Chapitre 18

Polynôme

Hugo Salou MP2I

Dernière mise à jour le 14 juin 2022

TABLE DES MATIÈRES

Dans ce chapitre, $\mathbb{K}$ désigne un corps

Première partie

Définition

Définition:

— Un polynôme à coefficients dans $\mathbb{K}$ est une suite presque nulle de $\mathbb{K}^{\mathbb{N}}$

— Le polynôme nul, noté 0 est la suite nulle.

— Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul.
$\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$ est non-vide et majoré. Le degré de P est $\max\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$, et on le note $\deg(P)$ et $a_{\deg(P)}$ est le coefficient dominant de P, il est noté $\mathrm{dom}(P)$.

— Le degré du polynôme nul est $-\infty$

Proposition – Définition: Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. Alors, $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$ est un polynôme appelé somme de P et Q.

Preuve:

$$\exists N_1 \in \mathbb{N}, \forall n \geqslant N_1, a_n = 0$$
$$\exists N_2 \in \mathbb{N}, \forall n \geqslant N_2, b_n = 0$$

On pose $N = \max(N_1, N_2)$ donc

$$\forall n \geqslant N, a_n + b_n = 0 + 0 = 0$$

donc $P + Q$ est une suite presque nulle. □

Proposition – Définition: Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. On pose

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

La suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle. Ce polynôme est appelé produit de P et Q et noté PQ.

Preuve:

$$\exists N_1 \in \mathbb{N}, \forall n \geqslant N_1, a_n = 0$$
$$\exists N_2 \in \mathbb{N}, \forall n \geqslant N_2, b_n = 0$$

On pose $N = N_1 + N_2$

$$\forall n \geqslant N, c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{N_1} a_k b_{n-k} + \sum_{k=N_1+1}^{n} a_k b_{n-k}$$

$\forall k \geqslant N_1 + 1,\ a_k = 0$ donc $\displaystyle\sum_{k=N_1+1}^{n} a_k b_{n-k} = 0$

$\forall k \leqslant N_1,\ b - k \geqslant n - N_1 \geqslant N_1 + N_2 - N_1 \geqslant N_2$ donc $\forall k \leqslant N_1, b_{n-k} = 0$ et donc $\displaystyle\sum_{k=0}^{N_1} a_k b_{n-k} = 0$

Donc

$$\forall n \geqslant N, c_n = 0$$

□

Remarque (Notation):
Soit $P = (a_n)_{n\in\mathbb{N}}$, un polynôme à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. Le polynôme $(\lambda a_n)_{n\in\mathbb{N}}$ est noté λP

Remarque (Notation):
On pose $X = (0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \ldots) = (\delta_{1,n})_{n\in\mathbb{N}}$

Exemple:

$$\begin{aligned} X^2 &= XX \\ &= (0 \times 0, 0 \times 1 + 1 \times 0, 0 \times 0 + 1 \times 1 + 0 \times 0, 0, \ldots) \\ &= (0, 0, 1, 0, \ldots) \end{aligned}$$

Théorème: Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul à coefficients dans $\mathbb{K}$. Alors

$$P = \sum_{k=0}^{n} a_k X^k \qquad \text{où } n = \deg(P) \text{ et } X^0 = (1, 0, \ldots)$$

Preuve:

Pour $k \in \mathbb{N}$, $\mathscr{P}(n)$: "$X^k = (\delta_{k,n})_{\in\mathbb{N}}$" où $\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{si } n \neq k \end{cases}$

- $\delta_{0,n} = (1, 0, \ldots) = X^0$ donc $\mathscr{P}(0)$ est vrai
- Soit $k \in \mathbb{N}$. On suppose $\mathscr{P}(k)$ vraie.

  $$X^{k+1} = X^k X = (c_n)_{n\in\mathbb{N}}$$

  où

  $$\forall n \in \mathbb{N}, c_n = \sum_{j=0}^{n} \delta_{k,j}\delta_{1,n-j}$$

  Donc, pour tout $n \in \mathbb{N}$ et pour tout $j \in [\![0, n]\!]$

  $$\delta_{k,j}\delta_{1,n-j} \neq 0 \iff \begin{cases} k = j \\ 1 = n - j \end{cases} \iff \begin{cases} k = j \\ n = k + 1 \end{cases}$$

  Donc, si $n \neq k + 1$, alors

  $$\forall j \in [\![0, n]\!], \delta_{k,j}\delta_{1,n-j} = 0$$

et donc $c_n = 0$

$$c_{k+1} = \sum_{j=0}^{k+1} \delta_{k,j}\delta_{1,j+1-j} = \delta_{k,k}\delta_{1,1} = 1$$

Donc

$$\forall n \in \mathbb{N}, c_n = \delta_{k+1,n}$$

donc $\mathscr{P}(k+1)$ est vraie
Ainsi, $\mathscr{P}(k)$ est vraie pour tout $k \in \mathbb{N}$. Soit $P = (a_0, \ldots, a_n, 0, \ldots)$ un polynôme de degré n.

$$\begin{aligned}\sum_{k=0}^{n} a_k X^k &= a_0(1,0,0,0,\ldots)\\ &+ a_1(0,1,0,0,\ldots)\\ &+ a_2(0,0,1,0,\ldots)\\ &\vdots\\ &+ a_n(0,\ldots,0,1,0,\ldots)\\ &= (a_0, a_1, \ldots, a_n, 0, \ldots)\\ &= P\end{aligned}$$

□

Remarque (Notation):
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ dont l'indéterminée $(0,1,0,\ldots)$ est notée X.

Proposition: $\big(\mathbb{K}[X], +, \times, \cdot\big)$ est une <u>$\mathbb{K}$-algèbre commutative</u> i.e.

1. $\big(\mathbb{K}[X], +, \times\big)$ est un anneau commutatif
2. $\big(\mathbb{K}[X], +, \cdot\big)$ est un $\mathbb{K}$-espace vectoriel
3. $\forall \lambda \in \mathbb{K}, \forall (P,Q) \in \big(\mathbb{K}[X]\big)^2, \lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$

Preuve: 1. $(\mathbb{K}[X], +)$ est un groupe abélien car $(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel

— $X^0 = (1, 0, \ldots)$ est le neutre de $\times$
En effet, $\forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, en posant $(c_n)_{n\in\mathbb{N}} = PX^0$ on a

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k \delta_{k,n-k} = a,$$

donc $PX^0 = P$
— $\times$ est commutative : $\forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X], \forall Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, on pose

$R = (c_n)_{n\in\mathbb{N}} = PQ$, $S = (d_n)_{n\in\mathbb{N}} = QP$ alors

$$\begin{aligned}\forall n \in \mathbb{N}, c_n &= \sum_{k=0}^{n} a_k b_{n-k} \\ &= \sum_{j=0}^{n} a_{n-j} b_j \qquad (j = n-k) \\ &= \sum_{j=0}^{n} b_j a_{n-j} \\ &= d_n\end{aligned}$$

donc $PQ = QP$

— Soient

$$\begin{cases} P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \\ Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \\ R = (c_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \end{cases}$$

On pose

$$\begin{cases} S = (d_n)_{n\in\mathbb{N}} = PQ \\ T = (e_n)_{n\in\mathbb{N}} = SR = (PQ)R \\ U = (f_n)_{n\in\mathbb{N}} = QR \\ V = (g_n)_{n\in\mathbb{N}} = PU = P(QR) \end{cases}$$

Donc,

$$\begin{aligned}\forall n \in \mathbb{N}, e_n &= \sum_{k=0}^{n} d_k c_{n-k} \\ &= \sum_{k=0}^{n} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) c_{n-k} \\ &= \sum_{j=0}^{n} \sum_{k=j}^{n} a_j b_{k-j} c_{n-k} \\ &= \sum_{j=0}^{n} a_j \sum_{k=j}^{n} b_{k-j} c_{n-k} \\ &= \sum_{j=0}^{n} a_j \sum_{\ell=0}^{n-j} b_\ell c_{n-j-\ell} \qquad (\ell = k-j) \\ &= \sum_{j=0}^{n} a_j f_{n-j} \\ &= g_n\end{aligned}$$

Donc $T = V$

— Soient $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}, R = (C_n)_{n\in\mathbb{N}}$ trois polynômes et $P(Q +$

