

Polynômes

Remarque : \mathbb{K} désigne \mathbb{R} ou \mathbb{C} . C'est le **corps des scalaires** dans lequel on va prendre les coefficients des polynômes.

1 Polynômes à une indéterminée sur le corps \mathbb{K}

Définition

On appelle **polynôme** sur \mathbb{K} toute expression de la forme :

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + a_nX^n = \sum$$

où $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{K}$ sont les **coefficients** de $P(X)$.

X est appelée l'**indéterminée** ; on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .

Remarque : le polynôme $P(X)$ est parfois simplement noté P .

Définition

Soit $P(X) = \sum_{k=0}^n a_k X^k$ un élément de $\mathbb{K}[X]$.

- On dit que P est le **polynôme nul** lorsque :
On le note 0 (ou $0_{\mathbb{K}[X]}$ si on veut insister sur la différence avec $0_{\mathbb{K}}$).
- Si $P \neq 0$, on appelle **degré** du polynôme $P(X)$ le plus grand indice dont le coefficient est non nul ; on le note $\deg P$.
- On pose $\deg 0 = -\infty$.
- On dit que P est un **polynôme constant** lorsque
- Pour $n \in \mathbb{N}$ on note $\mathbb{K}_n[X]$ l'ensemble des polynômes dont le degré est inférieur ou égal à n :
$$\mathbb{K}_n[X] =$$
- Le **coefficient dominant** de P est
- On dit que P est **unitaire** si
- On dit que P est un **monôme** (de degré d) si P est de la forme

Exemples :

$$\deg (X^4 - 5X^3 + 9i) =$$

$$\deg (0.X^3 - 3X + X^2) =$$

$$\deg \left(\sum_{k=1}^3 k! X^{2k} \right) =$$

Un polynôme unitaire :

Un monôme qui n'est pas un polynôme unitaire :

Remarques :

- a) Poser $\deg 0 = -\infty$ sert à rendre consistantes des propriétés que l'on verra plus loin dans le cas particulier du polynôme nul. Cela assure également que $0 \in \mathbb{K}_n[X]$ pour tout $n \in \mathbb{N}$.
- b) On fera la confusion entre \mathbb{K} et $\mathbb{K}_0[X]$.

c) Soit P un polynôme de degré d . On a alors $P = \sum_{k=0}^d a_k X^k$.

On peut poser, pour tout $k > d$, $a_k = 0$ et on a alors $P = \sum_{k=0}^{+\infty} a_k X^k$. Cette "astuce" va nous servir dans la définition ci-dessous.

Définition

Soit $\lambda \in \mathbb{K}$ et deux polynômes de $\mathbb{K}[X]$: $P(X) = \sum_{k=0}^n a_k X^k$ et $Q(X) = \sum_{k=0}^d b_k X^k$. On définit les opérations classiques d'addition, multiplication par un nombre, produit (de polynômes) et composition :

$$P + Q =$$

$$\lambda.P =$$

$$P \times Q =$$

$$P \circ Q =$$

Exemple : on considère $P(X) = X^2 - 3X + 5$ et $Q(X) = X^3 - 1$. Calculer les polynômes :

$$P + Q =$$

$$P \times Q =$$

$$P \circ Q =$$

$$Q \circ P =$$

Remarques :

a) L'addition et le produit sont **commutatifs**, mais pas la composition. On ne démontre pas les propriétés « naturelles » des opérations dans $\mathbb{K}[X]$, notez cependant que le produit est **intègre** ce qui veut dire

b) Dans $\mathbb{K}[X]$, on peut additionner et multiplier par un scalaire, on peut donc faire des

Proposition

(Conséquence des opérations sur le degré).

Soient P et Q deux polynômes non nuls. On a :

- Si $\deg(P) \neq \deg(Q)$, $\deg(P + Q) =$
- Si $\deg(P) = \deg(Q)$, $\deg(P + Q) =$
- $\deg(P \times Q) =$
- $\deg(P \circ Q) =$

Démonstration

Par exemple pour le produit, en notant $P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{j=0}^{+\infty} b_j X^j$.

