Chapitre XII : Polynômes

Retranscrit par Samy Youssoufine

1er mars 2026

UM6P University Mohammed VI Polytechnic | EMINES School of Industrial Management

Note importante

Peut contenir des erreurs.

Table des matières

Ce chapitre est consacré aux polynômes à coefficients dans un anneau. Nous y étudierons notamment les notions de degré, de racine, de division euclidienne, ainsi que les concepts de polynômes irréductibles et de factorisation dans ce contexte.

1 Polynômes à coefficients dans un anneau

1.1 Définitions

Définition 1.1.1.1

Soit $(A, +, \times)$ un anneau commutatif. On munit $A^{\mathbb{N}}$ par les deux lois $+$ et $\times$ tel que :
$\begin{cases} \forall (a_n)_n, (b_n)_n \in A^{\mathbb{N}} : (a_n)_n + (b_n)_n = (a_n + b_n)_n \\ \forall (a_n)_n, (b_n)_n \in A^{\mathbb{N}} : (a_n)_n \times (b_n)_n = (c_n)_n \text{ avec } c_n = \sum_{k=0}^{n} a_k b_{n-k} \end{cases}$
On peut aussi écrire $c_n = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n \\ i+j=n}} a_i b_j$.

Théorème 1.1.1.1

$(A^{\mathbb{N}}, +, \times)$ est un anneau commutatif. On l'appelle l'anneau des polynômes à coefficients dans A et on le note $A[X]$.

Preuve

Comme $(A, +)$ est un groupe abélien (sachant que $(A, +, \times)$ est un anneau), il en est de même pour $(A^{\mathbb{N}}, +)$. *(On rappelle que le groupe des applications de $\mathbb{N}$ dans un groupe abélien est lui-même un groupe abélien)*
La loi $\times$ est bien définie ; c'est une LCI dans $A^{\mathbb{N}}$ (stabilité par l'addition et la multiplication). De plus, la multiplication $\times$ est associative et commutative, et elle distribue par rapport à l'addition $+$. L'élément neutre de l'anneau $A^{\mathbb{N}}$ pour la loi $+$ est la suite nulle $(0)_n$ et l'élément neutre pour la loi $\times$ est la suite $(1, 0, 0, \ldots)$.

- Pour démontrer que $\times$ est une LCI, on utilise les propriétés de l'anneau A et la définition du produit $(c_n)_n$.
- Pour démontrer que $\times$ est associative, on considère trois suites $(x_n)_n$, $(y_n)_n$, et $(z_n)_n$ dans $A^{\mathbb{N}}$ et on montre que $((x_n)_n \times (y_n)_n) \times (z_n)_n = (x_n)_n \times ((y_n)_n \times (z_n)_n)$.
  - Pour cela, on va montrer que tous les termes de ces deux suites sont égaux.
  - On pose $(c_n)_n \times (z_n)_n = (\alpha_n)_n$ et on trouve que $\alpha_n = \sum_{k+l+j=n} (x_k \times y_l) \times z_j$.

- ▷ De même, on pose $(x_n)_n \times ((y_n)_n \times (z_n)_n) = (\beta_n)_n$ et on trouve que $\beta_n = \sum_{k+l+j=n} x_k \times (y_l \times z_j)$.
- ▷ En utilisant l'associativité de la multiplication dans A, on trouve que $\alpha_n = \beta_n$ pour tout n, **ce qui prouve l'associativité de** $\times$.
- ▷ Il faut noter qu'on a utilisé la distributivité de la multiplication par rapport à l'addition dans A pour réarranger les termes de ces sommes.

▶ Pour démontrer que $\times$ est commutative, on considère deux suites $(x_n)_n$ et $(y_n)_n$ dans $A^{\mathbb{N}}$ et on montre que $(x_n)_n \times (y_n)_n = (y_n)_n \times (x_n)_n$.

- ▷ On pose une suite $(c_n)_n = \sum_{i+j=n} x_i \times y_j$ et on pose $(d_n)_n = \sum_{i+j=n} y_i \times x_j$.
- ▷ En utilisant la commutativité de la multiplication dans A, on trouve que $c_n = d_n$ pour tout n, **ce qui prouve la commutativité de** $\times$.

▶ Pour déterminer l'élément neutre de la multiplication $\times$, on doit trouver une suite $e = (e_n)_n$ dans $A^{\mathbb{N}}$ telle que pour toute suite $(x_n)_n$ dans $A^{\mathbb{N}}$, on ait $e \times (x_n)_n = (x_n)_n$ et $(x_n)_n \times e = (x_n)_n$.

- ▷ On pose $e = (e_n)_n \in A^{\mathbb{N}}$ définie par $e_0 = 1_A$, et $\forall n \geq 1, e_n = 0_A$.
- ▷ On utilisera le *Symbole de Kronecker* pour montrer que e est l'élément neutre pour la multiplication $\times$.
  - — Le symbole de Kronecker $\delta_{x,y}$ est défini par $\delta_{x,y} = 1$ si $x = y$ et $\delta_{x,y} = 0$ sinon.
- ▷ Soit $(x_n)_n \in A^{\mathbb{N}}$. On pose $e \times (x_n)_n = (c_n)_n$.
- ▷ En utilisant la définition du produit, on trouve que $c_n = \sum_{k=0}^{n} \delta_{k,0} \times x_{n-k}$.
- ▷ En utilisant la définition du symbole de Kronecker, on trouve que $c_n = x_n$ pour tout n, et sachant que la multiplication est commutative dans A, **ce qui prouve que** e **est l'élément neutre pour la multiplication** $\times$.

▶ Pour montrer que $\times$ est distributive par rapport à $+$, on considère trois suites $(x_n)_n$, $(y_n)_n$, et $(z_n)_n$ dans $A^{\mathbb{N}}$ et on montre que $(x_n)_n \times ((y_n)_n + (z_n)_n) = (x_n)_n \times (y_n)_n + (x_n)_n \times (z_n)_n$.

- ▷ On a $(x_n)_n \times ((y_n)_n + (z_n)_n) = (x_n)_n \times (y_n + z_n)_n$.
- ▷ En utilisant la définition du produit, on trouve que $(x_n)_n \times ((y_n)_n + (z_n)_n) \left(\sum_{i+j} x_i \times (y_j + z_j)\right)_n$.
- ▷ En séparant les termes de cette somme, on trouve que $(x_n)_n \times ((y_n)_n + (z_n)_n) = \left(\sum_{i+j} x_i \times y_j\right)_n + \left(\sum_{i+j} x_i \times z_j\right)_n$.
- ▷ En utilisant la définition du produit, on trouve que $(x_n)_n \times ((y_n)_n + (z_n)_n) = (x_n)_n \times (y_n)_n + (x_n)_n \times (z_n)_n$, **ce qui prouve la distributivité de** $\times$ **par rapport à** $+$.

▶ On conclut que $(A^{\mathbb{N}}, +, \times)$ est un anneau commutatif, car il satisfait toutes les propriétés nécessaires :

- ▷ $(A^{\mathbb{N}}, +)$ est un groupe abélien.
- ▷ $\times$ est une LCI dans $A^{\mathbb{N}}$.
- ▷ $\times$ est associative et commutative.

- ▷ $\times$ distribue par rapport à $+$.
- ▷ Il existe un élément neutre pour la multiplication $\times$.

Par conséquent, $(A^{\mathbb{N}}, +, \times)$ satisfait la définition d'un anneau commutatif. ■

Propriété 1.1.1.1 ***(Conservation de l'intégrité)***

Si A est un anneau intègre, alors $A[X]$ est aussi un anneau intègre.

Preuve

- ▶ Supposons que $\exists (a_n)_n, (b_n)_n \in A^{\mathbb{N}}$ tels que $(a_n)_n \times (b_n)_n = 0_{A^{\mathbb{N}}}$ et $\begin{cases} (a_n)_n \neq 0_{A^{\mathbb{N}}} \\ (b_n)_n \neq 0_{A^{\mathbb{N}}} \end{cases}$.
- ▶ On pose $i_0 = \min(\{n \in \mathbb{N} \text{ tel que } a_n \neq 0\})$ et $\forall i < i_0, a_i = 0_A$. On pose aussi $j_0 = \min(\{n \in \mathbb{N} \text{ tel que } b_n \neq 0\})$ et $\forall j < j_0, b_j = 0_A$. i_0 et j_0 représentent les indices du premier terme non nul de $(a_n)_n$ et $(b_n)_n$ respectivement.
- ▶ On pose $(a_n)_n \times (b_n)_n = (c_n)_n$. Donc $\forall n \in \mathbb{N}, c_n = 0_A = \sum_{i+j=n} a_i \times b_j$.
  - ▷ On remarque qu'en particulier, pour $n = i_0 + j_0$, on a $c_{i_0+j_0} = 0_A = \sum_{i+j=i_0+j_0} a_i \times b_j$.
  - ▷ Cela implique que $\sum_{i+j=i_0+j_0} a_i \times b_j = 0_A$.
    - — Dans le cas où $i < i_0$ ou $j < j_0$, on a $a_i = 0_A$ ou $b_j = 0_A$, donc les termes correspondants de la somme sont nuls.
    - — Dans le cas contraire, c'est à dire lorsque $i \geq i_0$ et $j \geq j_0$, on a $c_{i_0+j_0} = 0_A + a_{i_0} \times b_{j_0} = 0_A$, car les autres termes de la somme sont nuls.
  - ▷ Comme A est un anneau intègre, on a $a_{i_0} \times b_{j_0} = 0_A \implies a_{i_0} = 0_A$ ou $b_{j_0} = 0_A$, ce qui contredit la définition de i_0 et j_0.
- ▶ Par conséquent, notre supposition est fausse, et il n'existe pas de tels éléments $(a_n)_n$ et $(b_n)_n$ dans $A^{\mathbb{N}}$.
- ▶ Ainsi, $A^{\mathbb{N}}$ est un anneau intègre.

