Chaînes de polynômes

Marc Lorenzi

10 février 2021

Résumé

Dans cet article, $\mathbb{K}$ désigne un corps de caractéristique différente de 2 (c'est à dire dans lequel $2 \neq 0$). La composition des polynômes est une opération qui n'est pas commutative. Cependant, il existe des familles de polynômes qui ont la propriété de commuter entre-eux : une famille $(P_n)_{n\geq 0}$ de polynômes est appelée une *chaîne* lorsque

- Pour tout entier n, $d^oP_n = n$
- Pour tous entiers m et n, $P_m \circ P_n = P_n \circ P_m$

Nous allons montrer qu'il existe « essentiellement » deux chaînes de polynômes. Notre hypothèse que $\mathbb{K}$ est de caractéristique différente de 2 ne sera pas rappelée à chaque fois, mais le lecteur se rendra compte de la nécessité permanente de faire des divisions par 2 dans ce qui va suivre.

1 Deux chaînes de polynômes

Commençons par exhiber deux chaînes.

1.1 Les puissances de X

La première chaîne est évidente.

Proposition 1. La famille $(X^n)_{n\geq 0}$ est une chaîne.

Démonstration. La condition sur les degrés est évidemment respectée. De plus,

$$X^m \circ X^n = (X^n)^m = (X^m)^n = X^n \circ X^m$$

□

1.2 Les polynômes de Tchebychev

Cette seconde chaîne est beaucoup moins évidente.

On définit les *polynômes de Tchebychev* T_n par récurrence sur n en posant $T_0 = 1$, $T_1 = X$, et, pour tout $n \geq 0$,

$$T_{n+2} = 2XT_{n+1} - T_n$$

Les premiers polynômes de Tchebychev sont $T_0 = 1$, $T_1 = X$, $T_2 = 2X^2 - 1$, $T_3 = 4X^3 - 3X$.

Proposition 2. Pour tout entier n, le degré de T_n est n.

Démonstration. On fait une récurrence à deux termes sur n.

C'est évident pour $n = 0, 1$.

Soit $n \geq 0$. Supposons $d^oT_n = n$ et $d^oT_{n+1} = n + 1$. On a alors

$$d^o(2XT_{n+1}) = n + 2 > d^oT_n$$

et donc

$$d^oT_{n+2} = d^o(2XT_{n+1} - T_n) = n + 2$$

□

Les deux lemmes qui vont suivre font appel à des notions sur les fractions rationnelles. Ils permettent de prouver dans le cas d'un corps quelconque la proposition 5. On pourra admettre les résultats.

Lemme 3. Soit P un polynôme vérifiant $P \circ (\frac{1}{2}(X + \frac{1}{X})) = 0$ dans le corps des fractions rationnelles $\mathbb{K}(X)$. Alors $P = 0$.

Démonstration. Soit $F = \frac{1}{2}(X + \frac{1}{X}) \in \mathbb{K}(X)$. Comme $d^oF = 1 > 0$, on a dans le corps $\mathbb{K}(X)$

$$d^o(P \circ F) = d^oP \times d^oF = d^oP$$

Si $P \circ F = 0$, alors $d^oP = -\infty$, donc $P = 0$. □

Lemme 4. On a pour tout entier n,

$$T_n \circ \left(\frac{1}{2}(X + \frac{1}{X})\right) = \frac{1}{2}(X^n + \frac{1}{X^n})$$

Démonstration. On fait une récurrence à deux termes sur n.

C'est clair pour $n = 0, 1$.

Soit $n \geq 0$. Supposons la propriété vérifiée pour n et $n + 1$. On a alors

$$\begin{aligned} T_{n+2} \circ \left(\frac{1}{2}(X + \frac{1}{X})\right) &= 2\frac{1}{2}(X + \frac{1}{X})\frac{1}{2}(X^{n+1} + \frac{1}{X^{n+1}}) - \frac{1}{2}(X^n + \frac{1}{X^n}) \\ &= \frac{1}{2}(X^{n+2} + \frac{1}{X^{n+2}}) \end{aligned}$$

où la dernière égalité est obtenue par un simple développement. □

Proposition 5. Pour tous entiers m et n,

$$T_m \circ T_n = T_{mn}$$

Démonstration. On a

$$\begin{aligned} T_m \circ T_n \circ \left(\frac{1}{2}(X + \frac{1}{X})\right) &= T_m \circ \left(\frac{1}{2}(X^n + \frac{1}{X^n})\right) \\ &= \frac{1}{2}(X^{mn} + \frac{1}{X^{mn}}) \\ &= T_{mn} \circ \left(\frac{1}{2}(X + \frac{1}{X})\right) \end{aligned}$$

Ainsi,

$$(T_m \circ T_n - T_{mn}) \circ \left(\frac{1}{2}(X + \frac{1}{X})\right) = 0$$

De là, par le lemme 3,

$$T_m \circ T_n = T_{mn}$$

□

Proposition 6. La famille $(T_n)_{n\geq 0}$ est une chaîne.

