Polynômes

Lundi 16 Février 2017

Structure Algébrique.

Définition :
Un polynôme à coefficient dans $\mathbb{K}$ est la donnée d'une suite (a_k) d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang. Cette suite est alors notée $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0$. L'ensemble des polynômes se note $\mathbb{K}[X]$, où X s'appelle l'indéterminée.

Sur $\mathbb{K}[X]$ on définit les lois suivantes, si $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0$, $Q(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_0$, $\lambda \in \mathbb{K}$, on pose alors :

$$\boxed{\begin{array}{l}(P+Q)(X) = \displaystyle\sum_{k=0}^{\max(n,m)} (a_k + b_k)X^k \\ (\lambda P)(X) = \displaystyle\sum_{k=0}^{n} \lambda a_k X^k \\ (PQ)(X) = \displaystyle\sum_{k=0}^{n+m} c_k X^k \text{ tel que } c_k = \sum_{i=0}^{k} a_i b_{k-i}\end{array}}$$

Avec la généralisation $a_k = 0 \quad \forall k \geqslant n+1, b_k = 0 \quad \forall k \geqslant m+1$.
$\mathbb{K}[X]$ est stable pour ces lois, on dit alors que c'est une algèbre.

Degré d'un polynôme.

Définition :
Soit P un polynôme non nul, on appelle degré de P, le plus grand indice de ses coefficients non nuls, et on le note $\deg P$.
Ainsi $\deg P = n \Leftrightarrow P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0$ avec $a_n \neq 0$, a_n s'appelle coefficient dominant de P et se note $\mathrm{co}(P)$. Par convention $\deg 0 = -\infty$.

Remarque.

$$P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 \Leftrightarrow \deg P \leqslant n$$

Théorème :

$$\deg(P+Q) \leqslant \max(\deg P, \deg Q)$$

Avec égalité dans le cas où $\deg P \neq \deg Q$ ou bien $\deg P = \deg Q$ mais $\deg P + \deg \neq 0$.

Théorème :
$\deg(PQ) = \deg P + \deg Q$. En particulier si λ, constante non nulle alors : $\deg \lambda P = \deg P$.

Remarque.
Pour $n \in \mathbb{N}$, on note par $\mathbb{K}_n[X]$ l'ensemble des polynômes de degrés inférieurs à n, on a $\mathbb{K}_n[X]$ est stable pour la somme et la multiplication par une constante, c'est un sous-espace vectoriel de $\mathbb{K}[X]$. En particulier $\mathbb{K}_0[X] = K$.

Division dans $\mathbb{K}[X]$.

Définition :

Soit A, B deux polynômes non nuls, on dit que B divise A dans $\mathbb{K}[X]$ si et seulement si $\exists Q \in \mathbb{K}[X]$ tel que $A = BQ$.

Remarque.
Si B divise A, alors $\deg B \leqslant \deg A$, en particulier un polynôme ne peut pas diviser un autre polynôme de degré inférieur strictement.

Vocabulaire.

- Deux polynômes P, Q sont dits associés si et seulement si $\exists \lambda \neq 0$ tel que $P = \lambda Q$.
- Un polynôme est dit irréductible dans $\mathbb{K}[X]$ si et seulement si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes ou ses polynômes associés.

Remarque.
Deux polynômes P et Q sont associés si et seulement si P divise Q avec $\deg P = \deg Q$. En particulier tout polynôme de degré 1 est irréductible.

Théorème :

$\forall (A, B) \in \mathbb{K}[X]$ tel que $B \neq 0$ $\exists ! (Q, R) \in \mathbb{K}[X]$ tel que $A = BQ + R$ avec $\deg R < \deg Q$. Q s'appelle le quotient de la division euclidienne de A par B et R son reste.

Remarque.
B divise A si et seulement si le reste de la division euclidienne de A par B est nul.

Algorithme d'Euclide.
Soit A, B deux polynôme non nuls, on effectue les divisions euclidiennes successives des quotients par leurs restes, jusqu'à arriver à un reste nul, alors le dernier reste non nul est un diviseur commun de A et B de degré minimal, ce reste un fois normalisé, s'appelle le PGCD de A et B et se note $A \wedge B$.

Propriétés.
le PGCD est commutatif, associatif et ne change pas si l'on multiplie l'un des polynômes par une constante.

Vocabulaire.
Deux polynômes sont dits premiers entre eux si leur PGCD est égal à 1.

