Quatrième composition de mathématiques [corrigé]

Exercice 1

Déterminer si le polynôme $P = X^5 - X - 1$ possède des racines complexes multiples.

Nous allons montrer que ça n'est pas le cas. Soit (par l'absurde) $z \in \mathbb{C}$ *une racine multiple de* P.

La racine z *est alors également racine de* $P' = 5X^4 - 1$, *c'est-à-dire qu'elle vérifie* $z^4 = \dfrac{1}{5}$.

En multipliant par z, *on en déduit* $z^5 = \dfrac{z}{5}$. *Mais la condition* $P(z) = 0$, *elle, impose* $z^5 = z + 1$.

On en déduit $z + 1 = \dfrac{z}{5}$, *c'est-à-dire* $z = -\dfrac{4}{5}$.

Mais cela est impossible, car $\left(-\dfrac{4}{5}\right)^4 = \dfrac{2^8}{5^4} \neq \dfrac{1}{5}$ *(les deux fractions sont irréductibles).*

Cela conclut : toutes les racines (complexes) de P *sont simples.*

Exercice 2

Soit $a, b, c \in \mathbb{C}$ trois nombres complexes non nuls tels que $a + b + c = \dfrac{1}{a} + \dfrac{1}{b} + \dfrac{1}{c} = 0$.

1. Calculer le polynôme $P = (X - a)(X - b)(X - c)$.

   Le calcul donne $P = X^3 - (a + b + c)X^2 + (ab + bc + ac)X - abc$, *les coefficients de degré* 2 *et* 0 *étant par ailleurs donnés par les relations coefficients racines.*

   L'hypothèse $a + b + c = 0$ *est directement exploitable.*

   Pour la deuxième, remarquons que $\dfrac{1}{a} + \dfrac{1}{b} + \dfrac{1}{c} = \dfrac{bc + ac + ab}{abc}$, *si bien que* $bc + ac + ab = 0$.

   Ainsi, en notant $p = abc$ *le produit des racines, on a* $P = X^3 - p$.

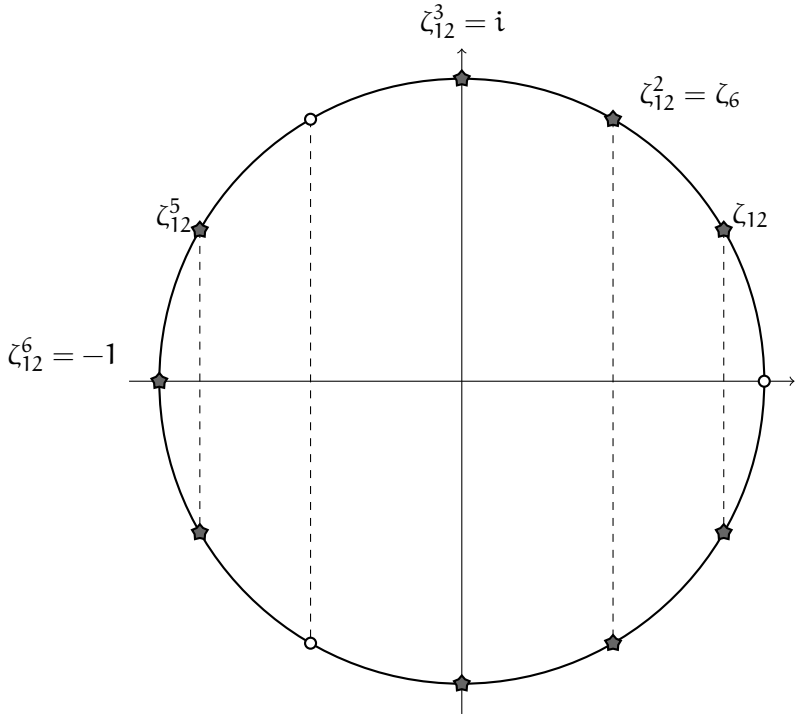
2. En déduire $|a| = |b| = |c|$.

   Le cours sur les complexes garantit que, puisque a *est une racine de* P, ***les*** *racines de* P *sont* a, ja *et* j^2a, *si bien qu'elles ont effectivement toutes le même module.*

Exercice 3

Décomposer $P = X^9 + X^6 + X^3 + 1$ en produit de polynômes irréductibles, dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

On a $(X^3 - 1)P = X^{12} - 1$, *donc la factorisation dans* $\mathbb{C}[X]$ *est* $P = \prod_{\omega \in \mathbb{U}_{12} \setminus \mathbb{U}_3} (X - \omega)$.



