M_2)$ un couple de polynômes unitaires tels que $M_1\mathbf{K}[X]=M_2\mathbf{K}[X]$. En ce cas, $M_1$ et $M_2$ sont associés. Comme ils sont unitaires, ils sont égaux.

- **Existence :** Considérons l'application degré $d^\circ : A\mathbf{K}[X] \cap B\mathbf{K}[X] \setminus \{0\} \to \mathbf{N}$ qui à tout multiple non nul de $A$ et de $B$ associe son degré. Son image est une partie non vide de $\mathbf{N}$. D'après la propriété $\mathbf{N}_2$, il existe un polynôme non nul de degré minimal dans $A\mathbf{K}[X] \cap B\mathbf{K}[X]$. Notons $M$ le polynôme unitaire de degré minimal dans $A\mathbf{K}[X] \cap B\mathbf{K}[X]$. Montrons que $A\mathbf{K}[X] \cap B\mathbf{K}[X] = M\mathbf{K}[X]$.

▶ Comme $M$ est un multiple commun de $A$ et $B$, tout multiple de $M$ est multiple de $A$ et $B$. Autrement dit

$$M\mathbf{K}[X] \subset A\mathbf{K}[X] \cap B\mathbf{K}[X]$$

▶ Réciproquement, soit $P \in A\mathbf{K}[X] \cap B\mathbf{K}[X]$. Effectuons la division euclidienne de $P$ par $M$ : il existe un couple $(Q, R)$ de polynômes, unique tel que

$$P = MQ + R \text{ avec } d^\circ R < d^\circ M$$

Comme $P$ et $M$ sont des multiples communs à $A$ et $B$, il s'ensuit que $R = P - MQ$ appartient à $A\mathbf{K}[X]B\mathbf{K}[X]$. Comme $M$ est le polynôme unitaire de plus bas degré dans $A\mathbf{K}[X]B\mathbf{K}[X]$, il en résulte que $R$ est nul. Par conséquent, $P = MQ \in M\mathbf{K}[X]$.
Ceci étant vrai pour tout polynôme $P \in A\mathbf{K}[X] \cap B\mathbf{K}[X]$, il s'ensuit que $A\mathbf{K}[X] \cap B\mathbf{K}[X] \subset M\mathbf{K}[X]$.

▶ Par double-inclusion, nous avons prouvé que $A\mathbf{K}[X] \cap B\mathbf{K}[X] = M\mathbf{K}[X]$. ▲

**Proposition 15.42.—** Soit $(A, B) \in \mathbf{K}[X]$ un couple de polynômes non nuls. Soit $C \in \mathbf{K}[X]$ un polynôme unitaire. Alors

$$PPCM(AC, BC) = PPCM(A, B) \times C$$

**Démonstration** ▽
Notons $M = A \vee B$ et $N = (AC) \vee (BC)$.
Comme $M$ est multiple de $A$ et $B$, $MC$ est multiple de $AC$ et $BC$. Par conséquent, $MC$ est un multiple de $N$.
Réciproquement, $N$ étant un multiple commun de $AC$ et $BC$, il est divisible par $C$. Il existe donc $D \in \mathbf{K}[X]$ tel $N = DC$.
Comme $AC$ et $BC$ divisent $N$, $D$ est divisible par $A$ et $B$. Par suite $D$ est un multiple commun de $A$ et $B$, ce qui revient à dire que $M \mid D$. Ainsi, $N$ est un multiple de $MC$.
Finalement, les polynômes $MC$ et $N$ sont associés. Comme ils sont unitaires, ils sont égaux. ▲

## 3 Polynômes premiers entre eux

### 3.a Définition

**Définition :** *Deux* ***polynômes*** *$A$ et $B$ sont dits* ***premiers entre eux*** *si leurs seuls diviseurs communs sont les polynômes constants et non nuls.*
*Autrement dit, $A$ et $B$ sont premiers entre eux si $A \wedge B = 1$.*

Pour une famille finie de polynômes, il y a deux notions de primarité.

