

Polynômes commutants

Marc Lorenzi

18 février 2021

Table des matières

1	Similitude	1
1.1	Polynômes inversibles pour la composition	1
1.2	Polynômes semblables	2
1.3	Polynômes qui commutent avec un polynôme fixé	2
2	Le cardinal de $C_k(f)$	3
2.1	Polynômes centrés	3
2.2	Le cardinal de S_f	4
2.3	Une bijection entre S_f et $C_k(f)$	5
3	Deux exemples	7
3.1	Les puissances de X	7
3.2	Les polynômes de Tchebychev	8

Dans tout cet article, $\mathbb{K}$ désigne un corps algébriquement clos de caractéristique nulle. Pour tout entier $n \geq 1$ nous noterons $\mathbb{U}_n$ l'ensemble des racines n èmes de l'unité dans $\mathbb{K}$. Cet ensemble possède n éléments car le polynôme $X^n - 1$ est scindé dans $\mathbb{K}$ (corps algébriquement clos) et sa dérivée nX^{n-1} est non nulle aux racines de celui-ci (caractéristique nulle). Nous noterons également $\mathbb{U}_0 = \mathbb{K}^*$ et $\mathbb{U}_{-1} = \{1\}$.

Nous utiliserons également le résultat suivant :

Proposition 1. *Soient $f, g, h \in \mathbb{K}[X]$. Supposons que le polynôme f n'est pas constant et que $g \circ f = h \circ f$. Alors $g = h$.*

Démonstration. On a $(g - h) \circ f = 0$. Comme f n'est pas constant,

$$d^o((g - h) \circ f) = d^o(g - h)d^o f = d^o 0 = -\infty$$

On en déduit que $d^o(g - h) = -\infty$, et donc $g = h$. $\square$

1 Similitude

1.1 Polynômes inversibles pour la composition

Proposition 2. *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, $d^0 P = 1$.

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

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

□

Notons S_X l'ensemble des polynômes de degré 1. On vérifie facilement que S_X est un groupe pour l'opération de composition des polynômes.

1.2 Polynômes semblables

Définition 1. Le polynôme f est *semblable* au polynôme g lorsqu'il existe un polynôme λ de degré 1 tel que

$$g = \lambda^{-1} \circ f \circ \lambda$$

On note dans la suite $f \sim g$ lorsque f est semblable à g . On note également $f \sim_\lambda g$ lorsque $g = \lambda^{-1} \circ f \circ \lambda$.

Proposition 3. La relation de similitude est une relation d'équivalence sur $\mathbb{K}[X]$.

Démonstration.

- Soit f un polynôme. On a $f \sim_X f$.
- Soient f et g deux polynômes. Supposons que $f \sim_\lambda g$. Alors $g \sim_\mu f$ où $\mu = \lambda^{-1}$.
- Soient f, g et h trois polynômes. Supposons que $f \sim_\lambda g$ et $g \sim_\mu h$. Alors $f \sim_\nu h$ où $\nu = \lambda \circ \mu$.

□

Définition 2. Soit $f \in \mathbb{K}[X]$. Un polynôme λ de degré 1 est appelé une *auto-similarité* de f lorsque $f \sim_\lambda f$. On note S_f l'ensemble des auto-similarités de f .

Lorsque $f = X$, on retrouve la notation vue plus haut, puisque tout polynôme λ de degré 1 vérifie $\lambda^{-1} \circ X \circ \lambda = X$. Remarquons également que S_f est aussi l'ensemble des polynômes de degré 1 qui commutent avec f .

Proposition 4. Soit $f \in \mathbb{K}[X]$. L'ensemble S_f est un groupe pour la composition des polynômes.

Démonstration. Vérifications faciles. C'est un sous-groupe de S_X . □

L'un des objectifs de cet article est le calcul du cardinal de S_f .

1.3 Polynômes qui commutent avec un polynôme fixé

Définition 3. Soit $f \in \mathbb{K}[X]$. Soit $k \geq 1$. On note $C_k(f)$ l'ensemble des polynômes de degré k qui commutent avec f .

Remarquons que $C_1(f) = S_f$.

Nous allons montrer dans cet article que si $d^0 f > 1$ et $C_k(f) \neq \emptyset$, alors $|C_k(f)| = |S_f|$, où les barres verticales dénotent le cardinal d'un ensemble.