En rassemblant les facteurs conjugués (on rappelle que, pour $z \in \mathbb{C} \setminus \mathbb{R}$, *le polynôme minimal réel* P_z *est* $(X - z)(X - \bar{z}) = X^2 - 2\,\mathrm{Ré}(z)X + |z|^2$*), on obtient la factorisation dans* $\mathbb{R}[X]$ *:*

$$\begin{aligned} P &= P_{\zeta_{12}} P_{\zeta_6} P_i P_{\zeta_{12}^5}(X+1) \\ &= \left(X^2 - 2\cos\left(\frac{\pi}{6}\right)X + 1\right)\left(X^2 - 2\cos\left(\frac{\pi}{3}\right)X + 1\right)(X^2+1)\left(X^2 - 2\cos\left(\frac{5\pi}{6}\right)X + 1\right)(X+1) \\ &= \left(X^2 - \sqrt{3}X + 1\right)\left(X^2 - X + 1\right)\left(X^2 + 1\right)\left(X^2 + \sqrt{3}X + 1\right)(X+1). \end{aligned}$$

Exercice 4. Équation (matricielle) de Fermat.

On note $M_2(\mathbb{Z})$ l'ensemble des matrices 2×2 dont les quatre coefficients sont des entiers relatifs.

Soit $n \geqslant 2$. Dans cet exercice, on cherche des solutions à l'équation $(F_n) : A^n + B^n = C^n$, sous la forme d'un triplet $(A, B, C) \in M_2(\mathbb{Z})^3$, sous certaines conditions de non-trivialité.

1. (a) Pour $i, j \in \{1, 2\}$, calculer la puissance $E_{i,j}^n$ de la matrice élémentaire $E_{i,j}$.

   Soit $i, j \in \{1, 2\}$.
   - *Si* $i = j$, *on a* $E_{i,j}^2 = E_{i,j} E_{i,j} = E_{i,j}$, *et une récurrence immédiate entraîne* $\forall k \geqslant 2, E_{i,j}^k = E_{i,j}$. *En particulier,* $E_{i,j}^n = E_{i,j}$.
   - *Si* $i \neq j$, *on a d'après le cours* $E_{i,j}^2 = E_{i,j} E_{i,j} = 0$. *Ainsi,* $E_{i,j}^n = E_{i,j}^2 E_{i,j}^{n-2} = 0$.

   (b) En déduire que (F_n) possède une solution $(A, B, C) \in M_2(\mathbb{Z})^3$, avec A, B et C non nulles.

   On a $E_{1,1}^n + E_{2,2}^n = E_{1,1} + E_{2,2} = I_2 = I_2^n$, *si bien que* $(E_{1,1}, E_{2,2}, I_2) \in M_2(\mathbb{Z})^3$ *est une solution de* (F_n) *constituée de matrices non nulles.*

   Remarque. *Rien n'interdisait que* B^n, *par exemple, soit nulle. Il y a donc plein d'autres solutions, plus ou moins dégénérées, parmi lesquelles* $(E_{1,1}, E_{1,2}, E_{1,1})$ *et* $(E_{1,2}, E_{1,2}, E_{1,2})$.

2. **Compléments sur le déterminant** 2×2**.**

   (a) Montrer $\forall A, B \in M_2(\mathbb{R}), \det(AB) = \det(A)\ \det(B)$.

   Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *et* $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{R})$. *On a*

$$\begin{aligned}
\det(AB) &= \begin{vmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{vmatrix} \\
&= (a\alpha + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) \\
&= \big(ac\alpha\beta + ad\alpha\delta + bc\beta\gamma + bd\gamma\delta\big) - \big(ac\alpha\beta + ad\beta\gamma + bc\alpha\delta + bd\gamma\delta\big) \\
&= ad\alpha\delta + bc\beta\gamma - ad\beta\gamma - bc\alpha\delta \\
&= ad(\alpha\delta - \beta\gamma) + bc(\beta\gamma - \alpha\delta) \\
&= (ad - bc)(\alpha\delta - \beta\gamma) \\
&= \det(A)\ \det(B).
\end{aligned}$$

   (b) **Théorème de Cayley-Hamilton pour les matrices** 2×2**.** Soit $A \in M_2(\mathbb{R})$. Montrer qu'il existe $\delta \in \mathbb{R}$ (que l'on déterminera) tel que $A^2 - \mathrm{tr}(A)\, A = \delta\, I_2$.

