# Algèbre 3
# TD 7
# Polynômes à une indéterminée

Licence 2 MAE 2020-2021

Université Paris Descartes

*Marc Briant*

---

**Dans tout ce TD, $(\mathbb{K},+,.)$ désigne un corps commutatif.**

## Des $\mathbb{K}$-ev et des calculs chez les polynômes

### Exercice 1

1) Soient $P_1 = X^2+1$, $P_2 = X^2+X$ et $P_3 = X^2+X+1$. Montrer que $(P_1,P_2,P_3)$ est une base de $\mathbb{R}_2[X]$.
2) Soient $(P_1,..,P_n)$ des polynômes de $\mathbb{C}[X]$ tels que $\deg(P_1) < .. < \deg(P_n)$. Montrer que $(P_1,..,P_n)$ est une famille libre de $\mathbb{C}[X]$.

**Solution.** Ce n'est pas parce que nous faisons des polynômes que nous perdons nos réflexes développés sur les ev. Donc nous restons précis dans nos définitions de familles libres et de bases.

**1)** Nous savons que $\dim(\mathbb{R}_2[X]) = 3$ donc comme la famille $(P_1,P_2,P_3)$ a trois éléments, si elle est libre alors c'est également une base de $\dim(\mathbb{R}_2[X]) = 3$. Montrons donc qu'elle est libre et prenons $\lambda_1$, $\lambda_2$ et $\lambda_3$ trois réels et supposons que

$$\lambda_1 P_1 + \lambda_2 P_2 + \lambda_3 P_3 = 0.$$

De manière générale quand nous écrivons des polynômes nous les écrivons par ordre croissant de puissances de $X$. Ainsi nous avons

$$(\lambda_1+\lambda_3)P_1 + \lambda_2 P_2 + \lambda_3 P_3 = \lambda_1 + (\lambda_2+\lambda_3)X + (\lambda_1+\lambda_2+\lambda_3)X^2 = 0.$$

Comme la famille $(1,X,X^2)$ est une famille libre de $\mathbb{R}[X]$ nous obtenons donc

$$\begin{cases} \lambda_1+\lambda_3 = 0 \\ \lambda_2+\lambda_3 = 0 \\ \lambda_1+\lambda_2+\lambda_3 = 0 \end{cases} \Leftrightarrow \begin{cases} \lambda_1 = -\lambda_3 \\ \lambda_3 = -\lambda_2 \\ \lambda_2 = 0 \end{cases} \Leftrightarrow \lambda_1 = \lambda_2 = \lambda_3 = 0.$$

Ainsi la famille $(P_1,P_2,P_3)$ est libre et donc c'est une base de $\mathbb{R}_2[X]$.

**2)** On nous parle de polynômes donc nous les écrivons. En notant $d_1 = \deg(P_1)$,..,$d_n = \deg(P_n)$ nous avons

$$P_1 = \sum_{k=0}^{d_1} a_{1k}X^k \quad P_2 = \sum_{k=0}^{d_2} a_{2k}X^k \quad \cdots \quad P_n = \sum_{k=0}^{d_n} a_{nk}X^k.$$

Nous voulons montrer que cette famille est libre donc nous prenons $n$ complexes $\lambda_1$,..,$\lambda_n$ tels que

$$\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n = 0.$$

Nous avons alors deux façons de rédiger pour conclure que les $\lambda_i$ sont tous nuls.

- <u>La bourrine qui marche toujours.</u> Nous écrivons (comme dans les ev) ce que vaut le gros polynôme de gauche. Ecrire un polynôme c'est l'écrire suivant des puissances de X croissantes donc nous nous souvenons que $d_1 < d_2 < ... < d_n$. Nous avons donc

$$\begin{aligned}
\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n &= \sum_{k=0}^{d_1} \lambda_1 a_{1k}X^k + \sum_{k=0}^{d_2} \lambda_2 a_{2k}X^k + \cdots + \sum_{k=0}^{d_n} \lambda_n a_{nk}X^k \\
&= \sum_{k=0}^{d_1} (\lambda_1 a_{1k} + \lambda_2 a_{2k} + \cdots + \lambda_n a_{nk}) X^k + \sum_{k=d_1+1}^{d_2} (\lambda_2 a_{2k} + \cdots + \lambda_n a_{nk}) X^k \\
&\quad + \sum_{k=d_2+1}^{d_3} (\lambda_3 a_{3k} + \cdots \lambda_n a_{nk}) X^k \\
&\quad + \cdots + \sum_{k=d_{n-2}+1}^{d_{n-1}} \left(\lambda_{n-1} a_{(n-1)k} + \lambda_n a_{nk}\right) X^k + \sum_{k=d_{n-1}+1}^{d_n} \lambda_n a_{nk} X^k \\
&= 0.
\end{aligned}$$

Comme la famille $(1, X, X^2, ..., X^{d_n})$ est une famille libre de $\mathbb{C}[X]$ nous voyons de suite que $\lambda_n a_{nd_n} = 0$ mais comme $a_{nd_n} \neq 0$ puisque $\deg(P_n) = d_n$ il vient que $\lambda_n = 0$. Ainsi la dernière somme est nulle et donc

$$\begin{aligned}
\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n &= \sum_{k=0}^{d_1} \lambda_1 a_{1k} X^k + \sum_{k=0}^{d_2} \lambda_2 a_{2k} X^k + \cdots + \sum_{k=0}^{d_n} \lambda_n a_{nk} X^k \\
&= \sum_{k=0}^{d_1} \left(\lambda_1 a_{1k} + \lambda_2 a_{2k} + \cdots + \lambda_n a_{nk}\right) X^k + \sum_{k=d_1+1}^{d_2} \left(\lambda_2 a_{2k} + \cdots + \lambda_n a_{nk}\right) X^k \\
&\quad + \sum_{k=d_2+1}^{d_3} \left(\lambda_3 a_{3k} + \cdots \lambda_n a_{nk}\right) X^k \\
&\quad + \cdots + \sum_{k=d_{n-2}+1}^{d_{n-1}} \lambda_{n-1} a_{(n-1)k} X^k \\
&= 0.
\end{aligned}$$

Avec les mêmes arguments que précédemment nous avons alors $\lambda_{n-1} = 0$. Et ainsi de suite jusqu'à avoir $\lambda_n = \lambda_{n-1} = .. = \lambda_2 = \lambda_1 = 0$.
*Ici une belle récurrence pourrait être un plus !*

- La délicate qui se sert du cours sur les polynômes. Comme $d_1 < d_2 < ... < d_n$, nous avons que si $\lambda_n \neq 0$ alors le polynôme $\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n$ est de degré $n$ (puisque aucun coefficient des polynômes $P_1$,..,$P_{n-1}$ ne peut annuler le coefficient dominant de $P_n$ puisqu'ils sont de degrés inférieurs). Mais cela n'est pas possible puisque le polynôme $\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n$ est nul Ainsi $\lambda_n = 0$. Nous avons donc en réalité

$$\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_{n-1} P_{n-1} = 0$$

et pour la même raison nous avons nécessairement $\lambda_{n-1} = 0$. En itérant nous trouvons donc bien $\lambda_n = \lambda_{n-1} = .. = \lambda_1 = 0$.
*Ici une belle récurrence pourrait être un plus !*

## Exercice 2

Soit un entier $n \geqslant 1$. Dans chacun des cas suivant montrer que $f$ est dans $L(\mathbb{R}_n[X])$ et exprimer sa matrice dans la base canonique de $\mathbb{R}_n[X]$.

1) $f(P)(X) = P(X+1)$ 2) $f(P)(X) = P - XP'$

**Solution.** Nous n'oublions pas ce que nous faisions dans les ev et les matrices ! Soyons précis et précises quand nous montrons que des applications sont linéaires et ensuite ne nous trompons pas en écrivant les matrices ! Nous rentrons les coordonnées de $f(e_j)$ dans la $j^{eme}$ colonne.

**1)** La fonction $f : P(X) \longrightarrow P(X+1)$ envoie bien un polynôme de $\mathbb{R}_n[X]$ dans $\mathbb{R}[X]$.

• Attention, n'oublions pas que l'énoncé veut montrer que $f$ est un endomorphisme de $\mathbb{R}_n[X]$ donc il faut s'assurer que le degré de $f(P)$ est bien plus petit que $n$. Si $P = \sum_{k=0}^{d} a_k X^k$ avec $d \leqslant n$ alors nous avons

$$f(P) = P(X+1) = \sum_{k=0}^{d} a_k (X+1)^k.$$

Le degré de $(1+X)^k$ est $k$ donc en sommant les $a_k(X+1)^k$ de 0 à $d$ on obtient un polynôme de degré inférieur ou égal à $d \leqslant n$. Ainsi $f$ est bien définie sur $\mathbb{R}_n[X]$ à valeurs dans $\mathbb{R}_n[X]$.

