Polynômes

Résumé

Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$

1/ $P(X) = 0 \iff (\forall\, 0 \leq i \leq n,\ a_i = 0)$

2/ $P(X) \neq 0 \iff (\exists\, 0 \leq i \leq n,\ a_i \neq 0)$

Prop

1/ $P \in \mathbb{K}_0[X] \iff \exists\, c \in \mathbb{K},\ P(X) = c$

2/ $P \in \mathbb{K}_1[X] \iff \exists\, (a,b) \in \mathbb{K}^2,\ P(X) = a + bX$

3/ $P \in \mathbb{K}_2[X] \iff \exists\, (a,b,c) \in \mathbb{K}^3,\ P(X) = a + bX + cX^2$

4/ $P \in \mathbb{K}_n[X] \iff \left(\exists\, (a_0, \ldots, a_n) \in \mathbb{K}^{n+1} \text{ tel que } P(X) = \sum_{k=0}^{n} a_k X^k\right)$

Operations sur les polynômes

Combinaisons linéaires de deux polynômes.

Déf : Soit $P(X) = \sum_{k=0}^{+\infty} a_k X^k$ et $Q(X) = \sum_{k=0}^{+\infty} b_k X^k$ deux polynômes de $\mathbb{K}[X]$.

1) Somme : $P(X) + Q(X) = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$

2) Multiplication par un scalaire $\alpha \in \mathbb{K}$:

$$\alpha P(X) = \sum_{k=0}^{+\infty} \alpha\, a_k X^k$$

3) Combinaison linéaire

$\forall \alpha, \beta \in \mathbb{K}, \alpha P(X) + \beta Q(X) = \sum_{k=0}^{+\infty} (\alpha a_k + \beta b_k) X^k$.

Produit de deux polynômes.

Définitions :

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

$$P(X) \cdot Q(X) = \sum_{k=0}^{+\infty} C_k X^k$$

où $C_k = \sum_{i=0}^{k} a_i b_{k-i}$, $\forall k \in \mathbb{N}$

NB :

$$C_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_{k-i} b_i$$

Corollaire $n \in \mathbb{N}$.

$\forall P, Q \in \mathbb{K}_n[X], \forall \alpha, \beta \in \mathbb{K}, (\alpha P + \beta Q) \in \mathbb{K}_n[X]$.

Prop : Soient P et $Q \in \mathbb{K}[X]$. On a :

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

Prop :

Soient P et $Q \in \mathbb{K}[X]$ on a :

$$PQ = 0 \Longleftrightarrow (P = 0 \text{ ou } Q = 0)$$

Prop : Binôme de Newton

Soient $n \in \mathbb{N}$; $P, Q, R \in \mathbb{K}[X]$ on a :

$$(P + Q)^n = \sum_{k=0}^{n} C_n^k P^k Q^{n-k}$$

Prop : On a aussi l'égalité de Bernoulli.

$$P^n - Q^n = (P-Q)\cdot\sum_{i=0}^{n-1} P^i Q^{n-1-i}$$

Prop :

$(\mathbb{K}[X], +, \times)$ est un anneau intègre.

Prop :

$\deg(P') = \deg(P) - 1$ si P n'est pas constant.

Prop : Soient $n \in \mathbb{N}$; $P, Q \in \mathbb{K}[X]$.

$$\left(\sum_{i=1}^{n} \lambda_i P_i\right)^{(n)} = \sum_{i=1}^{n} \lambda_i P_i^{(n)}$$

$$(PQ)^{(n)} = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)} \quad \text{(Leibniz)}$$

Prop :

1/ $\forall n \in \mathbb{N}$, $\forall\ 0 \leq k \leq n$ On a :

$$(X^n)^{(k)} = n \ldots (n-k+1) X^{n-k}$$

$$(X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k}$$

2/ $(X^n)^{(n)} = n!$

3/ $\forall k > n$; $(X^n)^{(k)} = 0$

Prop : Soient $n \in \mathbb{N}$, $0 \leq k \leq n$ et $a \in \mathbb{K}$ on a :

1/ $\left((X+a)^n\right)^{(k)} = \dfrac{n!}{(n-k)!}(X+a)^{n-k}$

2/ $\left((a-X)^n\right)^{(k)} = (-1)^k \dfrac{n!}{(n-k)!}(a-X)^{n-k}$

3/ $\left((a+bX)^n\right)^{(k)} = \dots\dots$

Coroll : Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$.