   Soit $a, b, c, d \in \mathbb{R}$ *tels que* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *On a*

$$\begin{aligned}
A^2 &= \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} \\
\textit{donc} \qquad A^2 - \mathrm{tr}(A)\, A &= \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} - (a + d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} - \begin{pmatrix} a^2 + ad & ab + bd \\ ac + cd & ad + d^2 \end{pmatrix} \\
&= \begin{pmatrix} bc - ad & 0 \\ 0 & bc - ad \end{pmatrix} \\
&= -(ad - bc) I_2,
\end{aligned}$$

   ce qui conclut, avec $\delta = -(ad - bc) = -\det(A)$.

Dans la suite de l'exercice, on note $\mathrm{GL}_2(\mathbb{Z}) = \left\{ A \in \mathrm{M}_2(\mathbb{Z}) \,\middle|\, \det A \in \{-1, 1\} \right\}$.

3. Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est stable par produit et par passage à l'inverse.

   ▸ *Soit* $A, B \in \mathrm{GL}_2(\mathbb{Z})$.
   - *La formule pour le produit de deux matrices montre clairement que* $AB \in \mathrm{M}_2(\mathbb{Z})$.
   - *D'après la question 2a, on a* $\det(AB) = \det(A)\,\det(B)$. *Comme* $\{\pm 1\}$ *est stable par produit, on en déduit* $\det(AB) \in \pm 1$.

   Ainsi, $AB \in \mathrm{GL}_2(\mathbb{Z})$.

   ▸ *Soit* $A \in \mathrm{GL}_2(\mathbb{Z})$.

   Déjà, $\det A = \pm 1 \neq 0$, *donc la matrice* A *est inversible. Il reste à montrer que* $A^{-1} \in \mathrm{GL}_2(\mathbb{Z})$.

   - *Notons* a, b, c *et* d *les coefficients de* A, *si bien que* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

     On sait alors que $A^{-1} = \dfrac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, *donc* $A^{-1} \in \mathrm{M}_2(\mathbb{Z})$.
   - *Toujours d'après la question 2a, on a* $\det(A)\,\det(A^{-1}) = \det(AA^{-1}) = \det(I_2) = 1$, *ce qui entraîne* $\det(A^{-1}) = \dfrac{1}{\det A} = \dfrac{1}{\pm 1} = \pm 1$.

   Ainsi, $A^{-1} \in \mathrm{GL}_2(\mathbb{Z})$.

4. (a) Déterminer toutes les matrices triangulaires $T \in \mathrm{M}_2(\mathbb{Z})$ telles que $T^2 = I_2$.

   Comme, pour tout $A \in \mathrm{M}_2(\mathbb{R})$, $(A^T)^2 = A^T A^T = (AA)^T = (A^2)^T$, *il suffit de traiter le cas des matrices triangulaires supérieures.*

   Analyse. *Soit* $T \in \mathrm{M}_2(\mathbb{Z})$ *triangulaire supérieure telle que* $T^2 = I_2$. *On peut trouver* $a, b, d \in \mathbb{Z}$ *tels que* $T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. *La relation* $T^2 = I_2$ *donne* $\begin{pmatrix} a^2 & ab + bd \\ 0 & d^2 \end{pmatrix} = I_2$, *c'est-à-dire les égalités* $a^2 = d^2 = 1$ *et* $(a + d)b = 0$. *Les premières égalités donnent déjà* $a, d \in \{\pm 1\}$. *On distingue alors deux cas.*

   ▸ *Si* $a = d$, *on a* $a + d \neq 0$, *si bien que la deuxième relation donne* $b = 0$.

   On a donc $T = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\, I_2 = \pm I_2$.

   ▸ *Si* $a = -d$, *la deuxième relation est inintéressante. Suivant* a, *on a alors* $T = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ *ou* $T = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$, *ce que l'on résumera en disant que* T *est du type* $\begin{pmatrix} \pm 1 & * \\ 0 & \mp 1 \end{pmatrix}$.