$R) = (d_n)_{n\in\mathbb{N}}$ et $PQ + PR = (e_n)_{n\in\mathbb{N}}$.

$$\begin{aligned}\forall n \in \mathbb{N}, d_n &= \sum_{k=0}^{n} a_k(b_{n-k} + c_{n-k}) \\ &= \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k c_{n-k} \\ &= e_n\end{aligned}$$

Donc, $\big(\mathbb{K}[X], +, \times\big)$ est un anneau commutatif

2. $\mathbb{K}[X] \subset \mathbb{K}^{\mathbb{N}}$
$\left(\mathbb{K}^{\mathbb{N}}, +, \cdot\right)$ est un $\mathbb{K}$-espace vectoriel. D'après la propriété précédente,

$$\mathbb{K}[X] = \mathrm{Vect}\big((X^n \mid n \in \mathbb{N})\big)$$

donc $\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$

3. Soit $\lambda \in \mathbb{K}, P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes. On pose $(c_n)_{n\in\mathbb{N}} = PQ, R = (d_n)_{n\in\mathbb{N}} = \lambda(PQ), S = (e_n)_{n\in\mathbb{N}} = (\lambda P)Q, T = (f_n)_{n\in\mathbb{N}} = P(\lambda Q)$.

$$\begin{aligned}\forall n \in \mathbb{N}, d_n = \lambda c_n &= \lambda \sum_{k=0}^{n} a_k b_{n-k} \\ &= \sum_{k=0}^{n} (\lambda a_k) b_{n-k} = e_n \\ &= \sum_{k=0}^{n} a_k(\lambda b_{n-k}) = f_n\end{aligned}$$

□

Remarque:
$(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre non commutative (si $n > 1$)

Proposition: $i : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K}[X] \\ \lambda & \longmapsto & \lambda X^0 \end{array}$ est un morphisme d'algèbre injectif, i.e.

$$\forall \lambda, \mu \in \mathbb{K}, \begin{cases} i(\lambda + \mu) = i(\lambda) + i(\mu) \\ i(\lambda \cdot \mu) = i(\lambda) \times i(\mu) \end{cases}$$

et i est injective.

Remarque (Notation):
On identifie $\lambda \in \mathbb{K}$ avec $\lambda X^0 \in \mathbb{K}[X]$. Ainsi, on peut écrire $X^0 = 1$, on peut écrire $2+X+3X^2$ au lieu de $2X^0 + X + 3X^2$

Proposition: Soient $P, Q \in \mathbb{K}[X]$

- $\deg(P + Q) \leqslant \max\big(\deg(P), deg(Q)\big)$
- Si $\deg(P) \neq \deg(Q)$, alors
  - $\deg(P + Q) = \max\big(\deg(P), \deg(Q)\big)$

— $\operatorname{dom}(P+Q) = \begin{cases} \operatorname{dom}(P) & \text{si } \deg(P) > \deg(Q) \\ \operatorname{dom}(Q) & \text{si } \deg(P) < \deg(Q) \end{cases}$

— Si $\deg(P) = \deg(Q)$ et $\operatorname{dom}(P) + \operatorname{dom}(Q) \neq 0$,
alors $\begin{cases} \deg(P+Q) = \deg(P) = \deg(Q) \\ \operatorname{dom}(P+Q) = \operatorname{dom}(P) + \operatorname{dom}(Q) \end{cases}$

— Si $\deg(P) = \deg(Q)$ et $\deg(P) + \deg(Q) = 0$, alors $\deg(P+Q) < \deg(P)$

Preuve: — Si $P = 0$, alors $\deg(P+Q) = \deg(Q)$ et donc $\max\big(\deg(P), \deg(Q)\big) = \max\big(-\infty, \deg(Q)\big)$
On a bien $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$

— De même avec $Q = 0$

— On suppose $P \neq 0$ et $Q \neq 0$

On pose $\begin{cases} P = \displaystyle\sum_{k=0}^{p} a_k X^k & p = \deg(P) \\ Q = \displaystyle\sum_{k=0}^{q} b_k X^k & q = \deg(Q) \end{cases}$

On peut supposer $p \geqslant q$. On pose $b_{q+1} = \ldots = b_p = 0$ si $p > q$

Ainsi, $Q = \displaystyle\sum_{k=0}^{p} b_k X^k$

$P + Q = \displaystyle\sum_{k=0}^{p} (a_k + b_k) X^k$ donc $\deg(P+Q) \leqslant p$ et $p = \max\big(\deg(P), \deg(Q)\big)$

De plus, $a_p + b_p = \begin{cases} \underset{\neq 0}{\operatorname{dom}(P)} & \text{si } p > q \\ \operatorname{dom}(P) + \operatorname{dom}(Q) & \text{si } p = q \end{cases}$

□

Proposition: Soient $P, Q \in \mathbb{K}[X]$. Alors

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

Preuve:
Si P ou Q est nul, alors la formule est vraie car

$$\begin{cases} \deg(PQ) = -\infty \\ \deg(P) + \deg(Q) = \begin{cases} \text{cste} - \infty = -\infty \\ -\infty + \text{cste} = -\infty \\ -\infty - \infty = -\infty \end{cases} \end{cases}$$

On suppose $P \neq 0$ et $Q \neq 0$. On pose $P = \displaystyle\sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ et $Q = \displaystyle\sum_{k=0}^{q} b_k X^k$ avec $b_q \neq 0$

$$\begin{aligned} PQ &= \left(\sum_{k=0}^{p} a_k X^k\right)\left(\sum_{\ell=0}^{q} b_\ell X^\ell\right) \\ &= \sum_{k=0}^{p} \sum_{\ell=0}^{q} a_k b_\ell X^{k+\ell} \end{aligned}$$

donc $\deg(PQ) \leqslant p+q$ et le coefficient devant X^{p+q} est $a_p b_q \neq 0$ (car $\mathbb{K}$ est intègre)
donc $\deg(PQ) = p+q$ $\square$

Deuxième partie

Évaluation

Définition: Soit A une $\mathbb{K}$-algèbre et $P \in \mathbb{K}[X]$. On pose $P = \sum_{k=0}^{n} e_k X^k$. Soit $a \in A$.

On pose

$$\begin{aligned} P(a) &= \sum_{k=0}^{n} e_k a^k \\ &= e_0 1_A + e_1 a + e_2 a^2 + \cdots + e_n a^n \in A \end{aligned}$$

On dit qu'on a <u>évalué</u> P en a, ou <u>spécialisé</u> X avec la valeur de a, ou <u>remplacé</u> X par a, <u>substitué</u> a à X.

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est une <u>racine de P</u> si $P(a) = 0_{\mathbb{K}}$.

Définition: Soit $P \in \mathbb{K}[X] \in \mathscr{M}_n(\mathbb{K})$. On dit que c'est un <u>polynôme de matrices</u>.

Exemple:
$P = 1 + 2X - 3X^2$, $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$$\begin{aligned} P(A) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - 3\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} - 3\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ -4 & 0 \end{pmatrix} \end{aligned}$$

Définition: Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$.

Alors $P(Q) = \sum_{k=0}^{n} a_k Q^k \quad \in \mathbb{K}[X]$
C'est la <u>composée</u> de P et Q.