Démonstration. La condition de degrés est respectée. De plus,

$$T_m \circ T_n = T_{mn} = T_{nm} = T_n \circ T_m$$

□

Nous allons maintenant préciser le sens du mot « essentiellement » cité au début du document en étudiant une relation d'équivalence sur l'ensemble des polynômes.

2 Polynômes conjugués

2.1 Polynômes inversibles pour la composition

Proposition 7. Les polynômes inversibles pour la composition sont les polynômes de degré 1.

Démonstration. Soit P un polynôme. Supposons qu'il existe un polynôme Q tel que $P \circ Q = X$. On a

$$d^o(P \circ Q) = d^oP \times d^oQ = d^oX = 1$$

Ainsi, $d^oP = 1$.

Inversement, supposons que $P = aX+b$ est de degré 1. Alors, P est inversible pour la composition. Son inverse est

$$P^{-1} = \frac{1}{a}X - \frac{b}{a}$$

□

2.2 Conjugaison

Le polynôme Q est *conjugué* du polynôme P lorsqu'il existe un polynôme λ de degré 1 tel que

$$Q = \lambda^{-1} \circ P \circ \lambda$$

On note dans la suite $P \sim Q$ lorsque Q est conjugué de P.

Proposition 8. La relation de conjugaison est une relation d'équivalence sur $\mathbb{K}[X]$.

Démonstration.

- Soit P un polynôme. On a $P = X^{-1} \circ P \circ X$, où $X^{-1} = X$ est sa propre réciproque. Et donc $P \sim P$.

- Soient P et Q deux polynômes. Supposons que $P \sim Q$. Il existe donc λ de degré 1 tel que $Q = \lambda^{-1} \circ P \circ \lambda$. On a alors
$$P = \mu^{-1} \circ Q \circ \mu$$
où $\mu = \lambda^{-1}$. Ainsi, $Q \sim P$.
- Soient P, Q et R trois polynômes. Supposons que $P \sim Q$ et $Q \sim R$. Il existe donc λ et μ de degré 1 tels que $Q = \lambda^{-1} \circ P \circ \lambda$ et $R = \mu^{-1} \circ Q \circ \mu$. On a alors
$$R = \nu^{-1} \circ Q \circ \nu$$
où $\nu = \lambda \circ \mu$. Ainsi, $P \sim R$.

□

Il est intéressant de remarquer que la relation de conjugaison permet, dans le cas des polynômes de degré 2, de se ramener à un coefficient dominant égal à 1 et d'éliminer le terme de degré 1.

Proposition 9. Soit $P = \alpha X^2 + \beta X + \gamma$ un polynôme de degré 2. Alors P est conjugué d'un polynôme $X^2 + c$, où $c \in \mathbb{K}$.

Démonstration. Soit $\lambda = aX + b$. On a, après simplifications,
$$\lambda^{-1} \circ P \circ \lambda = \alpha a X^2 + (2\alpha b + \beta)X + c$$
où $c \in \mathbb{K}$. On obtient le résultat en prenant $a = \frac{1}{\alpha}$ et $b = -\frac{\beta}{2\alpha}$. □

2.3 Conjugaison et chaînes

Montrons maintenant que la relation de conjugaison préserve la propriété de chaîne.

Proposition 10. Soient P et Q deux polynômes qui commutent. Pour tout polynôme λ de degré 1, les polynômes $\lambda^{-1} \circ P \circ \lambda$ et $\lambda^{-1} \circ Q \circ \lambda$ commutent.

Démonstration.
$$\begin{aligned}(\lambda^{-1} \circ P \circ \lambda) \circ (\lambda^{-1} \circ Q \circ \lambda) &= \lambda^{-1} \circ P \circ Q \circ \lambda \\ &= \lambda^{-1} \circ Q \circ P \circ \lambda \\ &= (\lambda^{-1} \circ Q \circ \lambda) \circ (\lambda^{-1} \circ P \circ \lambda)\end{aligned}$$

□

Proposition 11. Soit $(P_n)_{n\geq 0}$ une chaîne. Soit λ un polynôme de degré 1. La famille $(\lambda^{-1} \circ P_n \circ \lambda)_{n\geq 0}$ est encore une chaîne.