   Synthèse. *Réciproquement, il est clair que* $\pm I_2$ *et les matrices du type* $\begin{pmatrix} \pm 1 & * \\ 0 & \mp 1 \end{pmatrix}$ *sont triangulaires supérieures et un calcul immédiat montre que leur carré est* I_2.

   En réincorporant les matrices triangulaires inférieures, on obtient trois classes de matrices triangulaires dont le carré vaut I_2, *à savoir* $\pm I_2$, $\begin{pmatrix} \pm 1 & * \\ 0 & \mp 1 \end{pmatrix}$ *et* $\begin{pmatrix} \pm 1 & 0 \\ * & \mp 1 \end{pmatrix}$.

(b) En déduire qu'il existe $A, B \in \mathrm{GL}_2(\mathbb{Z})$ telles que $A^2 = B^2 = I_2$ et $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

D'après la question précédente, les matrices triangulaires $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ *et* $B = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$ *vérifient* $A^2 = B^2 = I_2$.

Un calcul (trivial) de déterminant montre que $\det A = \det B = -1$, *et un calcul (encore plus trivial) de somme montre que* $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(c) On suppose n impair. Montrer que (F_n) possède une solution $(A, B, C) \in \mathrm{GL}_2(\mathbb{Z})^3$.

On garde les deux matrices de la question précédente, et on pose $C = A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *qui est elle-même de déterminant* -1, *et donc élément de* $\mathrm{GL}_2(\mathbb{Z})$.

Comme $n \geqslant 2$ *est impair, on peut trouver un entier* $m \in \mathbb{N}^*$ *tel que* $n = 2m + 1$. *On en déduit* $A^n = (A^2)^m A = I_2^m A = A$ *et, pour la même raison,* $B^n = B$ *et* $C^n = C$.

On a donc $A^n + B^n = A + B = C = C^n$, *si bien que l'équation* (F_n) *possède bel et bien une solution dans* $\mathrm{GL}_2(\mathbb{Z})^3$.

5. Le but de cette question est de montrer que (F_6) ne possède pas de solution $(A, B, C) \in \mathrm{GL}_2(\mathbb{Z})^3$. Le théorème de Cayley-Hamilton (question 2b) sera utile.

On note $\mathscr{E} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) \;\middle|\; a, d \text{ impairs et } b, c \text{ pairs} \right\}$.

(a) Soit $M \in \mathrm{GL}_2(\mathbb{Z})$ telle que $\mathrm{tr}(M)$ soit paire. Montrer que $M^2 \in \mathscr{E}$.

La définition de $\mathscr{E}$, *avec ses conditions de parité sur les coefficients, rend assez évident que si* $U \in \mathscr{E}$ *et* $V \in \mathrm{M}_2(\mathbb{Z})$, *alors* $U + kV \in \mathscr{E}$, *pour tout entier pair* k. *On va utiliser cette remarque (qui est pour ainsi dire une manière de « travailler modulo 2 » dans* $\mathrm{M}_2(\mathbb{Z})$*).*

Le théorème de Cayley-Hamilton donne $M^2 = \mathrm{tr}(M)M - \det(M)I_2 = \mathrm{tr}(M)\, M \mp I_2$.

Comme $\mp I_2 \in \mathscr{E}$ *et que* $\mathrm{tr}(M)$ *est paire, la remarque liminaire montre que* $M^2 \in \mathscr{E}$.

(b) Soit $M \in \mathrm{GL}_2(\mathbb{Z})$. Montrer que $\mathrm{tr}(M^3)$ est paire.

En passant à la trace le théorème de Cayley-Hamilton, on obtient (par linéarité de la trace) l'égalité $\mathrm{tr}(M^2) = \mathrm{tr}(M)^2 \mp \mathrm{tr}(I_2) = \mathrm{tr}(M)^2 \mp 2$, *qui montre que* $\mathrm{tr}(M^2)$ *est de la même parité que* $\mathrm{tr}(M)^2$, *c'est-à-dire de la même parité que* $\mathrm{tr}(M)$. *Ainsi,* $\mathrm{tr}(M)$ *et* $\mathrm{tr}(M^2) \mp 1$ *sont de parités opposées.*

En multipliant (à gauche ou à droite, cela ne change rien) par M *la relation donnée par le théorème de Cayley-Hamilton, on obtient* $M^3 = \mathrm{tr}(M)\, M^2 \mp M$.