1) $P(X) = a_0 + \dots + a_n X^n \Longrightarrow P^{(n)}(X) = a_n \cdot n!$

2) $\deg(P) \leq n \Rightarrow (\forall k \geq n+1,\ P^{(k)} = 0)$

Prop : Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$.

Les assertions suivantes sont équivalentes :

1/ $P^{(n+1)} = 0$

2/ $\exists a_0, \dots, a_n \in \mathbb{K}^{n+1}, P = a_0 + \dots + a_n X^n$

3/ $P \in \mathbb{K}_n[X]$.

Arithmétique dans $\mathbb{K}[X]$.

Divisibilité

Déf : Soient A et $B \in \mathbb{K}[X]$.

On dit que A divise B si et ssi

$\exists C \in \mathbb{K}[X]\ ;\ B = AC$

Notation A/B

Prop

1/ $\forall A \in \mathbb{K}[X]$, $A/0$

2/ $\forall A \in \mathbb{K}[X]$, $\forall \lambda \in \mathbb{K}^*$ on a :

i) λ / A.

ii) $(\lambda A)/A$ et $A/(\lambda A)$.

3/ $(A/B \text{ et } B/C) \Rightarrow A/C$

4/ $\begin{pmatrix} A/B \\ A/C \end{pmatrix} \Longrightarrow A/(B \pm C)$

5/ $(\forall 1 \leq k \leq n, A/B_k) \Rightarrow A/\left(\sum_{k=1}^{n} \lambda_k B_k\right)$

où $\lambda_1, \dots, \lambda_n \in \mathbb{K}$.

6/ $\begin{pmatrix} A/B \\ C/D \end{pmatrix} \Longrightarrow AC/BD$

7/ $A/B \Longrightarrow \forall k \in \mathbb{N}, A^k/B^k$

8/ $\forall k \in [\![1, n]\!], A_k/B_k \Rightarrow \prod_{k=1}^{n} A_k / \prod_{k=1}^{n} B_k$

Notation : $[\![1, n]\!] = \{1, 2, \dots, n\}$

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

$A/B \Longrightarrow \deg(A) \leq \deg(B)$.

Prop 1 : Soient A et $B \in \mathbb{K}[X] \setminus \{0\}$
Les assertions suivantes sont équivalentes:
1/ A/B et B/A
2/ $\exists \lambda \in \mathbb{K}^* \; B = \lambda A$
3/ $\exists \mu \in \mathbb{K}^*, A = \mu B$

Déf : Soient A et $B \in \mathbb{K}[X] \setminus \{0\}$.
On dit que A et B sont associés si et ssi :
$$A/B \text{ et } B/A$$

Division euclidienne :

Prop : (Thm de la div eucli)
Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] / \{0\}$.
Il existe un unique $(Q, R) \in (\mathbb{K}[X])^2$ tq :
1/ $A = BQ + R$
2/ $d^\circ(R) < d^\circ(B)$

Prop : Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$
$$B/A \iff R = 0$$
où R est le reste de la div euclidienne de A par B.

Racines d'un polynome :

Déf : Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
a est dit racine de P si et ssi $P(a) = 0$.

(à retenir)

$n \geq 2$ et $P(X) = X^n - 1$.

Les racines complexes de $(X^n - 1)$ sont exactement les racines $n^{\text{ème}}$ de l'unité.

Prop :

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

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

Multiplicité d'une racine :

Prop

Soient $P \in \mathbb{K}$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

Les propositions suivantes sont équivalentes :

1) a racine de multiplicité m de P.

2) $(X - a)^m \mid P$ et $(X - a)^{m+1} \nmid P$.

3) $\begin{cases} P(a) = \dots = P^{(m-1)}(a) = 0 \\ P^{(m)}(a) \neq 0 \end{cases}$

4) $\exists\, Q \in \mathbb{K}[X]$ tq $\begin{cases} P(X) = (X - a)^m Q(X) \\ Q(a) \neq 0 \end{cases}$

NB : Si la multiplicité $m \geq r$, on dit que a est une racine de multiplicité au moins r.

Prop Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $(m,r) \in (\mathbb{N}^*)^2$.
Les prop suivantes sont équivalentes :
1/ a racine de multiplicité au moins r.
2/ $(X-a)^r / P$

Prop
$m \in \mathbb{N}^*$, $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$ on a :
$$(X-a)^m / P \iff \left(\forall\, 0 \leq k \leq m-1,\ P^{(k)}(a) = 0\right)$$

Nombre de racines d'un polynôme.

