Polynômes
Préparation DS

Une équation polynomiale

Pour tout (a, b) de $\mathbb{C}^2$, soit l'équation $(E_{a,b})$: $P(X^2) = P(X+a)P(X+b)$, d'inconnue P dans $\mathbb{C}[X]$.

Il est clair que les seuls polynômes constants vérifiant $(E_{a,b})$ sont $P = 0$ et $P = 1$.

On note $S_{a,b}$ l'ensemble (éventuellement vide) des polynômes non constants vérifiant $(E_{a,b})$.

I. Étude de quelques cas particuliers

Dans cette partie, on va étudier l'équation $(E_{a,b})$ dans quelques cas particuliers.

On va notamment constater qu'il est fort possible que $S_{a,b}$ soit vide.

Le cas particulier $a = b$

Dans cette question, on suppose $a = b$. On étudie donc l'équation $(E_{a,a})$: $P(X^2) = P^2(X+a)$.

Soit P un polynôme non constant de $\mathbb{C}[X]$. Soit $m \geqslant 1$ le nombre de ses racines *distinctes*.

1. (a) Préciser le nombre de racines distinctes du polynôme $Q(X) = P^2(X+a)$.
   (b) Même question avec $R(X) = P(X^2)$ (discuter selon que 0 est racine ou non de P).
2. (a) On suppose maintenant que P est dans $S_{a,a}$. Montrer que $P = X^m$.
   (b) En déduire finalement que si $a \neq 0$ alors $S_{a,a} = \emptyset$. Précisez l'ensemble $S_{0,0}$.

Le cas particulier $\{a, b\} = \{0, 1\}$

On suppose ici $\{a, b\} = \{0, 1\}$. On étudie donc l'équation $(E_{0,1})$: $P(X^2) = P(X)P(X+1)$.

3. Soit P un élément de $S_{0,1}$, et soit α une racine de P dans $\mathbb{C}$.
   (a) En considérant α^2, montrer que nécessairement $\alpha = 0$ ou $|\alpha| = 1$.
   (b) Montrer de même que $\alpha = 1$ ou $|\alpha - 1| = 1$.
   (c) Montrer finalement que les seules possibilités sont $\alpha = 0$ et $\alpha = 1$.
4. Déterminer l'ensemble $S_{0,1}$.

II. Quelques résultats généraux, dans le cas $S_{a,b} \neq \emptyset$

Dans cette partie, on suppose que $S_{a,b}$ est non vide.

1. (a) Montrer que tout élément de $S_{a,b}$ est unitaire.
   (b) Montrer que $S_{a,b}$ est stable par produit.
2. (a) On suppose que P et Q sont dans $S_{a,b}$, et qu'ils ont le même degré.
   On pose $D(X) = P(X) - Q(X)$ et $R(X) = P(X+a)D(X+b) + D(X+a)Q(X+b)$.
   En raisonnant sur les degrés, montrer que D est nul. Qu'en résulte-t-il ?
   (b) En déduire que $S_{a,b}$ possède un unique polynôme de degré minimum (et qu'il est unitaire).
   On l'appelle le *polynôme minimal* de l'équation $(E_{a,b})$.

III. De l'importance du polynôme minimal

Dans cette partie, on suppose que $S_{a,b}$ est non vide.

On note M le polynôme minimal de l'équation $(E_{a,b})$. On pose $\deg(M) = m \geqslant 1$.

L'objectif de cette partie est de montrer que $S_{a,b} = \{M^n,\ n \in \mathbb{N}^*\}$.

