

Chaînes de polynômes

Marc Lorenzi

Table des matières

1	Deux chaînes de polynômes	2
1.1	Les puissances de X	2
1.2	Les polynômes de Tchebychev	2
2	Polynômes conjugués	4
2.1	Polynômes inversibles pour la composition	4
2.2	Conjugaison	4
2.3	Conjugaison et chaînes	5
3	Une réciproque	5
3.1	Polynômes qui commutent avec un polynôme de degré 2	6
3.2	Le théorème de Block et Thielman	7
4	La caractéristique 2	9
4.1	Polynômes de degré 2 et de degré 3 qui commutent	9
4.2	Polynômes de degré 3 et de degré 5 qui commutent	10
4.3	Le cas de $X^3 + 1$ et $X^3 + X + 1$	11
4.4	La chaîne des puissances de X	11
4.5	Les polynômes de Tchebychev modifiés	11
4.6	Le théorème de Block et Thielman en caractéristique 2	12

Résumé

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 , $d^n P_n = n$
- 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.

Dans cet article, hormis dans la dernière partie, $\mathbb{K}$ désigne un corps de caractéristique différente de 2. 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 cette hypothèse 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 $d^o T_n = n$ et $d^o T_{n+1} = n + 1$. On a alors

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

et donc

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

□

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 $d^o F = 1 > 0$, on a dans le corps $\mathbb{K}(X)$

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

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

Lemme 4. On a pour tout entier n ,

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

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

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

où la dernière égalité est obtenue par un simple développement. $\square$

Proposition 5. Pour tous entiers m et n ,

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

Démonstration. On a

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

Ainsi,

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

De là, par le lemme 3,

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

$\square$

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

$$d^o(P \circ Q) = d^o P \times d^o Q = d^o X = 1$$

Ainsi, $d^o P = 1$.

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

$$R = \nu^{-1} \circ P \circ \nu$$

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,

$$\lambda^{-1} \circ P \circ \lambda = \alpha a X^2 + (2ab + \beta)X + c$$

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 $k \geq 1$. 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 $a \neq 0$, $a = 1$. $\square$

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 pléonisme 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. $\square$

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 $Q = X^3 - 3X$. $\square$

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

$$\begin{aligned} Q_1^2 + c &= Q_1 \circ (X^2 + c) \\ Q_2^2 + c &= Q_2 \circ (X^2 + c) \end{aligned}$$

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. $\square$

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. $\square$

4 La caractéristique 2

Nous allons maintenant nous placer dans un corps $\mathbb{K}$ de caractéristique 2. Un certain nombre de propriétés vues en caractéristique différente de 2 restent valables, mais d'autres ne le sont plus. Les points qui posent le plus gros problème sont les suivants :

- Les arguments de parité ou d'imparité ne fonctionnent plus, puisque $-1 = 1$.
- Un polynôme de degré 2 peut commuter avec plusieurs polynômes de degré donné : la démonstration d'unicité que nous avons faite dans la proposition 15 ne fonctionne plus, car en caractéristique 2 la somme de deux polynômes unitaires de même degré est de degré strictement plus petit. En effet, $1 + 1 = \dots 0$. Ceci va nous obliger à travailler avec des polynômes de degré 3, pour lesquels le résultat reste valable. L'inconvénient de cette méthode est qu'il va falloir étudier les polynômes de degré 3 qui commutent avec un polynôme de degré 5. Cette étude sera faite avec un système de calcul formel, en l'occurrence le module sympy de Python.
- Un polynôme de degré 2 n'est plus conjugué à un polynôme de la forme $X^2 + c$. Nous verrons qu'il est quand même conjugué à un polynôme unitaire, mais il n'est pas possible de faire disparaître le terme de degré 1. Ceci entraîne des complications dans les calculs.
- La suite $(T_n)_{n \geq 0}$ n'est plus une chaîne. C'est en fait la suite

$$(1, X, 1, X, \dots)$$

qui ne respecte pas les conditions de degré des chaînes. Nous verrons qu'elle peut heureusement être remplacée par une suite $(U_n)_{n \geq 0}$ de polynômes de Tchebychev *modifiés*.

4.1 Polynômes de degré 2 et de degré 3 qui commutent

Proposition 17. *Soit P un polynôme de degré 2. Alors P est conjugué d'un polynôme unitaire.*

Démonstration. Soit $P = \alpha X^2 + \beta X + \gamma$, où $\alpha \neq 0$. Prenons $\lambda = \frac{1}{\alpha}X$. Alors

$$\lambda^{-1} \circ P \circ \lambda = \alpha \left(\alpha \left(\frac{1}{\alpha} X \right)^2 + \beta \left(\frac{1}{\alpha} X \right) + \gamma \right) = X^2 + \beta X + \frac{\gamma}{\alpha}$$

est unitaire. $\square$

Proposition 18. *Soit P un polynôme unitaire de degré 2. Si P commute avec un polynôme Q de degré $k \geq 1$ alors Q est unitaire.*