Polynôme formel avec X et fonction polynômiale avec x : quelle différence ?

Etant donné un polynôme P et un scalaire α , on peut calculer $P(\alpha)$. Par exemple, si $P = X^2 + X + 1$ alors $P(2) = 7$. Un polynôme P permet donc de définir une application $\mathbb{K} \rightarrow \mathbb{K}$ et, si on prend \mathbb{R} comme ensemble de départ, on obtient une fonction réelle qu'on dira *polynômiale* : $x \mapsto P(x)$.

Mais on peut également appliquer un polynôme à d'autres objets, par exemple une fonction ou une matrice carrée. Voici une des façons de comprendre la notion de polynôme *formel* : X peut être tout objet pour lequel on sait calculer des sommes et des produits.

2 Arithmétique des polynômes

Définition

Soit A et B deux polynômes.

On dit que A est un **multiple** de B s'il existe un polynôme Q tel que $A = BQ$.

On dit aussi que A est **divisible** par B ou que B est un **diviseur** de A et on note $B|A$.

Exemples :

a) $(X - 1)|(X^4 - 1)$ car $X^4 - 1 = (X - 1)(X^3 + X^2 + X + 1)$.

b) Le polynôme nul

Proposition

Soit A un polynôme non nul. Si B est un diviseur de A alors $\deg B \leq \deg A$.

Démonstration

C'est une conséquence immédiate des propriétés du degré : si $B|A$ alors il existe un polynôme Q tel que $A = BQ$ donc $\deg A = \deg B + \deg Q \geq \deg B$. ■

Remarque : $\deg B \leq \deg A$ est une *condition nécessaire* pour que $B|A$ mais pas une *condition suffisante*.

Par exemple :

Exercice

Trouver tous les diviseurs unitaires de $X^2 + 1$ dans $\mathbb{C}[X]$

Proposition

Soit deux polynômes A et B . Si $A|B$ et $B|A$ alors il existe $\lambda \in \mathbb{K} \setminus \{0\}$ / $A = \lambda B$.

Démonstration

Supposons que $A|B$ et $B|A$: il existe des polynômes Q et R tels que $B = AQ$ et $A = BR$. On a donc $B = BRQ \iff B(1 - RQ) = 0$. Par intégrité du produit dans $\mathbb{K}[X]$, soit $B = 0$ et alors $A = 0$. On a donc $A = 1 \times B$ et la propriété est vraie. Sinon, $1 - RQ = 0 \iff RQ = 1$ ce qui implique, en considérant leurs degrés, que R et Q sont des polynômes constants. Mettons $R = \lambda$ et on a $A = \lambda B$, la propriété est, là encore, vérifiée. ■

Remarque : la propriété précédente est en fait une équivalence (la réciproque est évidente).

Proposition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $B \neq 0$. Il existe un unique couple de polynômes $(Q, R) \in (\mathbb{K}[X])^2$ qui vérifie :

$$\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$$

On dit que $A = BQ + R$ est la **division euclidienne** de A par B , Q est le **quotient**, R est le **reste**.

Démonstration

On garde les notations de la propriété.

- Unicité :

- Existence :

Remarque : on a fourni, une démonstration *constructive*.

Exemple : $X^3 + 3X^2 + X - 5 = X^2(X + 3) + X - 5$ est la division de $X^3 + 3x^2 - 5$ par X^2 .

Par contre, ce n'est pas

Méthode

Pour poser une division euclidienne de polynômes : on procède comme pour une division euclidienne d'entiers : par soustractions successives, en diminuant le degré à chaque étape. On arrête lorsque le reste a un degré strictement inférieur à celui du diviseur.

Exemple : Poser la division euclidienne de $X^5 - X$ par $X + 1$.

Remarque : pour la division dans $\mathbb{K}[X]$ le degré joue dans le rôle de $<$ dans \mathbb{Z} . On dit que c'est le **stathme** de la division euclidienne dans $\mathbb{K}[X]$. (On n'en parlera plus, ça peut néanmoins servir au scrabble).