1. Dans cette question, n est un élément de $\mathbb{N}^*$ fixé.
   On note $\{w_1, w_2, \ldots, w_n\}$ l'ensemble des racines $n$ièmes de l'unité.
   (a) Soient A, B dans $\mathbb{C}[X]$. Montrer que $A^n - B^n = \prod_{k=1}^{n}(A - \omega_k B)$.
   (b) En déduire que si P est dans $\mathbb{C}[X]$ et si $P^n \in S_{a,b}$ alors $P \in S_{a,b}$.
2. Dans cette question, P désigne un élément de $S_{a,b}$, de degré $n \geqslant 1$.
   On note $\delta = m \wedge n$. Il existe donc r, s dans $\mathbb{N}^*$ tels que $m = \delta r$ et $n = \delta s$, avec $r \wedge s = 1$.
   (a) Vérifier que M^s et P^r ont même degré, et en déduire qu'ils sont égaux : $M^s = P^r$.
   (b) L'égalité $M^s = P^r$ assure que M et P ont les mêmes racines distinctes $\lambda_1, \ldots, \lambda_q$ dans $\mathbb{C}$.
   On note $M = \prod_{k=1}^{q}(X - \lambda_k)^{\alpha_k}$ et $P = \prod_{k=1}^{q}(X - \lambda_k)^{\beta_k}$ les factorisations de M et P dans $\mathbb{C}[X]$.
      i. Pour tout k de $\{1, \ldots, q\}$, montrer qu'il existe un entier γ_k tel que $\alpha_k = \gamma_k r$.
      ii. En utilisant $Q = \prod_{k=1}^{q}(X - \lambda_k)^{\gamma_k}$ et la question (III.1), montrer que $r = 1$, donc $P = M^s$.
3. Énoncer de façon précise la conclusion de cette partie du problème.

IV. Existence d'un polynôme minimal de degré 1, 2, ou 3

On étudie ici quand $S_{a,b}$ est non vide et possède un polynôme minimal de degré 1 ou 2.

Pour simplifier les calculs, on pose $c = \dfrac{a+b}{2}$ et $d = \dfrac{b-a}{2}$.

1. **Existence d'un polynôme minimal de degré 1**
   (a) Montrer que si P est dans $S_{a,b}$ et de degré 1, alors nécessairement $P = X - c$.
   (b) Réciproquement, montrer que $X - c$ est dans $S_{a,b}$ si et seulement si $c = d^2$.
   (c) Montrer que si cette condition est réalisée, alors $S_{a,b} = \left\{(X-c)^n,\ n \in \mathbb{N}^*\right\}$.
2. **Existence d'un polynôme minimal de degré 2**
   Dans cette question, on suppose $c \neq d^2$ (donc $S_{a,b}$ ne contient pas de polynôme de degré 1).
   On va étudier à quelle condition $S_{a,b}$ contient un polynôme de degré 2 (nécessairement unitaire).
   Posons $P = (X-c)^2 + \alpha(X-c) + \beta$, écrit suivant les puissances décroissantes de $X - c$.
   (a) Montrer qui si P est dans $S_{a,b}$, alors nécessairement $\alpha = 0$.
   (b) En déduire que P est dans $S_{a,b}$ si et seulement si $\beta = \dfrac{1}{4} - c$ et $d^2 = \dfrac{1}{4}$.
   (c) Réciproquement, on suppose que $d^2 = \dfrac{1}{4}$ (c'est-à-dire $b = a \pm 1$), et que $c \neq \dfrac{1}{4}$.
   Montrer que $S_{a,b} = \{M^n,\ n \in \mathbb{N}^*\}$, où $M = (X-c)^2 + \dfrac{1}{4} - c$.
3. **Existence d'un polynôme minimal de degré 3**
   Dans cette question, on suppose $d^2 \neq \dfrac{1}{4}$ et $c \neq d^2$.
   D'après les questions (IV.1) et (IV.2), $S_{a,b}$ ne contient aucun polynôme de degré 1 ou 2.
   On va étudier à quelle condition $S_{a,b}$ contient un polynôme de degré 3 (nécessairement unitaire).
   Posons $P = (X-c)^3 + \alpha(X-c)^2 + \beta(X-c) + \gamma$ (puissances décroissantes de $X - c$).
   Dans un premier temps, on suppose que le polynôme P est solution de $(E_{a,b})$.
   On procédera par implications, avec des identifications (et une substitution judicieuse) dans $(E_{a,b})$.
   (a) Commencer par montrer $\alpha = 0$, puis $\gamma = 0$.
   (b) Réécrire $(E_{a,b})$ avec $\alpha = \gamma = 0$ et montrer cette fois $\beta = -\dfrac{9}{4}$.
   (c) Montrer finalement les égalités $c = \dfrac{25}{16}$ et $d = \pm\dfrac{1}{4}$.
   En déduire que $\{a, b\} = \left\{\dfrac{21}{16}, \dfrac{29}{16}\right\}$ et préciser la factorisation de P.
   (d) Conclure de façon précise cette question (3).