Proposition 5. Soient $f, g \in \mathbb{K}[X]$. Supposons que $f \sim_\lambda g$. Soit $k \geq 1$. Alors l'application $\Phi_k : C_k(f) \rightarrow C_k(g)$ définie par $\Phi_k(P) = \lambda^{-1} \circ P \circ \lambda$ est une bijection. Si $k = 1$ c'est un isomorphisme de groupes.

Démonstration. Soit $P \in C_k(f)$. Remarquons tout d'abord que $Q = \lambda^{-1} \circ P \circ \lambda$ vérifie

$$Q \circ g = (\lambda^{-1} \circ P \circ \lambda) \circ (\lambda^{-1} \circ f \circ \lambda) = \lambda^{-1} \circ P \circ f \circ \lambda$$

et de même

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

Comme f et P commutent, Q et g commutent aussi. Par ailleurs, $d^o Q = d^o P$. Ainsi, $Q \in C_k(g)$. La fonction Φ_k est donc bien définie.

La bijectivité de Φ_k est claire, sa réciproque est la fonction $\Psi_k : C_k(g) \rightarrow C_k(f)$ définie par $\Psi_k(Q) = \lambda \circ Q \circ \lambda^{-1}$.

Enfin, lorsque $k = 1$, on a pour $P, Q \in C_1(f)$,

$$\Phi_1(P \circ Q) = \lambda^{-1} \circ P \circ Q \circ \lambda = \Phi_1(P) \circ \Phi_1(Q)$$

La fonction Φ_1 est donc un morphisme de groupes. $\square$

2 Le cardinal de $C_k(f)$

2.1 Polynômes centrés

Définition 4. Soit $f = \sum_{k=0}^n a_k X^k$ un polynôme de degré $n \geq 1$. Le polynôme f est *centré* lorsque $a_{n-1} = 0$.

Pour alléger les notations, pour tout entier k nous désignerons par $O(X^k)$ un polynôme de degré inférieur ou égal à k .

Proposition 6. Soit $f \in \mathbb{K}[X]$ un polynôme de degré $n > 1$. Alors f est semblable à un polynôme unitaire centré.

Démonstration. Posons $f = \sum_{k=0}^n a_k X^k$. Soit $\lambda = aX + b$ où $a, b \in \mathbb{K}$, $a \neq 0$. On a

$$\lambda^{-1} \circ f \circ \lambda = \frac{1}{a} \left(a_n (aX + b)^n + a_{n-1} (aX + b)^{n-1} + O(X^{n-2}) \right)$$

Le coefficient de degré n de ce polynôme est $a_n a^{n-1}$. Il est égal à 1 si et seulement si a est une racine $(n-1)$ ième de $\frac{1}{a_n}$. Le corps $\mathbb{K}$ étant algébriquement clos, un tel choix est possible. Choisissons un tel a .

Le coefficient de degré $n-1$ de ce même polynôme est

$$\frac{1}{a} \left(n a_n a^{n-1} b + a_{n-1} a^{n-1} \right) = \frac{1}{a} \left(n b + \frac{a_{n-1}}{a_n} \right)$$

Ce coefficient est donc nul si l'on choisit $b = -\frac{a_{n-1}}{n a_n}$. $\square$

Proposition 7. Soit $f \in \mathbb{K}[X]$ un polynôme centré de degré $n > 1$. Soit $k \geq 1$. Soit $g \in C_k(f)$. Alors

- g est centré.
- Si f est unitaire ou si $k = 1$, alors le coefficient dominant b_k de g vérifie $b_k^{n-1} = 1$.

Démonstration. Écrivons $f = a_n X^n + O(X^{n-2})$ et $g = b_k X^k + b_{k-1} X^{k-1} + O(X^{k-2})$. De $f \circ g = g \circ f$, on déduit l'égalité des deux polynômes de degré kn :

$$\begin{aligned} & a_n (b_k X^k + b_{k-1} X^{k-1} + O(X^{k-2}))^n + O(X^{nk-2k}) \\ &= b_k (a_n X^n + O(X^{n-2}))^k + b_{k-1} (a_n X^n + O(X^{n-2}))^{k-1} + O(X^{nk-2k}) \end{aligned}$$

Les termes de degré nk sont égaux, ce qui donne

$$a_n b_k^n = b_k a_n^k$$

ou encore, puisque a_n et b_k sont non nuls,

$$b_k^{n-1} = a_n^{k-1}$$

Dans le cas où f est unitaire, c'est à dire lorsque $a_n = 1$, on obtient effectivement $b_k^{n-1} = 1$. De même, si $k = 1$, $a_n^{k-1} = a_n^0 = 1$ et donc $b_k^{n-1} = 1$.