Proposition

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $B \neq 0$.

$B|A$ si, et seulement si, la division euclidienne de A par B a un reste nul.

Démonstration

Définition

Soit A un polynôme. On dit que A est **irréductible** dans $\mathbb{K}[X]$ lorsque :

- $\deg A > 0$ (autrement dit A n'est pas constant) ;
- les seuls diviseurs de A dans $\mathbb{K}[X]$ sont les polynômes constants et les polynômes de la forme λA (avec λ un scalaire non nul).

Remarque : on dit que les polynômes de la forme λA (avec $\lambda \neq 0$) sont **associés** à A .

Exemple : $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$. En effet, on a trouvé tous ses diviseurs unitaires (exercice précédent) : 1 , $X - i$, $X + i$ et $X^2 + 1$ et tout diviseur de $X^2 + 1$ sera proportionnel à un de ses diviseurs unitaires. Dans $\mathbb{R}[X]$ on ne peut donc pas trouver de diviseur non constant et non proportionnel à $X^2 + 1$.

Proposition

Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.

Démonstration

Soit P , un polynôme de degré 1 de $\mathbb{K}[X]$.

Remarque : si on veut faire l'analogie avec l'arithmétique des entiers, les polynômes irréductibles correspondent aux

On a déjà croisé les polynômes irréductibles lors de

3 Dérivation des polynômes

Définition

Soit le polynôme $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$.

Le **polynôme dérivé** de P est le polynôme P' défini par : $P'(X) =$

Remarque : si $\deg P > 0$, on a donc $\deg P' = \deg P - 1$.

Proposition

On désigne par λ, μ des éléments de \mathbb{K} , par P, Q des polynômes de $\mathbb{K}[X]$.

i. la dérivation est **linéaire** :

ii. $(P \times Q)' =$

iii. $(P \circ Q)' =$

Exemples :

a) Donner la dérivée de $P(X) = 5X^3 + X^7 - 4$

b) Donner la dérivée de $Q(X) = (X + 1)^8$

c) Combien peut-on trouver de polynômes dont la dérivée vaut $5X^2 - 3$?

Remarque : dans le cas où $\mathbb{K} = \mathbb{R}$, le polynôme dérivé correspond à la dérivée de la fonction polynomiale. La différence entre les notions n'est pas cosmétique : la dérivée des fonctions est définie à-partir de calculs de limites pour une variable réelle. Ici, on définit le polynôme dérivé comme un nouveau polynôme, indifféremment du corps \mathbb{K} sur lequel on travaille. (Pour être parfaitement rigoureux, il faudrait donc démontrer que les formules de dérivation sont correctes dans le cadre de la dérivation formelle, c'est laissé en exercice et sera justifié d'une façon différente plus loin dans le chapitre).

Définition

Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. On définit par récurrence la dérivée d'ordre n de P de la façon suivante :

$$P^{(n)}(X) =$$

Exemples :

a) soit $P(X) = X^5$. Calculer $P^{(n)}(X)$ pour $n \in \llbracket 0; 6 \rrbracket$.

b) soit $n \in \mathbb{N}$ et $P(X) = X^n$. Pour $m \in \llbracket 1; n \rrbracket$, calculer $P^{(m)}(X)$.

Proposition

(formule de Leibniz)

Soient $(P, Q) \in (\mathbb{K}[X])^2$ et $n \in \mathbb{N}$. On a : $(PQ)^{(n)} =$

Proposition

Formule de Taylor

Soit $n \in \mathbb{N}^*$, $P \in \mathbb{K}_n[X]$ et $\alpha \in \mathbb{K}$. On a :

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

Démonstration

Soit un polynôme $P = \sum_{k=0}^{+\infty} a_k X^k$ et soit $n \in \mathbb{N}$.