Corrigé du problème

I. Étude de quelques cas particuliers

Le cas particulier $a = b$

1. Notons $A = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ l'ensemble des m racines *distinctes* de P dans $\mathbb{C}$.
   (a) Soit $Q(X) = P^2(X+a)$. On a $Q(z) = 0 \Leftrightarrow P(z+a) = 0 \Leftrightarrow z + a \in A$.
   Le polynôme Q a donc exactement m racines distinctes (les $\mu_k = \lambda_k - a$, où $1 \leqslant k \leqslant m$).
   (b) Soit $R(X) = P(X^2)$. On a $R(z) = 0 \Leftrightarrow P(z^2) = 0 \Leftrightarrow z^2 \in A$.
   Les racines de R dans $\mathbb{C}$ sont donc les racines carrées des λ_k.
   Ainsi le nombre de racines *distinctes* de R est :
   — égal à $2m$ si 0 n'est pas racine de P (chaque λ_k fournit deux racines carrées distinctes)
   — égal à $1 + 2(m-1) = 2m - 1$ si 0 est racine de P (0 ne fournit qu'une racine carrée)

2. (a) On suppose donc que P est dans $S_{a,a}$.
   Avec les notations précédentes, on a $Q(X) = R(X)$ donc $m = 2m$ (dans le cas où 0 n'est pas racine de P) ou $m = 2m - 1$ (dans le cas où 0 est racine de P).
   Mais $m \geqslant 1$, donc l'unique possibilité est $m = 1$, et 0 *est* racine de P (et c'est la seule !).
   Nécessairement, on a $P = \alpha X^m$, avec $\alpha \neq 0$.
   Mais $P(X^2) = P^2(X+a)$ donc $\alpha X^{2m} = \alpha^2 (X+a)^{2m}$, puis $\alpha = \alpha^2$: ainsi $\alpha = 1$ et $P = X^m$.
   (b) D'après ce qui précède, tout polynôme de $S_{a,a}$ s'écrit $P = X^n$, avec $n \geqslant 1$.
   Réciproquement, soit n dans $\mathbb{N}^*$ et $P(X) = X^n$.
   On a les équivalences : $P \in S_{a,a} \Leftrightarrow P(X^2) = P^2(X+a) \Leftrightarrow X^{2n} = (X+a)^{2n} \Leftrightarrow a = 0$.
   On peut donc conclure :
   — Si $a \neq 0$, alors l'ensemble $S_{a,a}$ est vide.
   — Si $a = 0$, alors $S_{0,0} = \{X^n,\ n \in \mathbb{N}^*\}$.

Le cas particulier $(a = 0, b = 1)$

On suppose $(a, b) = (0, 1)$. On étudie donc l'équation $(E_{0,1})$: $P(X^2) = P(X)P(X+1)$.

3. Soit P un élément de $S_{0,1}$ (donc $\deg P \geqslant 1$), et soit α une racine de P dans $\mathbb{C}$.
   (a) On a $P(\alpha^2) = P(\alpha)P(\alpha+1) = 0$ donc α^2 est également une racine de P.
   Par une récurrence évidente, et pour tout n de $\mathbb{N}$, les $u_n = \alpha^{2^n}$ sont des racines de P.
   Si on avait $0 < |\alpha| < 1$ ou $|\alpha| > 1$, la suite $n \mapsto |u_n|$ serait strictement monotone, donc les u_n seraient distincts (absurde, P ne pouvant posséder qu'un nombre fini de racines).
   Ainsi $\alpha = 0$ ou $|\alpha| = 1$.
   (b) Posons $\beta = (\alpha - 1)^2$. On a $P(\beta) = P(\alpha - 1)P(\alpha) = 0$ donc β est une racine de P.
   Il en résulte $\beta = 0$ ou $|\beta| = 1$, c'est-à-dire $\alpha = 1$ ou $|\alpha - 1| = 1$.
   (c) On a obtenu ($\alpha = 0$ ou $|\alpha| = 1$) et ($\alpha = 1$ ou $|\alpha - 1| = 1$).
   Cela équivaut à : $(\alpha = 0)$ ou $(\alpha = 1)$ ou $(\alpha = \mathrm{e}^{i\pi/3})$ ou $(\alpha = \mathrm{e}^{-i\pi/3})$
   Les solutions $\alpha = \mathrm{e}^{\pm i\pi/3}$ ne sont pas recevables (car α^2 doit *aussi* être une racine de P).
   Finalement, les seules racines *possibles* de P sont $\alpha = 0$ et $\alpha = 1$.