Remarque (⚠ Attention):
Ne pas confondre $\underbrace{P(X+1)}_{\text{composée}}$ et $\underbrace{P(X+1)}_{\text{produit}}$.
On a $\underbrace{P(X+1)}_{\text{produit}} = (X+1)\,P = P(X)\,(X+1) = P \times (X+1)$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ avec $\begin{cases} Q \neq 0 \\ P \neq 0 \end{cases}$. On a

$$\deg\big(P(Q)\big) = \deg(P) \times \deg(Q)$$

$\square$

EXEMPLE:
$\mathbb{K} = {}^{\mathbb{Z}}/_{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$

$P = X^2 + X + 1 \in \mathbb{K}[X]$ et $Q = 1 \in \mathbb{K}[X]$
$P \neq Q$

$$\begin{aligned} f_P : {}^{\mathbb{Z}}/_{2\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ x &\longmapsto P(x) \end{aligned}$$

$$\begin{aligned} f_Q : {}^{\mathbb{Z}}/_{2\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}/_{2\mathbb{Z}} \\ x &\longmapsto Q(x) \end{aligned}$$

$f_P\left(\overline{0}\right) = \overline{1} = f_Q\left(\overline{0}\right)$
$f_P\left(\overline{1}\right) = \overline{1} + \overline{1} + \overline{1} = \overline{1} = f_Q\left(\overline{1}\right)$
donc $f_P = f_Q$ alors que $P \neq Q$

Théorème: Soit A une $\mathbb{K}$-algèbre. L'application

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow A^A \\ P &\longmapsto f_P : \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & P(a) \end{array} \end{aligned}$$

vérifie

1. $\forall P, Q \in \mathbb{K}[X], \varphi(P+Q) = \varphi(P) + \varphi(Q)$
2. $\forall P, Q \in \mathbb{K}[X], \varphi(PQ) = \varphi(P) \times \varphi(Q)$
3. $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X], \varphi(\lambda P) = \lambda \varphi(P)$

$\square$

EXEMPLE:
$\mathbb{K} = \mathbb{R}$
$X^2 - 1 = (X-1)(X+1)$

— $\mathbb{C}$ est une $\mathbb{R}$-algèbre donc

$$\forall z \in \mathbb{C}, z^2 - 1 = (z-1)(z+1)$$

— $\mathscr{M}_2(\mathbb{R})$ est une $\mathbb{R}$-algèbre

$$\forall A \in \mathscr{M}_2(\mathbb{R}), A^2 - I_2 = (A - I_2)(A + I_2)$$

Définition: Soit $P \in \mathbb{K}[X]$,

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

Le polynôme dérivé de P est

$$P' = \sum_{k=0}^{n} k a_k X^{k-1} = \sum_{k=1}^{n} k a_k X^{k-1}$$

où

$$\forall k \in [\![1, n]\!], k a_k = \underbrace{a_k + \cdots + a_k}_{k \text{ fois}}$$

$$0_{\mathbb{N}} a_k = 0_{\mathbb{K}}$$

Remarque:

Si $P \in \mathbb{R}[X]$, $f_p : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P(x) \end{array}$

$f_{P'} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P'(x) \end{array}$ alors $f_{P'} = f'_P$

Proposition:

$$\forall P \in \mathbb{K}[X], \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) > 0 \\ -\infty & \text{sinon} \end{cases}$$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

1. $(P+Q)' = P' + Q'$
2. $(PQ)' = P'Q + PQ'$
3. $(\lambda P)' = \lambda P'$

Preuve:
On pose

$$P = \sum_{k=0}^{p} a_k X^k \qquad Q = \sum_{k=0}^{q} b_k X^k$$

1. On peut supposer $p \geqslant q$
   Si $p > q$, on pose $b_{q+1} = \cdots = b_p = 0$

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

   donc

$$\begin{aligned} (P+Q)' &= \sum_{k=0}^{p} k(a_k + b_k) X^{k-1} \\ &= \sum_{k=0}^{p} k a_k X^{k-1} + \sum_{k=0}^{p} k b_k X^{k-1} \\ &= P' + Q' \end{aligned}$$

2.

$$PQ = \sum_{k=0}^{p} \sum_{\ell=0}^{q} a_k b_\ell X^{k+\ell}$$

D'après 1.,

$$\begin{aligned}(PQ)' &= \sum_{k=0}^{p}\sum_{\ell=0}^{q}\left(a_k b_\ell X^{k+\ell}\right)' \\ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} a_k b_\ell (k+\ell) X^{k+\ell-1} \\ &= \sum_{k=0}^{p}\sum_{\ell=0}^{q} k a_k b_\ell X^{k-1+\ell} + \sum_{k=0}^{p}\sum_{\ell=0}^{q} \ell a_k b_\ell X^{k+\ell-1} \\ &= \sum_{k=0}^{p} k_k X^{l-1}\sum_{\ell=0}^{q} b_\ell X^\ell + \sum_{k=0}^{p} a_k X^k \sum_{\ell=0}^{q} \ell b_\ell X^{\ell-1} \\ &= P'Q + PQ'\end{aligned}$$

3.

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

donc

$$(\lambda P)' = \sum_{k=0}^{p} \lambda a_k k X^{k-1} = \lambda \sum_{k=0}^{p} k a_k X^{k-1} = \lambda P'$$

□

Définition: Pour $k \in \mathbb{N}$, on définit la dérivée k-ième d'un polynôme $P \in \mathbb{K}[X]$ par
- si $k = 0$, $P^{(k)} = P$
- si $k = 1$, $P^{(1)} = P'$
- si $k > 1$, $P^{(k)} = \left(P^{(k-1)}\right)'$

Proposition:

$$\forall k, j \in \mathbb{N}^2, \left(X^k\right)^{(j)} = \begin{cases} 0 & \text{si } j > k \\ k(k-1)\cdots(k-j+1)X^{k-j} = \dfrac{k!}{(k-j)!}X^k & \text{si } j \leqslant k \end{cases}$$

Preuve (par récurrence sur j à k fixé)*:*

□

Proposition: Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$
1. $\forall k \in \mathbb{N}, (P+Q)^{(k)} = P^{(k)} + Q^{(k)}$
2. $\forall k \in \mathbb{N}, (PQ)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} P^{(i)} Q^{(k-i)}$
3. $\forall k \in \mathbb{N}, (\lambda P)^{(k)} = \lambda P^{(k)}$

Preuve (par récurrence sur k)*:*

$\square$

Troisième partie

Arithmétique dans $\mathbb{K}[X]$

Définition: Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B (dans $\mathbb{K}[X]$) s'il existe $C \in \mathbb{K}[X]$ tel que
$$AC = B$$
On dit dans ce cas que A est un diviseur de B ou que B est un multiple de A. On le note alors $A \mid B$
On dit que A et B sont associés s'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$. Il s'agit d'une relation d'équivalence.

Proposition: Soient $A, B \in \mathbb{K}[X]$.
$$\left.\begin{matrix} A \mid B \\ B \mid A \end{matrix}\right\} \iff A \text{ et } B \text{ sont associés}$$

Preuve: " $\implies$ " Soit $C \in \mathbb{K}[X]$ tel que $AC = B$ et $D \in \mathbb{K}[X]$ tel que $BD = A$. D'où,
$$A = BD = ACD$$
Or, $\mathbb{K}[X]$ est un anneau intègre.
D'où
$$A(1 - CD) = 0$$
donc $A = 0$ ou $CD = 1$
Si $A = 0$, alors $B = 0 \times C = 0 = 1 \times A$ donc A et B sont associés
Si $CD = 1$, on sait que $\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$
Alors, A et B sont associés.
" $\impliedby$ " évident

$\square$

Lemme: $\mathbb{K}[X]$ est un anneau intègre.

Preuve:
Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. On suppose que $P \neq 0$ et $Q \neq 0$
Alors $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$
Or, $PQ = 0$ et $\deg(0) = -\infty$: $\lightning$ une contradiction $\square$

Lemme:
$$\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$$

Preuve:
Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 1$.
Alors, $0 = \deg(1) = \deg(PQ) = \deg(P) + \deg(Q)$
Comme $P \neq 0$, $\deg(P) \geqslant 0$. De même, $\deg(Q) \geqslant 0$
Done $\deg(P) = \deg(Q) = 0$ Donc, il existe $\lambda, \mu \in \mathbb{K}$ tels que $\lambda\mu = 1$
Donc $\lambda \in \mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ $\square$

Proposition: $|$ est une relation réflexive et transitive. □

Proposition: Soient $A, B, C \in \mathbb{K}[X]$ tels que $A \mid B$ et $A \mid C$. Alors

$$\forall (P, Q) \in \mathbb{K}[X]^2, A \mid BQ + CP$$

□

Proposition – Définition: Soit $A \in \mathbb{K}[X], B \in \mathbb{K}[X] \setminus \{0\}$.

$$\exists!(P, Q) \in \mathbb{K}[X]^2, \begin{cases} A = PQ + R \\ \deg(R) < \deg(B) \end{cases}$$

On dit que Q est le quotient et R le reste de la division (euclidienne) de A par B.