**Définition :** *Soit $(A_1, \dots, A_n) \in (\mathbf{K}[X] \setminus \{0\})^n$. On dit que*

- *$A_1, \dots, A_n$ sont* ***premiers entre eux dans leur ensemble*** *si $PGCD(A_1, \dots, A_n) = 1$.*
- *$A_1, \dots, A_n$ sont* ***deux à deux premiers entre eux*** *si $\forall (i, j) \in [\![1, n]\!]^2$, $i \neq j \Rightarrow A_i \wedge A_j = 1$.*

### 3.b Théorème de Bézout

**Théorème 15.43.— Théorème de Bézout —.** Soit $(A, B) \in \mathbf{K}[X]$ un couple de polynômes non nuls.

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

**Exemple :** soit $(a, b) \in \mathbf{K}^2$ tel que $a \neq b$. Comme

$$1 = \frac{1}{b-a}\big[(X-a) - (X-b)\big]$$

il découle du **Théorème de Bézout** que les polynômes $X - a$ et $X - b$ sont premiers entre eux.

**Démonstration** ▽
D'après l'égalité de Bézout, si $A \vee B = \Delta$, il existe $(U,V) \in \mathbf{K}[X]^2$ tel que $AU + BV = \Delta$. En particulier, si $A$ et $B$ sont premiers entre eux, il existe $(U,V) \in \mathbf{K}[X]^2$ tel que $AU + BV = 1$.
Réciproquement, supposons qu'il existe un couple $(U,V)) \in \mathbf{K}[X]^2$ tel que $AU + BV = 1$. Soit $P$ un diviseur de $A$ et $B$. Alors d'après l'égalité de Bézout, $P$ divise 1. Par conséquent $P$ est constant et non nul. ▲

Comme dans $\mathbf{Z}$, on en déduit

**Corollaire 15.44.—**
- Si $A \wedge B = 1$ et $A \wedge C = 1$, alors $A \wedge BC = 1$.
- Si $A \wedge B_1 = \cdots = A \wedge B_n = 1$, alors $A \wedge (B_1 \cdots B_n) = 1$
- Si $A \wedge B = 1$, alors $A^n \wedge B^m = 1$

**Exemple :** soit $(a,b) \in \mathbf{K}^2$ tel que $a \neq b$. Alors $(X-a)^r$ et $(X-b)^s$ sont premiers entre eux.

**Démonstration** ▽

- D'après le **Théorème** de Bézout, il existe $(U_1,V_1) \in \mathbf{K}[X]^2$ et $(U_2,V_2) \in \mathbf{K}[X]$ tels que

$$\begin{aligned} 1 &= AU_1 + BV_1 \\ 1 &= AU_2 + CV_2 \end{aligned}$$

  Multiplions membre à membre ces égalités dans $\mathbf{K}[X]$, il vient

$$1 = A\big[AU_1U_2 + BV_1U_2 + CU_1V_2\big] + (BC)\big[V_1V_2\big]$$

  D'après le **Théorème de Bézout**, cec revient précisément à dire que $A$ et $BC$ sont premiers entre eux.
- par récurrence à partir du premier •
- D'après le deuxième • $A$ et $B^m$ sont premiers entre eux. Il s'ensuit que $A^n$ et $B^m$ sont premiers entre eux. ▲

### 3.c Lemme de Gauss

**Théorème 15.45.— Lemme de Gauss —.**

$$\boxed{\textbf{Si } A \mid BC \text{ et } A \wedge B = 1 \textbf{ alors } A \mid C}$$

**Démonstration** ▽
Comme $A$ et $B$ sont premiers entre eux, il existe d'après le **Théorème de Bézout** un couple $(U,V) \in \mathbf{K}[X]^2$ tel que

$$1 = AU + BV$$

Il en résulte que $C = ACU + BCV$. Comme par hypothèse $A$ divise $BC$, il en découle finalement que $A$ divise $C$. ▲