• Regardons alors si $f$ est bien linéaire. Prenons donc $\alpha$ et $\beta$ deux réels et $P$ et $Q$ deux polynômes de $\mathbb{R}_n[X]$. On calcule

$$f(\alpha P + \beta Q) = (\alpha P + \beta Q)(X+1) = \alpha P(X+1) + \beta Q(X+1) = \alpha f(P) + \beta f(Q)$$

donc $f$ est bien un endomorphisme de $\mathbb{R}_n[X]$.

• Afin de construire la matrice de $f$ dans la base canonique $\mathcal{B} = (1, X, X^2)$ il faut calculer $f$ sur chacun des vecteurs de la base. Si nous n'arrivons pas trop à jongler avec des vecteurs et des polynômes rien n'empêche de nommer $e_1 = 1$, $e_2 = X$ et $e_3 = X^2$. Ainsi nous obtenons

$$f(1) = 1\ (= e_1) \quad f(X) = 1 + X\ (= e_1 + e_2) \quad f(X^2) = (1+X)^2 = 1 + 2X + X^2\ (= e_1 + 2e_2 + e_3)$$

et il suffit de recopier

$$M_{\mathcal{B}}(f) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

**2)** La fonction $f : P(X) \longrightarrow P(X+1)$ envoie bien un polynôme de $\mathbb{R}_n[X]$ dans $\mathbb{R}[X]$.

• Attention, n'oublions pas que l'énoncé veut montrer que $f$ est un endomorphisme de $\mathbb{R}_n[X]$ donc il faut s'assurer que le degré de $f(P)$ est bien plus petit que $n$. Si $P = \sum_{k=0}^{d} a_k X^k$ avec $d \leqslant n$ alors nous avons

$$f(P) = P - XP' = \sum_{k=0}^{d} a_k X^k - X \sum_{k=0}^{d} k a_k X^{k-1} = \sum_{k=0}^{d} a_k X^k - \sum_{k=0}^{d} k a_k X^k = \sum_{k=0}^{d} (1-k) a_k X_k$$

qui est bien un polynôme de degré inférieur ou égal à $d \leqslant n$. Ainsi $f$ est bien définie sur $\mathbb{R}_n[X]$ à valeurs dans $\mathbb{R}_n[X]$.

• Regardons alors si $f$ est bien linéaire. Prenons donc $\alpha$ et $\beta$ deux réels et $P$ et $Q$ deux polynômes de $\mathbb{R}_n[X]$. On calcule en se rappelant que la dérivation d'un polynôme est linéaire

$$f(\alpha P + \beta Q) = (\alpha P + \beta Q) - X(\alpha P + \beta Q)' = (\alpha P + \beta Q) - X(\alpha P' + \beta Q') = \alpha(P - XP') + \beta(Q - XQ') = \alpha f(P) + \beta f(Q)$$

donc $f$ est bien un endomorphisme de $\mathbb{R}_n[X]$.

• Afin de construire la matrice de $f$ dans la base canonique $\mathcal{B} = (1, X, X^2)$ il faut calculer $f$ sur chacun des vecteurs de la base. Si nous n'arrivons pas trop à jongler avec des vecteurs et des polynômes rien n'empêche de nommer $e_1 = 1$, $e_2 = X$ et $e_3 = X^2$. Ainsi nous obtenons

$$f(1) = 1 - X.0 = 1\ (= e_1) \quad f(X) = X - X.1 = 0\ (= 0) \quad f(X^2) = X^2 - X.(2X) = -X^2\ (= -e_3)$$

et il suffit de recopier

$$M_{\mathcal{B}}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

## Exercice 3 : *Relations entre racines et coefficients*

Cet exercice a pour but de rappeler que les coefficients d'un polynômes sont liés à ses racines lorsque le polynôme est scindé.

Dans chacun des cas suivants calculer la somme $S$ demandée.

1) $S = \alpha^2 + \beta^2$ où $\alpha$ et $\beta$ sont les racines complexes de $X^2 + bX + c$ avec $b$ et $c$ des complexes.
2) $S = \alpha^2 + \beta^2 + \gamma^2$ où $\alpha$, $\beta$ et $\gamma$ sont les racines complexes de $X^3 + aX^2 + bX + c$ avec $a$, $b$ et $c$ des complexes.
3) $S = \alpha^3 + \beta^3$ où $\alpha$ et $\beta$ sont les racines complexes de $X^2 - \sqrt{2}X - \sqrt{3}$.
4) $S = \alpha^4 + \beta^4 + \gamma^4$ où $\alpha$, $\beta$ et $\gamma$ sont les racines complexes de $X^3 - X + i$.

**Solution.** Dans cet exercice on nous demande de calculer des formules algébriques de racines de polynômes. Bien entendu il est hors de question de trouver ces racines explicitement ! Nous nous rappelons qu'il existe entre les coefficients d'un polynôme et ses racines des relations simples à retrouver. Par exemple :

$$P = (X-a)(X-b) = X^2 - (a+b)X + ab$$

ce qui fait que le coefficient d'ordre 1 de $P$ vaut moins la somme des racines tandis que le coefficient d'ordre 0 vaut le produit des racines. ce qu'il est important de retenir est surtout le cas général de la somme des racines et leur produit :

$$P = (X-a_1)(X-a_2)\cdots(X-a_n) = X^n - (a_1 + \cdots + a_n)X^{n-1} + \cdots + (-1)^n a_1 \cdots a_n.$$

ATTENTION : dans les exemples ci-dessus nous avons pris un polynôme unitaire ! Si son coefficient dominant n'est pas 1 mais $A$ alors il faut tout multiplier par $A$ :

$$P = A(X-a_1)(X-a_2)\cdots(X-a_n) = A\left(X^n - (a_1 + \cdots + a_n)X^{n-1} + \cdots + (-1)^n a_1 \cdots a_n\right).$$

Donc la stratégie est la suivante : nous nous servons de la propriété d'être racine pour réduire les puissances et ensuite nous trouvons les relations entre racines et coefficients.

**1)** Nous commençons par diminuer la puissance de notre expression. En effet, $\alpha$ et $\beta$ sont des racines de $X^2 + bX + c$ donc

$$\alpha^2 = -b\alpha - c \quad \text{et} \quad \beta^2 = -b\beta - c.$$

Ainsi nous avons

$$S = \alpha^2 + \beta^2 = -b\alpha - c + (-b\beta - c) = -b(\alpha + \beta) - 2c.$$

Soit nous nous rappelons des relations racines/coefficients soit nous les retrouvons. Comme $\alpha$ et $\beta$ sont racines du polynôme et que le polynôme est unitaire nous factorisons

$$X^2 + bx + c = (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta) + \alpha\beta$$

ce qui nous indique que $b=-(\alpha+\beta)$ et donc nous pouvons conclure

$$S=\alpha^2+\beta^2=b^2-2c.$$

**2)** Le premier réflexe est de diminuer les puissances des racines mais ici on nous demande des puissances 2 et le polynôme est de degré 3 donc nous ne pourrons pas diminuer plus... Ainsi nous allons directement retrouver les relations racines/coefficients. Comme le polynôme est unitaire nous factorisons

$$X^3+aX^2+bX+c=(X-\alpha)(X-\beta)(X-\gamma)=X^3-(\alpha+\beta+\gamma)X^2+(\alpha\beta+\gamma\beta+\alpha\gamma)X-\alpha\beta\gamma$$

ce qui nous indique que

$$a=-(\alpha+\beta+\gamma)\quad b=(\alpha\beta+\gamma\beta+\alpha\gamma)\quad c=-\alpha\beta\gamma.$$

Nous n'avons pas $S=\alpha^2+\beta^2+\gamma^2$ mais on peut le faire apparaître :

$$a^2=(\alpha+\beta+\gamma)^2=\alpha^2+\beta^2+\gamma^2+2\alpha\beta+2\beta\gamma+2\alpha\gamma=S+2b.$$