Preuve: — On prouve l'existence par récurrence sur le degré de A. On fixe $B \in \mathbb{K}[X] \setminus \{0\}$

$$\forall n \in \mathbb{N}, \mathscr{P}(n) : \text{“} \forall A \in \mathbb{K}[X] \text{ tel que } \deg(A) = n,$$
$$\exists (Q, R) \in \mathbb{K}[X]^2, \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases} \text{”}$$

— Soit $A \in \mathbb{K}[X]$. On suppose $\deg(A) = 0$

Si $\deg(B) > 0$ alors on pose $Q = 0$ et $R = A$. Ainsi $\begin{cases} BQ + R = A \\ \deg(R) = 0 < \deg(B) \end{cases}$

Si $\deg(B) = 0$, alors $A = \lambda$ et $B = \mu$ avec $(\lambda, \mu) \in (\mathbb{K} \setminus \{0\})^2$.

On pose $\begin{cases} Q = \mu^{-1}\lambda \\ R = 0 \end{cases}$. Alors, $\begin{cases} BQ + R = \mu\mu^{-1}\lambda = \lambda = A \\ \deg(R) = -\infty < 0 = \deg(B) \end{cases}$

Donc $\mathscr{P}(0)$ est vraie.

— Soit $n \in \mathbb{N}$. On suppose $\mathscr{P}(k)$ pour tout $k \leqslant n$. Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) = n + 1$. On pose $p = \deg(B)$

Si $p > n + 1$, on pose $\begin{cases} Q = 0 \\ R = A \end{cases}$ et on a

$$\begin{cases} BQ + R = A \\ \deg(R) = n + 1 < p = \deg(B) \end{cases}$$

Si $p \leqslant n + 1$. On pose $\begin{cases} Q = a_{n+1} b_b^{-1} X^{n+1-p} \\ R = A - BQ \end{cases}$ où $\begin{cases} a_{n+1} = \mathrm{dom}(A) \\ a_p = \mathrm{dom}(b) \end{cases}$ On a $A = BQ + R$

Or, $\begin{cases} \deg(BQ) = p + n + 1 - p = n + 1 = \deg(A) \\ \mathrm{dom}(BQ) = b_p b_p^{-1} a_{n+1} = a_{n+1} = \mathrm{dom}(A) \end{cases}$

donc $\deg(R) < \deg(A)$ donc $\deg(R) \leqslant n$

D'après $\mathscr{P}(n)$,

$$\exists (Q_1, R_1) \in \mathbb{K}[X]^2, \begin{cases} R = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases}$$

D'où,

$$\begin{aligned} A &= BQ + R \\ &= BQ + BQ_1 + R_1 \\ &= B(Q + Q_1) + R_1 \end{aligned}$$

et $\deg(R_1) < \deg(B)$ donc $\mathscr{P}(n+1)$ est vraie.
Donc, $\mathscr{P}(n)$ est vraire pour tout $n \in \mathbb{N}$ par récurrence forte. Si $A = 0$, on pose $Q = R = 0$ et on a bien $BQ + R = 0 = A$ et $\deg(R) = -\infty < \deg(B)$

— Unicité
Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On suppse que $A = BQ_1 + R_1 = BQ_2 + R_2$ avec $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ et $\begin{cases} \deg(R_1) < \deg(B) \\ \deg(R_2) < \deg(B) \end{cases}$
D'où,
$$B(Q_1 - Q_2) = R_2 - R_1$$
Or,
$$\deg(R_2 - R_1) \leqslant \max\big(\deg(R_2), \deg(R_1)\big) < \deg(B)$$
Or,
$$\begin{aligned} \deg\big(B(Q_1 - Q_2)\big) &= \deg(B) + \deg(Q_1 - Q_2) \\ &\geqslant \deg(B) \text{ si } Q_1 - Q_2 \neq 0 \end{aligned}$$
Donc,
$$\begin{cases} Q_1 - Q_2 = 0 \\ R_2 - R_1 = B(Q_2 - Q_1) = 0 \end{cases}$$
et donc
$$\begin{cases} Q_1 = Q_2 \\ R_2 = R_1 \end{cases}$$

$\square$

Exemple:
Division euclidienne de $A = X^5 + X^3 - X^2 + 1$ par $B = X^2 + \frac{1}{2}X - 1$ dans $\mathbb{R}[X]$

$$\begin{array}{rr|l}
 & X^5+X^3-X^2+1 & X^2+\frac{1}{2}X-1 \\ \cline{3-3}
- & X^5+\frac{1}{2}X^4-X^3 & \boxed{X^3-\frac{1}{2}X^2+\frac{9}{4}X-\frac{21}{8}} \\ \cline{1-2}
 & -\frac{1}{2}X^4+2X^3-X^2+1 & \qquad \text{quotient} \\
- & -\frac{1}{2}X^4-\frac{1}{4}X^3+\frac{1}{2}X^2 & \\ \cline{1-2}
 & \frac{9}{4}X^3-\frac{3}{2}X^2+1 & \\
- & \frac{9}{4}X^3+\frac{9}{8}X^2-\frac{9}{4}X & \\ \cline{1-2}
 & -\frac{21}{8}X^2+\frac{9}{4}X+1 & \\
- & -\frac{21}{8}X^2-\frac{21}{16}X+\frac{21}{8} & \text{reste} \\ \cline{1-2}
 & \boxed{\frac{57}{16}X-\frac{13}{8}} &
\end{array}$$

Théorème: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$P(a) = 0 \iff X - a \mid P$$

Preuve: “ $\Longleftarrow$ ” On suppose $P = (X - A) \times Q$ avec $Q \in \mathbb{K}[/]$. On substitue a à X

$$P(a) = (a - a) \times Q(a) = 0_{\mathbb{K}} \times Q(a) = 0_{\mathbb{K}}$$

“ $\Longrightarrow$ ” On suppose que $P(a) = 0$. On réalise la division euclidienne de P par $X - a$:

$$\begin{cases} P = (X-a) \times Q + R \\ \deg(R) < \deg(X-a) = 1 \end{cases}$$

donc $R = \lambda$ avec $\lambda \in \mathbb{K}$
D'où,

$$0 = P(a) = (a - a) \times Q(a) + R(a) = \lambda$$

donc

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

et donc

$$X - a \mid P$$

$\square$

Corollaire: Soit $P \in \mathbb{K}[X]$ non nul de degré n. Alors, P a au plus n racines distinctes dans $\mathbb{K}$

Preuve (par récurrence sur n): — C'est évident pour $n = 0$

— Soit $n \in \mathbb{N}$. On suppose la proposition vraie pour les polynômes de degré n.
Soit $P \in \mathbb{K}[X]$ de degré $n+1$
Si P n'a pas de racine alors le résultat est trivialement vrai pour P
Si P a une racine a, alors il existe $Q \in \mathbb{K}[X]$ non nul tel que $P = (X-a) \times Q$
$n+1 = \deg(P) = 1 + \deg(Q)$ donc $\deg(Q) = n$
D'après l'hypothèse de récurrence, Q a au plus n racines distinctes
Soit b une racine de P différente de a. Alors,

$$0 = P(b) = \underbrace{(b-a)}_{\neq 0} \times Q(b)$$

donc $Q(b) = 0$

Donc P a bien au plus $n+1$ racines. □

Définition: Soient A et B deux polynômes dont l'un au moins est non nul, $D \in \mathbb{K}[X]$. On dit que D est un PGCD de A et B si D est un diviseur commun de A et B et de degré maximal.

Proposition: Avec les hypothèse précédents, deux PGCD quelconques de A et B sont nécessairement associés

Preuve:
On forme

$$E = \left\{ AU + BV \mid (U,V) \in \mathbb{K}[X]^2 \right\}$$

— E est un sous-groupe de $(\mathbb{K}[X], +)$
— $\forall P \in E, \forall Q \in \mathbb{K}[X], PQ \in E$

On dit que E est un *idéal* de $\mathbb{K}[X]$

Soit $D \in E$ un polynôme non nul de degré minimal. Soit $P \in E$ On divise P par D :

$$\begin{cases} P = DQ + R \\ \deg(R) < \deg(D) \end{cases}$$

D'où

$$R = \underbrace{P}_{\in E} - \underbrace{DQ}_{\in E} \in E$$

$\deg(R) < \deg(D)$ donc $R = 0$
Donc,

$$\forall P \in E, D \mid P$$

$A \in E$ donc $D \mid A$
$B \in E$ donc $D \mid B$

Soit Δ un diviseur commun quelconque de A et B. On pose $D = AU + BV$

$$\left.\begin{matrix} \Delta \mid A \\ \Delta \mid B \end{matrix}\right\} \text{ donc } \Delta \mid AU + BV \text{ donc } \Delta \mid D$$

donc $\deg(\Delta) \leqslant \deg(D)$

Ainsi, D est un PGCD de A et B. De plus, Δ est un PGCD de A et B alors

$$\begin{cases} \Delta \mid D \\ \deg(\Delta) = \deg(D) \end{cases}$$

Donc $D = \Delta Q$ avec $\begin{cases} Q \in \mathbb{K}[X] \\ \deg(Q) = 0 \end{cases}$
donc D et Δ sont associés. □

Remarque:
Dans la preuve précédente, on a aussi montré les deux propositions suivantes.