Comme dans le cadre de l'arithmétique des entiers, on en déduit

**Corollaire 15.46.—** Si $A \wedge B = 1$, $A \mid C$ et $B \mid C$, alors $AB \mid C$.

**Exercice :** retrouvez le résultat établi lors de notre étude des racines multiples :
Soit $(\alpha_1, \ldots, \alpha_p)$ des racines distinctes de $P$, de multiplicités respectives $(r_1, \ldots, r_p)$. Alors

$$(X-\alpha_1)^{r_1} \times \cdots \times (X-\alpha_p)^{r_p} \text{ divise } P$$

**Proposition 15.47.—** Soit $(A,B) \in \mathbf{K}[X]^2$, un couple de polynômes unitaires, alors

$$\boxed{(A \vee B) \times (A \wedge B) = A \times B}$$

**Démonstration** ▽

- Supposons tout d'abord que $A$ et $B$ sont premiers entre eux. Comme $AB$ est un multiple commun de $A$ et $B$, il s'ensuit que $A \vee B \mid AB$. D'autre part, par définition $A \mid A \vee B$ et $B \mid A \vee B$. Comme par hypothèse $A$ et $B$ sont premiers entre eux, leur produit divise $A \vee B$. Ainsi, $AB$ et $A \vee B$ sont associés. Comme ils sont tous deux unitaires, ils sont égaux.
- Dans le cas général, notons $M = A \vee B$ et $\Delta = A \wedge B$. Écrivons $A = \Delta A_0$ et $B = \Delta B_0$. Comme

$$\Delta = (\Delta A_0) \wedge (\Delta B_0) = \Delta \times (A_0 \wedge B_0)$$

il s'ensuit que $A_0$ et $B_0$ sont premiers entre eux. D'après le premier •, il en résulte que $A_0 \vee B_0 = A_0 B_0$. Par conséquent

$$M = (\Delta A_0) \vee (\Delta B_0) = \Delta A_0 B_0$$

En multipliant les deux membres par $\Delta$ nous obtenons finalement

$$M\Delta = A \times B$$

▲

# V Factorisations en produits d'irréductibles

L'objet de cette partie du chapitre est de *décomposer* les polynômes en produit de facteurs le plus simple possible, c'est-à-dire **irréductibles**.

Dans cette optique, les **Théorèmes** 15.22 et 15.26 sont fondamentaux, puisqu'ils permettent de ramener les questions de divisibilité -ou de factorisation- en la recherche de racines.

## 1 Polynômes irréductibles de $\mathbf{K}[X]$

### 1.a Définition, exemples

**Définition :** *Un polynôme $P \in \mathbf{K}[X]$ est dit **irréductible** dans $\mathbf{K}[X]$ (ou sur $\mathbf{K}$) si :*

- *$P$ est non constant ($d^\circ P \geq 1$)*
- *les seuls diviseurs de $P$ sont les constantes non nulles et les polynômes associés à $P$.*

**Commentaires :** Autrement dit, $P$ est irréductible *si et seulement si* $P$ est non constant et

$$\left(\forall (A,B) \in \mathbf{K}[X]^2\right), \quad (P = A \times B \Rightarrow A \in \mathbf{K}^\star \text{ ou } B \in \mathbf{K}^\star)$$

**Exemple :** Bien sûr, les polynômes de degré 1 sont irréductibles, mais ce ne sont pas les seuls.

**Exercice :** Le polynôme $X^2 + 1$ est-il irréductible dans $\mathbf{C}[X]$ ? dans $\mathbf{R}[X]$ ?

**Remarque :** Dans notre parallèle avec $\mathbf{Z}$, les nombres entiers irréductibles sont les **nombres premiers**, *i.e.* les entiers relatifs qui ne sont divisibles que par eux-mêmes, leurs opposés et $\pm 1$.

### 1.b Propriétés

Les polynômes irréductibles jouent dans $\mathbf{K}[X]$, un rôle analogue à celui des nombres premiers dans $\mathbf{Z}$.

**Proposition 15.48.—** Soit $P \in \mathbf{K}[X]$ un polynôme irréductible de $\mathbf{K}[X]$. Pour tout couple $(A,B) \in \mathbf{K}[X]^2$, on a

- si $P$ divise $A$, alors $P \wedge A$ est le polynôme unitaire associé à $P$.
- si $P$ ne divise pas $A$, alors $P \wedge A = 1$.
- si $P$ divise $A \times B$, alors $P$ divise $A$ ou $P$ divise $B$.