4. Donc si P est dans $S_{0,1}$, il s'écrit $P = \lambda X^m (X-1)^n$, avec $\lambda \in \mathbb{C}^*$, $(m, n) \in \mathbb{N}^2$, $m + n \geqslant 1$.
   Réciproquement, pour un tel P, on a : $\begin{cases} P(X^2) = \lambda X^{2m}(X^2-1)^n = \lambda X^{2m}(X-1)^n(X+1)^n \\ P(X)P(X+1) = \lambda^2 X^{m+n}(X-1)^m(X+1)^n \end{cases}$
   Cela équivaut à $\lambda = 1$ et $m = n$, c'est-à-dire $P = (X(X-1))^n$.
   Conclusion : $S_{0,1} = \{M^n,\ n \in \mathbb{N}^*\}$, où $M = X^2 - X$.

II. Quelques résultats généraux, dans le cas $S_{a,b} \neq \emptyset$

1. (a) Soit P un élément de $S_{a,b}$, de degré $n \geqslant 1$, de coefficient dominant $c \neq 0$.
Les monômes dominants de $P(X^2)$, $P(X+a)$, $P(X+b)$ sont respectivement cX^{2n}, cX^n, cX^n.
Par identification des monômes dominants dans $E_{a,b}$, il vient $cX^{2n} = c^2X^{2n}$, donc $c = 1$.
En d'autres termes, tous les polynômes de $S_{a,b}$ sont unitaires.

(b) Soient P et Q dans $S_{a,b}$, donc tels que $\begin{cases} P(X^2) = P(X+a)P(X+b) \\ Q(X^2) = Q(X+a)Q(X+b) \end{cases}$

Soit $R = PQ$. Par produit terme à terme, on obtient : $R(X^2) = R(X+a)R(X+b)$.
Ainsi $R = PQ$ (non constant !) est dans $S_{a,b}$: cet ensemble est donc stable par produit.

2. (a) Soient P et Q sont deux éléments de $S_{a,b}$, de même degré $n \geq 1$.
P étant Q sont unitaires, $D = P - Q$ est nul ou de degré strictement inférieur à n.
Par l'absurde, supposons $D \neq 0$, donc $\deg D = m$, avec $0 \leqslant m < n$.
Définissons le polynôme $R(X) = P(X+a)D(X+b) + D(X+a)Q(X+b)$.
Le polynôme R est visiblement de degré $n+m$ (rappelons que P et Q sont unitaires).
En utilisant le fait que P et Q sont dans $S_{a,b}$, on trouve :

$$\begin{aligned} R(X) &= P(X+a)\big(P(X+b) - Q(X+b)\big) + \big(P(X+a) - Q(X+a)\big)Q(X+b) \\ &= P(X+a)P(X+b) - Q(X+a)Q(X+b) = P(X^2) - Q(X^2) = D(X^2) \end{aligned}$$

Ainsi $R(X) = D(X^2)$, alors que $\deg(R(X)) = n+m$, et que $\deg(D(X^2)) = 2m$.
Ainsi $n + m = 2m$, ce qui est absurde car $m < n$.
Ainsi $S_{a,b}$ ne peut contenir au plus qu'un polynôme de degré $n \geqslant 1$ (et il est unitaire).

(b) L'ensemble des degrés des polynômes de $S_{a,b}$ est une partie non vide et minorée de $\mathbb{N}^*$.
Cet exemple possède donc un plus petit élément $\delta \geqslant 1$.
Ce qui précède montre que $S_{a,b}$ possède un *unique* élément P de degré δ, et qu'il est unitaire.

III. De l'importance du polynôme minimal

1. (a) Dans $\mathbb{C}$, on connaît la factorisation $z^n - 1 = \prod_{k=1}^{n}(z - \omega_k)$.
En particulier, pour tout z de $\mathbb{C}$ qui n'est pas une racine de B, on a :

$$A^n(z) - B^n(z) = B^n(z)\left(\left(\frac{A(z)}{B(z)}\right)^n - 1\right) = B^n(z)\prod_{k=1}^{n}\left(\frac{A(z)}{B(z)} - \omega_k\right) = \prod_{k=1}^{n}\Big(A(z) - \omega_k B(z)\Big)$$

Les polynômes $A^n - B^n$ et $\prod_{k=1}^{n}(A - \omega_k B)$ coïncidant sur une partie infinie de $\mathbb{C}$, il sont égaux.