Nous obtenons donc

$$S=\alpha^2+\beta^2+\gamma^2=a^2-2b.$$

**3)** Le premier réflexe est de diminuer les puissances des racines ce que nous faisons en nous servant de la définition d'une racine :

$$\alpha^3=\alpha(\alpha^2)=\alpha\left(\sqrt{2}\alpha+\sqrt{3}\right)=\sqrt{2}\alpha^2+\sqrt{3}\alpha=\sqrt{2}\left(\sqrt{2}\alpha+\sqrt{3}\right)+\sqrt{3}\alpha=(2+\sqrt{3})\alpha+\sqrt{6}\quad\text{et}=\quad\beta^3=(2+\sqrt{3})\beta+\sqrt{6}.$$

Ainsi nous avons

$$S=\alpha^3+\beta^3=(2+\sqrt{3})(\alpha+\beta)+2\sqrt{6}.$$

Maintenant, soit nous nous rappelons des relations racines/coefficients soit nous les retrouvons. Comme $\alpha$ et $\beta$ sont racines du polynôme et que le polynôme est unitaire nous factorisons

$$X^2-\sqrt{2}X-\sqrt{3}=(X-\alpha)(X-\beta)=X^2-(\alpha+\beta)X+\alpha\beta$$

ce qui nous indique que $\sqrt{2}=\alpha+\beta$ et donc nous pouvons conclure

$$S=\alpha^3+\beta^3=(2+\sqrt{3})\sqrt{2}+2\sqrt{6}=2\sqrt{2}+3\sqrt{6}.$$

**4)** Le premier réflexe est de diminuer les puissances des racines ce que nous faisons en nous servant de la définition d'une racine :

$$\alpha^4=\alpha(\alpha^3)=\alpha\left(\alpha-i\right)=\alpha^2-i\alpha\quad\beta^3=\beta^2-i\beta\quad\gamma^4=\gamma^2-i\gamma.$$

Ainsi nous avons

$$S=\alpha^4+\beta^4+\gamma^4=(\alpha^2+\beta^2+\gamma^2)-i(\alpha+\beta+\gamma).$$

Maintenant, soit nous nous rappelons des relations racines/coefficients soit nous les retrouvons. Comme $\alpha$ et $\beta$ sont racines du polynôme et que le polynôme est unitaire nous factorisons

$$X^3-X+i=(X-\alpha)(X-\beta)(X-\gamma)=X^3-(\alpha+\beta+\gamma)X^2+(\alpha\beta+\alpha\gamma+\beta\gamma)X-\alpha\beta\gamma$$

ce qui nous indique que $0=\alpha+\beta+\gamma$ et $-1=\alpha\beta+\alpha\gamma+\beta\gamma$. Ainsi nous pouvons obtenir

$$0=(\alpha+\beta+\gamma)^2=\alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\alpha\gamma+\beta\gamma)=\alpha^2+\beta^2+\gamma^2-2.$$

Nous pouvons alors conclure

$$S=\alpha^4+\beta^4+\gamma^4=(\alpha^2+\beta^2+\gamma^2)-i(\alpha+\beta+\gamma)=2.$$

## Exercice 4 *: Des équations et des polynômes*

Résoudre dans $\mathbb{R}[X]$ les équations suivantes d'inconnue $P\in\mathbb{R}[X]$. *On se rappelera que ce qui est intéressant dans un polynôme de sont son degré et ses racines...*

1) $P(X^2)=(X^2+1)P(X)$ 2) $(P')^2=4P$ *N'hésitons pas à être complexes...*

**Solution.** Nous devons trouver les solutions d'une équation donc nous allons supposer que nous avons une solution, trouver tout ce qu'il y a à dire dessus et ensuite faire la synthèse. N'oublions pas que lorsque l'on a des polynômes nous aimons connaître leurs racines et leur degré. Souvent cela suffira à trouver tous les polynômes, mais si jamais cela ne suffit pas nous pourrons toujours faire la méthode bourrine en écrivant tout simplement $P = \sum_{k=0}^{d} a_k X^k$ mais cela mène à d'énormes calculs souvent donc on essaiera le plus possible d'être plus subtil.

**1)**Essayons de trouver quels $P$ peuvent convenir. Supposons que $P \in \mathbb{R}[X]$ satisfasse $P(X^2) = (X^2+1)P(X)$.

• Pouvons-nous dire quelque chose sur le degré de $P$. Si on note $d = \deg(P)$ alors il vient que soit $d = -\infty$ ( $P$ est le polynôme nul), soit

$$\deg(P(X^2)) = 2d \quad \text{et} \quad \deg((X^2+1)P(X)) = 2 + d.$$

Cela nous indique donc que $2d = d+2$ et donc $d = 2$.

• Nous savons que $d = 2$. Que pouvons-nous dire des racines de $P$ ? Nous voyons que $i$ annule le polynôme $X^2+1$ et donc en appliquant l'égalité à $i$ :

$$P(i^2) = 0.P(i) = 0$$

ce qui nous indique que $-1$ est racine de $P$. Mais alors si $-1$ est racine de $P$, appliquons-le à l'équation :

$$P((-1)^2) = P(1) = 2P(-1) = 0$$

et donc 1 est racine. Ainsi le degré de $P$ vaut 2 et il a deux racines 1 et $-1$ donc ce sont toutes ses racines et

$$P = a(X-1)(X+1) \quad \text{avec} \quad a \in \mathbb{R}.$$

Cela nous donne assez d'indications pour faire la synthèse puisque nous avons prouvé que si $P$ est solution alors il est nul ou il existe un réel $a$ tel que $P = a(X-1)(X+1)$.

Synthèse. Supposons que $P = a(X-1)(X+1) = a(X^2-1)$ avec $a$ un réel (notons que le cas du polynôme nul est inclus avec $a = 0$). Nous calculons

$$P(X^2) = a(X^4-1) \quad \text{et} \quad (X^2+1)P = a(X^2+1)(X^2-1) = a(X^4-1$$

ce qui indique bien que $P(X^2) = (X^2+1)P(X)$.

Les polynômes de $\mathbb{R}[X]$ qui satisfont$P(X^2) = (X^2+1)P(X)$ sont les polynômes de la forme $P = a(X^2-1)$ avec $a$ un réel.

**2)**Essayons de trouver quels $P$ peuvent convenir. Supposons que $P \in \mathbb{R}[X]$ satisfasse $(P')^2 = 4P$.

• Pouvons-nous dire quelque chose sur le degré de $P$. Si on note $d = \deg(P)$ alors il vient que soit $d = -\infty$ ( $P$ est le polynôme nul), soit

$$\deg(P') = d-1 \quad \text{donc} \quad \deg((P')^2) = 2(d-1) \quad \text{et} \quad \deg(4P) = d.$$

Cela nous indique donc que $2(d-1) = d$ et donc $d = 2$.

• Nous savons que $d = 2$. Que pouvons-nous dire des racines de $P$ ? Nous ne savons pas si $P$ a des racines dans $\mathbb{R}$ mais nous savons d'après le cours que $P$ a des racines dans $\mathbb{C}$. Si $z$ est une racine de $P$ alors il vient en appliquant l'égalité à $z$ :

$$(P'(z))^2 = 4P(z) = 0$$

ce qui indique que $z_0$ est aussi racine de $P'$. Comme $P(z_0) = P'(z_0) = 0$ nous trouvons que $z_0$ est une racine double de $P$. Ainsi comme le degré de $P$ vaut 2, $z_0$ est son unique racine et nous avons que dans $\mathbb{C}[X]$ :

$$P(X) = a(X-z_0)^2 \quad \text{avec} \quad a \in \mathbb{C}.$$

• Nous avons donc obtenu des polynômes possibles dans $\mathbb{C}[X]$ mais nous cherchons les polynômes de $\mathbb{R}[X]$. Si $z_0$ et $a$ sont des complexes alors

$$a(X-z_0)^2 = aX^2 - 2az_0X + az_0^2$$

et ce polynôme n'est dans $\mathbb{R}[X]$ que si $a \in \mathbb{R}$, $az_0 \in \mathbb{R}$ et $az_0^2 \in \mathbb{R}$ ce qui nous donne au final que $a$ et $z_0$ sont des réels.
Cela nous donne assez d'indications pour faire la synthèse puisque nous avons prouvé que si $P$ est solution alors il est nul ou il existe deux réels $a$ et $x_0$ tels que $P = a(X-x_0)^2$.

Synthèse. Supposons que $P = a(X-x_0)^2$ avec $a$ et $x_0$ deux réels (notons que le cas du polynôme nul est inclus avec $a = 0$). Nous calculons

$$P' = 2a(X-x_0) \quad \text{donc} \quad ((P')^2 = 4a^2(X-x_0)^2 = a^2(4P).$$

Ainsi $P$ est solution si et seulement si $a = a^2$ c'est-à-dire $a = 1$, ce qui nous permet de conclure.