Théorème (Théorème de Bézout)**:** Soient $A, B \in \mathbb{K}[X]$ tels que $A \neq 0$ ou $B \neq 0$
Soit D un PGCD de A et B. Alors

$$\exists (U, V) \in \mathbb{K}[X]^2, AU + BV = D$$

■

Proposition: Avec les hypothèses précédents,

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

$$\left.\begin{matrix} \Delta \mid A \\ \Delta \mid B \end{matrix}\right\} \iff \Delta \mid D$$

■

Définition: On dit qu'un polynôme est <u>unitaire</u> si sont coefficient dominant vaut 1.

Proposition – Définition: Soient A et B deux polynômes dont l'un au moins est non nul. Parmi tous les PGCD de A et B, un seul est unitaire. On le note $A \wedge B$.

Preuve:
Soit D un PGCD de A et B. Alors $\mathrm{dom}(D)^{-1}D$ est associé à D, donc c'est un PGCD de A et B et il est unitaire. Soient D et Δ deux PGCD unitaires de A et B. Ils sont associés

$$\Delta = \lambda D \text{ avec } \lambda \in \mathbb{K} \setminus \{0\}$$

D'où,

$$1 = \mathrm{dom}(\Delta) = \lambda\, \mathrm{dom}(D) = \lambda$$

Donc $\Delta = D$ □

Proposition: Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Soit R le reste de la division de A par B. Alors,

$$A \wedge B = B \wedge R$$

Preuve (idem que dans $\mathbb{Z}$): $\square$

Exemple:
$D = (5X^2 + 3X - 1) \wedge (X + 3)$

$$\begin{array}{r|l} X^2+3X-1 & X+3 \\ \cline{2-2} -\quad 5X^2+15X & 5X-12 \\ \hline -12X-1 & \\ -\quad -12X-36 & \\ \hline 35 & \end{array} \qquad \begin{array}{r|l} X+3 & 35 \\ \cline{2-2} -\quad X & \frac{1}{35}X+\frac{3}{35} \\ \hline 3 & \\ -\quad 3 & \\ \hline 0 & \end{array}$$

$$D = (X+3) \wedge 35 = 1$$

Théorème (Théorème de Gauß)**:** Soient A, B, C trois polynômes non nuls tels que
$\begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases}$
Alors, $A \mid C$

Preuve (idem que dans $\mathbb{Z}$): $\square$

Corollaire: Avec les notations précédentses,

$$\left.\begin{array}{l} A \mid B \\ B \mid C \\ A \wedge B = 1 \end{array}\right\} \implies AB \mid C$$

Proposition: Soient A et B deux polynômes non nuls et D un PGCD de A et B. Soit $x \in \mathbb{K}$.

$$A(x) = B(x) = 0 \iff D(X) = 0$$

Preuve: " $\implies$ " On suppose $A(x) = B(x) = 0$
D'après le théorème de Bézout,

$$D = AU + BV \text{ avec } (U, V) \in \mathbb{K}[X]^2$$

Donc,

$$D(x) = A(x)U(x) + B(x)V(x) = 0 + 0 = 0$$

" $\impliedby$ " On suppose $D(x) = 0$. On pose $\begin{cases} A = DA_1 \\ B = DB_1 \end{cases}$ avec $(A_1, B_1) \in \mathbb{K}[X]^2$

D'où,

$$\begin{cases} A(x) = D(x)A_1(x) = 0 \\ B(x) = D(x)B_1(x) = 0 \end{cases}$$

□

Définition: Soit $P \in \mathbb{K}[X]$.

On dit que P n'est pas irréductible si il existe $(Q, R) \in \mathbb{K}[X]^2$ non constants tels que $P = QR$ **ou** si P est constant.

Sinon, on dit que P est irréductible.

Exemple:

1. $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$
   On suppose que
   $$X^2 + 1 = QR \text{ avec } (Q, R) \in \mathbb{R}[X]^2$$
   $$\begin{cases} \deg(Q) > 0 \\ \deg(R) > 0 \end{cases}$$
   Donc, P et Q sont de degré 1, donc ont chacun une racine réelle donc $X^2 + 1$ a au moins une racine réelle : $\lightning$ une contradiction.
2. $X^2 + 1$ n'est pas irréductible dans $\mathbb{C}[X]$:
   $$X^2 + 1 = (X - i)(X + i)$$
3. $X^4 + 1$ n'est pas irréductible dans $\mathbb{R}[X]$ et pourtant il n'a aucune racine réelle.
   $$\begin{aligned} X^2 + 1 &= X^4 + 2X^2 + 1 - 2X^2 \\ &= \left(X^2 + 1\right)^2 - 2X^2 \\ &= \underbrace{\left(X^2 + 1 - \sqrt{2}X\right)}_{\in \mathbb{R}[X]} \underbrace{\left(X^2 + 1 + \sqrt{2}X\right)}_{\in \mathbb{R}[X]} \end{aligned}$$

Théorème (Théorème de D'Alembert - Gauß)**:**

$$\forall P \in \mathbb{C}[X] \text{ non constant}, \exists a \in \mathbb{C}, P(a) = 0$$

□

Corollaire: Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactemenent les polynômes de degré 1.

Preuve:
Les polynômes de degré 1 sont évidemment irréductibles.
Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geqslant 2$. Soit $a \in \mathbb{C}$ une racine de P.
Donc $X - a \mid P$.

$$\begin{cases} P = (X - a) \times Q \\ Q \in \mathbb{C}[X] \end{cases}$$

$\left.\begin{array}{l}\deg(Q) \geqslant 1 \\ \deg(X-a) = 1\end{array}\right\}$ donc P n'est pas irréductible. $\square$

Exemple:
Factoriser X^4+1 dans $\mathbb{C}$
Les racines complexes de X^4+1 sont $\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$ et $-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$
Donc,

$$\begin{aligned} X^4-1 &= \left(X-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)\left(X+\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right) \\ &\times \left(X+\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)\left(X-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right) \end{aligned}$$

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $\mu \in \mathbb{N}$.
On dit que a est une racine de P de multiplicité μ si

$$\begin{cases} (X-a)^\mu \mid P \\ (X-a)^{\mu+1} \nmid P \end{cases}$$

Si $\mu = 1$, on dit que a est une racine simple.
Si $\mu = 2$, on dit que a est une racine double.

Remarque:
a est une racine de multiplicité 0 si et seulement si $P(a) \neq 0$

Lemme: Soient $(A, B) \in \mathbb{R}[X]^2$ non nuls. On suppose que A divise B dans $\mathbb{C}[X]$
Alors, A divise B dans $\mathbb{R}[X]$

Preuve:
On suppose que

$$(*) \qquad B = AQ \text{ avec } Q \in \mathbb{C}[X]$$

On divise B par A dans $\mathbb{R}[X]$:

$$(**) \qquad B = AQ_1 + R_1 \text{ avec } \begin{cases} (Q_1, Q_2) \in \mathbb{R}[X]^2 \\ \deg(R_1) < \deg(A) \end{cases}$$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, $(**)$ est aussi le résultat de la division euclidienne de B par A dans $\mathbb{C}[X]$.
$(*)$ correspond aussi à une division euclidienne dans $\mathbb{C}[X]$
Par unicité, $\begin{cases} Q = Q_1 \in \mathbb{R}[X] \\ R_1 = 0 \end{cases}$
Donc A divise B dans $\mathbb{R}[X]$ $\square$

Proposition: Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$, $\mu \in \mathbb{N}$.
Si a est une racine de P de multiplicité μ alors $\overline{a}$ est une racine de P de multiplicité μ.