■

Définition 1.1.1.2

On définit la suite $X \in A^{\mathbb{N}}$ en utilisant le symbole de Kronecker : $X = (\delta_{n,1})_n$. Autrement dit, en posant $X = (x_n)_n$, on a $x_0 = 0_A$, $x_1 = 1_A$, et $\forall n \geq 2, x_n = 0_A$.

Propriété 1.1.1.2

$\forall k \in \mathbb{N}, X^k = \underbrace{X \times \cdots \times X}_{k \text{ fois}} = (\delta_{n,k})_n.$

Preuve

On va démontrer cette propriété par récurrence sur k.
Initialisation : Pour $k = 0$, on a $X^0 = 1_{A^{\mathbb{N}}} = (\delta_{n,0})_n$, ce qui est vrai.
Hérédité : Supposons que la propriété est vraie pour un certain $k \in \mathbb{N}$, c'est-à-dire que $X^k = (\delta_{n,k})_n$. Nous devons montrer qu'elle est également vraie pour $k+1$.
On a $X^{k+1} = X^k \times X = \underbrace{(\delta_{n,k})_n}_{=(a_n)_n} \times \underbrace{(\delta_{n,1})_n}_{=(b_n)_n}$.
On a $X^{k+1} = \left(\sum_{i=0}^{n} a_i \times b_{n-i}\right)_n$.
On obtient donc $X^{k+1} = \left(\sum_{i=0}^{n} \delta_{i,k} \times \delta_{n-i,1}\right)_n$.
Pour chaque $n \in \mathbb{N}$, on a :

$$\sum_{i=0}^{n} \delta_{i,k} \times \delta_{n-i,1} = \begin{cases} 1_A & \text{si } n = k+1 \\ 0_A & \text{sinon} \end{cases}$$

On en déduit que $X^{k+1} = (\delta_{n-1,k})_n$.
Et on a $\delta_{n-1,k} = 1 \iff n-1 = k \iff n = k+1 \iff \delta_{n,k+1} = 1$.
On en conclut que $X^{k+1} = (\delta_{n,k+1})_n$.
Ainsi, par le principe de récurrence, la propriété est vraie pour tout $k \in \mathbb{N}$. ■

Définition 1.1.1.3

On note $A[X] = \{a \in A^{\mathbb{N}} \text{ tel que } \exists n_0 \in \mathbb{N}, \forall n \geq n_0, a_n = 0_A\}$. Autrement dit, $A[X]$ est l'ensemble des suites dans $A^{\mathbb{N}}$ qui sont nulles à partir d'un certain rang.

Propriété 1.1.1.3

$A[X]$ est un sous-anneau de $(A^{\mathbb{N}}, +, \times)$.

Preuve

- Soient $(a_n)_n$ et $(b_n)_n$ deux éléments de $A[X]$. Par définition, il existe des entiers naturels n_a et n_b tels que $\forall n \geq n_a, a_n = 0_A$ et $\forall n \geq n_b, b_n = 0_A$.
- Les éléments neutre $1_{A^{\mathbb{N}}}$ et $0_{A^{\mathbb{N}}}$ appartiennent à $A[X]$ car ils sont nuls à partir du rang 1.
- On pose $n_0 = \max(n_a, n_b)$. Alors, pour tout $n \geq n_0$, on a :
  - $a_n = 0_A$ (car $n \geq n_a$)
  - $b_n = 0_A$ (car $n \geq n_b$)
  - Donc $a - b \in A[X]$.

- Ainsi, $A[X]$ est stable par soustraction, et par conséquent, il est stable par addition.
- Considérons maintenant le produit $(d_n)_n = (a_n)_n \times (b_n)_n$.
  Pour tout $n \geq n_0$, on a :
  - $d_n = \sum_{i=0}^{n} a_i \times b_{n-i}$
  - Si $n \geq n_0$, alors pour chaque terme de la somme, soit $i \geq n_a$ ou $n - i \geq n_b$, ce qui implique que soit $a_i = 0_A$ soit $b_{n-i} = 0_A$. Par conséquent, chaque terme de la somme est nul, et donc $d_n = 0_A$.
- Ainsi, $(d_n)_n$ appartient à $A[X]$, ce qui montre que $A[X]$ est stable par multiplication.
- Par conséquent, $A[X]$ est un sous-anneau de $(A^{\mathbb{N}}, +, \times)$.

■

Remarque 1.1.1.1

Si $a = (a_n)_n \in A^{\mathbb{N}}$ et $\lambda \in A$, on définit $\lambda \cdot a = (\lambda \times a_n)_n$ (loi de composition externe, qu'on verra dans le chapitre XIV).

Propriété 1.1.1.4

1. $\forall a \in A^{\mathbb{N}}, 1_A \cdot a = a$.
2. $\forall \lambda_1, \lambda_2 \in A, \forall a \in A^{\mathbb{N}}, (\lambda_1 + \lambda_2) \cdot a = \lambda_1 \cdot a + \lambda_2 \cdot a$.
3. $\forall \lambda \in A, \forall a, b \in A^{\mathbb{N}}, \lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$.
4. $\forall \lambda_1, \lambda_2 \in A, \forall a \in A^{\mathbb{N}}, (\lambda_1 \times \lambda_2) \cdot a = \lambda_1 \cdot (\lambda_2 \cdot a)$.

On sait que $\forall a \in A[X], \exists n_0 \in \mathbb{N}, \forall n \geq n_0, a_n = 0_A$.
i.e. $a = (a_0, a_1, \ldots, a_{n_0}, 0_A, 0_A, \ldots)$.

- On peut encore réécrire a sous la forme $a = (a_0, 0_A, 0_A, \ldots) + (0_A, a_1, 0_A, \ldots) + \ldots + (0_A, 0_A, \ldots, a_{n_0}, 0_A, \ldots)$.
- On peut aussi réécrire a sous la forme $a = a_0 \cdot (1_A, 0_A, 0_A, \ldots) + a_1 \cdot (0_A, 1_A, 0_A, \ldots) + \ldots + a_{n_0} \cdot (0_A, 0_A, \ldots, 1_A, 0_A, \ldots)$.

En utilisant la définition de X, on trouve que $a = a_0 \cdot 1_{A^{\mathbb{N}}} + a_1 \cdot X + \ldots + a_{n_0} \cdot X^{n_0}$.
Donc $a = \sum_{k=0}^{n_0} a_k \cdot X^k$.

Propriété 1.1.1.5 ***(Préservation de l'intégrité)***

Si A est un anneau intègre, alors $A[X]$ est aussi un anneau intègre.

Preuve

A intègre $\implies$ $A^{\mathbb{N}}$ intègre, et $A[X]$ est un sous-anneau de $A^{\mathbb{N}}$. Donc $A[X]$ est un

anneau intègre. ■

Propriété 1.1.1.6

Soient $a, b \in A[X]$. On a $a = b \iff \forall n, a_n = b_n$.
Donc, en particulier, $\sum a_k \cdot X^k = \sum_{b_k} \cdot X^k \iff \forall k, a_k = b_k$.

Définition 1.1.1.4

Soit A un anneau commutatif.
$P = \sum_{k=0}^{n} a_k X^k$ est appelé un polynôme à coefficients dans A.
L'ensemble des polynômes à coefficients dans A est noté $A[X]$.
Si $P \in A[X]$, alors on définit la **fonction polynômiale** associée à P comme étant la fonction $P : \begin{array}{ccc} A & \to & A \\ x & \mapsto & \tilde{P}(x) = \sum_{k=0}^{n} a_k x^k \end{array}$.

Remarque 1.1.1.2

Si $P, Q \in A[X]$, alors $P = Q \implies \forall x \in A, \tilde{P}(x) = \tilde{Q}(x)$, mais la réciproque est fausse en général. On donne un contre-exemple simple dans le cas où $A = \mathbb{Z}/2\mathbb{Z}$: $P = X^2 + X$ et $Q = 0$. On a $\tilde{P}(0) = 0$, $\tilde{P}(1) = 0$, $\tilde{Q}(0) = 0$, et $\tilde{Q}(1) = 0$, mais $P \neq Q$.

1.2 Degré d'un polynôme

Définition 1.1.2.5

Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ un polynôme à coefficients dans A. On définit le degré de P, noté $\deg(P)$ ou $d^\circ P$, comme étant le plus grand entier k tel que $a_k \neq 0_A$.

$$\deg(P) = \max\{k \in \mathbb{N} \text{ tel que } a_k \neq 0_A\} \text{ si } P \neq 0$$

Par convention, on pose $\deg(0) = -\infty$.

Remarque 1.1.2.3

1. Si $P \neq 0$, alors P peut être écrit sous la forme $P = \sum_{k=0}^{\deg(P)} a_k X^k$. Le coefficient $a_{\deg(P)}$ est appelé **le coefficient dominant** de P, noté $\mathrm{CD}(P)$. Si $P \in A[X]$ tel que $\mathrm{CD}(P) = 1$, alors on dit que P est un **polynôme unitaire**.
2. On note $A_n[X] = \{P \in A[X] \text{ tel que } \deg(P) \leq n\}$, c'est à dire l'ensemble des polynômes à coefficients dans A de degré inférieur ou égal à n.

Propriété 1.1.2.7

Soient A un anneau *intègre* (❗) et $P, Q \in A[X]$.

1. $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ et $\mathrm{CD}(P \cdot Q) = \mathrm{CD}(P) \times \mathrm{CD}(Q)$.
2. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$
   avec égalité si et seulement si $\begin{cases} \deg(P) \neq \deg(Q) \\ \text{ou } \deg(P) = \deg(Q) \text{ et } \mathrm{CD}(P) + \mathrm{CD}(Q) \neq 0_A \end{cases}$.

