Question 826

Vincent DEVINCK

Question. Soit un entier $a > 2$. Déterminer les polynômes P de $\mathbb{R}[X]$ tels que

$$P(X^a + 1) = (P(X))^a + 1.$$

Moubinool Omarjee

Solution. Posons $Q_a(X) = X^a + 1$. Remarquons qu'on cherche le commutant du polynôme Q_a dans $\mathbb{R}[X]$:

$$\mathcal{C}(Q_a) := \big\{P \in \mathbb{R}[X]\,;\, P \circ Q_a = Q_a \circ P\big\} = \big\{P \in \mathbb{R}[X]\,;\, P(X^a + 1) = (P(X))^a + 1\big\}$$

Dans la suite, on notera Q_a^n les *itérées* (au sens de la composition) du polynôme Q_a ; elles sont définies par

$$\begin{cases} Q_a^0(X) = X & \text{(identité)} \\ \forall n \in \mathbb{N},\ Q_a^{n+1}(X) = Q_a(Q_a^n(X)) \end{cases}$$

Donc $Q_a^1(X) = X^a + 1$, $Q_a^2(X) = (X^a + 1)^a + 1, \ldots$ On a clairement l'inclusion

$$\big\{Q_a^n\,;\, n \in \mathbb{N}\big\} \subset \mathcal{C}(Q_a)$$

La réponse à la question fait l'objet de la proposition suivante.

Proposition 1. 1. *Si l'entier a est pair, alors le commutant de Q_a coïncide avec l'ensemble de ses itérées* :

$$\mathcal{C}(Q_a) = \big\{Q_a^n\,;\, n \in \mathbb{N}\big\}$$

2. *Si a est impair ($a \geqslant 3$), alors*

$$\mathcal{C}(Q_a) = \big\{Q_a^n\,;\, n \in \mathbb{N}\big\} \cup \big\{\textit{le point fixe de } Q_a\big\}$$

Démonstration. Dans un premier temps, nous chercherons les polynômes constants solutions, puis nous nous intéresserons aux polynômes de degré 1 et nous traiterons enfin le cas général d'un polynôme solution de degré supérieur ou égal à 2.

- Commençons par chercher les polynômes constants qui commutent avec Q_a. Soit $P \in \mathbb{R}[X]$ un polynôme constant. En notant c la valeur constante prise par P, alors $P \in \mathcal{C}(Q_a)$ si et seulement si $c = c^a + 1$ (c'est-à-dire si et seulement si c est un point fixe de Q_a). On cherche donc si la fonction polynôme

$$f_a : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^a - x + 1 \end{cases}$$

s'annule. On distingue suivant la parité de a. Si $a = 2b$ est pair ($b \in \mathbb{N}^*$), alors on trouve que la fonction f_a est décroissante sur $]-\infty, \alpha]$ puis croissante sur $[\alpha, +\infty[$ où on a posé $\alpha = \left(\dfrac{1}{2b}\right)^{\frac{1}{2b-1}}$. Donc f_a présente un minimum en α qui vaut

$$f_a(\alpha) = \left(\frac{1}{2b}\right)^{\frac{2b}{2b-1}} \left[1 - 2b + (2b)^{1+\frac{1}{2b-1}}\right] > 0$$

Donc la fonction f_a ne s'annule pas sur $\mathbb{R}$, ce qui montre que le commutant de Q_a ne contient pas de polynômes constants. Supposons maintenant que $a = 2b + 1$ est impair ($b \in \mathbb{N}^*$). Posons $\beta = \left(\dfrac{1}{2b+1}\right)^{\frac{1}{2b}}$. On trouve le tableau de variations suivant :

x	$-\infty$		$-\beta$		β		$+\infty$
$f_a'(x)$		$+$	0	$-$	0	$+$	
$f_a(x)$	$-\infty$	$\nearrow$	$f_a(-\beta)$	$\searrow$	$f_a(\beta)$	$\nearrow$	$+\infty$

et un simple calcul (analogue à celui du cas pair) montre que $f_a(-\beta) > f_a(\beta) > 0$. La fonction f_a s'annule donc une et une seule fois et cela sur l'intervalle $]-\infty, -\beta[$.