En passant à la trace, il vient $\mathrm{tr}(M^3) = \mathrm{tr}(M)\ \mathrm{tr}(M^2) \mp \mathrm{tr}(M) = \mathrm{tr}(M) \left[\mathrm{tr}(M^2) \mp 1\right]$. *Ce nombre étant le produit de deux facteurs de parités opposées, il est pair.*

(c) Conclure.

Supposons par l'absurde qu'il existe $A, B, C \in \mathrm{GL}_2(\mathbb{Z})$ *telles que* $A^6 + B^6 = C^6$.

En appliquant les deux questions précédentes, on obtient d'abord que A^3 *est de trace paire, puis que* $(A^3)^2 = A^6$ *appartient à* $\mathscr{E}$. *De même,* B^6 *et* C^6 *appartiennent à* $\mathscr{E}$.

Cela fournit la contradiction souhaitée en examinant les coefficients diagonaux : par exemple, $[A^6]_{1,1}$ *et* $[B^6]_{1,1}$ *ne peuvent pas être tous les deux impairs, puisque que leur somme est* $[C^6]_{1,1}$, *lui-même censé être impair.*

Exercice 5

Le but de cet exercice est de déterminer les polynômes $P \in \mathbb{R}[X]$ tels que $P(X^2+1) = P^2+1$. $(*)$

On note $Q = X^2+1$, si bien que la relation $(*)$ s'écrit également $P \circ Q = Q \circ P$.

On note enfin

$$\mathscr{P} = \big\{A \in \mathbb{R}[X] \,\big|\, A(-X) = A\big\} \qquad \text{et} \qquad \mathscr{I} = \big\{B \in \mathbb{R}[X] \,\big|\, B(-X) = -B\big\}$$

les ensembles des polynômes *pairs* et *impairs*, respectivement.

1. Soit $R \in \mathbb{R}[X]$. Montrer qu'il existe un unique couple $(A,B) \in \mathscr{P} \times \mathscr{I}$ tels que $R = A+B$.

   On recopie la démonstration faite pour les fonctions en début d'année.

   Analyse. *Soit* $(A,B) \in \mathscr{P} \times \mathscr{I}$ *tels que* $R = A+B$.

   En composant avec $-X$, *on obtient* $R(-X) = A(-X) + B(-X) = A - B$.

   En faisant la demi-somme et la demi-différence, on obtient $A = \dfrac{R+R(-X)}{2}$ *et* $B = \dfrac{R-R(-X)}{2}$.

   Synthèse. *Posons* $A = \dfrac{R+R(-X)}{2}$ *et* $B = \dfrac{R-R(-X)}{2}$.

   - *Il est clair que* $R = A+B$.
   - *On a* $A(-X) = \dfrac{R(-X)+R(X)}{2} = A$, *donc* $A \in \mathscr{P}$.
   - *On a* $B(-X) = \dfrac{R(-X)-R(X)}{2} = -B$, *donc* $B \in \mathscr{I}$.

   Cela démontre $\exists!(A,B) \in \mathscr{P} \times \mathscr{I} : R = A+B$.

2. Soit $B \in \mathbb{R}[X]$. Montrer que $B \in \mathscr{I}$ si et seulement s'il existe $A \in \mathscr{P}$ tel que $B = XA$.

   Sens direct. *Supposons* $B \in \mathscr{I}$. *En particulier,* $B(0) = B(-0) = -B(0)$, *si bien que* $B(0) = 0$. *Par le lemme de factorisation, on peut trouver* $A \in \mathbb{R}[X]$ *tel que* $B = XA$.

   La relation $B(-X) = -B(X)$ *donne* $-XA(-X) = -XA(X)$, *si bien que* $X\big(A(X) - A(-X)\big) = 0$. *Par la règle du produit nul (comme* X *n'est pas le polynôme nul), on en déduit* $A(X) - A(-X) = 0$, *c'est-à-dire* $A \in \mathscr{P}$.

   Sens réciproque. *Supposons pouvoir trouver* $A \in \mathscr{P}$ *tel que* $B = XA$.

   On a alors $B(-X) = -XA(-X) = -XA(X) = -B$, *si bien que* $B \in \mathscr{I}$.

3. Soit $A \in \mathbb{R}[X]$. Montrer que $A \in \mathscr{P}$ si et seulement s'il existe $\widetilde{A} \in \mathbb{R}[X]$ tel que $A = \widetilde{A}(X^2)$.