Preuve

1. Si $P = 0$ ou $Q = 0$, alors $P \cdot Q = 0$, et $\deg(P \cdot Q) = -\infty = \deg(P) + \deg(Q)$.
   Dans le cas contraire, on pose $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ avec $a_n \neq 0_A$ et $b_m \neq 0_A$.
   En utilisant la définition du produit, on trouve que $P \cdot Q = \sum_{k=0}^{n+m} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i \times b_j$.
   En particulier, on a $c_{n+m} = a_n \times b_m \neq 0_A$ (car A est intègre), ce qui implique que $\deg(P \cdot Q) = n + m = \deg(P) + \deg(Q)$ et $\mathrm{CD}(P \cdot Q) = c_{n+m} = a_n \times b_m = \mathrm{CD}(P) \times \mathrm{CD}(Q)$.
2. Si $P = 0$ ou $Q = 0$, alors la démonstration est claire.
   Dans le cas contraire, on pose : $P = \sum_{k=0}^{n} a_k X^k, Q = \sum_{k=0}^{m} b_k X^k$. On suppose par exemple (et sans perte de généralité) que $n \leq m$, donc $P = \sum_{k=0}^{m} a_k X^k$ avec $\forall k > n, a_k = 0$.
   Donc $(P+Q) = \sum_{k=0}^{m} (a_k + b_k) X^k$.
   Cela implique que $\deg(P+Q) \leq m = \max(n, m) = \max(\deg(P), \deg(Q))$.
   Dans le cas où $n < m$, on a $\deg(P+Q) = m = \max(\deg(P), \deg(Q))$.
   Dans le cas où $n = m$, on a $\deg(P+Q) = n = m$ si et seulement si $a_n + b_n \neq 0_A$, c'est à dire $\mathrm{CD}(P) + \mathrm{CD}(Q) \neq 0_A$.
   Dans le cas contraire, on a $\deg(P+Q) < n = m$.

■

Exercice 1.1.2.1

On pose $\begin{cases} T_0 = 1, T_1 = X \\ \forall n \geq 0, T_{n+2} = 2X \cdot T_{n+1} - T_n \end{cases}$
$(T_n)_n$ est appelée les **polynômes de Tchebychev**.
Calculer $\deg(T_n)$ et $\mathrm{CD}(T_n)$ pour tout $n \in \mathbb{N}$.

Solution :

On remarque que $T_1 = X$ est un polynôme de degré 1 et de coefficient dominant 1, puis $T_2 = 2X^2 - 1$ est un polynôme de degré 2 et de coefficient dominant 2.
Il suffit donc de démontrer par récurrence double que $\forall n \in \mathbb{N}, T_n$ est un polynôme de degré n et de coefficient dominant 2^{n-1}.
L'initialisation est vérifiée pour $n = 0$ et $n = 1$.

L'hérédité doit supposer que, pour un $n \in \mathbb{N}$ fixe, $\begin{cases} \deg(T_n) = n \\ \deg(T_{n+1}) = n+1 \end{cases}$ et $\begin{cases} \mathrm{CD}(T_n) = 2^{n-1} \\ \mathrm{CD}(T_{n+1}) = 2^n \end{cases}$, et doit démontrer que $\begin{cases} \deg(T_{n+2}) = n+2 \\ \mathrm{CD}(T_{n+2}) = 2^{n+1} \end{cases}$.
Ensuite, on conclut que $\forall n \in \mathbb{N}, T_n$ est un polynôme de degré n et de coefficient dominant 2^{n-1}.

1.3 Dérivée d'un polynôme

Dans cette partie, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

Définition 1.1.3.6 *(Dérivée d'un polynôme)*

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$. On définit le polynôme dérivé de P, noté P', de la manière suivante :

$$P' = \begin{cases} 0 & \text{si } \deg(P) = 0 \\ \sum_{k=1}^{n} \underbrace{k \cdot a_k}_{\in \mathbb{K}} X^{k-1} & \text{si } \deg(P) \neq 0 \end{cases}$$

Définition 1.1.3.7 *(Dérivées successives d'un polynôme)*

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$. On définit les dérivées successives de P de la manière suivante :

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

Remarque 1.1.3.4

Si $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$ est un polynôme à coefficients dans $\mathbb{K}$ et de degré $\deg(P) = n$, alors :

$$P^{(k)} = \begin{cases} 0 & \text{si } k > n \\ \sum_{i=k}^{n} \frac{i!}{(i-k)!} a_i X^{i-k} & \text{si } k \leq n \end{cases}$$

Théorème 1.1.3.2 *(Formule de Taylor)*

Soient $P \in \mathbb{K}[X]$ tel que $\deg(P) = n$ et $a \in \mathbb{K}$. Alors :

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

Preuve

On pose $\forall i \in [\![0, n]\!], Q_i = X^i$.

$$\begin{aligned} \text{On a } \forall i \in [\![0,n]\!], Q_i &= (X-a+a)^i \\ &= \sum_{k=0}^{i} \mathrm{C}_i^k (X-a)^k a^{i-k} \end{aligned}$$

$$\begin{aligned} \text{On a } \forall k \in [\![0,i]\!], Q_i^{(k)}(a) &= \frac{i!}{(i-k)!} a^{i-k} \\ \implies Q_i^{(k)} &= k! \cdot \mathrm{C}_i^k a^{i-k}(X-a)^k \\ \implies \forall k \in [\![0,i]\!], \frac{Q_i^{(k)}(a)}{k!} &= \mathrm{C}_i^k a^{i-k} \end{aligned}$$

Donc $Q_i = \sum_{k=0}^{i} \frac{Q_i^{(k)}(a)}{k!}(X-a)^k$.
On écrit $P = \sum_{i=0}^{n} \lambda_i X^i = \sum_{i=0}^{n} \lambda_i Q_i$.
Donc, pour tout $k \leq n$, $P^{(k)} = \sum_{i=k}^{n} \lambda_i Q_i^{(k)}$.
Donc, pour tout $k \leq n$, $\boxed{P^{(k)}(a) = \sum_{i=k}^{n} \lambda_i Q_i^{(k)}(a)}$.
Comme $P = \sum_{i=0}^{n} \lambda_i Q_i$, on trouve que $P = \sum_{i=0}^{n} \lambda_i \sum_{k=0}^{i} \frac{Q_i^{(k)}(a)}{k!}(X-a)^k$.
En échangeant les sommes, on trouve que $P = \sum_{k=0}^{n} \frac{1}{k!} \underbrace{\left(\sum_{i=k}^{n} \lambda_i Q_i^{(k)}(a) \right)}_{=P^{(k)}(a)} (X-a)^k$.
Le terme entre parenthèses est égal à $P^{(k)}(a)$, d'après la formule encadrée ci-dessus.
Donc $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

■

Remarque 1.1.3.5

Si $P = \sum_{k=0}^{n} a_k X^k$.
Alors $\forall k \in [\![0,n]\!], a_k = \frac{P^{(k)}(0)}{k!}$.

2 Arithmétiques dans $\mathbb{K}[X]$

Dans cette partie, $\mathbb{K}$ désigne un corps commutatif.

2.1 Divisibilité dans $\mathbb{K}[X]$

Définition 2.2.1.8 *(Rappel)*

Soit $A, B \in \mathbb{K}[X]$. On dit que A divise B dans $\mathbb{K}[X]$ lorsqu'il existe $C \in \mathbb{K}[X]$ tel que $B = A \cdot C$, et on écrit $A \mid B$.

Attention

On rappelle que $\mathbb{K}[X]$ est un anneau intègre, mais pas forcément un corps.

Propriété 2.2.1.8

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0.

$$P \in \mathbb{U}_{\mathbb{K}[X]} \iff \deg(P) = 0$$

$$\mathbb{U}_{\mathbb{K}[X]} = \mathbb{K}^* = \mathbb{K}_0[X] \setminus \{0\}$$

Preuve

- Démonstration dans le sens $\implies$:
  - On a $P \in \mathbb{U}_{\mathbb{K}[X]} \iff \exists Q \in \mathbb{K}[X], P \cdot Q = 1$.
  - Donc $\deg(P \cdot Q) = \deg(P) + \deg(Q) = 0$, sachant que $P \neq 0$ et $Q \neq 0$ (car $1 \neq 0$).
  - Et comme $\deg(P), \deg(Q) \in \mathbb{N}$, on trouve que $\deg(P) = 0$ et $\deg(Q) = 0$.
- Démonstration dans le sens $\impliedby$:

- ▷ Si $\deg(P) = 0$, alors P est de la forme $P = a_0$ avec $a_0 \in \mathbb{K}$ et $a_0 \neq 0$ (car $P \neq 0$).
- ▷ Comme $\mathbb{K}$ est un corps, a_0 est inversible dans $\mathbb{K}$, donc il existe $a_0^{-1} \in \mathbb{K}$ tel que $a_0 \times a_0^{-1} = 1$.
- ▷ On pose $Q = a_0^{-1}$. Alors $P \cdot Q = a_0 \cdot a_0^{-1} = 1$, ce qui implique que P est inversible dans $\mathbb{K}[X]$.

▶ Par conséquent, les éléments inversibles de $\mathbb{K}[X]$ sont exactement les polynômes de degré 0.

■

Propriété 2.2.1.9

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

1. Si $A \mid B$ et $B \mid C$, alors $A \mid C$.
2. Si $A \mid B$ et $B \mid A$, alors :
   a) A et B sont associés.
   b) Il existe $\lambda \in \underbrace{\mathbb{U}_{\mathbb{K}[X]}}_{=\mathbb{K}^*}$ tel que $A = \lambda \cdot B$.
3. $\mathbb{K}[X]$ est un anneau intègre, donc toutes les propriétés de divisibilité dans un anneau intègre sont vérifiées dans $\mathbb{K}[X]$.