Démonstration. La condition de degrés est respectée et, comme nous venons de le voir, les polynômes $\lambda^{-1} \circ P_n \circ \lambda$ commutent. □

Ainsi, étant donnée une chaîne, il est possible par conjugaison de créer d'autres chaînes. Toutes ces chaînes sont « essentiellement » identiques.

3 Une réciproque

Nous allons tout d'abord montrer un certain nombre de résultats concernant les polynômes de degré 2.

3.1 Polynômes qui commutent avec un polynôme de degré 2

Lemme 12. Soit P un polynôme de degré 2 unitaire. Soit Q un polynôme de degré $k \geq 0$. Si P et Q commutent, alors Q est unitaire.

Démonstration. Écrivons $P = X^2 + \beta X + \gamma$. Posons $Q = aX^k + \hat{Q}$, où $d^o\hat{Q} < k$. On a

$$Q^2 + \beta Q + \gamma = aP^k + \hat{Q} \circ P$$

L'égalité des termes de degré $2k$ donne

$$a^2 = a$$

d'où, puisque $a \neq 0$, $a = 1$. □

Lemme 13. Soit $P = X^2 + c$ un polynôme qui commute avec un polynôme Q de degré impair. Alors Q est impair.

Démonstration. On a

$$Q^2 + c = Q \circ (X^2 + c)$$

et donc

$$Q(-X)^2 + c = Q \circ ((-X)^2 + c) = Q \circ (X^2 + c) = Q(X)^2 + c$$

où $Q(X)$ est un pléonasme pour Q. Ainsi,

$$Q(-X)^2 = Q(X)^2$$

De là, comme $\mathbb{K}[X]$ est un anneau intègre, $Q(-X) = \pm Q(X)$ et Q est donc pair ou impair. Comme Q est de degré impair, Q ne peut pas être pair. Donc Q est impair. □

Lemme 14. Soit $P = X^2 + c$ un polynôme qui commute avec un polynôme Q de degré 3. Alors

- Si la caractéristique de $\mathbb{K}$ est différente de 3, alors $P = X^2, Q = X^3$ ou $P = X^2 - 2, Q = X^3 - 3X$.
- Si la caractéristique de $\mathbb{K}$ est égale à 3 (c'est à dire si $3 = 0$ dans le corps $\mathbb{K}$), il faut rajouter la solution $P = X^2 - 1$, $Q = X^3$.

Démonstration. Par les deux lemmes précédents, Q est unitaire et impair : $Q = X^3 + bX$, où $b \in \mathbb{K}$. On a

$$(X^3 + bX)^2 + c = (X^2 + c)^3 + b(X^2 + c)$$

d'où, en égalant les coefficients des termes de même degré,

$$\begin{cases} 2b &= 3c \\ b^2 &= 3c^2 + b \\ c &= c^3 + bc \end{cases}$$

La dernière égalité suggère de discuter sur la nullité de c.

Cas 1 : $c = 0$. On a alors par la première égalité $b = 0$. Ainsi, $P = X^2$ et $Q = X^3$. Inversement, ces deux polynômes commutent.

Cas 2 : $c \neq 0$. On a par la dernière égalité $b = 1 - c^2$. En reportant dans la première égalité, on obtient

$$2c^2 + 3c - 2 = 0$$

d'où $c = -2$ ou $c = \frac{1}{2}$. Si $c = -2$, alors $b = \frac{3}{2}c = -3$. On a alors $P = X^2 - 2$ et $Q = X^3 - 3X$. On vérifie facilement que ces deux polynômes commutent.

Si $c = \frac{1}{2}$ alors $b = \frac{3}{2}c = \frac{3}{4}$. Mais alors,

$$b^2 = \frac{9}{16} \neq 3c^2 + b = \frac{3}{2}$$

sauf dans le cas où la caractéristique de $\mathbb{K}$ est égale à 3 ou 5. En effet, dans ce cas, $3 \times 16 - 9 \times 2 = 30 = 0$.

Si la caractéristique de $\mathbb{K}$ est 3, on trouve alors $c = \frac{1}{2} = -1$ et $b = 1 - c^2 = 0$. Inversement les polynômes $X^2 - 1$ et X^3 commutent.

Si la caractéristique de $\mathbb{K}$ est 5, alors $c = \frac{1}{2} = -2$ et $b = 1 - c^2 = -3$, et on retrouve les polynômes déjà obtenus $P = X^2 - 2$ et $Q = X^3 - 3X$. □

Proposition 15. Soit P un polynôme de degré 2. Soit $k \geq 1$. Alors P commute avec au plus un polynôme de degré k.