   On procède par double implication.

   Sens direct. *Supposons* $A \in \mathscr{P}$. *On peut trouver un entier* $n \in \mathbb{N}$ *tel que* $\deg A \leqslant 2n$ *(ce qui simplifie les écritures), donc on peut trouver* $a_0, \dots, a_{2n} \in \mathbb{R}$ *tels que* $A = \displaystyle\sum_{k=0}^{2n} a_k X^k$.

   On a alors $A = A(-X) = \displaystyle\sum_{k=0}^{2n} a_k (-X)^k = \sum_{k=0}^{2n} (-1)^k a_k X^k$.

   En identifiant les coefficients, on obtient $\forall k \in [\![0, 2n]\!]$, $a_k = (-1)^k a_k$. *En particulier, pour tout indice* $k \in [\![0, 2n]\!]$, $a_k = -a_k$, *donc* $a_k = 0$. *On peut éliminer ces coefficients de la somme et écrire alors* $A = \displaystyle\sum_{\ell=0}^{n} a_{2\ell} X^{2\ell} = \widetilde{A} \circ X^2$, *en posant* $\widetilde{A} = \displaystyle\sum_{\ell=0}^{n} a_{2\ell} X^\ell$.

Sens réciproque. *Supposons pouvoir trouver* $\widetilde{A} \in \mathbb{R}[X]$ *tel que* $A = \widetilde{A}(X^2)$.

On a alors $A(-X) = \widetilde{A}\big((-X)^2\big) = \widetilde{A}(X^2) = A$, *ce qui montre* $A \in \mathscr{P}$.

4. (a) Soit $R \in \mathbb{R}[X]$ tel que R^2 soit un polynôme pair. Montrer $R \in \mathscr{P} \cup \mathscr{I}$.

Remarquons rapidement qu'il est assez clair que le produit de deux éléments de $\mathscr{P}$ *et le produit de deux éléments de* $\mathscr{I}$ *sont éléments de* $\mathscr{P}$, *alors qu'un produit « croisé » d'un élément de* $\mathscr{P}$ *et d'un de* $\mathscr{I}$ *est élément de* $\mathscr{I}$.

D'après la première question, on peut trouver $A \in \mathscr{P}$ *et* $B \in \mathscr{I}$ *tels que* $P = A + B$. *En élevant au carré, on obtient*

$$\underbrace{P^2}_{\in\mathscr{P}} + \underbrace{0}_{\in\mathscr{I}} = P^2 = \underbrace{A^2 + B^2}_{\in\mathscr{P}} + \underbrace{2AB}_{\in\mathscr{I}}.$$

Or, la décomposition de la première question est unique. On en déduit donc $P^2 = A^2 + B^2$ *et (surtout)* $2AB = 0$. *D'après la règle du produit nul, on a donc* $A = 0$ *(donc* $R = B \in \mathscr{I}$*) ou* $B = 0$ *(donc* $R = A \in \mathscr{P}$*).*

(b) Est-il vrai qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ dont le carré est une fonction paire est nécessairement paire ou impaire ?

Considérons la fonction $f : \mathbb{R} \to \mathbb{R}$ *envoyant tous les réels* $\geqslant 0$ *sur* 1 *et tous les réels* < 0 *sur* -1. *En formule,* $f = \mathbb{1}_{\mathbb{R}_+} - \mathbb{1}_{\mathbb{R}_-^*}$.

Il est clair que $f^2 = 1$ *est paire.*

Pourtant, f *n'est ni paire (*$f(-1) = -1 \neq 1 = f(1)$*) ni impaire (*$f(0) = 1 \neq 0$*).*

La réponse est donc non.

Dans la suite de l'exercice, on fixe un polynôme $P \in \mathbb{R}[X]$ vérifiant $(*)$.

5. Montrer $P \in \mathscr{P} \cup \mathscr{I}$.

La relation $(*)$ *donne* $P^2 = P(X^2 + 1) - 1$, *ce qui montre immédiatement que* $P^2 \in \mathscr{P}$. *La question précédente conclut alors.*

6. On suppose $P \in \mathscr{I}$, et on définit une suite $(a_n)_{n\in\mathbb{N}}$ par $a_0 = 0$ et $\forall n \in \mathbb{N}, a_{n+1} = a_n^2 + 1$.