Les termes de degré $nk - 1$ sont égaux, ce qui donne

$$n a_n b_k^{n-1} b_{k-1} = 0$$

d'où $b_{k-1} = 0$. Le polynôme g est donc centré. $\square$

Nous avons en fait une réciproque.

Proposition 8. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$. Soit $k \geq 1$. Soit $g \neq X \in C_k(f)$. Alors f est centré si et seulement si g est centré.

Démonstration. Supposons f centré. Par la proposition 7, g est centré.

Inversement, supposons g centré. On a $f \in C_n(g)$. Prenons tout d'abord $k > 1$. Par la proposition 7, f est centré. Si $k = 1$, on a $g = bX$ où $b \neq 0, 1$ car g est centré et différent de X . Posons $f = \sum_{m=0}^n a_m X^m$. Comme f et g commutent, il vient

$$\sum_{m=0}^n a_m b^m X^m = b \sum_{m=0}^n a_m X^m$$

Les coefficients égaux de degré n donnent

$$a_n b^n = a_n b$$

et donc $b^n = b$. De même, les coefficients égaux de degré $n - 1$ donnent

$$a_{n-1} b^{n-1} = a_{n-1} b$$

Si $a_{n-1} \neq 0$, alors $b^n = b^{n-1} = b$, ce qui entraîne $b = 1$, contradiction. Ainsi, $a_{n-1} = 0$ et f est centré. $\square$

2.2 Le cardinal de S_f

Proposition 9. Soit f un polynôme centré de degré $n > 1$. Alors les auto-similarités de f sont de la forme $\lambda = bX$ où $b \in \mathbb{U}_{n-1}$ est une racine $(n-1)$ ième de l'unité.

Démonstration. C'est une conséquence immédiate de la proposition 7. $\square$

Corollaire 10. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$. Alors l'ordre du groupe S_f est inférieur ou égal à $n-1$.

Démonstration. f est semblable à un polynôme unitaire centré g , et les groupes S_f et S_g sont isomorphes. $\square$

Notation. Soit $f = \sum_{m=0}^{\infty} a_m X^m \in \mathbb{K}[X]$. On appelle *support* de f l'ensemble

$$\sigma_f = \{m \in \mathbb{N}, a_m \neq 0\}$$

Proposition 11. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$ centré. Alors l'ordre du groupe S_f est

$$|S_f| = \text{pgcd} \{m-1, m \in \sigma_f\}$$

Démonstration. Notons $f = \sum_{m=0}^n a_m X^m$. Par la proposition 9, les éléments de S_f sont de la forme $\lambda = bX$ où $b \in \mathbb{U}_{n-1}$. Pour un tel b , f commute avec $\lambda = bX$ si et seulement si

$$b \sum_{m=0}^n a_m X^m = \sum_{m=0}^n a_m b^m X^m$$

c'est à dire si et seulement si pour tout $m \in \llbracket 0, n \rrbracket$, $ba_m = a_m b^m$, ou encore $a_m(b^{m-1} - 1) = 0$. Ceci revient à dire que pour tout $m \in \llbracket 0, n \rrbracket$ tel que $a_m \neq 0$, $b \in \mathbb{U}_{m-1}$. Ainsi, $\lambda \in S_f$ si et seulement si

$$b \in \bigcap_{m \in \sigma_f} \mathbb{U}_{m-1} = \mathbb{U}_{\delta}$$

où $\delta = \text{pgcd} \{m-1, m \in \sigma_f\}$. $\square$

2.3 Une bijection entre S_f et $C_k(f)$

La proposition ci-dessous est le résultat central de l'article.

Proposition 12. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$. Soit $k \geq 1$. Soient $g, h \in C_k(f)$. Alors $h = \lambda \circ g$ où $\lambda \in S_f$.