Démonstration. Quitte à conjuguer, on peut supposer $P = X^2 + c$ où $c \in \mathbb{K}$. Supposons que P commute avec deux polynômes distincts Q_1 et Q_2 de degré k. On vérifie facilement que Q_1 et Q_2 sont unitaires. Posons $R = Q_1 - Q_2$. Le polynôme R est de degré strictement inférieur à k. On a

$$Q_1^2 + c = Q_1 \circ (X^2 + c)$$
$$Q_2^2 + c = Q_2 \circ (X^2 + c)$$

d'où, en soustrayant,

$$(Q_1 - Q_2)(Q_1 + Q_2) = (Q_1 - Q_2) \circ (X^2 + c)$$

ou encore

$$R(Q_1 + Q_2) = R \circ (X^2 + c)$$

Posons $r = d^o R$. Comme $d^o(Q_1 + Q_2) = k$, on a $r + k = 2r$, d'où $r = k$, contradiction. □

3.2 Le théorème de Block et Thielman

Nous voici arrivés au théorème central du document.

Proposition 16. Soit $\mathbb{K}$ un corps de caractéristique différente de 2. Il existe à conjugaison près exactement deux chaînes de polynômes à coefficients dans $\mathbb{K}$: $(X^n)_{n\geq 0}$ et $(T_n)_{n\geq 0}$.

Démonstration. Commençons par le cas où la caractéristique de $\mathbb{K}$ est différente de 3.

Soit $(P_n)_{n\geq 0}$ une chaîne de polynômes. Par une conjugaison judicieuse, on peut supposer $P_2 = X^2 + c$, où $c \in \mathbb{K}$. Comme P_2 et P_3 commutent et que P_3 est de degré 3, on a $P_2 = X^2$ ou $P_2 = X^2 - 2$.

Commençons par le cas où $P_2 = X^2$. Pour tout entier $k \geq 1$, P_2 commute avec au plus un polynôme de degré k. Or, P_2 commute avec X^k. Il en résulte que $P_k = X^k$. Enfin, P_2 commute avec $P_0 = a$ constant non nul. Il en résulte que $a^2 = a$, et donc $a = 1$. Ainsi, $P_0 = X^0$. Finalement, $(P_n)_{n\geq 0} = (X^n)_{n\geq 0}$.

Considérons maintenant le cas où $P_2 = X^2 - 2$. Conjuguons la chaîne $(P_n)_{n\geq 0}$ par $\lambda = 2X$. On a

$$\lambda^{-1} \circ P_2 \circ \lambda = \frac{1}{2} P_2(2X) = 2X^2 - 1 = T_2$$

On conclut alors, comme dans le premier cas, que la chaîne conjuguée est $(T_n)_{n\geq 0}$.

Regardons maintenant le cas où la caractéristique de $\mathbb{K}$ est égale à 3. Il reste à examiner ce qui se passe lorsque $P_2 = X^2 - 1$. Nous allons raisonner par contradiction et supposer que P_2 appartient à une chaîne. Le polynôme P commute alors avec le polynôme P_5, de degré 5. Par le lemme 12, le polynôme P_5 est unitaire. Par le lemme 13, il est impair. Ainsi, $P_5 = X^5 + aX^3 + bX$, où $a, b \in \mathbb{K}$. On a alors

$$(X^5 + aX^3 + bX)^2 - 1 = (X^2 - 1)^5 + a(X^2 - 1)^3 + b(X^2 - 1)$$

ce qui donne en regardant les coefficients de degrés 8, 6, 4 :

$$\begin{cases} 2a & = & 1 \\ a^2 + 2b & = & 1 + a \\ 2ab & = & -1 \end{cases}$$

La première égalité fournit $a = 2$. En reportant dans la seconde égalité, on obtient $4 + 2b = 3$ c'est à dire $1 + 2b = 0$, d'où $b = 1$. En reportant dans la troisième égalité, il vient $4 = -1$, ce qui est impossible en caractéristique 3 (car alors $1 = -1$ d'où $2 = 0$).

Il nous reste à montrer que les chaînes $(X^n)_{n\geq 0}$ et $(T_n)_{n\geq 0}$ ne sont pas conjuguées. Supposant le contraire, il existe $\lambda = aX + b$, où $a, b \in \mathbb{K}, a \neq 0$, tel que

$$T_2 = \lambda^{-1} \circ X^2 \circ \lambda$$

On en déduit

$$2X^2 - 1 = aX^2 + 2bX + \frac{b^2 - b}{a}$$

Ceci oblige à la fois $2b = 0$ et $\frac{b^2-b}{a} = -1$, ce qui est impossible. □