- Si $\alpha = 0$, on remarque que $P(0) = a_0$, $P'(0) = a_1$ et, par une récurrence immédiate :
 $\forall k \geq 0, P^{(k)}(0) = k!a_k \iff a_k = \frac{P^{(k)}(0)}{k!}$, d'où la formule de Taylor.
- Si $\alpha \neq 0$, on pose $Q(X) = P(X + \alpha)$.

On applique la formule de Taylor à Q en 0 : $Q(X) = \sum_{k=0}^n \frac{Q^{(k)}(0)}{k!} X^k$.

Or, pour tout $k \in \mathbb{N}$, $Q^{(k)}(0) = P^{(k)}(\alpha)$.

En composant avec $X - \alpha$, il vient $P(X) = Q(X - \alpha) = \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$.

Exercice

(Facultatif) Démontrer la formule de Taylor par récurrence sur le degré du polynôme P .

4 Racine d'un polynôme

Définition

Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine de P lorsque

Exemples :

- 3 est racine de $P(X) = X^2 - X - 6$:
- Donner un polynôme dont -2 est racine :
- Donner un polynôme dont π est racine :
- Donner un polynôme dont 1 n'est pas racine :

Proposition

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

α est racine de P si, et seulement si, $(X - \alpha) | P$.

Démonstration

■

Remarque : dans la démonstration, on a également prouvé que $P(\alpha) = R(\alpha)$.

Proposition

Un polynôme de degré $n > 0$ admet, au plus, n racines distinctes.

Démonstration

Soit $P \in \mathbb{K}[X]$ ayant pour racines distinctes $\alpha_1, \dots, \alpha_n$. Par une récurrence immédiate on obtient que $\prod_{i=1}^n (X - \alpha_i) | P(X)$. On en déduit que $\deg P \geq \deg \left(\prod_{i=1}^n (X - \alpha_i) \right) \iff \deg P \geq n$. ■

Méthode

Pour prouver que deux polynômes P et Q sont égaux :

1. il faut que leur degré soit égal, notons-le n ;
2. si $P - Q$ a plus de n racines alors $P - Q$ est le polynôme nul, autrement dit : $P = Q$.

Remarque : la méthode précédente permet de valider les formules de dérivation formelle des polynômes qu'on a « récupéré » de la dérivation des fonctions polynômiales.

Par exemple, pour le produit de deux polynômes P et Q : $(PQ)'$ est un polynôme, $P'Q + PQ'$ en est *a priori* un autre. Or, on sait que les fonctions polynômiales associées sont identiques, le polynôme $(PQ)' - (P'Q + PQ')$ a donc une infinité de racines, on déduit que c'est le polynôme nul ; autrement dit : $(PQ)' = P'Q + PQ'$.

Définition

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P .

On appelle (**ordre de**) **multiplicité** de la racine α le plus grand entier n tel que $(X - \alpha)^n | P$.

Remarque : toute racine du polynôme P a une multiplicité qui est dans $\llbracket 1; \deg P \rrbracket$.

Exemple : soit $P = 3X^3 - 5X^2 + X + 1$.

a) Prouver que 1 est racine de P

b) Déterminer la multiplicité de 1

Théorème

Soit P , un polynôme de $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$ une racine de P et $n \in \mathbb{N}^*$.

n est l'ordre de multiplicité de α si, et seulement si :

$$P(\alpha) = P'(\alpha) = \dots = P^{(n-1)}(\alpha) = 0 \quad \text{et} \quad P^{(n)}(\alpha) \neq 0.$$

Exemple : on reprend l'exemple précédent.

$$P' = \quad \quad \quad \text{et} \quad P'(1) =$$

$$P^{(2)} = \quad \quad \quad \text{et} \quad P^{(2)}(1) =$$

Démonstration

Ce théorème est une conséquence directe de ■

Proposition

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ une racine de P de multiplicité $r \geq 2$.

Alors, α est une racine de P' de multiplicité

Remarques :

- C'est un corollaire du théorème précédent.
- Si $\alpha \in \mathbb{K}$ est racine simple de P alors α n'est pas racine de P' . On aurait pu intégrer cette situation à l'énoncé précédent en posant que les scalaires qui ne sont pas racines d'un polynôme ont pour multiplicité 0.