Preuve (par récurrence sur μ):
On pose

$$\forall n \in \mathbb{N}, \mathscr{P}(n) : \text{“}\forall P \in \mathbb{R}[X] \text{ et } a \in \mathbb{C} \setminus \mathbb{R} \text{ racine de } P \text{ de multiplicité } \mu, \\ \text{alors } \overline{a} \text{ est aussi une racine de } P \text{ de multiplicité } \mu\text{”}$$

— Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ tel que $P(a) \neq 0$.

On pose $P = \sum_{i=0}^{p} \alpha_i X^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$$\begin{aligned} P(\overline{a}) &= \sum_{i=0}^{p} \alpha_i \overline{a}^i \\ &= \sum_{i=0}^{p} \overline{\alpha_i} \overline{a^i} \\ &= \sum_{i=0}^{p} \overline{\alpha_i a^i} \\ &= \overline{\left(\sum_{i=0}^{p} \alpha_i a^i\right)} \\ &= \overline{P(a)} \\ &\neq 0 \end{aligned}$$

Donc $\mathscr{P}(0)$ est vraie

— Soit $\mu \in \mathbb{N}$. On suppose $\mathscr{P}(\mu)$ vraie.
Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ une racine de P de multiplicité $\mu + 1$. On pose

$$\begin{cases} P = (X-a)^{\mu+1} Q \\ Q \in \mathbb{C}[X] \\ Q(a) \neq 0 \end{cases}$$

On pose aussi $P = \sum_{i=0}^{p} \alpha_i a^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$\mu + 1 \geqslant 1$ donc $P(a) = 0$. D'où, $P(\overline{a}) = \overline{P(a)} = \overline{0} = 0$
donc $\underbrace{(\overline{a} - a)^{\mu+1}}_{\neq 0} Q(\overline{a}) = 0$

Donc, $Q = (X - \overline{a}) Q_1$ avec $Q_1 \in \mathbb{C}[X]$
D'où

$$\begin{aligned} P &= (X-a)^{\mu+1} (X - \overline{a}) Q_1 \\ &= (X-a)(X-\overline{a})(X-a)^{\mu} Q_1 \end{aligned}$$

Or,

$$\begin{aligned} (X-a)(X-\overline{a}) &= X^2 - (a + \overline{a}) X + a\overline{a} \\ &= X^2 - 2\mathfrak{Re}(a) X = |a|^2 \in \mathbb{R}[X] \end{aligned}$$

D'après le lemme précédent, $(X-a)^{\mu} Q_1 \in \mathbb{R}[X]$
De plus,

$$0 \neq Q(a) = (\overline{a} - a) Q_1(a)$$

docn $Q_1(a) \neq 0$
Donc a est une racine de $(X-a)^{\mu} Q_1 \in \mathbb{R}[X]$ de multiplicité μ.

D'après $\mathscr{P}(\mu)$, $\overline{a}$ est aussi une racine de $(X-a)^{\mu}Q_1$ de multiplicité μ.
Donc, on peut écrire

$$(X-a)^{\mu}Q_1 = (X-\overline{a})^{\mu}Q_2 \text{ avec } \begin{cases} Q_2 \in \mathbb{C}[X] \\ Q_2(\overline{a}) \neq 0 \end{cases}$$

Donc,

$$P = (X-a)(X-\overline{a})^{\mu+1}Q_2$$

Donc $\overline{a}$ est une racine de P de multiplicité $\mu+1$

□

Corollaire: Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.

Preuve: — Les polynômes de de degré 1 sont évidemment irréductibles

- Les polynômes constants ne sont pas irréductibles par définition
- Les polynômes de degré 2 ayant au moins une racine réelle peuvent s'écrire comme produit de deux polynômes réels de degré 1 à coefficients réels
- Réciproquement, si un polynôme de degré 2 n'est pas irreductible, c'est forcémet un produit de 2 polynômes de degré 1 à coefficients réels et donc ce polynôme a au moins une racine réelle
- Soit $P \in \mathbb{R}[X]$ tel que $\deg(P) \geqslant 3$
  On note $a_1, \dots, a_r$ les racines réelles distictes de P,

$$a_{r+1}, \overline{a_{r+1}}, a_{r+2}, \overline{a_{r+2}}, \dots, a_s, \overline{a_s}$$

les récines non réelles distictes de P. On note aussi

$$\forall k \in [\![1, s]\!], \mu_k \text{ la multiplicité de } a_k$$

Donc

$$P = \mathrm{dom}(P)(X-a_1)^{\mu_1} \cdots (X-a_r)^{\mu_r}(X-a_{r+1})^{\mu_{r+1}}(X-\overline{a_{r+1}})^{\mu_{r+1}} \\ \times \cdots \times (X-a_s)^{\mu_s}(X-\overline{a_s})^{\mu_s}$$

Or,

$$\begin{aligned} \forall k \geqslant r+1, (X-a_k)^{\mu_k}(X-\overline{a_k})^{\mu_k} &= ((x-a)(x-\overline{a}))^{\mu_k} \\ &= (X^2 - 2\mathfrak{Re}(a)X + |a|^2 \\ &\in \mathbb{R}[X] \end{aligned}$$

D'où,

$$P = \underbrace{\mathrm{dom}(P)}_{\in\mathbb{R}} \underbrace{\prod_{k=1}^{r}(X-a_k)^{\mu_k}}_{\in\mathbb{R}[X]} \prod_{k=r+1}^{s} \underbrace{\left(X^2 - 2\mathfrak{Re}(a_k)X + |a_k|^2\right)^{\mu_k}}_{\in\mathbb{R}[X]}$$

$$P \text{ irréductible} \iff \left(\begin{array}{l} \text{il y a une unique racine réelle simple} \\ \text{et aucune racine non réelle} \\ \text{OU} \\ \text{il n'y a aucune racine réelle et 2 racines} \\ \text{non réelles conjuguées simples} \end{array} \right.$$

□

Théorème: Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Tout polynôme de $\mathbb{K}$ se découpe en produit de facteurs irréductibles dans $\mathbb{K}[X]$ et cette décomposition est unique à multiplication par une constante non nulle près. $\square$

Proposition: Soient $A, B \in \mathbb{C}[X]$ non nuls.

$$A \mid B \iff \begin{array}{l} \forall a \in \mathbb{C},\ \text{si } a \text{ est une racine de } A \text{ de multiplicité } \mu \in \mathbb{N}, \\ \text{alors } a \text{ est racine de } B \text{ avec une multiplicité } \geqslant \mu \end{array}$$

Preuve: " $\implies$ " On suppose $A \mid B$
Soit $a \in \mathbb{C}$ une racine de A de multiplicité μ
Alors, $(X-a)^\mu \mid A$ donc $(X-a)^\mu \mid B$
Donc a est une racine de B de multiplicité $\geqslant \mu$
" $\impliedby$ " On décompose A et B en produit de facteurs irréductibles sur $\mathbb{C}[X]$:

$$B = \mathrm{dom}(B) \prod_{a \in \mathscr{R}} (X-a)^{\nu_a}$$

où $\mathscr{R}$ est l'ensemble des racines de B ; et

$$A = \mathrm{dom}(A) \prod_{a \in \mathscr{S}} (X-a)^{\mu_a}$$

où $\mathscr{S}$ est l'ensemble des racines de A
On suppose que $\begin{cases} \mathscr{S} \subset \mathscr{R} \\ \forall a \in \mathscr{S}, \mu_a \leqslant \nu_a \end{cases}$
D'où,

$$B = \frac{\mathrm{dom}(B)}{\mathrm{dom}(A)} \underbrace{\mathrm{dom}(A) \prod_{a \in \mathscr{S}} (X-a)^{\mu_a}}_{A} \times \underbrace{\prod_{a \in \mathscr{S}} (X-a)^{\nu_a - \mu_a} \times \prod_{a \in \mathscr{R} \setminus \mathscr{S}} (X-a)^{\nu_a}}_{\in \mathbb{C}[X]}$$

Donc, $A \mid B$

$\square$

Exercice:
Montrer que $1 + X + X^2 \mid X^{3n} - 1$
Les racines de $1 + X + X^2$ sont j et j^2

$$j^{3n} - 1 = \left(j^3\right)^n - 1 = 1 - 1 = 0$$
$$\left(j^2\right)^{3n} = \left(j^3\right)^{2n} - 1 = 1 - 1 = 0$$

Proposition: Soit $P \in \mathbb{C}[X]$ de degré $n > 0$
Alors P a exactement n racines comptées avec multiplicité.