### 1.c Décomposition en produit d'irréductibles

**Théorème 15.49.—** Soit $A \in \mathbf{K}[X]$. Il existe des polynômes irréductibles, unitaires et deux à deux distincts, $P_1, \ldots, P_N$ et des entiers naturels non nuls $(\alpha_1, \ldots, \alpha_N)$ tels que :

$$\boxed{A = a_n \, P_1^{\alpha_1} \times \cdots \times P_n^{\alpha_N}}$$

De plus, cette décomposition est unique à l'ordre des facteurs près.

**Démonstration** ▽

La démonstration de ce théorème est analogue à celle du théorème. ▲

### 1.d Expression du PGCD et du PPCM en décomposition primaire

**Théorème 15.50.—** Soit $(A, B \in \mathbf{K}[X]^2$. On suppose qu'il existe des polynômes irréductibles $P_1, \ldots, P_N$ et des entiers naturels **éventuellement** nuls $(\alpha_1, \ldots, \alpha_N)$ et $(\beta_1, \ldots, \beta_n)$ tels que :

$$\begin{aligned} A &= a_n \, P_1^{\alpha_1} \times \cdots \times P_n^{\alpha_N} \\ B &= b_n \, P_1^{\beta_1} \times \cdots \times P_n^{\beta_N} \end{aligned}$$

Alors

$$\boxed{\begin{aligned} PGCD(A,B) &= \textstyle\prod_{k=1}^{N} P_k^{\min(\alpha_k,\beta_k)} \\ PPCM(A,B) &= \textstyle\prod_{k=1}^{N} P_k^{\max(\alpha_k,\beta_k)} \end{aligned}}$$

**Démonstration** ▽

- il est clair que $\displaystyle\prod_{k=1}^{N} P_k^{\min(\alpha_k,\beta_k)}$ divise $A$ et que $\prod_{k=1}^{N} P_k^{\min(\alpha_k,\beta_k)}$ divise $B$.

  Réciproquement, si $P$ est un diviseur commun à $A$ et $B$, $P$ s'écrit $P = \displaystyle\prod_{k=1}^{N} P_k^{\gamma_k}$. Comme de plus, $P$ divise $A$, on déduit du théorème de Gauss que pour tout $k \in [\![1, N]\!]$, $P_k^{\gamma_k}$ divise $P_k^{\alpha_k}$ et $P_k^{\gamma_k}$ divise $P_k^{\beta_k}$. Par conséquent, $\gamma_k$ doit être inférieur à $\alpha_k$ et à $\beta_k$. Autrement dit, $P_k^{\gamma_k}$ divise $P_k^{\min(\alpha_k,\beta_k)}$. Ceci étant vrai pour tout entier $k \in [\![1, n]\!]$, il s'ensuit que $P$ divise $\displaystyle\prod_{k=1}^{N} P_k^{\min(\alpha_k,\beta_k)}$. Par conséquent,

  $$PGCD(A,B) = \prod_{k=1}^{N} P_k^{\min(\alpha_k,\beta_k)}$$

- il est clair que $A$ divise $\prod_{k=1}^{N} P_k^{\max(\alpha_k,\beta_k)}$ et que $B$ divise $\prod_{k=1}^{N} P_k^{\max(\alpha_k,\beta_k)}$.
  Réciproquement, si $M$ est un multiple commun à $A$ et $B$, $P$ s'écrit $M = \prod_{k=1}^{N} P_k^{\gamma_k}$. Comme précédemment, on montre que pour tout $k \in [\![1, N]\!]$, $P_k^{\alpha_k}$ divise $P_k^{\gamma_k}$ et $P_k^{\beta_k}$ divise $P_k^{\gamma_k}$. Par conséquent, $P_k^{\max(\alpha_k,\beta_k)}$ divise $P_k^{\gamma_k}$. Ceci étant vrai pour tout entier $k \in [\![1, n]\!]$, il s'ensuit que $\prod_{k=1}^{N} P_k^{\max(\alpha_k,\beta_k)}$ divise $M$. Par conséquent,

  $$PPCM(A,B) = \prod_{k=1}^{N} P_k^{\max(\alpha_k,\beta_k)}$$

▲

## 2 Factorisation dans $\mathbf{C}[\mathbf{X}]$

Le résultat essentiel est le **Théorème de D'Alembert - Gauss** que nous avons déjà rencontré dans le chapitre nombres complexes.