2.2 Division euclidienne

Théorème 2.2.2.3

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tels que $A = B \cdot Q + R$ et $\deg(R) < \deg(B)$.

Preuve

- ▶ Si $\deg(B) < \deg(A)$,
  - ▷ Alors $B = 0 \cdot A + B$ est une division euclidienne de B par A.
  - ▷ Cela implique que $(Q, R) = (0, B)$ et $\deg(R) = \deg(B) < \deg(A)$.
- ▶ Si $\deg(B) \geq \deg(A)$,
  - ▷ Cela implique que $B \neq 0$.
  - ▷ On pose $B = \sum_{k=0}^{m} b_k X^k$ avec $b_m \neq 0$, et $A = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$.

▷ Le degré de B est m et le degré de A est n, donc $m \geq n$.

▷ Nous allons procéder par récurrence forte sur m.

— **Initialisation :** Si $m < n$, la propriété est vérifiée comme montré dans le premier cas.

— **Hérédité :** Supposons que la propriété est vérifiée pour tout $k \leq m-1$. Nous allons montrer qu'elle est également vérifiée pour m.

— On pose $B_1 = B - b_m a_n^{-1} X^{m-n} \cdot A$. Alors B_1 est un polynôme de degré inférieur à m (en prenant le degré de B et le degré de $b_m a_n^{-1} X^{m-n} \cdot A$).

— Le coefficient dominant de B_1 est nul, car $b_m - b_m a_n^{-1} a_n = 0$.

— Le degré de B_1 est donc strictement inférieur à m. On peut donc appliquer l'hypothèse de récurrence à B_1. On peut donc écrire $B_1 = A \cdot Q_1 + R$ avec $\deg(R) < \deg(A)$.
Donc $B = A \cdot Q + R$ avec $Q = Q_1 + b_m a_n^{-1} X^{m-n}$.

— On a donc trouvé un couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $B = A \cdot Q + R$ et $\deg(R) < \deg(B)$.

▷ Montrons maintenant l'unicité de ce couple.

— Supposons qu'il existe un autre couple $(Q', R') \in \mathbb{K}[X]^2$ tel que $B = A \cdot Q' + R'$ et $\deg(R') < \deg(B)$.

— En soustrayant les deux égalités, on trouve que $A \cdot \underbrace{(Q - Q')}_{=Q} = \underbrace{R' - R}_{=R}$.

— Comme $\deg(AQ) = \deg(A) + \deg(Q) = \deg(R) \leq \max(\deg(R), \deg(R'))$, on trouve que $\deg(Q) < 0$, ce qui implique que $Q = 0$, et par conséquent que $R = 0$.

— Donc $Q = Q'$ et $R = R'$, ce qui montre l'unicité du couple (Q, R).

■

Exemple 2.2.2.1

$\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$, $B = X^4 + X^3 - 2X + 1$, $A = 2X^2 + 4X - 1$.
(Pour être rigoureux, il aurait fallu noter $\overline{2}, \overline{4}$ et $\overline{1}$ au lieu de $2, 4$ et 1, mais on se permet de faire un léger abus de notation pour alléger les calculs.)
Après division euclidienne, on trouve que le quotient est $3X^2 + 2X$ et le reste est 1.

On peut utiliser la division euclidienne pour démontrer quelques autres propriétés de $\mathbb{K}[X]$, notamment le fait que c'est un anneau principal.

Propriété 2.2.2.10

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

Preuve

Soit I un idéal de $\mathbb{K}[X]$.

- Si $I = \{0\}$, alors $I = \langle 0 \rangle = 0 \cdot \mathbb{K}[X]$.
- Si I n'est pas réduit à $\{0\}$, alors il existe un polynôme non nul $P \in I$ de degré minimal d.
  - On pose $E = \{\deg(P) \text{ tel que } P \in I \setminus \{0\}\}$
  - On a $E \neq \emptyset$ (car $I \neq \{0\}$) et $E \subset \mathbb{N}$. E admet un minimum d (car $\mathbb{N}$ est bien ordonné).
  - On peut donc écrire $\exists P_0 \in I \setminus \{0\}$ tel que $\deg(P_0) = d$.
  - Montrons que $I = \langle P_0 \rangle = P_0 \cdot \mathbb{K}[X]$.
  - On a $\forall Q \in \mathbb{K}[X]$, $P_0 \cdot Q \in I$ car $P_0 \in I$ et I est un idéal.
  - Donc $P_0 \cdot \mathbb{K}[X] \subset I$.
  - Soit $B \in I$. Par la division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $B = P_0 \cdot Q + R$ et $\deg(R) < \deg(P_0) = d$.
  - On a $R = B - P_0 \cdot Q \in I$ (car $B \in I$, $P_0 \cdot Q \in I$, et I est un idéal, donc stable par soustraction).
    - Si $R \neq 0$, cela implique que $R \in I \setminus \{0\}$, et donc que $\deg(R) \in E$, ce qui implique que $\deg(R) \geq \deg(P_0) = d$ (car d est le minimum de E). C'est une contradiction, parce que $R = B - P_0 \cdot Q$ et $\deg(R) < \deg(P_0) = d$.
    - Donc $R = 0$, et par conséquent, $B = P_0 \cdot Q \in P_0 \cdot \mathbb{K}[X]$.
  - Ainsi, $I \subset P_0 \cdot \mathbb{K}[X]$.
  - Par conséquent, $I = P_0 \cdot \mathbb{K}[X] = \langle P_0 \rangle$.
- Donc, dans tous les cas, I est principal.

■

Remarque 2.2.2.6

Si I est un idéal non-nul de $\mathbb{K}[X]$, alors I est engendré par un unique polynôme unitaire de degré minimal.

$$\exists! P_0 \in I \setminus \{0\} \text{ tel que } P_0 \text{ unitaire et } I = \langle P_0 \rangle = P_0 \cdot \mathbb{K}[X]$$

Preuve

Soit I un idéal non-nul.
Nous allons montrer que I est engendré par un polynôme unitaire de degré minimal.
Donc $\exists P_1 \in \mathbb{K}[X] \setminus \{0\}$ tel que $I = \langle P_1 \rangle = P_1 \cdot \mathbb{K}[X]$.
On a donc $I = (\mathrm{CD}(P_1))^{-1} \cdot P_1 \cdot \mathbb{K}[X]$, sachant que $\mathrm{CD}(P_1) \in \mathbb{K}^*$ (car $P_1 \neq 0$ et $\mathbb{K}$ est un corps), et que donc les deux polynômes P_1 et $(\mathrm{CD}(P_1))^{-1} \cdot P_1$ sont associés.

On pose $P_0 = (\mathrm{CD}(P_1))^{-1} \cdot P_1$. Alors P_0 est unitaire, et $I = P_0 \cdot \mathbb{K}[X]$.
Nous allons maintenant montrer que P_0 est le *seul* polynôme unitaire de degré minimal qui engendre I.
Si $\exists Q_0$ unitaire tel que $I = P_0 \cdot \mathbb{K}[X] = Q_0 \cdot \mathbb{K}[X]$, alors P_0 et Q_0 sont associés.
Donc $\exists \lambda \in \mathbb{K}^*$ tel que $P_0 = \lambda \cdot Q_0$.
On sait que $\mathrm{CD}(P_0) = 1$ et $\mathrm{CD}(Q_0) = 1$, donc $\lambda = 1$, et par conséquent, $P_0 = Q_0$.
Donc P_0 est unique. ■

2.3 Racines d'un polynôme

Définition 2.2.3.9 ***(Racine d'un polynôme)***

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$. On dit que $a \in \mathbb{K}$ est une racine (ou zéro) de P si et seulement si $\tilde{P}(a) = 0$, c'est à dire $P(a) = 0$.

Exemple 2.2.3.2

- 2 est une racine de $X^2 + X - 6$ dans $\mathbb{K}[X]$.
- i est une racine de $X^2 + 1$ dans $\mathbb{K}[X]$, mais $X^2 + 1$ n'a pas de racine dans $\mathbb{R}[X]$.

Remarque 2.2.3.7

La notion de racine dépend très fortement du corps étudié.

Propriété 2.2.3.11

Soit $P \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$. Alors $a \in \mathbb{K}$ est une racine de P si et seulement si $(X - a) \mid P$.

Preuve

- La démonstration dans le sens indirect $\Longleftarrow$ est claire, car si $(X - a) \mid P$, alors $P = (X - a) \cdot Q$ pour un certain $Q \in \mathbb{K}[X]$, et donc $P(a) = (a - a) \cdot Q(a) = 0$.
- Dans le sens direct $\Longrightarrow$, si $P(a) = 0$, alors par la division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = (X - a) \cdot Q + R$ et $\deg(R) < \deg(X - a) = 1$. Donc R est une constante. En évaluant en a, on obtient $0 = P(a) = (a - a) \cdot Q(a) + R = R$, donc $R = 0$ et $P = (X - a) \cdot Q$, ce qui montre que $(X - a) \mid P$.