Les polynômes de $\mathbb{R}[X]$ qui satisfont$(P')^2 = 4P$ sont les polynômes de la forme $P = (X-x_0)^2$ avec $x_0$ un réel.

# Racines, factorisation et irréductibilité

## Exercice 5

Déterminer la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ des polynômes suivants.

1) $1+X+X^2+X^3$ 2) $X^8-2X^4+1$

3) $1+X^6$ 4) $1+X^4+X^8$

**Solution.** Pour déterminer les écritures en polynômes irréductibles de $\mathbb{R}[X]$ il est souvent bon de regarder si nous avons des racines évidentes $\lambda$ : $0$, $\pm 1$, $\pm i$, $\pm 2$ par exemple et ainsi mettre en facteur $(X-\lambda)$. Remarquons que pour cette étape nous pouvons aller trouver les racines complexes ce n'est pas un problème puisque si $P \in \mathbb{R}[X]$ et $z$ une racine complexe de $P$ alors

$$P(z) = \sum_{k=0}^{d} a_k z^k = 0 \quad \text{donc} \quad 0 = \overline{P(z)} = \sum_{k=0}^{d} \overline{a_k z}^k = \sum_{k=0}^{d} a_k \overline{z}^k$$

et donc $\overline{z}$ est aussi racine de $P$. Cela donnera donc la mise en facteur suivante

$$P = (X-z)(X-\overline{z})Q = (X^2 - (z+\overline{z})X + |z|^2)Q$$

et

$$X^2 - (z+\overline{z})X + |z|^2 = X^2 - 2\mathrm{Re}(z)X + |z|^2$$

est bien un polynôme irréductible de $\mathbb{R}[X]$ (puisque pas de racines réelles donc de déterminant négatif).

Une fois les efforts avec les racines "évidentes" terminés il va falloir essayer de trouver des factorisations telles que $(A-B)(A+B)$ ou $(A\pm B)^2$ où $A$ et $B$ sont des polynômes. Pour se faire nous aurons trois méthodes : trouver les racines par des calculs (elles seront complexes et conjuguées donc c'est utile de les écrire sous forme polaire), écrire le produit en irréductibles théorique pour obtenir des équations sur les coefficients ou alors “ruser” pour faire apparaître les identités remarquables manquantes (mais ce n'est pas toujours évident). L'exemple 3) ci-dessus présente plusieurs manières de résoudre dans les cas compliqués.

Faire tous ces efforts permet de diminuer le degré des polynômes mis en facteur jusqu'à du degré 1 ou 2.

**1)** Dans ce polynôme $P = 1+X+X^2+X^3$ nous essayons les racines les plus classiques et nous voyons que $P(-1)=0$ donc nous pouvons directement mettre $X+1$ en facteur

$$P = (X+1)(X^2+1)$$

et comme $X^2+1$ est un polynôme de $\mathbb{R}[X]$ de degré deux sans racine réelle il est bien irréductible dans $\mathbb{R}[X]$.

**2)** Dans ce polynôme $P = X^8-2X^4+1$ nous essayons les racines les plus classiques et nous voyons que $P(1)=P(-1)=0$ donc nous pouvons directement mettre $(X-1)(X+1)=(X^2-1)$ en facteur

$$P = (X^2-1)(X^6+X^4-X^2-1) = (X-1)(X+1)(X^6+X^4-X^2-1).$$

Le polynôme $X^6+X^4-X^2-1$ admet encore $1$ et $-1$ en racine donc nous remettons $(X^2-1)$ en facteur

$$P = (X-1)(X+1)(X^2-1)(X^4+2X^2+1) = (X-1)^2(X+1)^2(X^4+2X^2+1).$$

La polynôme restant $X^4+2X^2+1$ n'a pas de racines rélles puisque $x^4+2x^2+1 \geqslant 1$ pour tout $x\in\mathbb{R}$. Donc deux solutions

- $*$ Nous allons donc essayer de calculer ses racines dans $\mathbb{C}$. Lorsque nous devons calculer des racines non évidentes, il est bon de se ramener au cas du degré 2. Nous remarquons que

$$X^4+2X^2+1 = Q(X^2) \quad \text{avec} \quad Q = X^2+2X+1.$$

Nous trouvons que $Q$ a une unique racine : $-1$ et que donc

$$X^2+2X+1 = (X+1)^2 \quad \text{donc} \quad X^4+2X^2+1 = (X^2+1)^2.$$

- $*$ Nous essayons de trouver une identité remarquable ce qui est le cas ici : $X^4+2X^2+1 = (X^2+1)^2$.

Nous avons donc trouvé que

$$P = (X-1)^2(X+1)^2(X^2+1)^2$$

et comme $X^2+1$ est un polynôme de $\mathbb{R}[X]$ de degré deux sans racine réelle il est bien irréductible dans $\mathbb{R}[X]$.

**3)** Dans ce polynôme $P = 1+X^6$ nous essayons les racines les plus classiques et nous voyons que $P(i)=P(-i)=0$ donc nous pouvons directement mettre $(X-i)(X+i)=(X^2+1)$ en facteur

$$P = (X^2+1)(X^4-X^2+1).$$

Le polynôme $X^4-X^2+1$ ne semble pas se mettre aisément sous la forme d'une identité remarquable et ses racines ne sont pas directes. Nous avons donc trois méthodes.

* <u>Méthode 1 les racines.</u> Nous allons donc essayer de calculer ses racines dans $\mathbb{C}$. Lorsque nous devons calculer des racines non évidentes, il est bon de se ramener au cas du degré 2. Nous remarquons que

$$X^4 - X^2 + 1 = Q(X^2) \quad \text{avec} \quad Q = X^2 - X + 1.$$

Trouvons les racines de $Q$. Le calcul de son déterminant donne $\Delta = -3$ et donc les racines de $Q$ sont complexes conjuguées (car $Q$ est dans $\mathbb{R}[X]$, voir début de la solution) et valent

$$z = \frac{1 + i\sqrt{3}}{2} \quad \text{et} \quad \overline{z} = \frac{1 - i\sqrt{3}}{2}$$

ce qui implique que

$$X^2 - X + 1 = (X - z_1)(X - z_2) \quad \text{donc} \quad X^4 - X^2 + 1 = (X^2 - z)(X^2 - \overline{z}).$$

Ainsi nous sommes passés dans les complexes et nous trouvons

$$P = (X^2 + 1)(X^2 - z)(X^2 - \overline{z})$$

ce qui nous donne (et c'est normal) une décomposition dans $\mathbb{C}[X]$. Mais nous savons que nous pourrons trouver des polynômes de $\mathbb{C}[X]$ de degré 1 qui, multipliés ensemble donneront des polynômes réels de degré 2 irréductibles (voir explications en début de solution).
Il faut alors finir de trouver les racines de $(X^2 - z)(X^2 - \overline{z})$. Pour trouver de telles racines il est plus aisé d'écrire $z$ sous forme exponentielle (mais ce n'est pas obligatoire). Comme

$$\cos\left(\frac{\pi}{3}\right) = \frac{1}{2} \quad \text{et} \quad \sin\left(\frac{\pi}{3}\right) = \frac{\sqrt{3}}{2}$$

il vient

$$z = e^{i\frac{\pi}{3}} \quad \text{et} \quad \overline{z} = e^{i\frac{\pi}{3}}.$$

Ainsi nous trouvons que

$$\begin{aligned} X^2 - X + 1 &= (X^2 - e^{i\frac{\pi}{3}})(X^2 - e^{-i\frac{\pi}{3}}) = (X - e^{i\frac{\pi}{6}})(X + e^{i\frac{\pi}{6}})(X - e^{-i\frac{\pi}{6}})(X + e^{-i\frac{\pi}{6}}) \\ &= \left[(X - e^{i\frac{\pi}{6}})(X - e^{-i\frac{\pi}{6}})\right]\left[(X + e^{i\frac{\pi}{6}})(X + e^{-i\frac{\pi}{6}})\right] \quad \textit{On regroupe les conjugués} \\ &= (X^2 - (e^{i\frac{\pi}{6}} + e^{-i\frac{\pi}{6}})X + e^{i.0})(X^2 + (e^{i\frac{\pi}{6}} + e^{-i\frac{\pi}{6}})X + e^{i.0}) \\ &= (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1). \end{aligned}$$

