Une construction de l'algèbre des polynômes

Marc Lorenzi

8 février 2021

Soit $\mathbb{K}$ un corps. Nous allons dans cet article prouver le théorème suivant.

Proposition 1. Il existe un couple $(\mathbb{A}, X)$ vérifiant

- $\mathbb{A}$ est une $\mathbb{K}$-algèbre commutative.
- $X \in A$.
- La famille $(X^k)_{k\geq 0}$ est une base de l'espace vectoriel $\mathbb{A}$.

Si $(\mathbb{B}, Y)$ est un autre couple vérifiant ces propriétés, alors il existe un et un seul isomorphisme d'algèbres $\varphi : \mathbb{A} \to \mathbb{B}$ tel que $\varphi(X) = Y$.

1 Introduction

1.1 Notion de polynôme

Un *polynôme à coefficients dans* $\mathbb{K}$ est une suite presque nulle d'éléments de $\mathbb{K}$, c'est à dire dont tous les termes sont nuls sauf un nombre fini.

Pour tout $n \in \mathbb{N}$, soit

$$X_n = (0, \dots, 0, 1, 0, \dots)$$

où le 1 est en $n$ième position. On pose en particulier $X = X_1$. Au vu de notre définition, les X_n sont donc des polynômes.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Remarque. D'où vient la notation $\mathbb{K}[X]$? L'idée est de construire une algèbre qui contient le corps $\mathbb{K}$ et une *indéterminée* $X \notin \mathbb{K}$. Une telle algèbre doit aussi contenir $X^2, X^3, \dots$ et toutes les combinaisons des puissances de X, bref, tous les objets de la forme $\sum_{k=0}^{\infty} a_k X^k$ où les $a_k \in \mathbb{K}$ sont presque tous nuls. Notre choix de représenter $\mathbb{K}[X]$ par l'ensemble des suites presque nulles d'éléments de $\mathbb{K}$ en vaut un autre : il reste évidemment à mettre sur $\mathbb{K}[X]$ des *opérations* qui lui donneront les propriétés voulues.

1.2 Degré

Definition 1. Soit $A = (a_k)_{k\geq 0}$ un polynôme non nul. Le *degré* de A, noté d^oA, est le plus grand entier k tel que $a_k \neq 0$. On pose également $d^o0 = -\infty$.

Par exemple, $d^o(1, 0, 2, 0, -4, 3, 0, 0, \dots) = 5$.

1.3 Structure d'espace vectoriel

Munissons $\mathbb{K}^{\mathbb{N}}$ des opérations usuelles d'addition de deux suites et de multiplication d'une suite par un scalaire. Ces opérations font de $\mathbb{K}^{\mathbb{N}}$ un $\mathbb{K}$-espace vectoriel.

Proposition 2. Soient A et B deux polynômes et λ un scalaire. Alors $A+B$ et λA sont encore des polynômes. De plus,

- $d^o(A+B) \leq \max(d^oA, d^oB)$
- Si $\lambda \neq 0$, $d^o(\lambda A) = d^oA$
- Si $\lambda = 0$, $d^o(\lambda A) = -\infty$

Démonstration. Facile, laissée en exercice. □

Corollaire 3. $\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$. La famille $(X_k)_{k\geq 0}$ est une base de $\mathbb{K}[X]$.

Démonstration. La stabilité pour l'addition et le produit par un scalaire sont une conséquence immédiate de la proposition 1. La famille $(X_k)_{k\geq 0}$ est une base de $\mathbb{K}[X]$ car

$$(a_0, a_1, a_2, \ldots) = a_0X_0 + a_1X_1 + a_2X_2 + \ldots$$

□

Tout polynôme A s'écrit donc de façon unique

$$A = \sum_{k=0}^{\infty} a_k X_k$$

où les a_k sont des scalaires presque tous nuls. Les a_k sont les *coefficients* du polynôme A.

Convention. Nous noterons systématiquement les polynômes par des lettres majuscules A, B, etc. Les coefficients des polynômes seront notés par les lettres minuscules correspondantes a_k, b_k, etc.

2 Structure d'anneau

2.1 Produit

Soient $A, B \in \mathbb{K}[X]$. On considère la suite C définie pour tout entier k par

$$c_k = \sum_{i+j=k} a_i b_j$$

Par exemple,

$$(1,2,2,0,0,\ldots) \times (2,1,0,0,\ldots) = (2,5,6,2,0,0,\ldots)$$

Proposition 4. C est un polynôme.

Démonstration. Si $A = 0$ ou $B = 0$, c'est évident car alors $C = 0$. Supposons donc A et B non nuls. Soient d et d' les degrés de A et B. Soit $k > d + d'$. Si $i > d$, alors $a_i = 0$. Si $i \leq d$, alors $j = k - i \geq k - d > d'$ et donc $b_j = 0$. Ainsi, $c_k = 0$. On en déduit que C est un polynôme, et que de plus $d^oC \leq d^oA + d^oB$. □

Definition 2. Le polynôme C est appelé le *produit* des polynômes A et B. On le note bien entendu AB.

2.2 Degré d'un produit

Proposition 5. Soient $A, B \in \mathbb{K}[X]$. On a $d^o(AB) = d^oA + d^oB$.