Prop
Soient $P(X) \in \mathbb{K}[X]$ et $x_1 \neq x_2 \in \mathbb{K}$.
$$\left(P(x_1) = P(x_2) = 0\right) \iff (X-x_1)(X-x_2) / P(X)$$

En général, on a la prop suivante :

Prop : soit $n \geq 2$. soient $x_1, \dots, x_n \in \mathbb{K}$ distincts deux à deux on a :
$$\left(P(x_1) = \dots = P(x_n) = 0\right) \iff \left((X-x_1) \dots (X-x_n) / P(X)\right)$$

Prop : Soient $P \in \mathbb{R}[X]$ et $w \in \mathbb{C}$.
w racine de $P \iff \bar{w}$ racine de P.

Prop Soit $n \in \mathbb{N}^*$
Si $\begin{cases} 1/\ d°(P) \leq n \\ 2/\ P \text{ possède } (n+1) \text{ racines distinctes} \end{cases}$
Alors $P = 0$

Corollaire

Un polynôme ayant une infinité de racines est nul.

Cas des racines complexes :

Prop (Théorème de d'Alembert-Gauss)

Tout polynôme de degré ≥ 1 admet au moins une racine complexe.

Polynômes irréductibles.

Def

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

P est dit irréductible dans $\mathbb{K}[X]$ si et ssi :

1/ $d^\circ(P) \geq 1$

2/ Les seuls diviseurs de P dans $\mathbb{K}[X]$ sont ses associés et les polynômes constants non nuls.

NB :

2/ Veut dire que ses seuls diviseurs sont de la forme (λP) et μ où λ et $\mu \in \mathbb{K}^*$.

Les polynômes irréductibles dans $\mathbb{R}$ et dans $\mathbb{C}$.

Prop : Dans $\mathbb{C}$, les polynômes irréductibles sont les polynômes de degré 1.

Prop : Dans $\mathbb{R}$, les polynômes irréductibles sont les polynômes de degré 1 et ceux de degré 2 à discriminant <0

Décomposition d'un polynôme en produit de facteurs irréductibles.

Vocab : On parle aussi de « factorisation ».

Prop

1/ Tout polynôme $P \in \mathbb{K}[X]$, de degré ≥ 1 s'écrit sous la forme :

$$P = \lambda P_1 \cdots P_r$$

où $\lambda \in \mathbb{K}^*$ et les P_i unitaires et irréductibles dans $\mathbb{K}[X]$

NB : Decomposition dans $\mathbb{C}$.

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

où $\begin{cases} \lambda = Cd(P) \\ n = \deg(P) \\ x_1, \dots, x_n \text{ les racines de } P, \text{ non forcément distincts 2 à 2.} \end{cases}$

2/ $P(X) = \lambda \prod_{i=1}^{s} (X - a_i)^{m_i}$

où $\lambda = cd(P)$, $\deg(P) = \sum_{i=1}^{s} m_i$

$a_1, \dots, a_s$ les racines de P 2 à 2 distincts entre eux.

m_i étant la multiplicité de la racine a_i.

NB : Décomposition dans $\mathbb{R}$.

$$P(X) = \lambda \prod_{i=1}^{s} (X - x_i)^{m_i} \cdot \prod_{k=1}^{r} (X^2 + b_k X + c_k)^{n_k}$$

Où $\lambda = cd(P)$, $d^\circ(P) = \sum_{i=1}^{s} m_i + \sum_{k=1}^{r} 2n_k$.

Les x_i sont les racines réelles de P distinctes 2 à 2

$\forall k,\ b_k^2 - 4c_k < 0$

Polynômes scindés

Déf Un polynôme $P \in \mathbb{K}[X]$ est dit scindé dans $\mathbb{K}$ si et ssi :

1/ $\deg(P) \geq 1$.

2/ P s'écrit comme produit de polynômes de degrés 1 et à coéfficients dans $\mathbb{K}$.

Prop

Dans $\mathbb{C}$, tout polynôme de degré ≥ 1 est scindé.

NB : Soit $P \in \mathbb{K}[X]$ scindé dans $\mathbb{K}$.