*Pour calculer plus vite nous avons utilisé que*

$$(X - z)(X - \overline{z}) = (X^2 - (z + \overline{z})X + |z|^2) = X^2 - (z + \overline{z})X + |z|^2 = X^2 - 2Re(z)X + |z|^2.$$

* <u>Méthode 2 l'écriture directe en facteur</u> Sinon nous savons que $X^4 - X^2 + 1$ n'est pas irréductible dans $\mathbb{R}[X]$ ce qui implique qu'il existe deux polynômes $A$ et $B$ de degré 2 de $\mathbb{R}[X]$ tels que $X^4 - X^2 + 1 = AB$. Comme $X^4 - X^2 + 1$ est unitaire nous avons donc l'existence de $a, b, c, d$ des réels tels que

$$X^4 - X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + db.$$

Comme $(1, X, X^2, X^3, X^4)$ est une famille libre nous n'avons qu'à résoudre le système

$$\begin{aligned} &\begin{cases} a + c = 0 \\ b + d + ac = -1 \\ ad + bc = 0 \\ db = 1 \end{cases} \Leftrightarrow \begin{cases} c = -a \\ b + d + 1 = a^2 \\ a(d - b) = 0 \\ b \neq 0 \text{ et } d = \frac{1}{b} \end{cases} \Leftrightarrow \left( \begin{cases} c = -a \\ b \neq 0 \text{ et } d = \frac{1}{b} \\ a = 0 \\ b + \frac{1}{b} + 1 = 0 \end{cases} \text{ou} \begin{cases} c = -a \\ b \neq 0 \text{ et } d = \frac{1}{b} \\ b = d = \frac{1}{b} \\ 2b + 1 = a^2 \end{cases} \right) \\ &\Leftrightarrow \left( \begin{cases} c = -a \\ b \neq 0 \text{ et } d = \frac{1}{b} \\ a = 0 \\ \frac{b^2 + b + 1}{b} = 0 \end{cases} \text{ou} \begin{cases} c = -a \\ b \neq 0 \text{ et } d = \frac{1}{b} \\ b = 1 \\ 3 = a^2 \end{cases} \text{ou} \begin{cases} c = -a \\ b \neq 0 \text{ et } d = \frac{1}{b} \\ b = -1 \\ -1 = a^2 \end{cases} \right) \end{aligned}$$

Comme $b^2 + b + 1 = 0$ et $-1 = a^2$ n'ont pas de solutions réelles il ne reste donc plus qu'une possibilité

$$a = \sqrt{3} \quad b = 1 \quad c = -\sqrt{3} \quad d = 1$$

ce qui nous indique que

$$X^4 - X^2 + 1 = (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1).$$

Nous avons donc trouvé que

$$P = (X^2 + 1)(X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1)$$

et comme $X^2 - \sqrt{3}X + 1$ et $X^2 + \sqrt{3}X + 1$ sont deux polynômes de $\mathbb{R}[X]$ de degré deux sans racine réelle ils sont bien irréductibles dans $\mathbb{R}[X]$.

**4)** Dans ce polynôme $P = 1 + X^4 + X^8$ nous ne voyons pas de racines évidentes mais nous voyons que

$$P = Q(X^4) \quad \text{avec} \quad Q = 1 + X + X^2$$

pour lequel nous pouvons calculer les racines complexes grâce à son déterminant et nous trouvons (voir les détails de calculs en 3))

$$Q = (X - z)(X - \overline{z}) \quad \text{avec} \quad z = \frac{-1 + i\sqrt{3}}{2} = e^{i\frac{2\pi}{3}}.$$

Ceci nous indique donc que

$$\begin{aligned}
P = Q(X^4) &= \left(X^4 - e^{i\frac{2\pi}{3}}\right)\left(X^4 - e^{-i\frac{2\pi}{3}}\right) = \left(X^2 - e^{i\frac{2\pi}{6}}\right)\left(X^2 + e^{i\frac{2\pi}{6}}\right)\left(X^2 - e^{-i\frac{2\pi}{6}}\right)\left(X^2 + e^{-i\frac{2\pi}{6}}\right)\\
&= \left(X - e^{i\frac{2\pi}{12}}\right)\left(X + e^{i\frac{2\pi}{12}}\right)\left(X + ie^{i\frac{2\pi}{12}}\right)\left(X - ie^{i\frac{2\pi}{12}}\right)\left(X - e^{-i\frac{2\pi}{12}}\right)\left(X + e^{-i\frac{2\pi}{12}}\right)\left(X - ie^{-i\frac{2\pi}{12}}\right)\left(X + ie^{-i\frac{2\pi}{12}}\right)\\
&= \textit{On regroupe les complexes conjugués}\\
&= \left[\left(X - e^{i\frac{2\pi}{12}}\right)\left(X - e^{-i\frac{2\pi}{12}}\right)\right]\left[\left(X + e^{i\frac{2\pi}{12}}\right)\left(X + e^{-i\frac{2\pi}{12}}\right)\right]\left[\left(X + ie^{i\frac{2\pi}{12}}\right)\left(X - ie^{-i\frac{2\pi}{12}}\right)\right]\left[\left(X - ie^{i\frac{2\pi}{12}}\right)\left(X + ie^{-i\frac{2\pi}{12}}\right)\right]\\
&= (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1)(X^2 - X + 1)(X^2 + X + 1).
\end{aligned}$$

*Pour calculer plus vite nous avons utilisé que*

$$(X - z)(X - \overline{z}) = (X^2 - (z + \overline{z})X + |z|^2) = X^2 - (z + \overline{z})X + |z|^2 = X^2 - 2Re(z)X + |z|^2.$$

Tous les polynômes en présence sont des polynômes de $\mathbb{R}[X]$ sont de degré 2 sans racine réelle et sont donc bien irréductibles.

## Exercice 6

Factoriser les polynômes suivants en produits d'irréductibles sur $\mathbb{C}[X]$ puis sur $\mathbb{R}[X]$.

1) $X^8 - 1$
2) $(X^2 - X + 1)^2 + 1$
3) $1 + X + X^2 + X^3 + X^4 + X^5$
4) $1 + X^2 + X^4 + X^6$

**Solution.** Cet exercice est exactement identique au précédent sauf que l'on demande de trouver également les polynômes de degré 1 de $\mathbb{C}[X]$ qui divisent. Nous renvoyons au début de la solution de l'exercice 5 pour une description détaillée des méthodes.

**1)** Les polynômes $P = X^8 - 1$ a des racines connues puisque ce sont les racines $8^{eme}$ de l'unité : $e^{2ik\frac{\pi}{8}} = e^{i\frac{k\pi}{4}}$ avec $0 \leqslant k \leqslant 7$. Comme expliqué en exercice 5 elles peuvent toutes être écrites sous forme $z$ et $\overline{z}$ deux à deux :

$$\{\text{racine de } P\} = \left\{-1, 1, e^{i\frac{\pi}{4}}, e^{-i\frac{\pi}{4}}, e^{i\frac{2\pi}{4}}, e^{-i\frac{2\pi}{4}}, e^{i\frac{3\pi}{4}}, e^{-i\frac{3\pi}{4}}\right\}.$$

Nous avons donc la composition en facteurs irréductibles dans $\mathbb{C}[X]$ qui est

$$\begin{aligned}
X^8 - 1 &= (X+1)(X-1)(X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X - e^{i\frac{\pi}{2}})(X - e^{-i\frac{\pi}{2}})(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}})\\
&= (X+1)(X-1)(X-i)(X+i)(X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}}).
\end{aligned}$$

Pour obtenir des polynômes irréductibles de $\mathbb{R}[X]$ il suffit, comme nous l'avons vu plus haut, de regrouper les polynômes avec des racines conjuguées car

$$(X - z)(X - \overline{z}) = (X^2 - (z + \overline{z})X + |z|^2) = X^2 - (z + \overline{z})X + |z|^2 = X^2 - 2\mathrm{Re}(z)X + |z|^2.$$

D'où

$$\begin{aligned}
P &= (X+1)(X-1)(X^2+1)\left[(X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})\right]\left[(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}})\right]\\
&(X+1)(X-1)(X^2+1)(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).
\end{aligned}$$

Tous les polynômes de degré 2 sont irréductibles sur $\mathbb{R}[X]$ puisqu'ils n'ont aucune racine réelle.