**Théorème 15.51.— Théorème Fondamental de l'Algèbre —.**

Tout polynôme $P \in \mathbf{C}[X]$ **non constant** admet (au moins) une racine.

On en déduit grâce au **Théorème** 15.22 que :

**Théorème 15.52.— Décomposition primaire dans $\mathbf{C}[X]$**

Tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{C}_n[X]$ de degré $n \in \mathbf{N}^\star$ est le produit de $n$ facteurs du premier degré. Plus précisément

si $\alpha_1, \ldots, \alpha_p$ sont les racines distinctes de $P$ de multiplicités respectives $r_1, \ldots, r_p$, alors

$$P = a_n \ (X-\alpha_1)^{r_1} \times \cdots (X-\alpha_p)^{r_p} \qquad \text{où} \qquad \sum_{k=1}^{p} r_k = n$$

**Commentaires :** un polynôme $P \in \mathbf{C}[X]$, de degré $n$ admet donc $n$ racines distinctes ou confondues. Il est donc scindé.

**En pratique :** la factorisation d'un polynôme $P$ dans $\mathbf{C}[X]$ revient donc à déterminer les racines distinctes de $P$ ainsi que leurs ordres de multiplicité respectifs. La méthode est donc

1 Résoudre dans $\mathbf{C}$ l'équation polynomiale $P(z) = 0$ afin de déterminer les racines distinctes $\alpha_1$, ...,$\alpha_p$ de $P$.

2 Pour chaque racine $\alpha_k$, déterminer son ordre de multiplicité $r_k$ ;

3 Enfin, par identification, déterminer le coefficient $a_n$.

**Démonstration** ▽

La preuve sera par récurrence sur $n \in \mathbf{N}^\star$. Notons

$\mathcal{P}(n)$ tout polynôme de degré $n$ est le produit de $n$ facteurs du premier degré.

**Initialisation :** lorsque $n = 1$, il n'y a rien à montrer !

**Hérédité :** soit $n \in \mathbf{N}^\star$ tel que $\mathcal{P}(n)$ soit vraie, et considérons un polynôme $P$ de degré $n+1$. Comme $n+1 > 0$, d'après le **Théorème fondamental de l'algèbre** (**Théorème** 15.51), $P$ possède une racine dans $\mathbf{C}$. Notons-la $\alpha$. D'après le **Théorème** 15.22, il existe un polynôme $Q \in \mathbf{C}[X]$ tel que

$$P = (X-\alpha) \times Q$$

En identifiant les degrés, il en résulte que $n+1 = 1+d^\circ Q$. Par conséquent, $Q$ est de degré $n$. Par hypothèse de récurrence, $Q$ peut donc s'écrire sous la forme d'un produit de $n$ facteurs de degré 1. Comme $P = (X-\alpha) \times Q$ , $P$ peut donc s'écrire comme produit de $n+1$ facteurs de degré 1.

**Conclusion :** par récurrence, nous avons démontré que tout polynôme $P$ s'écrit sous la forme d'un produit de facteurs de degré 1.

Écrivons chacun de ces facteurs sous la forme $\gamma_i(X-\beta_i)$, pour $i = 1, \ldots, n$, nous obtenons

$$P = \gamma_1(X-\beta_1) \times \gamma_2(X-\beta_2) \times \cdots \times \gamma_n(X-\beta_n)$$

Finalement, en notant $\alpha_1$, ...,$\alpha_p$ les $\beta_i$ deux à deux distincts, nous obtenons

$$P = \gamma \ (X-\alpha_1)^{r_1} \times \cdots \times (X-\alpha_p)^{r_p}$$

En identifiant les coefficients dominants de ces deux polynômes, et en utilisant la **Caractérisation de racines multiples**, il en résulte que $\gamma = a_n$ et $\alpha_1, \ldots, \alpha_p$ sont les racines distinctes de $P$ de multiplicités respectives $r_1, \ldots, r_p$.
Finalement en identifiant les degrés, il découle de la **Proposition** 15.4 que $\sum_{k=1}^{p} r_k = n$. ▲

**Corollaire 15.53.—** Les polynômes irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré égal à 1.

**Exercice :** Soit $n \in \mathbf{N}$ un entier supérieur ou égal à 2. On considère le polynôme

$$P = X^{n-1} + X^{n-2} + \cdots + X + 1$$

Le but de l'exercice est de déterminer la factorisation de $P$ en polynômes irréductibles de $\mathbf{C}[X]$.