■

Conséquence 2.2.3.1

Soient $P \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$, et $a_1, a_2, \ldots, a_k$ des racines deux à deux distinctes de P. Alors $(X - a_1)(X - a_2) \cdots (X - a_k) \mid P$.

$$\prod_{i=1}^{k} (X - a_i) \mid P$$

Preuve

On procède par récurrence sur $k \in \mathbb{N}^*$.
Initialisation : Pour $k = 1$, le résultat est trivialement vrai, car $(X - a_1) \mid P$ si a_1 est une racine de P.
Hérédité : Supposons que le résultat soit vrai pour un certain $k \geq 1$, c'est-à-dire que si $a_1, a_2, \ldots, a_k$ sont des racines deux à deux distinctes de P, alors $(X - a_1)(X - a_2) \cdots (X - a_k) \mid P$.
Soit a_{k+1} une racine distincte de P. Alors, par la propriété précédente, $(X - a_{k+1}) \mid P$.
On sait qu'il existe un $Q \in \mathbb{K}[X]$ tel que $P = (X - a_k) \cdot Q$.
Et on a $P(a_{k+1}) = 0$, donc $Q(a_{k+1}) = 0$, ce qui implique que a_{k+1} est une racine de Q, et donc que $(X - a_{k+1}) \mid Q$.
Par hypothèse de récurrence, $(X - a_1)(X - a_2) \cdots (X - a_k) \mid P$.
On obtient donc $(X - a_1)(X - a_2) \cdots (X - a_k)(X - a_{k+1}) \mid P$.
Conclusion : Par le principe de récurrence, le résultat est vrai pour tout $k \in \mathbb{N}^*$.
■

2.4 Multiplicité d'une racine

Remarque 2.2.4.8

1. Si P est un polynôme dont le nombre de racines distinctes est supérieur au degré de P, alors P est le polynôme nul.
2. Si P admet une infinité de racines, alors $P = 0$.

Définition 2.2.4.10 *(Racine de multiplicité s d'un polynôme)*

Soient $P \in \mathbb{K}[X]$, et $\alpha \in \mathbb{K}$ un scalaire, et $s \in \mathbb{N}^*$.
On dit que α est une **racine de multiplicité** s de P si et seulement si

$$(X - \alpha)^s \mid P \text{ et } (X - \alpha)^{s+1} \nmid P$$

Exemple 2.2.4.3

Considérons le polynôme $P = X^3 - 4X^2 + 5X - 2$ dans $\mathbb{R}[X]$.
1 est une racine de multiplicité 2 de P, et 2 est une racine de multiplicité 1 de P, parce qu'on a $P = (X-1)^2(X-2)$, et que P n'est pas divisible par $(X-1)^3$ ni par $(X-2)^2$.
1 est aussi dite **racine double** de P, et 2 est dite **racine simple** de P.

Propriété 2.2.4.12

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $s \in \mathbb{N}^*$. Alors α est une racine de multiplicité s de P si et seulement si $\forall k \in [\![0, s-1]\!], P^{(k)}(\alpha) = 0$, et $P^{(s)}(\alpha) \neq 0$.
Concrètement, une racine de multiplicité s d'un polynôme est une racine qui annule les s premières dérivées du polynôme, mais pas la s-ième dérivée du polynôme.

Preuve

La démonstration utilisera la formule de Taylor.
On pose $n = \deg(P)$.

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

On remarque que Q et R sont respectivement le quotient et le reste de la division euclidienne de P par $(X-\alpha)^s$.
On suppose maintenant que α est une racine de multiplicité s de P dans $\mathbb{K}[X]$.

$$\begin{aligned} \alpha \text{ racine de multiplicité } s &\iff \Big(((X-\alpha)^s \mid P) \text{ et } ((X-\alpha)^{s+1} \nmid P)\Big) \\ &\iff (R = 0 \text{ et } P^{(s)}(\alpha) \neq 0) \\ &\iff (R = 0 \text{ et } Q(\alpha) \neq 0) \\ &\iff \begin{cases} \forall k \in [\![0, s-1]\!], P^{(k)}(\alpha) = 0 \\ P^{(s)}(\alpha) \neq 0 \end{cases} \end{aligned}$$

On en déduit donc que α est une racine de multiplicité s de P si et seulement si $\forall k \in [\![0, s-1]\!], P^{(k)}(\alpha) = 0$, et $P^{(s)}(\alpha) \neq 0$. ■

Remarque 2.2.4.9

1. Si α est une racine de multiplicité s de P, alors :

$$s = \max(\{k \in \mathbb{N}, (X-\alpha)^k \mid P\})$$

2. Si $m \in \mathbb{N}^*$ tel que $(X-\alpha)^m \mid P$, alors la multiplicité de α est $\geq$ à m.

2.5 Polynômes scindés

Définition 2.2.5.11 *(Polynôme scindé)*

Un polynôme $P \in \mathbb{K}[X]$ est dit **scindé** dans $\mathbb{K}[X]$ s'il admet $\deg(P)$ racines (pas forcément distinctes) dans $\mathbb{K}$.
Autrement dit, P est scindé dans $\mathbb{K}[X]$ s'il existe $a_1, a_2, \ldots, a_n \in \mathbb{K}$ (pas forcément distincts) tels que $P = \mathrm{CD}(P)\prod_{i=1}^{n}(X-a_i)$, où $n = \deg(P)$.

Remarque 2.2.5.10

1. Les x_i ne sont pas forcément distincts, car P peut admettre des racines de multiplicité supérieure ou égale à 2.
2. Si P est scindé dans $\mathbb{K}[X]$, alors :

$$\begin{cases} \exists x_1, \ldots, x_q \in \mathbb{K} \text{ deux à deux distincts} \\ \exists s_1, \ldots, s_q \in \mathbb{N}^* \text{ tels que } \sum_{i=1}^{q} s_i = n \text{ et } P = \mathrm{CD}(P)\prod_{i=1}^{q}(X-x_i)^{s_i} \end{cases}$$

3. La notion de polynôme scindé dépend très fortement du corps étudié, car la notion de racine dépend très fortement du corps étudié. Par exemple, X^2+1 n'est pas scindé dans $\mathbb{R}[X]$, mais il est scindé dans $\mathbb{C}[X]$.

Propriété 2.2.5.13 *(Relations racines/coeffs. d'un polynôme scindé)*

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme scindé dans $\mathbb{K}[X]$, et $x_1, x_2, \ldots, x_n$ les racines de P (pas forcément distinctes) dans $\mathbb{K}$.
On pose $\forall k \in [\![1, n]\!], \sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}$, c'est à dire que σ_k est la somme de tous les produits de k racines distinctes de P.
Alors $\forall k \in [\![0, n]\!], \sigma_k = (-1)^k \cdot \frac{a_{n-k}}{a_n}$, où a_n est le coefficient dominant de P (Formule de Viète).

Preuve

La démonstration se fait par récurrence sur $n = \deg(P) \in \mathbb{N}^*$. Elle est assez complexe et ne sera pas détaillée dans ce cours. ■

Remarque 2.2.5.11

1. $\sigma_1 = \sum_{k=1}^{n} x_k$
   $\sigma_n = \prod_{k=1}^{n} x_k$.
2. Dans le cas où $\deg(P) = 2 = n$, on a $P = a_2X^2+a_1X+a_0 = a_2(X-x_1)(X-x_2)$, ce qui nous donne $P = a_2(X^2 - (x_1 + x_2)X + x_1x_2)$, et donc par égalité des polynômes, $\sigma_1 = x_1 + x_2 = -\frac{a_1}{a_2}$ et $\sigma_2 = x_1x_2 = \frac{a_0}{a_2}$.
3. Dans le cas où $\deg(P) = 3 = n$, on a $P = a_3X^3 + a_2X^2 + a_1X + a_0 = a_3(X - x_1)(X-x_2)(X-x_3)$, ce qui nous donne $P = a_3(X^3-(x_1+x_2+x_3)X^2+(x_1x_2+x_1x_3+x_2x_3)X-x_1x_2x_3)$, et donc par égalité des polynômes, $\sigma_1 = x_1+x_2+x_3 = -\frac{a_2}{a_3}$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = \frac{a_1}{a_3}$ et $\sigma_3 = x_1x_2x_3 = -\frac{a_0}{a_3}$.

Application 2.2.5.1

1. Résoudre dans $\mathbb{R}^3$ le système d'équations suivant :

$$\begin{cases} x + y + z = 1 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2 \\ xyz = -2 \end{cases}$$

2. Soient $x_1, \ldots, x_n$ les racines d'un polynôme $P \in \mathbb{K}[X]$ scindé de degré n. Calculer $\sum_{k=1}^{n} x_k^2$ en fonction des coefficients de P.

Solution (1) :
On pose :

$$\begin{cases} \sigma_1 = x + y + z = 2 \\ \sigma_2 = xy + xz + yz = 1 \\ \sigma_3 = xyz = -2 \end{cases}$$

x, y, z sont les racines du polynôme $P = X^3 - \sigma_1X^2 + \sigma_2X - \sigma_3 = X^3 - 2X^2 + X + 2$.
L'ensemble des solutions du système est donc $\{(x, y, z) \in \mathbb{R}^3, P(x) = P(y) = P(z) = 0\}$.
Il faut ensuite continuer réciproquement... Ou au moins mentionner que les solutions restent valident réciproquement.
Solution (2) :
On a $\sigma_1 = \sum_{k=1}^{n} x_k$ et $\sigma_2 = \sum_{1\le i<j\le n} x_ix_j$.
On a alors $\sum_{k=1}^{n} x_k^2 = (\sum_{k=1}^{n} x_k)^2 - 2\sum_{1\le i<j\le n} x_ix_j = \sigma_1^2 - 2\sigma_2$.

2.6 PGCD et PPCM de polynômes

Théorème 2.2.6.4

Soient $P_1, \dots, P_n \in \mathbb{K}[X]$.