**2)** Nous voyons que ce polynôme n'a pas de racines réelles donc essayons tout d'abord de trouver une identité remarquable pour le simplifier avant de trouver les racines complexes.

$$P = (X^2 - X + 1)^2 + 1 = (X^2 - X + 1)^2 - i^2 = (X^2 - X + 1 - i)(X^2 - X + 1 + i).$$

Regardons si nous certaines racines complexes évidentes apparaissent :

$$(-i)^2 - (-i) + 1 - i = 0 \quad \text{donc} \quad X^2 - X + 1 - i = (X + i)(X - (1 + i))$$

et de même
$$i^2 - i + 1 + i = 0 \quad \text{donc} \quad X^2 - X + 1 + i = (X - i)(X + (i - 1))$$
ce qui implique la décomposition de $P$ en éléments irréductibles de $\mathbb{C}[X]$
$$P = (X + i)(X - (1 + i))(X - i)(X + (i - 1)).$$
Pour obtenir la décomposition en irréductibles dans $\mathbb{R}[X]$ nous regroupons les racines conjuguées.
$$P = [(X - i)(X + i)]\,[(X - (1 + i))(X - (1 - i))] = (X^2 + 1)(X - 2X + 2).$$
Tous les polynômes de degré 2 sont irréductibles sur $\mathbb{R}[X]$ puisqu'ils n'ont aucune racine réelle.

**3)** Nous voyons que $P = 1 + X + X^2 + X^3 + X^4 + X^5$ a une racine aisée : $P(-1) = 0$ et donc nous trouvons
$$P = (X + 1)(X^4 + X^2 + 1).$$
Ici, nous devons trouver les racines de $X^4 + X^2 + 1 = Q(X^2)$ avec $Q = X^2 + X + 1$. Nous les trouvons grâce à la formule du déterminant et nous trouvons deux racines qui sont conjuguées (voir explications en exercice 5)
$$z = \frac{-1 + i\sqrt{3}}{2} = e^{\frac{4\pi}{3}} \quad \text{et} \quad \overline{z} = e^{-\frac{4\pi}{3}}.$$
Ainsi $Q = (X - z)(X - \overline{z})$ et donc
$$P = (X + 1)(X^2 - e^{\frac{4\pi}{3}})(X^2 - e^{-\frac{4\pi}{3}}) = (X + 1)(X - e^{\frac{4\pi}{6}})(X + e^{\frac{4\pi}{6}})(X - e^{-\frac{4\pi}{6}})(X + e^{-\frac{4\pi}{6}})$$
qui est la décomposition de $P$ en irréductibles de $\mathbb{C}[X]$.
Pour obtenir la décomposition en irréductibles dans $\mathbb{R}[X]$ nous regroupons les racines conjuguées.
$$P = (X + 1)\left[(X - e^{\frac{4\pi}{6}})(X - e^{-\frac{4\pi}{6}})\right]\left[(X + e^{\frac{4\pi}{6}})(X + e^{-\frac{4\pi}{6}})\right] = (X + 1)(X^2 + X + 1)(X^2 - X + 1).$$
Tous les polynômes de degré 2 sont irréductibles sur $\mathbb{R}[X]$ puisqu'ils n'ont aucune racine réelle.

**4)** Si $P = 1 + X^2 + X^4 + X^6$ n'a pas de racine réelle, puisque pour tout réel $x$ on a $1 + x + x^2 + x^3 + x^4 + x^5 \geqslant 1$, mais nous avons que $P(i) = P(-i) = 0$ donc on peut mettre $(X - i)(X + i) = (X^2 + 1)$ en racine :
$$P = (X^2 + 1)(X^4 + 1).$$
Au lieu de calculer les racines de $X^4 + 1$ nous pouvons y trouver une identité remarquable.
$$P = (X^2 + 1)(X^4 + 1) = (X^2 + 1)(X^4 - i^2) = (X^2 + 1)(X^2 - i)(X^2 + i).$$
Les racines de $i$ et $-i$ sont aisément trouvables si, comme dans tous les exercices ci-dessus, nous écrivons $i$ sous forme polaire
$$i = e^{i\frac{\pi}{2}} \quad \text{et} \quad -i = e^{-i\frac{\pi}{2}}.$$
Nous pouvons donc continuer
$$P = (X^2 + 1)(X^2 - i)(X^2 + i) = (X - i)(X + i)(X - e^{i\frac{\pi}{4}})(X + e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X + e^{-i\frac{\pi}{4}})$$
qui est donc bien la décomposition en facteurs irréductibles de $P$ dans $\mathbb{C}[X]$.
Pour obtenir la décomposition en irréductibles dans $\mathbb{R}[X]$ nous regroupons les racines conjuguées.
$$P = (X^2 + 1)\left[X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})\right]\left[X + e^{i\frac{\pi}{4}})(X + e^{-i\frac{\pi}{4}})\right] = (X^2 + 1)(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$
Tous les polynômes de degré 2 sont irréductibles sur $\mathbb{R}[X]$ puisqu'ils n'ont aucune racine réelle.

## Exercice 7

Nous définissons
$$P_1 = X^3 - 3X + 1 \quad P_2 = X^3 - 3X - 1 \quad Q(X) = P_1(X^2 - 2).$$

a) Vérifier que $P_1(-X) = -P_2(X)$ et que $Q = P_1P_2$.

b) Démontrer que $P_1$ a trois racines distinctes situées dans $]-2, 2[$.

c) Linéariser $\cos^3\theta$ puis résoudre $P_1(2\cos\theta) = 0$ pour en déduire les zéros de $P_1$, $P_2$ et $Q$.

**Solution.** Dans ce genre d'exercice il y a fort à parier que les premières questions servent dans les dernières alors si nous sommes bloqué·es n'oublions pas ce que nous avons démontré !

**a)** Cette question n'est que pure vérification alors faisons-la soigneusement.

$$P_1(-X) = (-X)^3 - 3(-X) + 1 = -X^3 + 3X + 1 = -(X^3 - 3X - 1) = -P_2(X).$$

Pour la deuixème égalité nous allons écrire $Q$ puis essayer de mettre $P_1$ en facteur par exemple.

$$P_1Q = P_1(X^2-2) = (X^2-2)^3 - 3(X^2-2)+1 = X^6 - 6X^4 + 9X^2 - 1 \quad \text{et} \quad (X^3-3X+1)(X^3-3X-1) = X^6 - 6X^4 + 9X^2 - 1$$

ce qui indique bien que $Q = P_1P_2$.

**b)** Le polynômes $P_1$ est de degré 3 et donc il a au maximum trois racines. L'énoncé ne nous demande pas de les calculer donc inutile d'essayer de les trouver. Comment trouver si une fonction s'annule quelque part ? Nous faisons un tableau de variation. Nous regardons donc la fonction polynôme associée à $P_1$ qui est définie par

$$\forall x \in \mathbb{R}, \quad f(x) = P_1(x) = x^3 - 3x + 1$$

qui est une fonction dérivable sur $\mathbb{R}$ et donc sur $]-2,2[$. Nous calculons

$$\forall x \in ]-2,2[, \quad f'(x) = 3x^2 - 3 = 3(x^2-1) = 3(x+1)(x-1).$$

Nous pouvons donc construire le tableau de variation de $f$ : le faire ! ! Les valeurs à placer sont

$$f(-2) = -1 < 0 \quad f(-1) = 3 > 0 \quad f(1) = -1 < 0 \quad f(2) = 3$$

ce qui indique par le théorème des valeurs intermédiaires que $f$ s'annule dans $]-2,-1[$ , dans $]-1,1[$ et dans $]1,2[$ puisqu'elle change de signe et est continue. Ainsi $P_1$ possède au moins trois racines distinctes dans $]-2,2[$ et comme $\deg(P_1) = 3$ ce sont toutes ses racines.