- Soit $P(X) = \lambda X + \mu \in \mathbb{R}[X]$ un polynôme de degré 1 (donc $\lambda \in \mathbb{R}^*$). En appliquant la formule du binôme de Newton et en identifiant les coefficients des polynômes, il vient

$$\begin{aligned}
P \in \mathcal{C}(Q_a) &\iff \lambda(X^a + 1) + \mu = (\lambda X + \mu)^a + 1 \\
&\iff \lambda X^a + \lambda + \mu = \lambda^a X^a + \sum_{k=1}^{a-1} \binom{a}{k} \lambda^k \mu^{a-k} X^k + \mu^a + 1 \\
&\iff \left\{ \begin{array}{c} \lambda^a = \lambda \\ \forall k \in [\![1, a-1]\!],\ \lambda^k \mu^{a-k} = 0 \\ \lambda + \mu = \mu^a + 1 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \lambda = 1 \\ \mu = 0 \end{array} \right.
\end{aligned}$$

car $\lambda \neq 0$. On trouve donc que le seul polynôme de degré 1 appartenant au commutant de Q_a est $Q_a^0(X) = X$.

- Passons au cas général. Soit $P \in \mathcal{C}(Q_a)$ de degré supérieur ou égal à 2. L'égalité $P(X^a + 1) = (P(X))^a + 1$ nous donne, en posant $\omega = \mathrm{e}^{\frac{2\,\mathrm{i}\,\pi}{a}}$, l'égalité $\left(\dfrac{P(\omega X)}{P(X)}\right)^a = 1$. En se plaçant sur une composante connexe C de l'intervalle de définition de la fonction rationnelle $x \longmapsto \dfrac{P(\omega x)}{P(x)}$, on trouve qu'il existe $k \in [\![0, a-1]\!]$ tel que cette fonction soit constante égale à ω^k sur C (par continuité de la fonction rationnelle sur C). Les polynômes $P(\omega X)$ et $\omega^k P(X)$ coïncident alors en une infinité de valeurs donc $P(\omega X) = \omega^k P(X)$. Nous allons montrer que $k = 0$ en raisonnant par l'absurde. Si $k \in [\![1, a-1]\!]$, alors en substituant à X la valeur 0, il vient $P(0) = \omega^k P(0)$ ce qui impose que $P(0) = 0$ puisque $\omega^k \neq 1$. Si on définit la suite $(u_n)_{n\in\mathbb{N}}$ par $u_0 = 0$ et $u_{n+1} = u_n^a + 1$ pour tout entier naturel n, alors une récurrence immédiate montre qu'on a $P(u_n) = u_n$ pour tout entier naturel n. Par conséquent, on a l'égalité $P(X) = X$, ce qui est absurde car on a supposé que $\deg(P) \geqslant 2$. Posons maintenant

$$P(X) = \sum_{j=0}^{d} c_j X^j \qquad \text{où} \quad c_j \in \mathbb{R} \quad \text{et} \quad d = \deg(P) \geqslant 2$$

L'égalité $P(\omega X) = P(X)$ fournit, en identifiant les coefficients des deux polynômes :

$$\forall j \in [\![0, d]\!], \qquad j \not\equiv 0 \pmod{a} \Longrightarrow c_j = 0$$

En particulier, le degré n de P est un multiple de a (notons le $d = am$ où $m \in \mathbb{N}^*$) et on a

$$P(X) = \sum_{j=0}^{m} c_{aj} (X^a)^j$$

Par conséquent, $P(X)$ appartient à l'espace vectoriel vect$\big\{(X^a)^k\,;\;k\in [\![0,m]\!]\big\}$ dont la famille $\big((X^a+1)^k\big)_{k\in[\![0,m]\!]}$ en est une base. Il existe donc un (unique) polynôme $R(X)\in\mathbb{R}[X]$ tel que $P(X)=R(Q_a(X))$. Donc

$$\begin{aligned} P\in\mathcal{C}(Q_a) &\iff P\circ Q_a=Q_a\circ P\\ &\iff (R\circ Q_a)\circ Q_a=(Q_a\circ R)\circ Q_a\\ &\iff R\in\mathcal{C}(Q_a)\end{aligned}$$

car les polynômes $R\circ Q_a$ et $Q_a\circ R$ prennent la même valeur en une infinité de points. De plus, $\deg(R)=\frac{\deg(P)}{a}<\deg(P)$. Ou bien $\deg(R)=1$, auquel cas $R(X)=X$ (d'après le deuxième point) et $P=Q_a$, ou bien $\deg(R)\geqslant 2$ et on itère le raisonnement précédent. Un raisonnement par récurrence montre alors qu'il existe $k\in\mathbb{N}^*$ tel que $P(X)=Q_a^k(X)$. La proposition est démontrée. □

Remarques.

- La proposition précédente prend aussi en compte le cas $a=2$.
- Un calcul immédiat montre que pour $a=1$, on a

$$\mathcal{C}(X+1)=\big\{X+\lambda\,;\;\lambda\in\mathbb{R}\big\}$$