Démonstration. Supposons d'abord $f = \sum_{m=0}^n a_m X^m$ centré et unitaire (et donc $a_n = 1$ et $a_{n-1} = 0$). Par la proposition 7, on a alors

$$g = bX^k + \sum_{m=0}^{k-2} b_m X^m$$

et

$$h = cX^k + \sum_{m=0}^{k-2} c_m X^m$$

où $b, c \in \mathbb{U}_{n-1}$. Notons ρ une racine primitive $(n-1)$ ième de l'unité. Il existe alors $i, j \in \llbracket 0, n-2 \rrbracket$ tels que $b = \rho^i$ et $c = \rho^j$. Soit $\alpha = j - i$. Soit $r = \rho^\alpha g - h$. On a alors

$$\begin{aligned} r \circ f &= \rho^\alpha g \circ f - h \circ f \\ &= \rho^\alpha f \circ g - f \circ h \\ &= \rho^\alpha \sum_{m=0}^n a_m g^m - \sum_{m=0}^n a_m h^m \\ &= a_n((\rho^\alpha g)^n - h^n) + O(X^{k(n-2)}) \\ &= (\rho^\alpha g - h) \sum_{s=0}^{n-1} (\rho^\alpha g)^{n-1-s} h^s + O(X^{k(n-2)}) \end{aligned}$$

On a utilisé à l'avant-dernière ligne le fait que $\rho^\alpha \in \mathbb{U}_{n-1}$, et donc :

$$(\rho^\alpha)^n = \rho^\alpha (\rho^\alpha)^{n-1} = \rho^\alpha$$

Remarquons que

$$d^o \left(\sum_{s=0}^{n-1} (\rho^\alpha g)^{n-1-s} h^s \right) = k(n-1)$$

En effet, ce polynôme est clairement de degré inférieur ou égal à $k(n-1)$, et son coefficient de degré $k(n-1)$ est

$$\sum_{s=0}^{n-1} (\rho^\alpha)^{n-s-1} (\rho^i)^{n-s-1} (\rho^j)^s = n$$

Remarquons que $t = d^o r < k$. Par le calcul ci-dessus, on a

$$d^o(r \circ f) = tn = t + k(n-1)$$

d'où, si $t \neq -\infty$, $t = k$. Contradiction. Ainsi, $t = -\infty$ et donc $r = 0$. Ainsi, $h = \rho^\alpha g = \lambda \circ g$ où $\lambda = \rho^\alpha X$.

Montrons maintenant que $\lambda = \rho^\alpha X \in S_f$. On a $f \circ h = h \circ f$, et donc

$$f \circ \lambda \circ g = f \circ (\rho^\alpha g) = \rho^\alpha g \circ f = \rho^\alpha f \circ g = \lambda \circ f \circ g$$

Ainsi,

$$(f \circ \lambda) \circ g = (\lambda \circ f) \circ g$$

et donc $f \circ \lambda = \lambda \circ f$ par la proposition 1. Ainsi, $\lambda \in S_f$.

Considérons pour terminer le cas général, où f n'est pas nécessairement centré et unitaire. Par la proposition 6, il existe μ de degré 1 tel que $\mu^{-1} \circ f \circ \mu = \hat{f}$ soit centré et unitaire. Soient $\hat{g} = \mu^{-1} \circ g \circ \mu$ et $\hat{h} = \mu^{-1} \circ h \circ \mu$. On a

$$\hat{g} \circ \hat{f} = \mu^{-1} \circ (g \circ f) \circ \mu = \mu^{-1} \circ (f \circ g) \circ \mu = \hat{f} \circ \hat{g}$$

et, de même,

$$\hat{h} \circ \hat{f} = \hat{f} \circ \hat{h}$$

Ainsi, Il existe $\lambda \in S_{\hat{f}}$ tel que $\hat{h} = \lambda \hat{g}$, c'est à dire

$$\mu^{-1} \circ h \circ \mu = \lambda \circ \mu^{-1} \circ g \circ \mu$$

d'où

$$h = (\mu \circ \lambda \circ \mu^{-1}) \circ g = \nu \circ g$$

Il ne reste plus qu'à montrer que $\nu \in S_f$:

$$\begin{aligned}\nu \circ f &= \mu \circ \lambda \circ \mu^{-1} \circ f \\ &= \mu \circ \lambda \circ \hat{f} \circ \mu^{-1} \\ &= \mu \circ \hat{f} \circ \lambda \circ \mu^{-1} \\ &= f \circ \mu \circ \lambda \circ \mu^{-1} \\ &= f \circ \nu\end{aligned}$$

□

Examinons maintenant la réciproque de la proposition précédente.

Proposition 13. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$. Soit λ un polynôme de degré 1. Soit $k \geq 1$. Soit $g \in C_k(f)$. Alors $\lambda \circ g \in C_k(f)$ si et seulement si $\lambda \in S_f$.

