Composition des polynômes

Marc Lorenzi

9 février 2021

Soient A et B deux polynômes. On appelle *composée* de A et B le polynôme

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

La composition des polynômes admet X pour élément neutre.

Cette opération n'est pas commutative. En effet,

$$X^2 \circ (X+1) = (X+1)^2 = X^2 + 2X + 1$$

alors que

$$(X+1) \circ X^2 = X^2 + 1$$

Ce contre-exemple ne fonctionne que si $2 \neq 0$ dans le corps $\mathbb{K}$. Dans le cas où $2 = 0$, il suffit de remarquer que $X^3 \circ (X+1) \neq (X+1) \circ X^3$.

Proposition 1. Soient A et B deux polynômes tels que $d^oB \geq 1$. Alors

$$d^o(A \circ B) = d^oA \times d^oB$$

Démonstration. Si $A = 0$, on a $A \circ B = 0$. De là,

$$d^o(A \circ B) = -\infty = -\infty \times d^oB$$

Supposons maintenant $A \neq 0$. Soit $d = d^oA$. Écrivons

$$A \circ B = \sum_{k=0}^{d} a_k B^k = a_d B^d + \sum_{k=0}^{d-1} a_k B^k$$

Comme $a_d \neq 0$, le degré de $a_d B^d$ est $d^(B^d) = d \times d^oB$. Pour tout $k \leq d-1$,

$$d^o(a_k B^k) \leq d^o(B^k) = k d^oB < d \times d^oB$$

Ici, le fait que $d^oB \geq 1$ est essentiel. Le degré de $\sum_{k=0}^{d-1} a_k B^k$ est donc strictement inférieur à $d \times d^oB$, d'où le résultat. □

Remarque. Si $d^oB \leq 0$ alors $B = b \in \mathbb{K}_0[X]$ (où $b \in \mathbb{K}$). On a alors

$$A \circ B = \sum_{k=0}^{\infty} a_k b^k \in \mathbb{K}_0[X]$$

Ainsi, $d^o(A \circ B) \leq 0$. Ce degré est $-\infty$ ou zéro selon que b est *racine* de A ou pas.

Corollaire 2. Les polynômes inversibles pour la loi $\circ$ sont les polynômes de degré 1.

Démonstration. Soit A un polynôme. Supposons qu'il existe un polynôme B tel que $A \circ B = X$. B ne peut pas être constant, donc $d^o A \times d^o B = d^o X = 1$. Il en résulte que $d^o A = d^o B = 1$. Inversement, soit $A = aX + b$ où $a, b \in \mathbb{K}$, $a \neq 0$. Soit $B = \frac{1}{a}X - \frac{b}{a}$. On a

$$A \circ B = a\left(\frac{1}{a}X - \frac{b}{a}\right) + b = X$$

et

$$B \circ A = \frac{1}{a}(aX + b) - \frac{b}{a} = X$$

Ainsi, A est inversible pour la loi $\circ$. $\square$

La loi $\circ$ n'est pas distributive à droite par rapport à l'addition. En effet,

$$X^2 \circ (X + X) = 4X^2$$

alors que

$$X^2 \circ X + X^2 \circ X = 2X^2$$

Ce contre-exemple ne fonctionne que si $2 \neq 0$ dans le corps $\mathbb{K}$. Dans le cas où $2 = 0$, il suffit de remarquer que

$$X^2 \circ (X + 2X) = 9X^2$$

alors que

$$(X + 2X) \circ X^2 = 3X^2$$

En revanche, il y a distributivité à gauche. En fait, la loi $\circ$ est distributive à gauche par rapport à l'addition **et** à la multiplication.

Proposition 3. Pour tous polynômes A, B, C et tout $\lambda \in \mathbb{K}$, on a

- $(A + B) \circ C = A \circ C + B \circ C$
- $(\lambda A) \circ C = \lambda(A \circ C)$
- $(AB) \circ C = (A \circ C)(B \circ C)$

Démonstration. Faisons la preuve pour le produit.

$$\begin{aligned}
(A \circ C)(B \circ C) &= \sum_{i=0}^{\infty} a_i C^i \sum_{j=0}^{\infty} b_j C^j \\
&= \sum_{i,j=0}^{\infty} a_i b_j C^{i+j} \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) C^k \\
&= (AB) \circ C
\end{aligned}$$

$\square$

Corollaire 4. Pour tous polynômes B et C et tout entier k, $B^k \circ C = (B \circ C)^k$.

Démonstration. Simple récurrence sur k. $\square$

Proposition 5. La composition des polynômes est associative.

Démonstration. Soient A, B, C trois polynômes. On a

$$\begin{aligned} A \circ (B \circ C) &= \sum_{k=0}^{\infty} a_k (B \circ C)^k \\ &= \sum_{k=0}^{\infty} a_k (B^k \circ C) \\ &= \sum_{k=0}^{\infty} ((a_k B^k) \circ C) \\ &= \left(\sum_{k=0}^{\infty} a_k B^k \right) \circ C \\ &= (A \circ B) \circ C \end{aligned}$$

□