(b) Soit P dans $\mathbb{C}[X]$, avec P^n dans $S_{a,b}$, donc tel que $P^n(X^2) = P^n(X+a)P^n(X+b)$.
Ainsi $A^n - B^n = 0$, avec $A(X) = P(X^2)$ et $B(X) = P(X+a)P(X+b)$.
Or $A^n - B^n = \prod_{k=1}^{n}(A - \omega_k B)$, et $\mathbb{C}[X]$ est *intègre* donc : $\exists\, k \in \{1, \ldots, n\}$ tel que $A - \omega_k B = 0$.
Enfin, d'après (II.1a) on sait que P, donc A et B, sont des polynômes unitaires.
La seule possibilité est donc $\omega_k = 1$, c'est-à-dire $A = B$.
Autrement dit, on a $P(X^2) = P(X+a)P(X+b)$, ce qui signifie que P est dans $S_{a,b}$.

2. (a) On observe que $\begin{cases} \deg(M^s) = s\deg(M) = sm = \delta rs \\ \deg(P^r) = r\deg(P) = rn = \delta rs \end{cases}$, donc $\deg(M^s) = \deg(P^r)$.
D'après (II.1.b), $S_{a,b}$ est stable pour le produit. Il en résulte que M^s et P^r sont dans $S_{a,b}$.
D'après (II.2.a), $S_{a,b}$ possède au plus un polynôme de degré donné. Il en résulte $M^s = P^r$.

(b) i. On note $M = \prod_{k=1}^{q} (X - \lambda_k)^{\alpha_k}$ et $P = \prod_{k=1}^{q} (X - \lambda_k)^{\beta_k}$ les factorisations de M et P dans $\mathbb{C}[X]$.

Par unicité de la factorisation, l'égalité $M^s = P^r$ donne $\alpha_k s = \beta_k r$ pour tout k de $\{1, \ldots, q\}$.

Or $r \wedge s = 1$. Il en résulte que $r \mid \alpha_k$ pour $1 \leqslant k \leqslant q$ (donc les égalités $\alpha_k = \gamma_k r$).

ii. Avec ce qui précède, on trouve $M = \prod_{k=1}^{q} (X - \lambda_k)^{\alpha_k} = Q^r$, où $Q = \prod_{k=1}^{q} (X - \lambda_k)^{\gamma_k}$.

Ainsi Q^r (avec $r \geqslant 1$) est dans $S_{a,b}$. D'après (III.1.b), il en résulte que Q est dans $S_{a,b}$.

Donc $M = Q^r$ (avec Q dans $S_{a,b}$) alors que M est de degré minimal dans $S_{a,b}$.

Nécessairement $r = 1$, et l'égalité $M^s = P^r$ devient $P = M^s$.

3. Il est temps de conclure pour cette partie du problème !

— Quand $S_{a,b} \neq \emptyset$, il existe dans $S_{a,b}$ un unique polynôme (unitaire) M de degré minimal.

— Par stabilité, on sait que toute puissance de M^n de M (avec $n \geqslant 1$) est encore dans $S_{a,b}$.

— Réciproquement, on a vu dans (III.2) que tout élément de $S_{a,b}$ est une puissance de M.

En résumé : si $S_{a,b} \neq \emptyset$, alors $S_{a,b} = \{M^n, \ n \in \mathbb{N}^*\}$, où M est le polynôme minimal de $S_{a,b}$.

IV. Existence d'un polynôme minimal de degré 1, 2 ou 3

1. **Existence d'un polynôme minimal de degré 1**

(a) On sait que P est nécessairement unitaire. On le cherche donc sous la forme $P = X - \lambda$.

L'égalité $P(X^2) = P(X + a)P(X + b)$ s'écrit $X^2 - \lambda = (X + a - \lambda)(X + b - \lambda)$.

En identifiant les termes de degré 1, on a nécessairement $a + b - 2\lambda = 0$ c'est-à-dire $\lambda = c$.

(b) Réciproquement posons $P = X - c$, donc $P(X^2) = X^2 - c$.