Démonstration. Posons $P = X^2 + \alpha X + \beta$. Posons $Q = aX^k + \hat{Q}$ où $a \neq 0$ et $d^o \hat{Q} < k$. Supposons que $P \circ Q = Q \circ P$. Il vient

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

Les coefficients de degré $2k$ des deux membres sont égaux, ce qui donne

$$a^2 = a$$

Ainsi, $a = 0$ ou $a = 1$. Comme $a \neq 0$, on a finalement $a = 1$. $\square$

Remarque. Si $k = 0$, on a donc $Q = a$ où $a \neq 0$. P et Q commutent si et seulement si $a^2 + \alpha a + \beta = a$, ce qui ne permet pas de conclure que $a = 1$.

Proposition 19. *Soit P un polynôme unitaire de degré 2. Si P commute avec un polynôme Q de degré 3, alors P est conjugué de X^2 et Q est conjugué, par la même conjugaison, de l'un des polynômes X^3 , $X^3 + 1$, $X^3 + X$, $X^3 + X + 1$.*

Démonstration. Par la proposition précédente, Q est unitaire. Posons $P = X^2 + \alpha X + \beta$ et $Q = X^3 + aX^2 + bX + c$. Conjuguons Q par $\lambda = X - a$. Il vient

$$\begin{aligned}\lambda^{-1} \circ Q \circ \lambda &= (X - a)^3 + a(X - a)^2 + b(X - a) + c + a \\ &= X^3 + (a^2 + b)X + ab + c + a\end{aligned}$$

Ce conjugué est toujours unitaire, et son coefficient de degré 2 est nul. On vérifie de même que $\lambda^{-1} \circ P \circ \lambda$ est toujours unitaire. On peut donc supposer, quitte à conjuguer, que $a = 0$. On a donc

$$(X^2 + \alpha X + \beta) \circ (X^3 + bX + c) = (X^3 + bX + c) \circ (X^2 + \alpha X + \beta)$$

En développant et en égalant les coefficients des deux membres de l'égalité, on obtient

$$\begin{cases} \alpha &= 0 \\ \alpha^2 + \beta &= 0 \\ \alpha^3 + \alpha &= 0 \\ \alpha^2\beta + b^2 - b &= 0 \\ \alpha\beta^2 &= 0 \\ \alpha c + b\beta + \beta^3 + \beta + c^2 - c &= 0 \end{cases}$$

Les deux premières égalités fournissent $\alpha = \beta = 0$, et donc $P = X^2$. La quatrième et la dernière égalité donnent ensuite $b^2 - b = c^2 - c = 0$, d'où les polynômes Q annoncés dans la proposition. $\square$

4.2 Polynômes de degré 3 et de degré 5 qui commutent

Proposition 20. *Soit P un polynôme unitaire de degré 3. Si P commute avec un polynôme Q de degré $k \geq 1$ alors Q est unitaire.*

Démonstration. Posons $P = X^3 + \alpha X^2 + \beta X + \gamma$. Posons $Q = aX^k + \hat{Q}$ où $a \neq 0$ et $d^o \hat{Q} < k$. Supposons que $P \circ Q = Q \circ P$. Il vient

$$Q^3 + \alpha Q^2 + \beta Q + \gamma = aP^k + \hat{Q} \circ P$$

Les coefficients de degré $3k$ des deux membres sont égaux, ce qui donne

$$a^3 = a$$

Ainsi, $a = 0$, $a = -1$ ou $a = 1$. Comme $a \neq 0$ et que $-1 = 1$, on a finalement $a = 1$. $\square$

Proposition 21. Soit P un polynôme unitaire de degré 3. Soit $k \geq 1$. Alors P commute avec au plus un polynôme de degré k .

Démonstration. Soit $P = X^3 + \alpha X^2 + \beta X + \gamma$ un polynôme unitaire de degré 3. Soient Q_1 et Q_2 deux polynômes distincts de degré k . Supposons que P commute avec Q_1 et Q_2 . Par la proposition précédente, Q_1 et Q_2 sont unitaires. Posons $R = Q_1 - Q_2$. En notant $r = d^o R$, on a donc $r < k$. On a

$$\begin{cases} Q_1^3 + \alpha Q_1^2 + \beta Q_1 + \gamma &= Q_1 \circ P \\ Q_2^3 + \alpha Q_2^2 + \beta Q_2 + \gamma &= Q_2 \circ P \end{cases}$$

Soustrayons. Il vient

$$R(Q_1^2 + Q_1 Q_2 + Q_2^2 + \alpha(Q_1 + Q_2) + \beta) = R \circ P$$

Le degré du polynôme entre parenthèses est $2k$. En effet, il est clairement de degré inférieur ou égal à $2k$ et son coefficient de degré $2k$ est $1 + 1 + 1 = 1$. On en déduit que $r + 2k = 3r$, ou encore $r = k$ ce qui est impossible. $\square$

4.3 Le cas de $X^3 + 1$ et $X^3 + X + 1$

Proposition 22. $X^3 + 1$ et $X^3 + X + 1$ ne commutent avec aucun polynôme de degré 5.