**1.** Résoudre dans $\mathbf{C}$ l'équation $z^n - 1 = 0$. (1)
**2.** En déduire l'ensemble des solutions complexes de l'équation $P(z) = 0$. (2)
**3.** En déduire la factorisation de $P$ recherchée.

*Solution* ▽

**1.** *Les solutions de l'équation proposée sont les $n$ racines $n^{ièmes}$ complexes de l'unité :*

$$\mathbf{U}_n = \{1, \omega, \dots, \omega^{n-1}\}$$

**2.** *Il est clair que 1 n'est pas solution de l'équation (2), aussi pouvons-nous écrire :*

$$\begin{aligned} \forall z \in \mathbf{C}, \quad P(z) = 0 &\iff z \neq 1 \text{ et } P(z) = 0 \\ &\iff z \neq 1 \text{ et } (z-1) \times P(z) = 0 \\ &\iff z \neq 1 \text{ et } z^n - 1 = 0. \end{aligned}$$

*Par conséquent, les racines de $P$ sont les $n-1$ racines $n^{ièmes}$ de 1 différentes de 1 lui-même*

**3.** *Notons $r_1, \dots r_{n-1}$ les ordres de multiplicité respectifs de $\omega, \omega^2, \dots, \omega^{n-1}$. D'après la question précédente, ces entiers sont tous non nuls. De plus, d'après le* **Théorème** *15.52, il existe $a_{n-1} \in \mathbf{C}$ tel que*

$$P = a_{n-1} \ (X - \omega)^{r_1} \times \cdots \left(X - \omega^{n-1}\right)^{r_{n-1}}$$

*Par identification, il en résulte immédiatement que $a_{n-1} = 1$ et $r_1 = \cdots = r_{n-1} = 1$. Par conséquent*

$$P = (X - \omega) \times \cdots \left(X - \omega^{n-1}\right).$$

▲

**Exercice :** Soit $\theta \in \mathbf{R}$, décomposez en produits de facteurs irréductibles dans $\mathbf{C}[X]$ le polynôme $P = X^2 - 2\cos\theta X + 1$.

## 3 Factorisation dans $\mathbf{R}[X]$

Soit $P \in \mathbf{R}[X]$ un polynôme à coefficients réels. Ainsi que nous l'avons déjà remarqué, $P$ peut être considéré comme un polynôme à coefficients complexes. D'après le **Théorème** 15.52, il en résulte que $P$ peut s'écrire sous la forme d'un produit de polynômes de degré 1 **à coefficients complexes**. Ce n'est pas nécessairement une factorisation dans $\mathbf{R}[X]$. Pour construire la factorisation dans $\mathbf{R}[X]$ du polynôme $P$, nous utilisons le fait suivant :

**Proposition 15.54.—** Soit $P \in \mathbf{R}[X]$ alors pour tout $\alpha \in \mathbf{C}$ et pour tout $k \in \mathbf{N}^\star$

$\alpha$ est racine d'ordre $k$ de $P$ *si et seulement si* $\bar{\alpha}$ est racine d'ordre $k$ de $P$

**Commentaires :** en clair, les racines complexes d'un polynôme à coefficients réels sont 2 à 2 conjuguées et ont la même multiplicité.

**Démonstration** ▽
Soit $\alpha \in \mathbf{C}$ une racine d'ordre $k \in \mathbf{N}^\star$ de $P \in \mathbf{R}[X]$. Il s'agit de montrer que $\bar{\alpha}$ est aussi racine de multiplicité $k$ de $P$. Pour ce faire utilisons la caractérisation des racines multiples de $P$ : il vient

$$P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \ \text{ et } \ P^{(k)}(\alpha) \neq 0$$