Sachant que $c - a = b - c = d$, on a : $P(X + a)P(X + b) = (X - d)(X + d) = X^2 - d^2$

On voit que P est dans $S_{a,b}$ si et seulement si $c = d^2$.

(c) On suppose qu'on a effectivement $c = d^2$: le polynôme $P = X - c$ est donc dans $S_{a,b}$.

Ce polynôme est bien sûr le polynôme minimal de $S_{a,b}$.

En utilisant la partie III, on énonce : Si $c = d^2$, alors $S_{a,b} = \left\{(X - c)^n, \ n \in \mathbb{N}^*\right\}$

2. **Existence d'un polynôme minimal de degré 2**

(a) On suppose que $P = (X - c)^2 + \alpha(X - c) + \beta$ est dans $S_{a,b}$.

Rappelons qu'avec les notations de l'énoncé, on a : $a - c = -d$ et $b - c = d$.

L'égalité $(E_{a,b})$ s'écrit donc :

$$\begin{aligned}(X^2 - c)^2 + \alpha(X^2 - c) + \beta &= \big((X - d)^2 + \alpha(X - d) + \beta\big)\big((X + d)^2 + \alpha(X + d) + \beta\big)\\ &= \big(X^2 + (\alpha - 2d)X + d^2 - \alpha d + \beta\big)\big(X^2 + (\alpha + 2d)X + d^2 + \alpha d + \beta\big)\end{aligned}$$

Dans cette égalité, l'identification des termes de degré 3 donne immédiatement $\alpha = 0$.

(b) Sachant que $\alpha = 0$, L'égalité $(E_{a,b})$ s'écrit maintenant :

$$(X^2 - c)^2 + \beta \ = \big((X - d)^2 + \beta\big)\big((X + d)^2 + \beta\big) = (X^2 - d^2)^2 + 2\beta(X^2 + d^2) + \beta^2$$

Par identification des coefficients, on en déduit :

$$P \in S_{a,b} \Leftrightarrow \begin{cases} -2c = -2d^2 + 2\beta \\ c^2 + \beta = (d^2 + \beta)^2 \end{cases} \Leftrightarrow \begin{cases} \beta = d^2 - c \\ c^2 + d^2 - c = (2d^2 - c)^2 \end{cases} \Leftrightarrow \begin{cases} \beta = d^2 - c \\ d^2 - c = 4d^2(d^2 - c) \end{cases}$$

Mais $c \neq d^2$. Finalement $P \in S_{a,b} \Leftrightarrow \begin{cases} \beta = d^2 - c \\ 4d^2 = 1 \end{cases} \Leftrightarrow \begin{cases} \beta = 1/4 - c \\ d^2 = 1/4 \end{cases} \Leftrightarrow \begin{cases} \beta = 1/4 - c \\ b - a = \pm 1 \end{cases}$

(c) Réciproquement, on suppose $d^2 = \dfrac{1}{4}$ (c'est-à-dire $b = a \pm 1$), et $c \neq \dfrac{1}{4}$.

La condition $c \neq \dfrac{1}{4}$, donc $c \neq d^2$, nous assure que $S_{a,b}$ ne possède pas de polynôme de degré 1.

Enfin la condition $d^2 = \dfrac{1}{4}$ nous assure que $M = (X-c)^2 - c + \dfrac{1}{4}$ est dans $S_{a,b}$.

Ce polynôme M est donc le polynôme minimal de $S_{a,b}$.

La partie III donne alors : $S_{a,b} = \{M^n,\ n \in \mathbb{N}^*\}$, où $M = (X-c)^2 + \dfrac{1}{4} - c$.

Remarque : les deux racines de M sont distinctes (il ne pouvait pas en être autrement : dans le cas contraire M s'écrirait $M = Q^2$, avec $\deg Q = 1$, donc Q serait dans $S_{a,b}$ d'après III.1.b).

Plus précisément, si ω est l'une des deux racines carrées (distinctes) de $c - 1/4$, les racines de M sont $z_1 = c + \omega$ et $z_2 = c - \omega$, qui sont symétriques par rapport au milieu c de $[a, b]$.

3. **Existence d'un polynôme minimal de degré 3**

(a) On suppose que $P = (X-c)^3 + \alpha(X-c)^2 + \beta(X-c) + \gamma$ est dans $S_{a,b}$.