Déterminer la suite $\big(P(a_n)\big)_{n\in\mathbb{N}}$ et en déduire $P = X$.

▶ *Pour tout* $n \in \mathbb{N}$, *on note* $A(n)$ *l'assertion* $P(a_n) = a_n$. *Montrons* $\forall n \in \mathbb{N}, A(n)$ *par récurrence.*

Initialisation. *Comme* $P \in \mathscr{I}$, *on a* $P(0) = 0$, *ce qui montre* $A(0)$.
Hérédité. *Soit* $n \in \mathbb{N}$ *tel que* $A(n)$. *On a alors*

$$\begin{aligned} P(a_{n+1}) &= P(a_n^2 + 1) \\ &= P(a_n)^2 + 1 && \text{(d'après } (*)\text{)} \\ &= a_n^2 + 1 && \text{(d'après } A(n)\text{)} \\ &= a_{n+1}, \end{aligned}$$

ce qui montre $A(n+1)$, *et clôt la récurrence.*

▶ *Une récurrence immédiate montre que* $(a_n)_{n\in\mathbb{N}}$ *est une suite d'entiers naturels. En particulier, pour tout* $n \in \mathbb{N}$, *on a* $a_n^2 \geqslant a_n$, *donc* $a_{n+1} = a_n^2 + 1 > a_n$, *si bien que la suite* $(a_n)_{n\in\mathbb{N}}$ *est strictement croissante. En particulier, elle prend une infinité de valeurs distinctes.*

- *D'après ce qui précède, les polynômes* P *et* X *coïncident sur l'ensemble infini* $\{a_n \mid n \in \mathbb{N}\}$. *Par rigidité, on en déduit* $P = X$.

7. On suppose $P \in \mathscr{P}$.
   (a) Montrer qu'il existe un polynôme $P^{\langle 1\rangle}$ tel que $P = P^{\langle 1\rangle} \circ Q$.

   Comme $P \in \mathscr{P}$, *la question 3 entraîne l'existence d'un polynôme* $\widetilde{P}$ *tel que* $P = \widetilde{P}(X^2)$.

   En posant $P^{\langle 1\rangle} = \widetilde{P}(X-1)$, *on a* $P = \widetilde{P}(X^2+1-1) = P^{\langle 1\rangle}(X^2+1) = P^{\langle 1\rangle} \circ Q$.

   (b) Montrer que $P^{\langle 1\rangle}$ vérifie $P^{\langle 1\rangle} \circ Q = Q \circ P^{\langle 1\rangle}$.

   La relation $(*)$ *se réécrit* $P^{\langle 1\rangle} \circ Q \circ Q = Q \circ P^{\langle 1\rangle} \circ Q$. *Pour conclure, il suffit alors d'appliquer le lemme suivant aux polynômes* $P^{\langle 1\rangle} \circ Q$ *et* $Q \circ P^{\langle 1\rangle}$.

   Lemme. *Soit* $A, B \in \mathbb{R}[X]$ *tels que* $A \circ Q = B \circ Q$. *Alors* $A = B$.

   Démonstration. Soit $y \in [1, +\infty[$. *En posant* $x = \sqrt{y-1}$, *on a* $y = Q(x)$, *et donc l'égalité* $A(y) = (A \circ Q)(x) = (B \circ Q)(x) = B(y)$.

   On a ainsi montré que les deux polynômes A *et* B *coïncidaient sur l'ensemble (infini)* $[1, +\infty[$, *ce qui conclut, par rigidité.*

8. Conclure.

L'idée est de recommencer la construction : la question précédente montre que $P^{\langle 1\rangle}$ *vérifie* $(*)$. *Il est donc élément de* $\mathscr{P} \cup \mathscr{I}$. *S'il est élément de* $\mathscr{I}$, *on a* $P^{\langle 1\rangle} = X$, *donc* $P = X \circ Q = Q$. *S'il est élément de* $\mathscr{P}$, *on peut trouver* $P^{\langle 2\rangle}$ *tel que* $P^{\langle 1\rangle} = P^{\langle 2\rangle} \circ Q$, *donc* $P = P^{\langle 2\rangle} \circ Q \circ Q$ *et ainsi de suite.*

On pourrait rédiger cela en définissant par récurrence une suite (finie ou infinie) $(P^{\langle t\rangle})_t$ *de polynômes vérifiant la relation* $(*)$ *en définissant* $P^{\langle 0\rangle} = P$ *puis, pour tout* $t \in \mathbb{N}$,