Proposition :

Soient P et Q deux polynômes non nuls, et D leurs PGCD, alors

$$P = DP', Q = DQ' \text{ avec } Q \wedge Q' = 1$$

Remarque.
Si P polynôme irréductible et Q polynôme quelconque, alors $P \wedge Q = 1$ ou P, en particulier deux polynômes irréductibles distincts sont toujours premiers entre eux.

Théorème :

Théorème de Bezout. Soit $(A, B) \in \mathbb{K}[X]$ tel que $A \wedge B = 1$ alors

$$\exists (A, B) \in \mathbb{K}[X] \text{ tel que } AU + BV = 1$$

Théorème :

Théorème de Gauss. Soit $(A, B, C) \in \mathbb{K}[X]$ tel que A divise BC et $A \wedge B = 1$ alors A divise C.

Conséquences.

- $A \wedge B = A \wedge C = 1 \Rightarrow A \wedge BC = 1$.
- $A \wedge B = 1 \Leftrightarrow A \wedge B^\beta = 1 \Leftrightarrow A^\alpha \wedge B^\beta = 1$.
- Si A et B divisent C et sont premiers entre eux, alors AB divise C.

Racines d'un polynôme :

Définition :

A chaque polynôme $P(X) = a_n X^n + \ldots + a_0 \in \mathbb{K}[X]$, on associé la fonction réelle :

$$\begin{aligned} \widehat{P}(x) : \mathbb{K} &\to \mathbb{K} \\ x &\mapsto a_n x^n + \ldots + a_0 \end{aligned}$$

appelée fonction polynômiale de P et on dit que $\alpha \in K$ est une racine de P si et seulement si $\widehat{P}(\alpha) = 0$, dans la suite on notera $P(\alpha) = 0$ au lieu de $\widehat{P}(\alpha)$.

Théorème :

Soit $P \in \mathbb{K}[X], \alpha \in K$, alors α est une racine de P si et seulement si $X - a$ divise P dans $\mathbb{K}[X]$.

Conséquences.

- Un polynôme irréductible dans $\mathbb{K}[X]$ de degré $\geqslant 2$ n'admet jamais de racine dans $\mathbb{K}$.
- Un polynôme, non nul de degré $n \in \mathbb{N}$ admet au maximum n racines.
- Tout polynôme qui admet un nombre de racines supérieur strictement à son degré est nul, en particulier tout polynôme qui admet une infinité de racines est nul.

lemme 1.
Tout polynôme, non constant admet au moins un facteur (diviseur) irréductible.

Théorème :

Tout polynôme, non constant, P se décompose de façon unique en facteurs irréductibles sous la forme

$$P = \lambda P_1^{\alpha_1} \ldots P_r^{\alpha_r}$$

avec $\lambda \in \mathbb{K}$, $\alpha_i \in \mathbb{N}^*$ et P_i des polynômes irréductibles unitaires.

Théorème :

Théorème de D'Alembert
Tout polynôme, non constant admet au moins une racine dans $\mathbb{C}$.

Conséquences.

- Les polynômes irréductibles dans $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
En particulier la décomposition de P dans $\mathbb{C}[X]$ est de la forme
$$P(X) = \lambda(X - z_1)^{\alpha_1} \dots (X - z_r)^{\alpha_r}$$
où les z_i sont les racines de P.
- Les polynômes irréductibles dans $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 ou ceux de degré 2 à discriminant strictement négatif.
En particulier la décomposition de P dans $\mathbb{R}[X]$ est de la forme
$$P(X) = \prod_{i=1}^{r} \lambda(X - x_i)^{\alpha_i} \prod_{i=1}^{p} (X^2 - 2\mathfrak{Re}(z_i) + |z_i|^2)^{\beta_i}$$
où les x_i sont les racines réelles de P et z_i ceux complexes non réelles.
Il faut noter que si $P \in \mathbb{R}[X]$ et $z \in \mathbb{C} \diagup \mathbb{R}$ racine de P, alors $\overline{z}$ aussi racine de P.

Dérivation dans $\mathbb{K}[X]$.

Définition :
Soit $P(X) = a_n X^n + \dots + a_0$, on appelle polynôme dérivé de P, le polynôme noté P' défini par $P'(X) = n a_n X^{n-1} + \dots + a_1$.

Propriétés.