Montrons que $P(\bar{\alpha}) = 0$. Supposons que $P$ s'écrive $P = \sum_{k=0}^{n} a_i X^i$. Par hypothèse, $0 = P(\alpha) = \sum_{k=0}^{n} a_i \alpha^i$. Comme les coefficients de $P$ sont réels, nous obtenons en conjugant cette égalité :

$$0 = \bar{P}(\alpha) = \overline{\sum_{k=0}^{n} a_i \alpha^i} = \sum_{k=0}^{n} a_i \overline{\alpha^i} = \sum_{k=0}^{n} a_i \bar{\alpha}^i = P(\bar{\alpha})$$

Par conséquent, $\bar{\alpha}$ est racine de $P$.
Procédons de la même manière pour les dérivées d'odre supérieur de $P$, comme les dérivées successives de $P$ sont des polynômes à coefficients réels, il en résulte finalement que

$$P(\bar{\alpha}) = P'(\bar{\alpha}) = \cdots = P^{(k-1)}(\bar{\alpha}) = 0 \ \text{ et } \ P^{(k)}(\bar{\alpha}) \neq 0$$

ce qui prouve que $\bar{\alpha}$ est racine d'ordre $k$ de $P$. ▲

Ainsi, les racines d'un polynôme à coefficients réels sont ou bien réelles, ou bien complexes conjuguées. Finalement, en regroupant les facteurs conjugués, nous en déduisons :

**Théorème 15.55.— Décomposition primaire dans $\mathbf{R}[X]$**
Tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{R}_n[X]$ de degré $n \in \mathbf{N}^\star$ est le produit de facteurs du premier ou du deuxième degré.
Plus précisément, si $\alpha_1, \ldots, \alpha_p$ sont les racines **réelles** distinctes de $P$ de multiplicités respectives $r_1, \ldots, r_p$, alors

$$\boxed{P = a_n \prod_{k=1}^{p} (X - \alpha_k)^{r_k} \prod_{j=1}^{q} \left(X^2 + \beta_j X + \gamma_j\right)^{s_j}}$$

où $\sum_{k=1}^{p} r_k + 2 \times \sum_{j=1}^{q} s_j = n$ et les polynômes à coefficients réels $\left(X^2 + \beta_j X + \gamma_j\right)$ ne possèdent pas de racines réelles.

**En pratique :** pour déterminer la factorisation de $P \in \mathbf{R}[X]$ en produit de facteurs irréductibles de $\mathbf{R}[X]$, la méthode est la suivante :

1. Considérez $P$ comme un polynôme à coefficients complexes et décomposez-le en produit de facteurs $(X - \zeta_i)^{r_i}$, où les $\zeta_i$ sont les racines *a priori* complexes de $P$ dans $\mathbf{C}[X]$.
2. Comme les racines complexes de $P$ sont deux à deux conjuguées, vous pouver regrouper les facteurs $(X - \zeta_j)^{s_j}(X - \bar{\zeta}_j)^{s_j} = \left(X^2 - 2\,\mathfrak{Re}\,\zeta_j\, X + |\zeta_j|^2\right)^{s_j}$
3. Déterminez le coefficient $a_n$ par identification.

**Remarque :** Avant de procéder à la démonstration du **Théorème**, remarquons qu'il s'agit bien d'une décomposition en produit de facteurs irréductibles de $\mathbf{R}[X]$. En effet, il est clair que les $X - \alpha_k$ sont irréductibles puisqu'ils sont de degré 1. D'autre part, un polynôme de degré 2, $X^2 + \beta_j X + \gamma_j$, sans racines réelles, est aussi irréductible. En effet si $Q$ était réductible dans $\mathbf{R}[X]$, nous pourrions écrire

$$X^2 + \beta_j X + \gamma_j = A(X) \times B(X)$$

avec $A$ et $B$ deux polynômes de degré 1. Ainsi $Q$ admettrait au moins une racine réelle : celle de $A$ !

**Démonstration** ▽

- Notons $\alpha_1, \ldots, \alpha_p$ les racines réelles distinctes de $P$ et $\zeta_1, \bar{\zeta}_1, \ldots, \zeta_q, \bar{\zeta}_q$ ses racines complexes –non réelles– deux à deux conjuguées [2]. D'après le **Théorème** 15.52, la factorisation de $P$ comme produit de facteurs irréductibles de $\mathbf{C}[X]$ est :

$$P = a_n \prod_{k=1}^{p} (X - \alpha_k) \times \prod_{j=1}^{q} (X - \zeta_j)^{s_j} \, (X - \bar{\zeta}_j)^{s_j}, \tag{15.6}$$

  où $n = \sum_{k=1}^{p} r_k + 2 \times \sum_{j=1}^{q} s_j$.