Preuve:

$$P = \operatorname{dom}(P) \times \prod_{a \in \mathscr{R}} (X-a)^{\mu_a}$$

où $\mathscr{R}$ est l'ensemble des racines distinctes de P
$n = \deg(P) = \sum_{a \in \mathscr{R}} \deg\left((X-a)^{\mu_a}\right) = \sum_{a \in \mathscr{R}} \mu_a$ $\square$

Quatrième partie

L'espace vectoriel $\mathbb{K}[X]$

Remarque (Rappel):
$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel engendré par $(1, X, X^2, \dots)$

Proposition: La famille $(X^n)_{n\in\mathbb{N}}$ est libre.

Preuve:
Soit $(\lambda_n)_{n\in\mathbb{N}}$ une famille presque nulle de scalairees telle que $\sum\limits_{n\in\mathbb{N}} \lambda_n X^n = 0$
$(\lambda_n)_{n\in\mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$: on le note P.
Or,

$$\sum_{n\in\mathbb{N}} \lambda_n X^n = (\lambda_0, \lambda_1, \dots, \lambda_n, \dots) = P$$

Donc $P = 0$ donc

$$\forall n \in \mathbb{N}, \lambda_n = 0$$

□

Corollaire:

$$\dim\big(\mathbb{K}[X]\big) = +\infty$$

□

Définition: Pour $n \in \mathbb{N}$, on note

$$\mathbb{K}_n[X] = \big\{P \in \mathbb{K}[X] \mid \deg(P) \leqslant n\big\}$$

Théorème: $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n+1$

Preuve:
$\mathbb{K}_n[X] = \mathrm{Vect}\left(1, X, \dots, X^n\right)$ □

Proposition: Soit $(P_i)_{i\in I}$ une famille de polynômes non nuls telle que

$$\forall i \neq j, \deg(P_i) \neq \deg(P_j)$$

Alors $(P_i)_{i\in I}$ est libre.

Preuve:
Soit $n \in \mathbb{N}$ et $i_1, \dots, i_n$ des éléments distincts de I
Soient $\lambda_1, \dots, \lambda_n \in \mathbb{K}$. On suppose

$$\lambda_1 P_{i_1} + \cdots + \lambda_n P_{i_n} = 0$$

Quitte à renuméroter les polynômes, on peut supposer que

$$\forall k \in [\![1, n]\!], \deg\left(P_{i_n}\right) > \deg\left(P_{i_k}\right)$$

Si $\lambda_n \neq 0$,

$$\deg\left(\lambda_1 P_{i_1} + \cdots + \lambda_n P_{i_n}\right) = \deg\left(P_{i_n}\right) \neq -\infty$$

Donc $\lambda_n = 0$
Donc $\lambda_1 P_{i_1} + \cdots + \lambda_{n-1} P_{i_{n-1}} = 0$

On conclut par récurrence sur n. $\square$

Théorème (Formule de Taylor)**:** Soit $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$.

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

Preuve:
$\left(1, X-a, \ldots, (X-a)^n\right)$ est libre.
Comme $\dim\left(\mathbb{K}_n[X]\right) = n+1$, c'est une base de $\mathbb{K}_n[X]$.
Donc, il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que

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

On remarque que

$$P(a) = \lambda_0$$

$$\begin{aligned}\forall i \in [\![1, n]\!], P^{(i)}(a) &= \sum_{k=0}^{n} \lambda_k \underbrace{\left((X-a)^k\right)^{(i)}(a)}_{=\begin{cases} 0 & \text{si } k < i \\ i! & \text{si } k = i \\ \frac{k!}{(k-i)!}(X-a)^{k+1} & \text{si } k > i \end{cases}} \\ &= \lambda_i i!\end{aligned}$$

Donc $\lambda_i = \dfrac{P^{(i)}(a)}{i!}$ $\square$

Proposition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$\left.\begin{array}{r} a \text{ est une racine de } P \\ \text{de multiplicité } \mu \end{array}\right\} \iff \left\{\begin{array}{l} \forall k \leqslant \mu - 1, P^{(k)}(a) = 0 \\ P^{(\mu)}(a) \neq 0 \end{array}\right.$$

Preuve:
On pose $n = \deg(P)$

" $\Longleftarrow$ "

$$\begin{aligned} P &= \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \\ &= \sum_{k=\mu}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \\ &= (X-a)^\mu \underbrace{\sum_{k=\mu}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-\mu}}_{Q\in\mathbb{K}[X]} \end{aligned}$$

Donc $\begin{cases} (X-a)^\mu \mid P \\ Q(a) = \dfrac{P^{(\mu)}(a)}{\mu!} \neq 0 \end{cases}$

" $\Longrightarrow$ "

$\begin{cases} P = (X-a)^\mu Q \\ Q(a) \neq 0 \end{cases}$

$$\begin{aligned} \forall k \leqslant \mu - 1, P^{(k)}(a) &= \sum_{j=0}^{k} \binom{k}{j} \left((X-a)^\mu\right)^{(j)}(a) Q^{(k-j)}(a) \\ &= \sum_{j=0}^{k} \binom{k}{j} \frac{\mu!}{(\mu-j)!} \underbrace{(a-a)^{\mu-j}}_{=0} Q^{(k-j)}(a) \\ &= 0 \end{aligned}$$

$$\begin{aligned} P^{(\mu)}(a) &= \binom{\mu}{\mu} \times \mu! \times 1 \times Q^{(0)}(a) \\ &= Q(a) \\ &\neq 0 \end{aligned}$$

□

Corollaire: Avec les notations précédentes, si a est une racine de P de multiplicité μ, alors a est une racine de P' de multiplicité $\mu - 1$

□

Définition: On dit qu'un polynôme P est scindé sur $\mathbb{K}$ si P est un produit de polynômes de $\mathbb{K}[X]$ de degré 1, i.e. toutes les racines de P sont dans $\mathbb{K}$

Exercice:

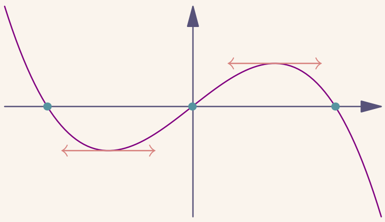
1. Soit $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$ à racines simples avec $\deg(P) \geqslant 2$. Montrer que P' est scindé sur $\mathbb{R}$ à racines simple.
2. Soit $P \in \mathbb{R}[X]$ scindé avec $\deg(P) \geqslant 2$. Montrer que P' est scindé.

Solution

1.

Soit $P \in \mathbb{R}[X]$ avec $\deg(P) = n$ scindé sur $\mathbb{R}$.
On note $x_1 < x_2 < \cdots < x_n$ les n racines de P
Soit $f_P : \mathbb{R} \to \mathbb{R}$ la fonction polynomiale. Aussi, f_P est $\mathscr{C}^\infty$ sur $\mathbb{R}$.
D'après le théorème de Rolle,

$$\forall i \in [\![1, n-1]\!], \exists y_i \in]x_i, x_{i+1}[, f_P'(y_i) = 0$$



Donc $y_1, \ldots, y_{n-1}$ sont racines de P'.
De plus,

$$y_1 < x_2 < y_2 < x_3 < y_3 < \cdots < y_{n-1}$$

On a donc trouvé $n-1$ racines distinctes de P'. Or, $\deg(P') = n - 1$.
Donc, on a trouvé TOUTES les racines complexes de P'. Donc P' est sciendé à racines simples.

2. On note $x_1 < \cdots < x_p$ les racines de P et $n = \deg(P)$. On note pour tout $i \in [\![1, p]\!]$, μ_i la multiplicité de x_i. Donc,

$$\sum_{i=1}^{p} \mu_i = n$$

D'après le théorème de Rolle,

$$\forall i \in [\![1, p-1]\!], \exists y_i \in]x_i, x_{i+1}[, P'(y_i) = 0$$

On a trouvé $p-1$ racines réelles de P'. $\forall i \in [\![1, p]\!], x_i$ est une racine de P' de multiplicité $\mu - 1$.