Rappelons qu'avec les notations de l'énoncé, on a : $a - c = -d$ et $b - c = d$.

On écrit (sans la développer inutilement) l'égalité $(E_{a,b})$:

$$\begin{aligned}&(X^2-c)^3 + \alpha(X^2-c)^2 + \beta(X^2-c) + \gamma\\ &\quad= \Big((X-d)^3 + \alpha(X-d)^2 + \beta(X-d) + \gamma\Big)\Big((X+d)^3 + \alpha(X+d)^2 + \beta(X+d) + \gamma\Big)\end{aligned}$$

Le premier membre est pair. Le coefficient 2α de X^5 au second membre est donc nul.

On réécrit $(E_{a,b})$ sachant que α est nul :

$$\begin{aligned}&(X^2-c)^3 + \beta(X^2-c) + \gamma\\ &\quad= \Big((X-d)^3 + \beta(X-d) + \gamma\Big)\Big((X+d)^3 + \beta(X+d) + \gamma\Big)\\ &\quad= (X^2-d^2)^3 + 2\beta(X^2-d^2)(X^2+d^2) + 2\gamma X(X^2+3d^2) + \beta^2(X^2-d^2) + 2\beta\gamma X + \gamma^2\end{aligned}$$

Toujours par parité, le coefficient 2γ de X^3 est nécessairement nul.

On a donc $\alpha = \gamma = 0$.

(b) Sachant que α et γ sont nuls :

$(E_{a,b}) \Leftrightarrow (X^2-c)\Big((X^2-c)^2 + \beta\Big) = (X^2-d^2)\Big((X^2-d^2)^2 + 2\beta(X^2+d^2) + \beta^2\Big)$

Identifier les termes de degré 4 donne $-3c = -3d^2 + 2\beta$ donc l'égalité $\beta = \dfrac{3}{2}(d^2 - c) \neq 0$.

Substituer d à X donne $(d^2-c)^3 + \beta(d^2-c) = 0$ donc $\beta = -(d^2-c)^2$.

On a donc obtenu $\beta^2 = -\dfrac{9}{4}\beta$, c'est-à-dire $\beta = -\dfrac{9}{4}$.

(c) On identifie les termes de degré 2 dans $E_{a,b}$, et on sait que $3(d^2 - c) = 2\beta$.

Ainsi $3c^2 + \beta = 3d^4 + \beta^2$ donc $3(d^2-c)(d^2+c) = \beta(1-\beta) =$ donc $d^2 + c = \dfrac{1-\beta}{2} = \dfrac{13}{8}$.

Ainsi $(\star) \Leftrightarrow \dfrac{3}{4}(d^2-c)\Big(3(d^2-c) - 2 + 4(d^2+c)\Big) = 0 \Leftrightarrow d^2 = \dfrac{2-c}{7}$ et $\beta = \dfrac{3(1-4c)}{7}$.

On a $d^2 - c = \dfrac{2\beta}{3} = -\dfrac{3}{2}$ et $d^2 + c = \dfrac{13}{8}$, donc $c = \dfrac{25}{16}$ et $d^2 = \dfrac{1}{16}$ donc $d = \pm\dfrac{1}{4}$.

Finalement $\{a, b\} = \{c-d, c+d\} = \left\{\dfrac{21}{16}, \dfrac{29}{16}\right\}$.

Enfin : $P = \left(X - \dfrac{25}{16}\right)\left(\left(X - \dfrac{25}{16}\right)^2 - \dfrac{9}{4}\right) = \left(X - \dfrac{1}{16}\right)\left(X - \dfrac{25}{16}\right)\left(X - \dfrac{49}{16}\right)$

(d) Les valeurs obtenues pour c et d vérifient bien les hypothèses $d^2 \neq \dfrac{1}{4}$ et $c \neq d^2$.

On est donc certain qu'il n'y a pas de polynôme de degré 1 ou 2 dans $S_{a,b}$.

C'est donc uniquement pour $\{a, b\} = \left\{\dfrac{21}{16}, \dfrac{29}{16}\right\}$ qu'il y a un polynôme minimal de degré 3.

Ce polynôme est $M = \left(X - \dfrac{1}{16}\right)\left(X - \dfrac{25}{16}\right)\left(X - \dfrac{49}{16}\right)$, et on a $S_{a,b} = \{M^n,\ n \in \mathbb{N}^*\}$.