

Polynômes : à retenir (J-Y D)

On se place ici sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} .

Notation

(a) L'ensemble des polynômes à coefficients dans \mathbb{K} est :

$$\mathbb{K}[X] := \{a_n X^n + \cdots + a_1 X + a_0 ; n \in \mathbb{N} \text{ et } a_0, a_1, \dots, a_n \in \mathbb{K}\}.^{(*)}$$

(b) Soit $N \in \mathbb{N}$. On note : $\mathbb{K}_N[X] = \{a_N X^N + \cdots + a_1 X + a_0 ; a_0, a_1, \dots, a_N \in \mathbb{K}\}$.

(c) Soient $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$, $x \in \mathbb{K}$ et $Q \in \mathbb{K}[X]$. On pose :

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \text{ et } P(Q) = a_n Q^n + \cdots + a_1 Q + a_0.$$

Définition-Proposition

(a) Une fonction polynomiale sur \mathbb{K} est une application f de \mathbb{K} dans \mathbb{K} telle qu'il existe un polynôme P à coefficients dans \mathbb{K} pour lequel $f(x) = P(x)$ pour tout $x \in \mathbb{K}$.

Dans ce cas : si $f = 0$ alors $P = 0$ (calculer les dérivées successives de $f|_{\mathbb{R}}$ en 0).

(b) Le *degré* d'un polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ non nul, noté $\deg P$, est le plus grand $d \in \mathbb{N}$ tel que $a_d \neq 0$. Par convention on pose : $\deg 0 := -\infty$.

(c) Un *polynôme unitaire* de degré n ($n \in \mathbb{N}$) est un polynôme de la forme suivante :

$$P = a_n X^n + \cdots + a_1 X + a_0 \text{ avec } a_0, \dots, a_n \in \mathbb{K} \text{ et } a_n = 1.$$

Proposition

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

(a) On a : $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ et $\deg(PQ) = \deg(P) + \deg(Q)$.

En particulier : si $PQ = 0$ alors $P = 0$ ou $Q = 0$.

(b) On a : $(P + Q)^n = \sum_{k=0}^n \binom{n}{k} P^{n-k} Q^k$ pour tout $n \in \mathbb{N}$ « formule du binôme de Newton ».

(c) On a : $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(n-k)} Q^{(k)}$ pour tout $n \in \mathbb{N}$ « formule de Leibniz ».

Définition

Soient $A, B \in \mathbb{K}[X]$. On dit que B *divise* A (ou A est *multiple de* B), et note $B \mid A$, si :

$$\text{il existe } Q \in \mathbb{K}[X] \text{ tel que } A = BQ.$$

Théorème

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$. Il existe un unique $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$A = BQ + R \text{ et } \deg R < \deg B \text{ « division euclidienne de } A \text{ par } B \text{ ».}$$

Dans ce cas, R s'appelle *le reste* et Q s'appelle *le quotient*, de la division de A par B .

Définition-Proposition

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

On dit que r est *racine de* P si r vérifie l'une des deux propriétés équivalentes suivantes :

- (i) $P(r) = 0$ (**);
- (ii) $X - r$ divise P .

(*) Du point de vue mathématique, le polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ est en fait la suite a_0, \dots, a_n de ses coefficients, autrement dit la suite $P = (a_k)_{k \geq 0}$ d'éléments de \mathbb{K} obtenue en posant $a_k = 0$ quand $k > n$.

Le symbole X représente donc la suite $(a_k)_{k \geq 0}$ qu'on obtient en choisissant $a_1 = 1$ et $a_k = 0$ quand $k \neq 1$.

(**) De même que personne ne résout l'équation $r^2 - 1 = 0$ en écrivant « $\pi^2 - 1 = 0 \iff \pi \in \{-1, 1\}$ », on ne cherchera pas les racines du polynôme $X^2 - 1$ en écrivant « $X^2 - 1 = 0 \iff X \in \{-1, 1\}$ », mais en écrivant :

$$\forall r \in \mathbb{K} \quad r^2 - 1 = 0 \iff r \in \{-1, 1\}.$$

Corollaire

Un polynôme non-nul $P \in \mathbb{K}[X] \setminus \{0\}$ de degré n a au plus n racines dans \mathbb{K} .

Lemme (« formule de Taylor »)

Soit $n \in \mathbb{N}$. Pour tous $P \in \mathbb{K}_n[X]$ et $r \in \mathbb{C}$, on a :

$$P(X) = P(r) + \frac{P'(r)}{1!}(X-r) + \dots + \frac{P^{(n)}(r)}{n!}(X-r)^n.$$

Définition-Proposition

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

(a) On appelle *ordre de multiplicité de r dans P* l'unique $m \in \mathbb{N}$ tel que :

$$(X-r)^m \text{ divise } P \quad \text{et} \quad (X-r)^{m+1} \text{ ne divise pas } P.$$

$m = 1$: « r est racine simple de P » ; $m \geq 2$: « r est racine multiple de P ».

(b) L'ordre de multiplicité m de r dans P est caractérisé (sachant que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}) par :

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

Définition

Un *polynôme irréductible à coefficients dans \mathbb{K}* est un élément P de $\mathbb{K}[X]$ non-constant tel que les seules égalités $P = AB$ avec $A, B \in \mathbb{K}[X]$ s'obtiennent quand A ou B est constant.

Théorème

Soit $P \in \mathbb{K}[X] \setminus \{0\}$.

(a) Il existe $\lambda \in \mathbb{K} \setminus \{0\}$, $k \in \mathbb{N}$, des polynômes unitaires irréductibles distincts P_1, \dots, P_k et $\alpha_1, \dots, \alpha_k \in \mathbb{N} \setminus \{0\}$, tels que : $P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$.

(b) Pour toute autre décomposition $P = \mu Q_1^{\beta_1} \dots Q_l^{\beta_l}$, on a :

$$\mu = \lambda \quad \text{et} \quad \{(Q_1, \beta_1), \dots, (Q_l, \beta_l)\} = \{(P_1, \alpha_1), \dots, (P_k, \alpha_k)\}.$$

(c) Quand P est décomposé comme au (a), les éléments de $\mathbb{K}[X]$ qui divisent P sont les polynômes de la forme $\mu P_1^{\beta_1} \dots P_k^{\beta_k}$ avec $\mu \in \mathbb{K} \setminus \{0\}$ et $0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_k \leq \alpha_k$.

Remarque

Soient $P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k} \in \mathbb{K}[X] \setminus \{0\}$ comme ci-dessus et $r \in \mathbb{K}$.

On a : r est racine de P si et seulement si $X-r$ est l'un des P_i , $1 \leq i \leq k$.

Dans ce cas α_i est la multiplicité de la racine r de P .

Théorème

 (« théorème de d'Alembert-Gauss »)

Tout polynôme non-constant à coefficients dans \mathbb{C} a au moins une racine dans \mathbb{C} .

On en déduit que :

- les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1 ;
- les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.