1. **PGCD :**
   - **a)** $\exists! D \in \mathbb{K}[X]$ avec $\begin{cases} D \text{ unitaire} \\ \text{ou} \\ D = 0 \end{cases}$ tel que :
     $\sum_{i=1}^{n} P_i\mathbb{K}[X] = D \cdot \mathbb{K}[X]$ et $\forall i \in [\![1, n]\!], D \mid P_i$.
   - **b)** Si $\exists \Delta \in \mathbb{K}[X]$ tel que $\forall i \in [\![1, n]\!], \Delta \mid P_i$, alors $\Delta \mid D$.
     D est appelé le **plus grand commun diviseur** (PGCD) de $P_1, \dots, P_n$, et est noté $\text{pgcd}(P_1, \dots, P_n)$.
2. **PPCM :**
   - **a)** $\exists! M \in \mathbb{K}[X]$ avec $\begin{cases} M \text{ unitaire} \\ \text{ou} \\ M = 0 \end{cases}$ tel que :
     $\bigcap_{i=1}^{n} P_i \cdot \mathbb{K}[X] = M \cdot \mathbb{K}[X]$ et $\forall i \in [\![1, n]\!], P_i \mid M$.
   - **b)** Si $\exists A \in \mathbb{K}[X]$ tel que $\forall i \in [\![1, n]\!], P_i \mid A$, alors $M \mid A$.
     M est appelé le **plus petit commun multiple** (PPCM) de $P_1, \dots, P_n$, et est noté $\text{ppcm}(P_1, \dots, P_n)$.

Preuve

La preuve est analogue à celle du théorème sur le PGCD et le PPCM dans un anneau (chapitre 11). ■

Propriété 2.2.6.14

Soient $P_1, \dots, P_n, Q \in \mathbb{K}[X]$.

1. $\text{pgcd}(P_1Q, P_2Q, \dots, P_nQ) = \text{pgcd}(P_1, P_2, \dots, P_n) \cdot \frac{Q}{\text{CD}(Q)}$.
2. $\text{ppcm}(P_1Q, P_2Q, \dots, P_nQ) = \text{ppcm}(P_1, P_2, \dots, P_n) \cdot \frac{Q}{\text{CD}(Q)}$.

Attention

Il ne faut pas oublier que le PGCD et le PPCM sont définis à une unité près, c'est à dire que $\text{pgcd}(P_1, P_2, \dots, P_n)$ et $\text{ppcm}(P_1, P_2, \dots, P_n)$ sont définis à une unité près. C'est pour cela que dans les égalités ci-dessus, on divise Q par son coefficient dominant $\text{CD}(Q)$ pour s'assurer que le PGCD et le PPCM restent unitaires.

Définition 2.2.6.12

Soient $A_1, \dots, A_n \in \mathbb{K}[X]$.

1. On dit que $A_1, \dots, A_n$ sont **premiers entre eux** si et seulement si $\text{pgcd}(A_1, \dots, A_n) = 1$.
2. On dit que $A_1, \dots, A_n$ sont **premiers entre eux deux à deux** si et seulement si $\forall i, j \in [\![1, n]\!], i \neq j \implies \text{pgcd}(A_i, A_j) = 1$.

Remarque 2.2.6.12

La deuxième propriété implique la première, mais la réciproque n'est pas vraie. Par exemple, les polynômes $A_1 = (X-2)(X-3)$, $A_2 = (X-1)(X-3)$ et $A_3 = (X-1)(X-2)$ sont premiers entre eux, car $\text{pgcd}(A_1, A_2, A_3) = 1$, mais ils ne sont pas premiers entre eux deux à deux, car $\text{pgcd}(A_1, A_2) = X - 3 \neq 1$, $\text{pgcd}(A_1, A_3) = X - 2 \neq 1$ et $\text{pgcd}(A_2, A_3) = X - 1 \neq 1$.

Les preuves des propriétés qui suivront sont analogues à celles des propriétés sur le PGCD et le PPCM dans un anneau principal (chapitre 11).

Propriété 2.2.6.15

Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$.

$$\begin{cases} A \wedge B = 1 \\ C \mid B \end{cases} \implies A \wedge C = 1$$

Théorème 2.2.6.5 ***(Égalité de Bézout)***

Soient $P_1, \dots, P_n \in \mathbb{K}[X]$.

$$D = \text{pgcd}(P_1, \dots, P_n) \implies \exists Q_1, \dots, Q_n \in \mathbb{K}[X] \text{ tel que } D = \sum_{i=1}^{n} P_i Q_i$$

Propriété 2.2.6.16

Soient $P_1, \dots, P_n \in \mathbb{K}[X]$ et $D \in \mathbb{K}[X]$.

$$\text{si } \exists U_1, \dots, U_n \in \mathbb{K}[X] \text{ tel que } D = P_1U_1 + P_2U_2 + \cdots + P_nU_n$$

avec $\forall 1 \leq i \leq n, D \mid P_i$ et D est unitaire (ou nul).
Alors $D = \text{pgcd}(P_1, \dots, P_n)$.

Conséquence 2.2.6.2

Soient $P_1, \dots, P_n \in \mathbb{K}[X]$.

$$\text{pgcd}(P_1, \dots, P_n) = 1 \iff \exists Q_1, \dots, Q_n \in \mathbb{K}[X] \text{ tel que } 1 = P_1Q_1 + P_2Q_2 + \cdots + P_nQ_n$$

Théorème 2.2.6.6 ***(Théorème de Gauss)***

Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$.

$$\begin{cases} A \wedge B = 1 \\ A \mid C \\ B \mid C \end{cases} \implies AB \mid C$$

Conséquence 2.2.6.3

Soient $A, P_1, \dots, P_n \in \mathbb{K}[X] \setminus \{0\}$.

$$\begin{cases} P_i \mid A \quad \forall i \in [\![1, n]\!] \\ (P_1, \dots, P_n) \text{ premiers entre eux deux à deux distincts} \end{cases} \implies \left(\prod_{i=1}^{n} P_i \right) \mid A$$

Propriété 2.2.6.17

Si $P_1, \dots, P_n$ sont premiers entre eux deux à deux, alors :

$$\text{ppcm}(P_1, \dots, P_n) = \frac{1}{\prod_{i=1}^{n} \text{CD}(P_i)} \prod_{i=1}^{n} P_i$$

Conséquence 2.2.6.4

Soient $A, B \in \mathbb{K}[X] \setminus \{0\}$.

$$(A \wedge B)(A \vee B) = \frac{1}{\text{CD}(AB)} AB$$

Théorème 2.2.6.7 ***(Lemme d'Euclide)***

Si $A = B \cdot Q + R$ avec $A, B, Q, R \in \mathbb{K}[X]$ et $\deg(R) < \deg(B)$, alors $A \wedge B = B \wedge R$.

2.7 Les polynômes irréductibles

Définition 2.2.7.13 ***(Polynôme irréductible)***

Un polynôme $P \in \mathbb{K}[X]$ de degré ≥ 1 est dit **irréductible** (ou premier) dans $\mathbb{K}[X]$ lorsque les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les polynômes constants non-nuls et les polynômes associés à P (λP tel que $\lambda \in \mathbb{K}^*$).
Dans le cas contraire, P est dit réductible dans $\mathbb{K}[X]$.

Attention

- Un polynôme irréductible **n'est pas** forcément un polynôme qui n'admet pas de racines dans $\mathbb{K}$. Par exemple $(X^2+1)^2$ est un polynôme réductible dans $\mathbb{R}[X]$, mais il n'admet pas de racines dans $\mathbb{R}$. Idem pour le polynôme X^4+1 dans $\mathbb{R}[X]$, qui est réductible mais n'admet pas de racines dans $\mathbb{R}$.
- Par définition, un polynôme irréductible est de degré ≥ 1. Par conséquent, les polynômes constants non-nuls ne sont pas considérés irréductibles dans $\mathbb{K}[X]$.

Exemple 2.2.7.4

1. Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.
2. X^2+1 est irréductible dans $\mathbb{R}[X]$, mais il est réductible dans $\mathbb{C}[X]$.

Exercice 2.2.7.2

Soit $A \in \mathbb{R}[X]$ tel que $\deg(A) = 2n+1$ et $n \in \mathbb{N}^*$. Montrer que A est réductible dans $\mathbb{R}[X]$.
Solution :
Pour démontrer ce résultat, nous allons utiliser le théorème de la valeur intermédiaire généralisé sur une fonction polynomiale.

à faire chez soi

Remarque 2.2.7.13

1. En général, si $P = P_1 \cdot P_2$ avec $P_1, P_2 \in \mathbb{K}[X]$ des polynômes non-constants, alors P est réductible dans $\mathbb{K}[X]$.
2. Le résultat de l'exercice précédent n'est pas valable dans $\mathbb{Q}[X]$. Par exemple, le polynôme $P = X^3 + X - 1$ est de degré 3, mais il est irréductible dans $\mathbb{Q}[X]$.

   - Pour le démontrer, on peut supposer que P est réductible, donc qu'il est factorisable en produit de deux polynômes (au moins), et donc qu'il existe $A, B \in \mathbb{Q}[X]$ tels que $P = A \cdot B$ avec $1 \leq \deg(A), \deg(B) \leq 2$.
   - Prenons, par exemple et sans perte de généralité, $\deg(A) = 1$ et $\deg(B) = 2$.

Donc $\exists (a,b) \in \mathbb{Q}^* \times \mathbb{Q}$ tels que $A = aX + b$. Donc $r = -\frac{b}{a}$ est une racine de P. On écrit $r = \frac{p}{q}$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$.

- On a donc $r^3 + r - 1 = 0$, ce qui équivaut à dire que $p^3 + p \cdot q^2 - q^3 = 0$, ce qui implique que $p^3 = q(q^2 - pq)$, et donc que $q \mid p^3$ et par conséquent $q \mid 1$ donc $q = 1$ et par suite $r = p$ et $p(p^2+1) = 1$ donc $p \mid 1$ alors $p = \pm 1$. Donc $r = \pm 1$ est une racine de P, ce qui est absurde, car $P(1) = 1^3 + 1 - 1 = 1 \neq 0$ et $P(-1) = (-1)^3 + (-1) - 1 = -3 \neq 0$.
- On en déduit que P est irréductible dans $\mathbb{Q}[X]$.