Proposition

Soit $P \in \mathbb{R}[X]$ et α un nombre complexe non réel qui est une racine de P .

Si α a pour multiplicité $m \in \mathbb{N}^*$, alors $\bar{\alpha}$ est aussi une racine de P de multiplicité m .

Démonstration

C'est une conséquence de la linéarité de la conjugaison :

5 Théorème de D'Alembert-Gauss et conséquences

5.1 Polynômes scindés

Définition

Soit $P \in \mathbb{K}[X]$. On dit que P est **scindé** s'il est possible de l'écrire sous la forme :

$$P(X) = \lambda(X - x_1)(X - x_2) \dots (X - x_n) \quad \text{avec } (\lambda, x_1, \dots, x_n) \in \mathbb{K}^{n+1}$$

n est alors le degré de P et λ son coefficient dominant.

Remarque : dans la définition précédente, les x_i sont les racines de P mais ne sont pas nécessairement distincts deux-à-deux. On peut reformuler la définition ainsi :

$$P(X) = \lambda(X - \alpha_1)^{n_1} \dots (X - \alpha_r)^{n_r} \quad \text{avec } i \neq j \implies \alpha_i \neq \alpha_j$$

Alors, n_i est la multiplicité de la racine α_i et on a $n_1 + \dots + n_r = \deg P$.

Théorème

(D'Alembert-Gauss)

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

Remarques :

- attention, ce n'est pas vrai sur \mathbb{R} ! Un contre-exemple :
- On peut reformuler le théorème : sur \mathbb{C} , toute équation polynomiale de degré n a n solutions (en comptant les multiplicités).
- Ce théorème assure l'existence de racines, mais il ne dit pas comment les trouver.
- Le théorème de D'Alembert Gauss est très important, il est d'ailleurs également appelé *théorème fondamental de l'algèbre*. Sa démonstration est hors programme.

5.2 Décomposition d'un polynôme en produit de facteurs irréductibles

Du théorème de D'Alembert-Gauss, on déduit la nature des polynômes irréductibles sur \mathbb{C} et \mathbb{R} :

Proposition

- i. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- ii. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 **ainsi que** les polynômes de degré 2 dont le discriminant est strictement négatif.

Théorème

Tout polynôme P de $\mathbb{K}[X]$ se décompose en un produit de polynômes irréductibles.

Exemples :

a) décomposer $X^3 - X^2 - 4$ en produit de polynômes irréductibles sur $\mathbb{R}[X]$ puis sur $\mathbb{C}[X]$.

b) décomposer $X^6 - 1$ en produit de polynômes irréductibles sur $\mathbb{C}[X]$ puis sur $\mathbb{R}[X]$.

5.3 Somme et produit des racines d'un polynôme

Proposition

Soit un polynôme de $\mathbb{K}[X]$, $P(X) = \sum_{k=0}^n a_k X^k$. Sur \mathbb{C} , P est scindé et s'écrit :

$$P(X) = a_n(X - x_1)(X - x_2) \dots (X - x_n)$$

Alors :

- i. $x_1 \times x_2 \times \dots \times x_n = (-1)^n \frac{a_0}{a_n}$
- ii. $x_1 + x_2 + \dots + x_n = -\frac{a_{n-1}}{a_n}$

Démonstration

Il suffit de développer le produit $P(X) = a_n(X - x_1)(X - x_2) \dots (X - x_n)$ et de considérer les coefficients de degré 0 et $n - 1$. ■

On reprend la proposition précédente dans le cas particulier des polynômes de degré 2 :

Proposition

Soit $P(X) = aX^2 + bX + c$ un polynôme de $\mathbb{K}[X]$ (avec $a \neq 0$) et r_1, r_2 ses racines. On a :

$$r_1 \times r_2 = \quad \quad \quad \text{et} \quad \quad \quad r_1 + r_2 =$$

Exercice

Déterminer deux complexes dont la somme vaut $1 + i$ et le produit vaut 2.