- Si $\deg P = n$, alors $\deg P' = n - 1$ et $co(P') = n co(P)$. En particulier la dérivée d'un polynôme est nul si et seulement si il est constant.
- $\forall (P, Q) \in \mathbb{K}[X]^2 \quad \forall \lambda \in \mathbb{K}$, on a : $(P + \lambda Q)' = P' + \lambda Q'$, en conséquence l'application : $\begin{array}{rcl} \mathbb{K}_n[X] & \to & \mathbb{K}_{n-1}[X] \\ P(X) & \mapsto & P'(X) \end{array}$ est linéaire.

Définition :
Soit $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}^*$, on définit par récurrence la dérivée *k–ème* de P à l'aide de la formule $P^{(k)} = (P^{(k-1)})' = (P')^{(k-1)}$.
Et on convient d'écrire $P^{(0)} = P$.

- Si $\deg P = n$, alors $\deg P^{(k)} = n - k$ et $co P^{(k)} = A_n^k co P$, avec la convention $\mathcal{A}_n^k = 0$ si $k > n$.
En particulier la dérivée *k–ème* d'un polynôme est nul si et seulement si ce polynôme est de degré inférieur à $k - 1$.
- Si $\deg = n$ alors $P^{(n)} = n! co P$.
- $\forall (P, Q) \in \mathbb{K}[X]^2 \quad \forall \lambda \in \mathbb{K}$, on a : $(P + \lambda Q)^{(k)} = P^{(k)} + \lambda Q^{(k)}$, en conséquence l'application : $\begin{array}{rcl} \mathbb{K}_n[X] & \to & \mathbb{K}_{n-k}[X] \\ P(X) & \mapsto & P^{(k)}(X) \end{array}$ est linéaire.
- $\forall (P, Q) \in \mathbb{K}[X]^2 \quad \forall n \in \mathbb{N}$ on a : $(PQ)^{(n)} = \sum_{k=0}^{n} \mathcal{C}_n^k P^{(k)} Q^{(n-k)}$ Formule de Leibniz

Définition :
Soit $P \in \mathbb{K}[X]$, on dit qu'une racine $a \in \mathbb{K}$ de P est de multiplicité $n \in \mathbb{N}^*$ si et seulement si $P(a) = \dots P^{(n-1)}(a) = 0$ mais $P^{(n)}(a) \neq 0$. Et convient de dire que a est multiplicité nulle dans P lorsqu'elle n'est pas une racine de P.

Théorème :

Soit $P \in \mathbb{K}[X]$, $\forall n \in \mathbb{N}$, $\quad \forall a \in \mathbb{K}$ on a : $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

Théorème :

Soit $P \in \mathbb{K}[X], n \in \mathbb{N}$ et $a \in \mathbb{K}$, les propriétés suivantes sont équivalentes :

- a est une racine de P de multiplicité n
- $(X-a)^n$ divise P, $(X-a)^{n+1}$ ne divise pas P.
- $\exists Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^n$ avec $Q(a) \neq 0$.

Polynômes scindés.

Définition :

On dit qu'un polynôme $P \in \mathbb{K}[X]$ est scindé dans $\mathbb{K}$ si et seulement si toutes ses racines sont dans $\mathbb{K}$.

Remarques.

- Tout polynôme non constant est scindé dans $\mathbb{C}$.
- Un polynôme $P \in \mathbb{R}[X]$ est scindé dans $\mathbb{R}$ si et seulement si toutes ses racines sont réelles.

Théorème :

Soit $P \in \mathbb{K}[X]$ scindé dans $\mathbb{K}$, alors $P(X) = \mathrm{co}(P)\prod_{k=1}^{n}(X-z_k)^{\alpha_k}$ où z_k sont les racines de P et α_k leurs multiplicités respectives.

En particulier $\deg P = \sum_{k=1}^{n} \alpha_k$.

Formules de Newton entre racines et coefficients d'un polynôme scindé :
Soit $P(X) = a_n X^n + \ldots + a_0$ un polynôme scindé de degré n, et $z_1, \ldots, z_n$ ses racines distincts ou non, on a les formules suivantes :

$$\boxed{\begin{array}{l}
\displaystyle\sum_{k=0}^{n} z_k = -\frac{a_{n-1}}{a_n} \\
\displaystyle\sum\prod_{i<j} z_i z_j = \frac{a_{n-2}}{a_n} \\
\displaystyle\sum\prod_{i_1<\ldots<i_k} z_{i_1}\ldots z_{i_k} = (-1)^k\frac{a_{n-k}}{a_n} \\
\displaystyle\prod_{k=1}^{n} z_k = (-1)^n\frac{a_0}{a_n}
\end{array}}$$

FIN