Démonstration. En supposant que ces polynômes commutent avec un polynôme Q de degré 5, le polynôme Q est unitaire. On écrit les relations de commutation, ce qui amène à évaluer deux polynômes de degré 15, et on aboutit à une contradiction. La vérification est plutôt fastidieuse, elle a été faite en Python. Voir le document joint. $\square$

Conséquence. À conjugaison près, les seuls polynômes de degré 3 qui peuvent appartenir à une chaîne sont X^3 et $X^3 + X$. Il reste évidemment à montrer que ces deux polynômes appartiennent à une et une seule chaîne.

4.4 La chaîne des puissances de X

Bien évidemment, la famille $(X^n)_{n \geq 0}$ est une chaîne de polynômes.

4.5 Les polynômes de Tchebychev modifiés

On pose $U_0 = 0$, $U_1 = X$ et, pour tout entier n , $U_{n+2} = XU_{n+1} + U_n$. Nous appellerons les U_n les *polynômes de Tchebychev modifiés*. Les premiers polynômes de Tchebychev modifiés sont $U_0 = 0$, $U_1 = X$, $U_2 = X^2$, $U_3 = X^3 + X$, $U_4 = X^4$, $U_5 = X^5 + X^3 + X$, $U_6 = X^6 + X^2$.

Proposition 23. Pour tout entier $n \geq 1$, le degré de U_n est n .

Démonstration. Analogie à ce qui a été fait pour les polynômes T_n . $\square$

Proposition 24. *Pour tous entiers m et n , $U_m \circ U_n = U_{mn}$.*

Démonstration. Analogue à ce qui a été fait pour les polynômes T_n , en remplaçant $\frac{1}{2} \left(X + \frac{1}{X} \right)$ par $X + \frac{1}{X}$. $\square$

Proposition 25. *La famille $(U_n)_{n \geq 0}$ est une chaîne de polynômes.*

Démonstration. Analogue à ce qui a été fait pour les polynômes T_n . En toute rigueur, c'est presque une chaîne, car $d^o U_0 \neq 0$. $\square$

4.6 Le théorème de Block et Thielman en caractéristique 2

Proposition 26. *Soit $\mathbb{K}$ un corps de caractéristique 2. Il existe à conjugaison près exactement deux chaînes de polynômes : les puissances de X et les polynômes de Tchebychev modifiés.*

Démonstration. Soit $(P_n)_{n \geq 0}$ une chaîne de polynômes. Par la proposition 17, P_2 est conjugué d'un polynôme unitaire. Quitte à conjuguer on peut donc supposer P_2 unitaire. P_2 commute avec P_3 donc, par la proposition 18, P_3 est égal à l'un des polynômes X^3 , $X^3 + X$, $X^3 + 1$ et $X^3 + X + 1$. Maintenant, P_3 commute avec P_5 , donc, par la proposition 22, P_3 ne peut pas être égal à $X^3 + 1$ ou $X^3 + X + 1$. Il reste donc deux cas à examiner.

Supposons que $P_3 = X^3$. Pour tout entier $k \geq 1$, X^3 commute avec au plus un polynôme de degré k . Or, X^3 commute avec X^k . Ainsi, $P_k = X^k$. Enfin, X^3 commute avec P_0 . Le polynôme $P_0 = a$ est constant non nul. On a donc $a^3 = a$, d'où $a = 1$.

Supposons maintenant que $P_3 = X^3 + X = U_3$. Pour tout entier $k \geq 1$, U_3 commute avec au plus un polynôme de degré k . Or, U_3 commute avec U_k . Ainsi, $P_k = U_k$. Enfin, U_3 commute avec P_0 . Le polynôme $P_0 = a$ est constant (et est censé être non nul). On a donc $a^3 + a = a$, d'où $a^3 = 0$ et donc $a = 0$. Ainsi, $P_0 = U_0$.

En conclusion, toute chaîne de polynômes est conjuguée à $(X^n)_{n \geq 0}$ ou à $(U_n)_{n \geq 0}$.

Il reste à voir que ces deux chaînes ne sont pas conjuguées. Supposons par l'absurde qu'elles le sont. Il existe $\lambda = aX + b$ (où $a \neq 0$) tel que $U_3 = \lambda^{-1} \circ X^3 \circ \lambda$, d'où $\lambda \circ U_3 = X^3 \circ \lambda$ c'est à dire

$$a(X^3 + X) + b = (aX + b)^3$$

d'où, en développant,

$$aX^3 + aX + b = a^3X^3 + a^2bX^2 + ab^2X + b^3$$

L'égalité des coefficients de degré 3 impose $a^3 = a$, c'est à dire $a = 1$. Il reste donc

$$X + b = bX^2 + b^2X + b^3$$

ce qui est impossible. $\square$