Ce qui fait, $\displaystyle\sum_{i=1}^{p}(\mu_i - 1) = n - p$ racines réelles de P' comptées avec multiplicité.
En tout, on a trouvé $n - 1$ racines réelles de P' comptées avec multiplicité.
Comme $\deg(P') = n - 1$, P' n'a pas d'autres racines donc P' est scindé.

Exercice (Problème):
Soient $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tels que

$$\forall i \neq j, x_i \neq x_j$$

Soient $(y_1, \ldots, y_n) \in \mathbb{K}^n$. On cherche $P \in \mathbb{K}[X]$ de <u>degré minimal</u> tel que

$$(*) \quad \forall i \in [\![1, n]\!], P(x_i) = y_i$$

Soit $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & \big(P(x_1), \ldots, P(x_n)\big) \end{array}$

$$(*) \iff \varphi(P) = (y_1, \ldots, y_n)$$

On cherche, parmi tous les antécédants de $(y_1, \ldots, y_n)$ celui de plus bas degré.
φ est linéaire :

$$\begin{aligned} &\forall P, Q \in \mathbb{K}[X], \forall \alpha, \beta \in \mathbb{K}, \\ &\qquad \varphi(\alpha P + \beta Q) = \big(\alpha P(x_1) + \beta Q(x_1), \ldots, \alpha P(x_n) + \beta Q(x_n)\big) \\ &\qquad\qquad = \big(\alpha P(x_1), \ldots, \alpha P(x_n)\big) + \big(\beta Q(x_1), \ldots, \beta Q(x_n)\big) \\ &\qquad\qquad = \alpha\varphi(P) + \beta\varphi(Q) \end{aligned}$$

— Donc φ est un morphisme de groues additifs.
— $(y_1, \ldots, y_n) = \displaystyle\sum_{i=0}^{n} y_i e_i$ où $(e_1, \ldots, e_n)$ est la bade canonique de $\mathbb{K}^n$

Si on trouve $L_1, \dots, L_n \in \mathbb{K}[X]$ tels que $\varphi(L_1) = e_1, \ \dots \ \varphi(L_n) = e_n$, alors

$$\begin{aligned}\varphi\left(\sum_{i=1}^{n} y_i L_i\right) &= \sum_{i=0}^{n} y_i \varphi(L_i) \\ &= \sum_{i=1}^{n} y_i e_i \\ &= (y_1, \dots, y_n)\end{aligned}$$

—

$$\begin{aligned}P \in \operatorname{Ker}(\varphi) &\iff \varphi(P) = (0, \dots, 0) \\ &\iff \forall i \in [\![1, n]\!], P(x_i) = 0 \\ &\iff \exists Q \in \mathbb{K}[X], P = (X - x_1) \cdots (X - x_n) Q\end{aligned}$$

Soit $i \in [\![1, n]\!]$ et $L_i \in \mathbb{K}[X]$.

$$\begin{aligned}\varphi(L_i) = e_i &\iff \big(L_i(x_1), L_i(x_2), \dots, L_i(x_n)\big) = (0, \dots, 0, \underbrace{1}_{i}, 0, \dots, 0) \\ &\iff \begin{cases} L_i(x_i) = 1 \\ \forall j \neq i, L_i(x_j) = 0 \end{cases} \\ &\iff \begin{cases} \exists Q \in \mathbb{K}[X], L_i = \displaystyle\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - x_j) Q \\ 1 = \displaystyle\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (x_i - x_j) Q(x_i) \end{cases} \\ &\Longleftarrow L_i = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}\end{aligned}$$

D'où,

$$\varphi(P) = (y_1, \dots, y_n) \iff \exists Q \in \mathbb{K}[X], P = \underbrace{\sum_{i=1}^{n} y_i L_i}_{\substack{\text{solution particulière} \\ \deg(\cdot) \leqslant n-1}} + \underbrace{\prod_{k=1}^{n} (X - x_k) Q}_{\substack{\text{solutions de l'équation} \\ \text{homogène associée} \\ \deg(\cdot) \geqslant n}}$$

<u>Le</u> polynôme de plus bas degré solution du problème d'interpolation est

$$\sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}$$

Définition: Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

On pose

$$\forall i \in [\![1, n]\!], L_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$$

L_i est le <u>i-ème polynôme interpolateur de Lagrange</u> associé à $(x_1, \dots, x_n)$:

$$\forall j \in [\![1, n]\!], L_i(x_j) = \delta_{i,j}$$

Proposition: Avec les notations précédentes, $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$.

Preuve: — $\forall i \in [\![1, n]\!]\,, \deg(L_i) = n - 1$
— Soit $P \in \mathbb{K}_{n-1}[X]$. On pose

$$\forall i \in [\![1, n]\!]\,, y_i = P(x_i)$$

On pose $Q = \sum_{i=1}^{n-1} y_i L_i$. Q est le seul polynôme de degré $\leqslant n-1$ tel que $Q(x_i) = y_i$ pour tout i.
Donc, $P = Q \in \mathrm{Vect}(l_1, \dots, L_n)$. Donc $(L_1, \dots, L_n)$ est une famille génératrice de $\mathbb{K}_{n-1}[X]$. Or, $\dim\big(\mathbb{K}_{n-1}[X]\big) = n$. Donc $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$

□

Exemple:
$\mathbb{K} = {}^{\mathbb{Z}}/_{5\mathbb{Z}}$ et $n = 3$

$x_1 = \overline{2}$ $\quad y_1 = \overline{1}$
$x_2 = \overline{0}$ $\quad y_2 = \overline{1}$
$x_3 = \overline{-1}$ $\quad y_3 = \overline{2}$

Le seul polynôme de degré $\leqslant 2$ tel que $P(x_i) = y_i$ pour tout $i \in [\![1, 2]\!]$ est $\displaystyle\sum_{i=1}^{3} y_i \prod_{\substack{1 \leqslant j \leqslant 3 \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$

$$\begin{aligned} L_1 &= (x_1 - x_2)^{-1}(x_1 - x_3)^{-1}(X - x_2)(X - x_3) \\ &= \overline{3} \times \overline{2} \times X\left(X + \overline{1}\right) = X\left(X + \overline{1}\right) = X^2 + X \end{aligned}$$

$$\begin{aligned} L_2 &= (x_2 - x_1)^{-1}(x_2 - x_3)^{-1}(X - x_1)(X - x_3) \\ &= \overline{2} \times \overline{1}\left(X - \overline{2}\right) \times \left(X - \overline{1}\right) \\ &= \overline{2}X^2 + \overline{3}X + \overline{1} \end{aligned}$$

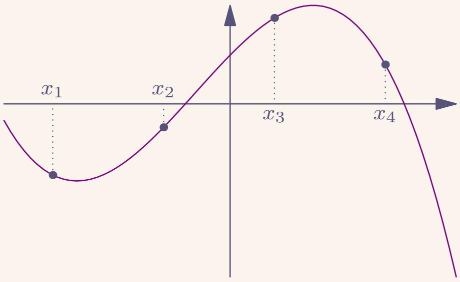
$$\begin{aligned} L_3 &= (x_3 - x_1)^{-1}(x_3 - x_2)^{-1}(X - x_1)(X - x_2) \\ &= \overline{3} \times \overline{4} \times \left(X - \overline{2}\right) \times X \\ &= \overline{2}X\left(X - \overline{2}\right) \\ &= \overline{2}X^2 + X \end{aligned}$$

Donc,

$$\begin{aligned} P &= X^2 + X + \overline{2}X + \overline{3}X + \overline{1} + \overline{4}X^2 + \overline{2} \\ &= \overline{2}X^2 + X + \overline{1} \end{aligned}$$

Vérification :

$$\begin{aligned} P\left(\overline{2}\right) &= \overline{3} + \overline{2} + \overline{1} = \overline{1} = y_1 \\ P\left(\overline{0}\right) &= \overline{1} = y_2 \\ P\left(\overline{-1}\right) &= \overline{2} - \overline{1} + \overline{1} = \overline{2} = y_3 \end{aligned}$$


x_1
x_2
x_3
x_4