- Remarquons que si $(X - \zeta_j)$ n'est pas un polynôme à coefficients réels, en revanche, $(X - \zeta_i) \times (X - \bar{\zeta}_j)$ l'est puisque :

$$(X - \zeta_j) \times (X - \bar{\zeta}_j) = X^2 - (\zeta_j + \bar{\zeta}_j)\, X + \zeta_j \bar{\zeta}_j = X^2 - 2\,\mathfrak{Re}\,\zeta_j\, X + |\zeta_j|^2$$

  Posons $\beta_j = -2\,\mathfrak{Re}\,\zeta_j \in \mathbf{R}$ et $\gamma_j = |\zeta_j|^2 \in \mathbf{R}$, de sorte que $X^2 + 2\beta_j\, X + \gamma_j \in \mathbf{R}[X]$ est un polynôme à coefficients réels.
  Ainsi, en regroupant deux par deux les facteurs à coefficients complexes de (15.6), nous avons obtenu la factorisation dans $\mathbf{R}[X]$ :

$$P = a_n \prod_{k=1}^{p} (X - \alpha_k)^{r_k} \prod_{j=1}^{q} \left(X^2 + \beta_j X + \gamma_j\right)^{s_j}$$

▲

2. d'après la proposition précédente

**Corollaire 15.56.— Polynômes irréductibles dans $\mathbf{R}[X]$ —.** Les polynômes irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

**Démonstration** ▽
Comme nous l'avons établi à la remarque précédente, les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles (i.e. de discriminant strictement négatif) sont irréductibles dans $\mathbf{R}[X]$.
Réciproquement, soit $P$ un polynôme irréductible dans $\mathbf{R}[X]$. D'après le théorème précédent, $P$ peut s'écrire sous la forme d'un produit de polynômes de degré 1 et de polynômes de degré 2 sans racines réelles. Comme $P$ est irréductible, ce produit ne contient qu'un seul facteur non constant. Par suite $P$ est lui-même un polynôme de degré 1 ou un polynôme de degré 2 sans racines réelles ! ▲

**Corollaire 15.57.—** Tout polynôme $P \in \mathbf{R}[X]$ à coefficients réels de degré impair admet au moins une racine réelle.

**Démonstration** ▽
La preuve sera par l'*absurde*.
Supposons *au contraire* que $P$ soit un polynôme à coefficients réels de degré impair $n$ et n'admette aucune racine réelle. D'après le **Théorème** 15.55, $P$ se factorise sous la forme d'un produit de facteurs irréductibles de degré 2 :

$$P = a_n \prod_{j=1}^{q} \left(X^2 + \beta_j X + \gamma_j\right)^{s_j}$$

En particulier $n = 2\sum_{j=1}^{q} s_j$, ce qui est absurde vu que $n$ est impair. ▲

**Exercice :** Donnez les décompositions primaires dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$ du polynôme $P = X^5 - 1$.

## 4 Exemples de factorisation

Pour déterminer une factorisation dans $\mathbf{C}[X]$ aussi bien que dans $\mathbf{R}[X]$, la méthode suit les mêmes étapes que la résolution des équations algébriques, avec pour objectif de faire baisser le degré.

### 4.a À l'aide d'identités remarquables

**Exercice :** Donnez la décomposition primaire dans $\mathbf{R}[X]$ de

1. $P = (1 - X^2)^3 + 8X^3$
2. $P = X^8 - 1$.

### 4.b À l'aide de changement d'indéterminée

**Exercice :**

1. Factorisez dans $\mathbf{C}[X]$ le polynôme $P = X^4 + X^2 + 1$ à l'aide du changement d'indéterminée $Y = X^2$.
2. Factorisez dans $\mathbf{C}[X]$ le polynôme $P = X^4 + 4X^3 + 5X^2 + 4X + 1$ à l'aide du changement d'inconnue $y = x + \dfrac{1}{x}$.

# VI COMPLÉMENTS : les démonstrations du théorème de D'Alembert-Gauss