Théorème 2.2.7.8 *(Théorème de D'Alembert-Gauss)*

Tout polynôme non-constant $P \in \mathbb{C}[X]$ de degré $n \geq 1$ admet au moins une racine dans $\mathbb{C}$.

Preuve

À faire comme DL (ou voir CNC 2007). ■

Conséquence 2.2.7.5

1. Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.
2. Tout polynôme non-constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$. (Une conséquence qui sera abordée bien plus tard est que toute matrice $M_1 \in \mathcal{M}_1(\mathbb{C})$ à coefficients complexes est trigonalisable, c'est-à-dire qu'elle est semblable à une matrice triangulaire).

Propriété 2.2.7.18 *(Conjugaison complexe d'un polynôme)*

Soit $P \in \mathbb{C}[X]$.

$$P \in \mathbb{R}[X] \iff \forall z \in \mathbb{C}, \overline{P(z)} = P(\overline{z})$$

Preuve

Dans le sens direct ($\Longrightarrow$), la démonstration est triviale. Si $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$, alors $\overline{P(z)} = \sum_{k=0}^{n} \overline{a_k}\overline{z^k} = \sum_{k=0}^{n} a_k \overline{z^k} = P(\overline{z})$.
Dans le sens réciproque ($\Longleftarrow$), supposons que $\forall z \in \mathbb{C}, \overline{P(z)} = P(\overline{z})$. On pose $P = \sum_{k=0}^{n} a_k X^k$. Alors $\overline{P(z)} = \sum_{k=0}^{n} \overline{a_k}\overline{z^k}$ et $P(\overline{z}) = \sum_{k=0}^{n} a_k \overline{z^k}$.
Donc $\sum_{k=0}^{n} (\overline{a_k} - a_k)\overline{z^k} = 0$ pour tout $z \in \mathbb{C}$.
Donc Q admet une infinité de racines, et par conséquent Q est le polynôme nul, c'est à dire que $\forall k \in [\![0,n]\!], \overline{a_k} - a_k = 0$, ce qui implique que $\forall k \in [\![0,n]\!], a_k \in \mathbb{R}$, et donc $P \in \mathbb{R}[X]$. ■

→ Conséquence 2.2.7.6

Soient $P \in \mathbb{R}[X]$, $z \in \mathbb{C} \setminus \mathbb{R}$ et $s \in \mathbb{N}^*$. Alors z est une racine de multiplicité s de P dans $\mathbb{C}[X]$ si et seulement si $\overline{z}$ est une racine de multiplicité s de P dans $\mathbb{C}[X]$.

Preuve

Nous allons utiliser les propriétés liées aux polynômes dérivés et à la conjugaison complexe d'un polynôme.
On sait que z est une racine de multiplicité s de P dans $\mathbb{C}[X]$.
Par définition, cela équivaut à dire que $\forall k \in [\![0, s-1]\!], P^{(k)}(z) = 0$ et $P^{(s)}(z) \neq 0$.
Cela implique que $\forall k \in [\![0, s-1]\!], \overline{P^{(k)}(z)} = 0$ et $\overline{P^{(s)}(z)} \neq 0$.
Donc $\forall k \in [\![0, s-1]\!], P^{(k)}(\overline{z}) = 0$ et $P^{(s)}(\overline{z}) \neq 0$, ce qui équivaut à dire que $\overline{z}$ est une racine de multiplicité s de P dans $\mathbb{C}[X]$. ■

→ Conséquence 2.2.7.7

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racines dans $\mathbb{R}$, c'est à dire les polynômes dont le discriminant Δ est strictement négatif < 0.

Preuve

Soit $P \in \mathbb{R}[X]$.

- Si P est de degré 1, alors P est irréductible dans $\mathbb{R}[X]$.
- Si P est de degré 2...
  - Si $\Delta \geq 0$, alors P admet au moins une racine dans $\mathbb{R}$, et par conséquent P est réductible dans $\mathbb{R}[X]$.
  - Dans le cas où $\Delta < 0$, on procède par absurde en supposant que P est réductible.
    - Supposons que P est réductible dans $\mathbb{R}[X]$. Alors il existe $P_1 \in \mathbb{R}[X]$ un polynôme de degré 1 tel que $P_1 \mid P$, or P_1 admet une racine réelle, et par conséquent P admet une racine réelle, ce qui est absurde, car $\Delta < 0$.
    - On en déduit que P est irréductible dans $\mathbb{R}[X]$.
- Si P est de degré ≥ 3, alors :
  - Si P admet un au moins une racine réelle a, alors $X - a \mid P$, et par conséquent P est réductible dans $\mathbb{R}[X]$.
  - Dans le cas contraire, on sait que $P \in \mathbb{R}[X] \subset \mathbb{C}[X]$, donc d'après le théorème de D'Alembert-Gauss, P admet au moins une racine complexe z, cette racine z n'est pas réelle (elle appartient à $\mathbb{C} \setminus \mathbb{R}$). $\overline{z}$ est aussi une racine de P, donc $X - z \mid P$ et $X - \overline{z} \mid P$, et par conséquent $(X - z)(X - \overline{z}) \mid P$, et comme $(X - z)(X - \overline{z}) = X^2 - 2\Re(z)X + |z|^2 \in \mathbb{R}[X]$, cela implique que P est réductible dans $\mathbb{R}[X]$.

■

2.8 Décomposition primaire d'un polynôme

Propriété 2.2.8.19

Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) \geq 1$. Alors $\exists P \in \mathbb{K}[X]$ irréductible tel que $P \mid A$.

Preuve

On pose $E = \{\deg(D) \text{ tel que } D \mid A \text{ et } \deg(D) \geq 1\}$.
On a $A \mid A$ donc $\deg(A) \in E$ et par conséquent E est non-vide. Donc E admet un minimum $m \in \mathbb{N}^*$, et il existe $P \in \mathbb{K}[X]$ tel que $\deg(P) = m$ et $P \mid A$.
Supposons que P est réductible dans $\mathbb{K}[X]$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $1 \leq \deg(Q) < \deg(P)$ et $Q \mid P$. Or $P \mid A$, alors $Q \mid A$, donc $\deg Q \in E$ et $\deg(Q) < m$, ce qui est absurde, car m est le minimum de E.
On en déduit que P est irréductible dans $\mathbb{K}[X]$ et que $P \mid A$. ■

Théorème 2.2.8.9 ***(Décomposition primaire d'un polynôme)***

Soit $A \in \mathbb{K}[X]$. Alors il existe une décomposition primaire de A, c'est-à-dire des polynômes irréductibles $P_1, \ldots, P_s \in \mathbb{K}[X]$ tels que :

$$A = \mathrm{CD}(A) P_1 \ldots P_s$$

Cette décomposition est unique à une permutation près.
i.e. si $A = \mathrm{CD}(A) \prod_{i=1}^{r} Q_i$ avec Q_i irréductible, alors $r = s$ et $\{P_1, \ldots, P_s\} = \{Q_1, \ldots, Q_r\}$.

Preuve

L'existence est démontrée par récurrence forte sur $\deg(A)$.
Démonstration de l'unicité :
Supposons que $A = \mathrm{CD}(A) P_1 \ldots P_s$ et $A = \mathrm{CD}(A) Q_1 \ldots Q_r$ avec P_i, Q_j irréductibles.
On a donc $\forall i \in [\![1, s]\!], P_i \mid A$
Donc $\exists j \in [\![1, r]\!]$ tel que $P_i \mid Q_j$, car $P_1, \ldots, P_s$ sont irréductibles.
Comme Q_j est irréductible, cela implique que :

$$\begin{cases} P_i \text{ constant non-nul} \\ \exists \lambda \in \mathbb{K}^* \text{ tel que } P_i = \lambda Q_j \end{cases}$$

Or $\mathrm{CD}(P_i) = 1$ et $\mathrm{CD}(Q_j) = 1$, donc $\lambda = 1$, et par conséquent $P_i = Q_j$. ■

Conséquence 2.2.8.8

Soit A un polynôme de $\mathbb{K}[X]$ de degré ≥ 1.
Alors $\exists P_1, \dots, P_r \in \mathbb{K}[X]$ irréductibles deux à deux distincts, et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ tels que $A = \mathrm{CD}(A) \prod_{i=1}^{r} P_i^{\alpha_i}$.
Cette décomposition est unique à une permutation près des $(P_k)_{1 \leq k \leq r}$.

Remarque 2.2.8.14

1. Dans $\mathbb{C}[X]$, il existe $x_1, \dots, x_r \in \mathbb{C}$ deux à deux distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ tels que $A = \mathrm{CD}(A) \prod_{i=1}^{r} (X - x_i)^{\alpha_i}$.
2. Dans $\mathbb{R}[X]$, il existe $x_1, \dots, x_r \in \mathbb{R}$ deux à deux distincts, et il existe $(b_1, c_1), \dots, (b_s, c_s) \in \mathbb{R}^2$ tels que $b_i^2 + c_i^2 > 0$ pour tout $i \in [\![1, s]\!]$, et $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s \in \mathbb{N}$ tels que $A = \mathrm{CD}(A) \prod_{i=1}^{r} (X - x_i)^{\alpha_i} \prod_{j=1}^{s} (X^2 + b_j X + c_j)^{\beta_j}$ avec $\forall j \in [\![1, s]\!], b_j^2 - 4c_j < 0$.