1/ P s'écrit sous la forme :

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

où $\begin{cases} \lambda \text{ et les } x_k \in \mathbb{K}. \\ d^\circ(P) = n \\ x_1, \dots, x_n \text{ les racines de } P, \text{ non forcément distincts} \\ 2 \text{ à } 2. \end{cases}$

2/ P s'écrit aussi sous la forme

$$P(X) = \lambda \prod_{i=1}^{s} (X - a_i)^{m_i}$$

où : $\begin{cases} \lambda \text{ et les } a_i \in \mathbb{K}. \\ d^\circ(P) = \sum_{i=1}^{s} m_i \\ a_1, \dots, a_s \text{ sont les racines de } P \text{ distinctes } 2 \text{ à } 2 \end{cases}$

m_i = la multiplicité de la racine a_i.

Relations de Viète entre les racines et les coeff d'un polynôme scindé

Prop

Soit $n \geq 1$

Soit $P(X) = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$ de degré n, scindé dans $\mathbb{K}$.

Soient $x_1, \dots, x_n$ ses racines, non forcément distincts 2 à 2. On a :

1/ $\displaystyle\sum_{k=1}^{n} x_k = \frac{-a_{n-1}}{a_n}$

2/ $\displaystyle\prod_{k=1}^{n} x_k = \frac{(-1)^n a_0}{a_n}$

Prop : Formule de viète (cas général)

$P \in \mathbb{K}[X]$, $\deg(P) = n \geq 1$.

$P(X) = a_0 + \dots + a_n X^n$.

$x_1, \dots, x_n$ Les racines de P (non forcément distinctes 2 à 2) On a :

$$\forall\, 1 \leq k \leq n \; ; \quad \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k} = \frac{(-1)^k a_{n-k}}{a_n}$$

Formule de Taylor polynomiale Composition polynomiale

Formule de Taylor.

Prop

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, On a :

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

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

Composition de polynômes.

Déf

Soient $P(X) = \sum_{k=0}^{+\infty} a_k X^k$ et $Q(X) \in \mathbb{K}[X]$.

$$(P \circ Q)(X) \overset{\text{déf}}{=} \sum_{k=0}^{+\infty} a_k (Q(X))^k.$$

Prop

Soient P et $Q \in \mathbb{K}[X] \setminus \{0\}$.

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

Polynôme d'interpolation de Lagrange

Notations : $n \in \mathbb{N}^*$, $a_0, \dots, a_n \in \mathbb{K}$, distincts 2 à 2. Pour $k \in [\![0,n]\!]$, on note :

$$L_k(X) = \prod_{\substack{j=0 \\ j \neq k}}^{n} \left(\frac{X - a_j}{a_k - a_j} \right)$$

Prop :

1) Soit $k \in [\![0,n]\!]$, $L_k(X)$ est un polynôme de degré n.

2) Soient $k, i \in [\![0,n]\!]$, $\begin{cases} L_k(a_i) = 0 & \text{si } k \neq i \\ L_k(a_i) = 1 & \text{si } k = i \end{cases}$

Prop : Soient $a_0, \dots, a_n \in \mathbb{K}$ distincts 2 à 2.
Soient $y_0, \dots, y_n \in \mathbb{K}$.

1) Il existe un unique polynôme $P \in \mathbb{K}_n[X]$ tel que

$$\forall k \in [\![0,n]\!], P(a_k) = y_k$$

2) Ce polynôme P est exactement :

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

Prop :

Les polynômes $T \in \mathbb{K}[X]$ vérifiant :
$\forall i \in [\![0,n]\!]$, $T(a_i) = y_i$.
sont exactement ceux de la forme :

$$T(X) = P(X) + \left(\prod_{k=0}^{n} (X - a_k)\right) \cdot Q(X)$$

où $P(X)$ est celui de la prop et $Q \in \mathbb{K}[X]$ quelconque.

Pgcd de deux polynômes tous deux non nuls.

Déf

Soient P et $Q \in \mathbb{K}[X]$, non tous deux nuls.
Le Pgcd de P et Q, noté $P \wedge Q$, est le polynôme unitaire de plus haut degré appartenant à $\mathcal{D}(P) \cap \mathcal{D}(Q)$.

NB :

1/ Tout polynôme associé à $P \wedge Q$ est dit un pgcd de P et Q.

2/ $P \wedge Q$ impose qu'il soit unitaire

NB :

1/ Si $A \mid B$ alors

i) $A \wedge B = \dfrac{A}{cd(A)}$

ii) A est un pgcd de A et B.