Démonstration. Supposons que $\lambda \circ g \in C_k(f)$. Par la proposition précédente, il existe $\mu \in S_f$ tel que $\lambda \circ g = \mu \circ g$. De là, $\lambda = \mu \in S_f$ par la proposition 1.

Supposons inversement que $\lambda \in S_f$. On a alors

$$\lambda \circ g \circ f = \lambda \circ f \circ g = f \circ \lambda \circ g$$

et donc $\lambda \circ g \in C_k(f)$. □

Proposition 14. Soit $f \in \mathbb{K}[X]$ de degré $n > 1$. Soit $k \geq 1$. Supposons que $C_k(f) \neq \emptyset$. Alors

$$|C_k(f)| = |S_f|$$

Démonstration. Soit $g \in C_k(f)$. Par la proposition 13, pour tout $\lambda \in S_f$, $\lambda \circ g \in C_k(f)$. On définit donc une application $\Psi : S_f \rightarrow C_k(f)$ en posant $\Psi(\lambda) = \lambda \circ g$.

L'application Ψ est injective. En effet, si $\Psi(\lambda) = \Psi(\mu)$, alors $(\lambda - \mu) \circ g = 0$ et donc $\lambda = \mu$ par la proposition 1.

L'application Ψ est surjective par la proposition 12. □

Corollaire 15. Soit f un polynôme centré de degré $n > 1$. Soit $k \geq 1$. Si $C_k(f)$ est non vide, alors

$$|C_k(f)| = \text{pgcd} \{k-1, k \in \sigma_f\}$$

Démonstration. C'est une conséquence immédiate des propositions 11 et 14. En particulier, ce cardinal est inférieur ou égal à $n-1$. □

3 Deux exemples

3.1 Les puissances de X

Posons, pour tout entier n , $P_n = X^n$. Les polynômes P_n commutent évidemment entre-eux et donc, pour tous entiers n et k , $C_k(P_n)$ est non vide (car il contient P_k). Le support de P_n est $\sigma_{P_n} = \{n\}$. Pour $n > 1$ et $k \geq 1$, on a donc

$$|C_k(P_n)| = n-1$$

Remarquons maintenant que pour tout $b \in \mathbb{U}_{n-1}$,

$$P_n \circ (bX^k) = b^n X^{nk} = b(X^n)^k = (bX^k) \circ P_n$$

Ainsi,

$$C_k(P_n) = \{bX^k, b \in \mathbb{U}_{n-1}\}$$

3.2 Les polynômes de Tchebychev

Définissons la suite $(T_n)_{n \geq 0}$ des polynômes de Tchebychev par $T_0 = 1$, $T_1 = X$, et, pour tout entier n , $T_{n+2} = 2XT_{n+1} - T_n$. On a les propriétés ci-dessous :

- T_n est de degré n .
- T_n a la même parité que n . Ainsi, les polynômes T_n sont centrés.
- $T_n \circ \frac{1}{2}(X + \frac{1}{X}) = \frac{1}{2}(X^n + \frac{1}{X^n})$ (par récurrence sur n). De là,
- $T_n \circ T_k = T_{nk}$, et donc $T_n \circ T_k = T_k \circ T_n$.
- $\sigma_{T_n} = \{n, n-2, n-4, \dots\}$ (moins évident).

Pour tous entiers $n > 1$ et $k \geq 1$, l'ensemble $C_k(T_n)$ contient T_k , il est donc non vide. Ainsi,

$$|C_k(T_n)| = |S_{T_n}| = \text{pgcd} \{m-1, m \in \sigma_{T_n}\} = \text{pgcd} \{n-1, n-3, \dots\}$$

Si $n \geq 2$ est pair, ce pgcd vaut 1. Il en résulte que

$$C_k(T_n) = \{T_k\}$$

Si $n \geq 3$ est impair, ce pgcd vaut 2. Comme T_n est impair et commute avec T_k , T_n commute aussi avec $-T_k$. Ainsi,

$$C_k(T_n) = \{T_k, -T_k\}$$

Références

- [Boy72] William M. Boyce. On polynomials which commute with a given polynomial. *Proceedings of the American Mathematical Society*, 1972.
- [BT50] H. D. Block and H. P. Thielman. Commutative polynomials. 1950.
- [Wil] Samuel Williams. An analysis of polynomials that commute under composition.
- [Zim07] Karl Zimmermann. Commuting polynomials and self-similarity. *New York Journal of Mathematics*, 2007.