Démonstration. C'est clair si A ou B est nul. Supposons donc A et B non nuls. Nous avons déjà montré que $d^oC \leq d^oA + d^oB$. De plus, en reprenant les notations de la démonstration de la proposition précédente, on constate que

$$c_{d+d'} = a_d b'_d \neq 0$$

Ainsi, $d^oC \geq d^oA + d^oB$. □

2.3 Structure d'anneau

En tant qu'espace vectoriel, $(\mathbb{K}[X], +)$ est un groupe abélien. Il est de plus évident que la multiplication des polynômes est commutative. Enfin, le polynôme $X_0 = (1, 0, \ldots)$ est neutre pour la multiplication. Il nous reste à regarder l'associativité et la distributivité.

Proposition 6. La multiplication des polynômes est associative.

Démonstration. Soient A, B, C trois polynômes. Soient $D = AB$ et $E = (AB)C = DC$. On a pour tout entier k,

$$\begin{aligned} e_k &= \sum_{i+j=k} d_i c_j \\ &= \sum_{i+j=k} \sum_{p+q=i} a_p b_q c_j \\ &= \sum_{p+q+j=k} a_p b_q c_j \end{aligned}$$

On trouve les mêmes valeurs en calculant les coefficients de $A(BC)$. □

Proposition 7. La multiplication des polynômes est distributive par rapport à l'addition.

Démonstration. Soient A, B, C trois polynômes. Soit $D = A(B + C)$. On a pour tout entier k,

$$\begin{aligned} d_k &= \sum_{i+j=k} a_i (b_j + c_j) \\ &= \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j \end{aligned}$$

On trouve les mêmes coefficents en considérant $AB + AC$. □

Proposition 8. $(\mathbb{K}[X], +\times)$ est un anneau commutatif intègre.

Démonstration. Il reste à montrer l'intégrité. Soient A et B deux polynômes. Supposons que $AB = 0$. On a alors

$$-\infty = d^o(AB) = d^oA + d^oB$$

Il en résulte que $d^oA = -\infty$ ou $d^oB = -\infty$, c'est à dire $A = 0$ ou $B = 0$. □

2.4 Les puissances de X

Rappelons que $X = (0, 1, 0, \ldots)$. Remarquons également l'égalité évidente

$$X_n = \sum_{k=0}^{\infty} \delta_{nk} X_k$$

Les coefficients du polynôme X_n sont donc les symboles de Kronecker δ_{nk}.

Proposition 9. Pour tout entier n, $X^n = X_n$.

Démonstration. Montrons la proposition par récurrence sur n.

Tout d'abord, $X^0 = 1 = (1, 0, \ldots) = X_0$.

Soit $n \in \mathbb{N}$. Supposons $X^n = X_n$. Soit $A = X^{n+1} = X^n X$. On a pour tout entier k

$$a_k = \sum_{i+j=k} \delta_{ni}\delta_{1j} = \delta_{n(k-1)} = \delta_{(n+1)k}$$

Ainsi,

$$X^{n+1} = \sum_{k=0}^{\infty} \delta_{(n+1)k} X_k = X_{n+1}$$

□

En conclusion, la famille $(X^k)_{k\geq 0}$ est une base de $\mathbb{K}[X]$: tout polynôme A s'écrit de façon unique

$$A = \sum_{k=0}^{\infty} a_k X^k$$

où les a_k sont des scalaires presque tous nuls.

3 Unicité de l'algèbre $\mathbb{K}[X]$

Proposition 10. Soit $\mathbb{B}$ une $\mathbb{K}$ algèbre commutative. On suppose qu'il existe $Y \in \mathbb{B}$ tel que la famille $(Y^k)_{k\geq 0}$ soit une base de l'espace l'espace vectoriel $\mathbb{B}$. Alors il existe un unique isomorphisme d'algèbres $\varphi : \mathbb{K}[X] \to \mathbb{B}$ tel que $\varphi(X) = Y$.

Démonstration. Supposons qu'un tel isomorphisme existe. On a alors pour tout $A \in \mathbb{K}[X]$

$$\begin{aligned}\varphi(A) &= \varphi\left(\sum_{k=0}^{\infty} a_k X^k\right) \\ &= \sum_{k=0}^{\infty} a_k \left(\varphi(X)\right)^k \\ &= \sum_{k=0}^{\infty} a_k Y^k\end{aligned}$$

On en déduit l'unicité de φ. Il reste à vérifier que l'application φ définie ci-dessus est bien un isomorphisme d'algèbres.

- φ est surjective car $(Y^k)_{k\geq 0}$ est génératrice de $\mathbb{B}$.

- φ est injective car $(Y^k)_{k\geq 0}$ est libre.
- On a $\varphi(1) = \varphi(X^0) = Y^{\overline{0}} = 1$.
- L'additivité de φ est laissée en exercice.
- Montrons la multiplicativité. Soient A et B deux polynômes. Soit $C = AB$. On a

$$\begin{aligned}
\varphi(A)\varphi(B) &= \sum_{p=0}^{\infty} a_p Y^p \sum_{q=0}^{\infty} b_q Y^q \\
&= \sum_{p,q=0}^{\infty} a_p b_q Y^{p+q} \\
&= \sum_{k=0}^{\infty} \left(\sum_{p+q=k} a_p b_q \right) Y^k \\
&= \sum_{k=0}^{\infty} c_k Y^k \\
&= \varphi(C)
\end{aligned}$$

□

Conclusion. La construction de $\mathbb{K}[X]$ que nous avons faite dans cet article est **une** construction possible de l'algèbre des polynômes à coefficients dans $\mathbb{K}$. Ce que montre la dernière proposition, c'est que toutes les constructions fournissent des algèbres qui sont isomorphes entre-elles.