- *soit* $P^{\langle t\rangle}$ *est élément de* $\mathscr{I}$ *et la question 6 montre que* $P^{\langle t\rangle} = X$, *auquel cas on arrête la construction à cette étape ;*
- *soit* $P^{\langle t\rangle}$ *n'est pas élément de* $\mathscr{I}$, *auquel cas la question 5 montre qu'il est élément de* $\mathscr{P}$, *puis la question 7 montre l'existence d'un polynôme* $P^{\langle t+1\rangle}$ *vérifiant* $(*)$ *tel que* $P^{\langle t\rangle} = P^{\langle t+1\rangle} \circ Q$.

Un examen des degrés montrerait alors que la suite s'arrête nécessairement, si bien qu'en notant T *la dernière étape, on aurait*

$$P = P^{\langle 0\rangle} = P^{\langle T\rangle} \circ \underbrace{(Q \circ Q \circ \cdots \circ Q)}_{T \text{ occurrences de la lettre } Q} = X \circ Q \circ Q \circ \cdots \circ Q = Q \circ Q \circ \cdots \circ Q.$$

Remarquons d'ailleurs que la notation $P^{\langle 1\rangle}$ *de l'énoncé pousse à rédiger de cette façon.*

Pour le plaisir de montrer une autre manière de rédiger, je vais procéder différemment.

Pour tout entier $k \in \mathbb{N}^*$, *je note ici* $Q^{\circ k} = Q \circ Q \circ \cdots \circ Q$, *avec* k *occurrences de la lettre* Q. *Il est naturel de prolonger cette notation en posant* $Q^{\circ 0} = X$.

- *Le polynôme* Q *étant non constant, on a, pour tout* $k \in \mathbb{N}$, $\deg Q^{\circ k} = \big(\deg Q\big)^k = 2^k$. *Plus généralement, pour tout* $S \in \mathbb{R}[X]$, *la composée* $S \circ Q^{\circ k}$ *est de degré multiple de* 2^k.

  Notre polynôme P *vérifiant* $(*)$ *ne peut pas être constant (il faudrait que sa valeur* r *vérifie* $r^2 = r+1$, *qui est une équation sans solution réelle), donc son degré est un entier non nul. Il n'est donc divisible que par un nombre fini de puissances de 2.*

  L'ensemble des entiers $k \in \mathbb{N}$ *tels que* P *puisse s'écrire sous la forme* $S \circ Q^{\circ k}$, *pour un certain polynôme* $S \in \mathbb{R}[X]$ *vérifiant* $S \circ Q = Q \circ S$, *est donc fini, et il est non vide car on a bien sûr* $P = P \circ Q^{\circ 0}$.

On peut donc considérer le plus grand entier k *possédant cette propriété, et noter* $S \in \mathbb{R}[X]$ *un polynôme tel que* $S \circ Q = Q \circ S$ *et* $P = S \circ Q^{\circ k}$.

- *En appliquant à* S *les questions précédentes, on constate que* S *est nécessairement élément de* $\mathscr{P} \cup \mathscr{I}$, *mais qu'il ne peut pas être élément de* $\mathscr{P}$. *S'il l'était, on obtiendrait en effet un nouveau polynôme* $S^{\langle 1 \rangle}$ *tel que* $S^{\langle 1 \rangle} \circ Q = Q \circ S^{\langle 1 \rangle}$, *si bien que* P *s'écrirait* $P = S^{\langle 1 \rangle} \circ Q^{\circ(k+1)}$, *contredisant ainsi la définition de* k.

  Le polynôme S *est donc élément de* $\mathscr{I}$ *et, ainsi,* $S = X$.

  On a donc montré $P = X \circ Q^{\circ k}$, *c'est-à-dire* $P = Q^{\circ k}$.

Tout ce qui précède était la phase d'analyse d'une grande analyse-synthèse, dont la phase de synthèse est parfaitement immédiate : il est clair que, pour tout $k \in \mathbb{N}$, *les polynômes* $Q^{\circ k}$ *vérifient la relation* $(*)$.

In fine, *les polynômes vérifiant la relation du problème sont exactement les polynômes* $Q^{\circ k}$, *pour* $k \in \mathbb{N}$.