2/ $\begin{cases} P / A \\ P / B \end{cases} \iff P / (A \wedge B)$

3/ On a L'algorithme d'Euclide qui est analogue à celui pour les entiers.
Il donne un pgcd.

4/ L'algorithme d'Euclide, tout comme pour les entiers, il donne une relation de Bézout

5/ Si D est un pgcd de A et B, alors il existe U et $V \in \mathbb{K}[X]$ tels que :

$$AU + BV = D.$$

PPCM de deux polynômes non nuls

Déf Soient P et $Q \in \mathbb{K}[X] \setminus \{0\}$.
Le ppcm de P et Q, noté $P \vee Q$ est le polynôme unitaire, de plus petit degré parmi les multiples commun à P et à Q.

1/ $A/B \Rightarrow A \vee B = \dfrac{B}{cd(B)}$.

2/ $\begin{cases} P/A \\ Q/A \end{cases} \Rightarrow P \vee Q / A$

3/ $(A \wedge B) \cdot (A \vee B) \equiv AB$
associé

Pgcd d'un nombre fini de polynômes

NB

1/ $(A_1 \wedge A_2) \wedge A_3 = A_1 \wedge (A_2 \wedge A_3)$.
qu'on note $A_1 \wedge A_2 \wedge A_3$ qui est le pgcd de A_1, A_2 et A_3

2/ Pareil aux entiers.

NB₂ : On parle ainsi de $(A_1 \wedge \dots \wedge A_n)$, le pgcd de $A_1, \dots, A_n$.
C'est défini d'une manière récurrente.

NB₃ : On parle de m du pgcd de plusieurs entiers $a_1, \dots, a_n$ et se note :
$a_1 \wedge \dots \wedge a_n$ (Pour les entiers).

Vocabulaire :

Dans l'arithmetique des entiers.
si $a_1 \wedge \dots \wedge a_n = 1$, on dit que $a_1, \dots, a_n$.
sont premiers entre eux dans leurs ensemble.

Voc :

1/ Dans l'arithm des polynômes :

Si $A_1 \wedge \dots \wedge A_n = 1$, on dit que les polynômes $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble.

2/ $\begin{pmatrix} A_1, \dots, A_n \text{ premier} \\ \text{entr eux 2 à 2} \end{pmatrix} \Rightarrow \begin{pmatrix} A_1, \dots, A_n \text{ premiers entre} \\ \text{eux dans leur ensembles} \end{pmatrix}$

Car $A_1 \wedge A_2 \wedge \dots \wedge A_n = 1 \wedge (A_3 \wedge \dots \wedge A_n) = 1$

La réciproque est en générale fausse.

Prop (Thm de Bezout)

1/ $A \wedge B = 1 \iff \exists U, V \in \mathbb{K}[X],\ AU + BV = 1$

2/ $A_1 \wedge \dots \wedge A_n = 1 \iff \exists U_1, \dots, U_n \in \mathbb{K}[X],\ \sum_{i=1}^{n} A_i U_i = 1$

Prop : $\forall a \neq b,\ (X-a) \wedge (X-b) = 1$

Prop :

Si $A \wedge B = 1$ alors $A^m \wedge B^s = 1$

et ce, pour tout $m, s \in \mathbb{N}$.

Corollaire :

Si $a_1, \dots, a_n \in \mathbb{K}$ distincts 2 à 2, alors

$(X-a_1)^{S_1}, \dots, (X-a_n)^{S_n}$ sont 2 à 2 premiers entre

eux, et ce pour tout $S_1, \dots, S_n \in \mathbb{N}$.

Prop : Lemme d'Euclide :

Si $(A/P,\ B/P,\ A\wedge B=1)$ alors AB/P.

Prop (Lemme de Gauss)

Si $\begin{cases} A/(BC) \\ A\wedge B = 1 \end{cases}$ alors A/C

Prop :

Les éléments inversibles de l'anneau $(\mathbb{K}[X],+,\times)$ sont les polynômes constants non nuls.

C-à-d $\quad \mathcal{U}(\mathbb{K}[X]) = \mathbb{K}^*$

NB : $P(X) = \prod_{i=1}^{n} (X-a_i)^{m_i}$, m_i multiplicité de a_i

$Q(X) = \prod_{i=1}^{n} (X-a_i)^{r_i}$, r_i multiplicité de a_i

On a : $P/Q \iff \forall i \in [\![1,n]\!],\ m_i \leq r_i$