**c)**• On nous demande de linéariser $\cos^3(\theta)$, c'est-à-dire de l'écrire avec des cos et des sin sans puissance. Il y a plusieurs façons de faire, nous proposons de passer tout simplement par la définition du cosinus.

$$\cos^3\theta = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^3 = \frac{e^{3i\theta}+3e^{2i\theta}e^{-i\theta}+3e^{i\theta}e^{-2i\theta}+e^{-3i\theta}}{8} = \frac{e^{3i\theta}+e^{-3i\theta}}{8} + 3\frac{e^{i\theta}+e^{-i\theta}}{8} = \frac{1}{4}\left(\cos(3\theta)+3\cos(\theta)\right).$$

• On nous demande de regarder $P_1(2\cos\theta)$ pour trouver ses racones. Comme les racines de $P_1$ sont dans $]-2,2[$, $2\cos\theta$ décrit $]-2,2[$ pour $\theta \in ]0,\pi[$. Prenons alors $\theta$ dans $]0,\pi[$ et résolvons

$$P_1(2\cos\theta) = 0 \Leftrightarrow 8\cos^3\theta - 6\cos\theta + 1 = 0 \Leftrightarrow 2(\cos(3\theta)+3\cos\theta) - 6\cos\theta + 1 = 0 \Leftrightarrow \cos(3\theta) = -\frac{1}{2}.$$

Comme nous avons pris $\theta$ dans $]0,\pi[$ nous avons $3\theta \in ]0,3\pi[$ et ainsi nous pouvons trouver les $\theta$ solutions.

$$\forall \theta \in ]0,2\pi[, \quad P_1(2\cos\theta) = 0 \Leftrightarrow \cos(3\theta) = -\frac{1}{2} \Leftrightarrow \left(3\theta = \frac{2\pi}{3} \text{ ou } 3\theta = \frac{4\pi}{3} \text{ ou } 3\theta = \frac{8\pi}{3}\right) \Leftrightarrow \left(\theta = \frac{2\pi}{9} \text{ ou } \theta = \frac{4\pi}{9} \text{ ou } \theta = \frac{8\pi}{9}\right).$$

Nous obtenons donc trois valeurs possibles de $\theta$ et donc trois valeurs différentes de $2\cos\theta$ qui annulent $P_1$ et ce sont donc les racines de $P_1$.

$$\{\text{racines de } P_1\} = \left\{2\cos\left(\frac{2\pi}{9}\right), 2\cos\left(\frac{4\pi}{9}\right), 2\cos\left(\frac{8\pi}{9}\right)\right\}.$$

• Grâce à la question $a$) nous savons que pour tout complexe $z$,

$$P_2(z) = 0 \Leftrightarrow -P_1(-z) = 0 \Leftrightarrow P_1(-z) = 0.$$

Nous connaissons 3 valeurs de $z$ telles que $P_1(-z) = 0$ et donc $P_2(z) = 0$. Comme $\deg(P_2) = 3$ ce sont donc toutes ses racines et nous venons de prouver que

$$\{\text{racines de } P_2\} = \left\{-2\cos\left(\frac{2\pi}{9}\right), -2\cos\left(\frac{4\pi}{9}\right), -2\cos\left(\frac{8\pi}{9}\right)\right\}.$$

*Remarquons que cette manière de rédiger quant au nombre de racine complexes est importante, même si ici cela semble inutile, car imaginons que $P_2(x^2) = P_1(x)$ nous pourrions trouver les racines positives de $P_1$ mais pas forcément toutes ses racines si l'on en avait des négatives. Il faut donc bien regarder les racines dans $\mathbb{C}$, là où on sait qu'il y en a toujours.*

• Grâce à la question $a$) nous savons que pour tout complexe $z$,

$$Q(z) = 0 \Leftrightarrow P_1(z)P_2(z) = 0 \Leftrightarrow (P_1(z) = 0 \text{ ou } P_2(z) = 0).$$

Nous connaissons 3 valeurs de $z$ telles que $P_1(z) = 0$ et 3 autres valeurs telles que $P_2(z) = 0$. Ainsi nous connaissons 6 racines de $Q$ et comme $\deg(Q) = 6$ ce sont donc toutes ses racines et nous venons de prouver que

$$\{\text{racines de } Q\} = \left\{-2\cos\left(\frac{2\pi}{9}\right), -2\cos\left(\frac{4\pi}{9}\right), -2\cos\left(\frac{8\pi}{9}\right), 2\cos\left(\frac{2\pi}{9}\right), 2\cos\left(\frac{4\pi}{9}\right), 2\cos\left(\frac{8\pi}{9}\right)\right\}.$$

*Remarquons que cette manière de rédiger quant au nombre de racine complexes est importante, même si ici cela semble inutile, car imaginons que $Q(x^2) = P_1(x)P_2(x)$ nous pourrions trouver les racines positives de $P_1$ mais pas forcément toutes ses racines si l'on en avait des négatives. Il faut donc bien regarder les racines dans $\mathbb{C}$, là où on sait qu'il y en a toujours.*

### Exercice 8

Dans les cas suivants, démontrer que les racines du polynôme $P$ dans $\mathbb{C}[X]$ sont toutes distinctes.

$$1) \quad P = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!} + \frac{X^4}{4!} \qquad\qquad 2) \quad (X+1)^4 - X^4$$

**Solution.** Montrer que des racines sont simples revient à montrer qu'elles ne sont pas doubles. Qu'est-ce que veut dire "$a$ racine double de $P$" ? Cela veut dire que $(X-a)^2|P$ ou encore que $P(a) = P'(a) = 0$. Ce sont les seuls résultats du cours donc nous allons bien évidemment nous en servir. Souvent passer par le polynôme dérivé est plus simple que les divisibilités...

**1)**• Soit $z$ une racine de $P$. Supposons que $z$ soit une racine multiple. Alors nous avons $P(z) = P'(z) = 0$. Nous connaissons le polynôme dérivé de $P$ :

$$P' = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!}$$

Ainsi nous avons

$$1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \frac{z^4}{4!} = 0 \quad \text{et} \quad 1 + z + \frac{z^2}{2} + \frac{z^3}{3!} = 0.$$

Ainsi en combinant les deux inégalités nous trouvons que $z^4 = 0$ et donc $z = 0$.

• La seule racine multiple possible de $P$ est 0 mais il se trouve que $P(0) = 1 \neq 0$ et donc ce n'est pas une racine de $P$. Donc $P$ n'a que des racines simples.

**2)**• Soit $z$ une racine de $P$. Supposons que $z$ soit une racine multiple. Alors nous avons $P(z) = P'(z) = 0$. Nous connaissons le polynôme dérivé de $P$ :

$$P' = 4(X+1)^3 - 4X^3$$

Ainsi nous avons

$$(1+z)^4 - z^4 = 0 \quad \text{et} \quad 4(z+1)^3 - 4z^3 = 0.$$

Combinons alors les deux égalités :

$$(1+z)^4 = z^4 = zz^3 = z(1+z)^3$$

ce qui implique que $z = 0$ ou $z = -1$.

• Les seules racines multiples possibles de $P$ sont 0 et $-1$ mais il se trouve que $P(0) = 1 \neq 0$ et $P(1) = 2^4 - 1 \neq 0$ et donc ce ne sont pas des racines de $P$. Donc $P$ n'a que des racines simples.

## Arithmétique et algorithmique au pays des polynômes

### Exercice 9 : *Parlons division euclidienne*

Effectuer la division euclidienne dans $\mathbb{C}[X]$ de $A$ par $B$ dans les cas suivants.

1) $A = 2X^4 - 3X^3 + 4X^2 - 5X + 6$ et $B = X^2 - 3X + 1$.
2) $A = 4X^3 + X^2$ et $B = X + 1 + i$.
3) $A = X^4 + 2X^3 + X^2 - 9$ et $B = X^2 + X + 1$.
4) $A = X^4 + 7X^3 + 7X^2 + 28X + 12$ et $B = X^2 + 7X + 3$.

Dans les cas suivants, déterminer le reste de la division euclidienne de $A$ par $B$ dans $\mathbb{R}[X]$.

5) $A$ quelconque et $B = (X-a)(X-b)$ où $a \neq b$ sont deux réels.
6) $A = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$ et $B = (X-1)^3$, où $n$ est un entier naturel non nul.

**Solution.** On nous demande d'effectuer des division euclidienne de $A$ par $B$ ce qui veut dire trouver $Q$ et $R$ des polynômes tels que $A = BQ + R$ et $\deg(R) < \deg(B)$. La manière de faire est simple, répétitive, algorithmique (on peut également parfois voir des astuces plus rapides mais sinon ne nous prenons pas la tête et effectuons la division sans réfléchir). En gros nous allons mettre $B$ en facteur dans $A$ en éliminant successivement les degré de $A$. Exemple :

$$Q_1 = \frac{\text{coef dominant de } A}{\text{coef dominant de } B} X^{\deg(A) - \deg(B)}$$

est un polynôme tek que $BQ_1$ est de degré le degré de $A$ et de coefficient dominant celui de $A$ et ainsi

$$R_1 = A - BQ_1 \quad \text{est tel que} \quad \deg(R_1) < \deg(A)$$

et nous avons

$$A = BQ_1 + R_1.$$

Et nous recommençons alors la même stratégie avec $B$ et $R_1$ pour obtenir $Q_2$ et $R_2$ et nous continuons jusqu'à obtenir un $R_n$ tel que $\deg(R_n) < \deg(B)$.