Théorème 2.2.8.10 *(PGCD et PPCM par décomposition primaire)*

Soient A, B deux polynômes de $\mathbb{K}[X]$ de degré ≥ 1.
On écrit :

$$\begin{cases} A = \mathrm{CD}(A) \prod_{i=1}^{r} P_i^{\alpha_i} \\ B = \mathrm{CD}(B) \prod_{i=1}^{r} P_i^{\beta_i} \end{cases}$$

avec $P_1, \dots, P_r \in \mathbb{K}[X]$ irréductibles deux à deux distincts
et $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$.
Le PGCD et le PPCM de A et B sont alors donnés par les formules suivantes :

$$A \wedge B = \prod_{i=1}^{r} P_i^{\min(\alpha_i, \beta_i)}$$

$$A \vee B = \prod_{i=1}^{r} P_i^{\max(\alpha_i, \beta_i)}$$

Remarque 2.2.8.15

1. $A \wedge B = D \iff \exists A_1, B_1 \in \mathbb{K}[X]$ tel que $\begin{cases} A = A_1 D \\ B = B_1 D \\ A_1 \wedge B_1 = 1 \end{cases}$
2. **Caractérisation des polynômes premiers entre eux dans $K[X]$ avec K un sous-corps de $\mathbb{C}$:**
   a) Soient K un sous-corps de $\mathbb{C}$ et $P, Q \in \mathbb{K}[X]$.

$$P \wedge Q = 1 \iff P \text{ et } Q \text{ n'ont aucune racine commune dans } \mathbb{C}$$

Preuve *(Démonstration de la caractérisation (2))*

- La démonstration de l'implication ($\Longrightarrow$) est assez simple.
  - On suppose que $P \wedge Q = 1$.
  - Par conséquent, il existe $A, B \in \mathbb{K}[X]$ tels que $1 = AP + BQ$.
  - Soit $z \in \mathbb{C}$ une racine de P et de Q. Alors $1 = AP(z) + BQ(z) = 0$, ce qui est absurde.
  - On en déduit que P et Q n'ont aucune racine commune dans $\mathbb{C}$.
- La démonstration de l'implication ($\Longleftarrow$) est plus complexe.
  - On suppose que les deux polynômes P et Q n'ont aucune racine commune dans $\mathbb{C}$.
  - On pose $D = P \wedge Q$.
  - Donc $\exists P_1, Q_1 \in \mathbb{K}[X]$ tels que $P = DP_1$ et $Q = DQ_1$.
  - Nous allons raisonner par absurde en supposant que $\deg(D) \geq 1$.
  - Comme $\deg(D) \geq 1$, alors D admet au moins une racine $z \in \mathbb{C}$.
  - Donc $P(z) = D(z)P_1(z) = 0$ et $Q(z) = D(z)Q_1(z) = 0$, ce qui est absurde, car P et Q n'ont aucune racine commune dans $\mathbb{C}$.
  - On en déduit que $\deg(D) = 0$, et comme D est unitaire, alors $D = 1$, et par conséquent $P \wedge Q = 1$.

■

3 Complément : Interpolation de Lagrange

L'objectif de ce complément est de pouvoir construire une fonction polynomiale qui prend des valeurs données en des points donnés. Par exemple, étant donné n points $x_1, \dots, x_n$ deux à deux distincts dans $\mathbb{K}$, et n éléments $y_1, \dots, y_n$ de $\mathbb{K}$, on souhaite construire un polynôme $P \in \mathbb{K}[X]$ tel que $P(x_i) = y_i$ pour tout $i \in [\![1, n]\!]$, et donc déterminer $P(x), \forall x \neq x_k$ tel que $k \in [\![1, n]\!]$. Cela nous permettra de prédire la valeur d'une fonction polynomiale à partir de quelques points, ce qui est très utile en analyse numérique, en cryptographie, en théorie de l'information, etc.

Définition 3.3.0.14 *(Polynômes élémentaires de Lagrange)*

Soient $n \in \mathbb{N}, x_0, \dots, x_n$ des éléments de $\mathbb{R}$ distincts deux à deux.
On pose $\forall k \in [\![0, n]\!], l_k = \prod_{\substack{0 \leq j \leq n \\ j \neq k}} \frac{X - x_j}{x_k - x_j}$.

Ce polynôme l_k est appelé le **polynôme élémentaire de Lagrange** associé à $(x_k)_{0 \leq k \leq n}$. Il est de degré $\leq n$ (donc $\in \mathbb{R}_n[X]$).

Remarque 3.3.0.16

Soit $k \in [\![0, n]\!]$.

$$\forall 0 \leq i \leq n, l_k(x_i) = \delta_{i,k} \begin{cases} 1 & \text{si } i = k \\ 0 & \text{si } i \neq k \end{cases}$$

Théorème 3.3.0.11

Soient f une fonction continue sur le segment $[a, b]$ et $a \leq x_0 < x_1 < \cdots < x_n \leq b$ des éléments de $[a, b]$.
On souhaite "approximer" en quelque sorte la fonction f par un polynôme $P \in \mathbb{R}_n[X]$ tel que $P(x_i) = f(x_i)$ pour tout $i \in [\![0, n]\!]$.
Alors $P \in \mathbb{R}_n[X]$ est unique et est donné par la formule suivante :

$$P = \sum_{k=0}^{n} f(x_k) l_k$$

où $(l_k)_{0 \leq k \leq n}$ sont les polynômes élémentaires de Lagrange associés à $(x_k)_{0 \leq k \leq n}$.

P est appelé le **polynôme d'interpolation de Lagrange** (ou l'interpolé) de f aux points $x_0, \dots, x_n$.

Preuve

- Démontrons que P est un polynôme.
  - On sait que $\forall k \in [\![0, n]\!], l_k \in \mathbb{R}_n[X]$, donc $P = \sum_{k=0}^{n} f(x_k) l_k \in \mathbb{R}_n[X]$.
  - Et on a bien $P(x_i) = \sum_{k=0}^{n} f(x_k) l_k(x_i) = f(x_i)$ pour tout $i \in [\![0, n]\!]$.
  - On a donc construit un polynôme P tel que $P(x_i) = f(x_i)$ pour tout $i \in [\![0, n]\!]$.
- Démontrons que P est unique.
  - Supposons qu'il existe un autre polynôme $Q \in \mathbb{R}_n[X]$ tel que $Q(x_i) = f(x_i)$ pour tout $i \in [\![0, n]\!]$.
  - Alors $P(x_i) = Q(x_i)$ pour tout $i \in [\![0, n]\!]$.
  - Donc $(P - Q)(x_i) = 0$ pour tout $i \in [\![0, n]\!]$.
  - Par conséquent, le polynôme $P - Q$ admet au moins $n+1$ racines distinctes, ce qui est absurde, car $\deg(P - Q) \leq n$.
  - On en déduit que $P - Q$ est le polynôme nul, c'est à dire que $P = Q$, et par conséquent P est unique.

■

Théorème 3.3.0.12 *(Erreur d'interpolation de Lagrange)*

Soient f une fonction de classe $\mathcal{C}^{n+1}$ à image dans $\mathbb{K}$ sur le segment $[a, b]$ et $a \leq x_0 < x_1 < \cdots < x_n \leq b$ des éléments de $[a, b]$.
L'erreur d'interpolation de Lagrange est donnée par la formule suivante :

$$\forall x \in [a, b], \exists \varepsilon_x \in [a, b], e(x) = f(x) - P(x) = \frac{f^{(n+1)}(\varepsilon_x)}{(n+1)!} \prod_{k=0}^{n} (x - x_k)$$

Preuve

- Soit $x \in [a, b]$.
- Si $x = x_k$ tel que $0 \leq k \leq n$, alors $e(x_k) = f(x_k) - P(x_k) = 0$, et la formule est vérifiée.
  - De même, $\prod_{i=0}^{n} (x_k - x_i) = 0$ pour tout $k \in [\![0, n]\!]$, donc la formule est vérifiée.
- Dans le cas où $x \neq x_k$ pour tout $k \in [\![0, n]\!]$, on pose la fonction $g : [a, b] \to \mathbb{K}$ définie par $g : t \mapsto f(t) - P(t) - e(x) \prod_{k=0}^{n} (t - x_k)$.

- ▷ Cette fonction est de classe $\mathcal{C}^{n+1}$ (car toutes les fonctions qui la composent sont aussi de classe $\mathcal{C}^{n+1}$).
- ▷ $\forall k \in [\![0, n]\!], g(x_k) = f(x_k) - P(x_k) - e(x)\prod_{i=0}^{n}(x_k - x_i) = 0$. La fonction admet donc au moins $n+1$ racines distinctes.
- ▷ Comme x a été fixé au début de la preuve, on a $g(x) = f(x) - P(x) - e(x)\prod_{k=0}^{n}(x - x_k) = 0$, donc g admet au moins $n+2$ racines distinctes.
- ▷ On peut donc procéder en utilisant le théorème de Rolle (plus précisément, Rolle itéré) pour montrer que $g^{(n+1)}$ admet au moins une racine dans $[a, b]$, sachant que Rolle itéré nécessite $n+2$ racines distinctes pour garantir l'existence d'une racine de $g^{(n+1)}$, car g est de classe $\mathcal{C}^{n+1}$.
- ▷ Donc $\exists \varepsilon_x \in [a, b]$ tel que $g^{(n+1)}(\varepsilon_x) = 0$.
- ▷ Or $g^{(n+1)}(t) = f^{(n+1)}(t) - P^{(n+1)}(t) - e(x)\prod_{k=0}^{n}(t - x_k)$. Comme P est de degré $\leq n$, alors $P^{(n+1)}$ est le polynôme nul, et par conséquent $g^{(n+1)}(t) = f^{(n+1)}(t) - e(x)\prod_{k=0}^{n}(t - x_k)$.
- ▷ On en déduit que $0 = g^{(n+1)}(\varepsilon_x) = f^{(n+1)}(\varepsilon_x) - e(x)\prod_{k=0}^{n}(\varepsilon_x - x_k)$, et par conséquent $e(x) = \frac{f^{(n+1)}(\varepsilon_x)}{(n+1)!}\prod_{k=0}^{n}(x - x_k)$.

■

Fin du Chapitre XII.