**1)** Nous calculons au fur et à mesure.

$$\begin{aligned}A &= 2X^4-3X^3+4X^2-5X+6 = 2X^2(X^2-3X+1)+6X^3-2X^2-3X^3+4X^2-5X+6\\ &= 2X^2B+3X^3+2X^2-5X+6 = 2X^2B+3X(X^2-3X+1)+9X^2-3X+2X^2-5X+6\\ &= (2X^2+3X)B+11X^2-8X+6 = (2X^2+3X)B+11(X^2-3X+1)+33X-11-8X+6\\ &= (2X^2+3X+11)B+25X-5.\end{aligned}$$

Comme $\deg(25X-5)=1<\deg(B)=2$ nous avons fait la DE de $A$ par $B$ et

$$A=BQ+R \quad \text{avec} \quad Q=2X^2+3X+11 \text{ et } R=25X-5.$$

**2)** Nous calculons au fur et à mesure.

$$\begin{aligned}A &= 4X^3+X^2 = 4X^2(X+1+i)-(4+4i)X^2+X^2\\ &= 4X^2B-(3+4i)X^2 = 4X^2B-(3+4i)X(X+1+i)+(3+4i)(1+i)X\\ &= (4X^2-(3+4i)X)B+(7i-1)X = (4X^2-(3+4i)X)B+(7i-1)(X+1+i)-(7i-1)(1+i)\\ &= (4X^2-(3+4i)X+(7i-1))B+(8-6i).\end{aligned}$$

Comme $\deg(-8+6i)=0<\deg(B)=1$ nous avons fait la DE de $A$ par $B$ et

$$A=BQ+R \quad \text{avec} \quad Q=4X^2-(3+4i)X+(7i-1) \text{ et } R=8-6i.$$

**3)** Nous calculons au fur et à mesure.

$$\begin{aligned}A &= X^4+2X^3+X^2-9 = X^2(X^2+X+1)-X^3-X^2+2X^3+X^2-9\\ &= X^2B+X^3-9 = X^2B+X(X^2+X+1)-X^2-X-9\\ &= (X^2+X)B-(X^2+X+1)+X+1-X-9\\ &= (X^2+X-1)B-8\end{aligned}$$

Comme $\deg(-8)=0<\deg(B)=2$ nous avons fait la DE de $A$ par $B$ et

$$A=BQ+R \quad \text{avec} \quad Q=X^2+X-1 \text{ et } R=-8.$$

**4)** Nous calculons au fur et à mesure.

$$\begin{aligned}A &= X^4+7X^3+7X^2+28X+12 = X^2(X^2+7X+3)-7X^3-3X^2+7X^3+7X^2+28X+12\\ &= X^2B+4X^2+28X+12 = X^2B+4(X^2+7X+3)-28X-12+28X+12\\ &= (X^2+4)B.\end{aligned}$$

Comme $\deg(0)=-\infty<\deg(B)=2$ nous avons fait la DE de $A$ par $B$ et

$$A=BQ+R \quad \text{avec} \quad Q=X^2+4 \text{ et } R=0$$

Ce qui indique que $B$ divise $A$ dans $\mathbb{R}[X]$.

**5)**• ATTENTION !!! Lisons bien l'énoncé. Il nous demande de trouver le RESTE de la division euclidienne et non la division euclidienne totale ! La division euclidienne de $A$ par $B$ donne l'existence et l'unicité de $Q$ et $R$ dans $\mathbb{R}[X]$ tels que

$$A=BQ+R \quad \text{avec} \quad \deg(R)<\deg(B).$$

• Nous avons ici $\deg(B)=2$ ce qui implique que $\deg(R)=1$ et donc il existe $\alpha$ et $\beta$ des réels tels que $R=\alpha X+\beta$. La division euclidienne est donc

$$A=BQ+\alpha X+\beta.$$

Nous n'avons pas besoin de trouver $Q$ ici, seulement $\alpha$ et $\beta$. Comme $Q$ nous embête, que pouvons-nous faire ? L'enlever en regardant la division euclidienne aux racines de $B$ : $a$ et $b$ !
Appliquons cela au point $a$ et nous trouvons

$$A(a)=0+\alpha a+\beta.$$

Puis appliquons-la au point $b$ et nous trouvons

$$A(b)=0+\alpha b+\beta.$$

Ce qui nous donne un joli système pour trouver $\alpha$ et $\beta$ :

$$\left\{\begin{array}{l}\alpha a+\beta=A(a)\\ \alpha b+\beta=A(b)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}\beta=A(a)-\alpha a\\ \alpha(b-a)+A(a)=A(b)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}\alpha=\frac{A(b)-A(a)}{b-a}\\ \beta=A(a)-\frac{A(b)-A(a)}{b-a}a\end{array}\right. .$$

Notons que l'hypothèse $a \neq b$ est très importante pour pouvoir résoudre le système ! Ainsi le reste de la division euclidienne de $A$ par $(X-a)(X-b)$ est

$$R = \frac{A(b)-A(a)}{b-a}(X-a) + A(a).$$

**6)**• ATTENTION !!! Lisons bien l'énoncé. Il nous demande de trouver le RESTE de la division euclidienne et non la division euclidienne totale ! La division euclidienne de $A$ par $B$ donne l'existence et l'unicité de $Q$ et $R$ dans $\mathbb{R}[X]$ tels que

$$A = BQ + R \quad \text{avec} \quad \deg(R) < \deg(B).$$

• Nous avons ici $\deg(B) = 3$ ce qui implique que $\deg(R) = 2$ et donc il existe $\alpha$, $\beta$ et $\gamma$ des réels tels que $R = \alpha X^2 + \beta X + \gamma$. La division euclidienne est donc

$$A = BQ + \alpha X^2 + \beta X + \gamma.$$

Nous n'avons pas besoin de trouver $Q$ ici, seulement $\alpha$ et $\beta$. Comme $Q$ nous embête, que pouvons-nous faire ? L'enlever en regardant la division euclidienne aux racines de $B$ :1 ! Malheureusement cela ne nous donne qu'une seule équation qui est

$$n - (n+2) + (n+2) - n = 0 + \alpha + \beta + \gamma \quad \text{soit} \quad \alpha + \beta + \gamma = 0.$$

Il faut alors penser au fait que 1 est racine triple de $B$ ce qui signifie que $B$, $B'$ et $B''$ s'annulent en 1. Nous voulons des dérivées donc nous les mettons en dérivant la division euclidienne :

$$A' = n(n+2)X^{n+1} - (n+2)(n+1)X^n + (n+2) = QB' + Q'B + 2\alpha X + \beta$$

ce qui donne appliqué au point 1

$$n(n+2) - (n+2)(n+1) + (n+2) = 0 + 0 + 2\alpha + \beta \quad \text{soit} \quad 2\alpha + \beta = 0.$$

Il nous reste à utiliser le fait que $B''(1) = 0$. Nous voulons des dérivées secondes donc nous les mettons en dérivant la division euclidienne :

$$A'' = n(n+2)(n+1)X^n - (n+2)(n+1)nX^{n-1} = QB'' + 2Q'B' + Q''B + 2\alpha$$

ce qui donne appliqué au point 1

$$n(n+2)(n+1) - (n+2)(n+1)n = 0 + 0 + 0 + 2\alpha \quad \text{soit} \quad 2\alpha = 0.$$

Notons que l'hypothèse $n \geqslant 1$ est importante pour avoir cette puissance $X^{n-1}$.
Nous venons donc d'obtenir un joli système de trois équations avec trois inconnues :

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ 2\alpha + \beta = 0 \\ \alpha = 0 \end{cases} \Leftrightarrow \alpha = \beta = \gamma = 0.$$

Ainsi le reste de la division euclidienne de $A$ par $B$ est nul donc $B$ divise $A$.

## Exercice 10

Dans les cas suivants déterminer le PGCD des polynômes $A$ et $B$ et en déduire, s'il y en a, les zéros communs à $A$ et $B$.
1) $A = 2X^4 - 17X^3 + 31X^2 - 15X$ et $B = X^2 - 7X + 5$.
2) $A = X^5 + X^4 - 6X^3 - X^2 - X + 6$ et $B = X^4 + 2X^3 - X - 2$.

**Solution.** L'algorithme pour trouver le PGCD de deux polynômes est l'algorithme d'Euclide qui a été décrit dans le cours et correspond exactement à l'algorithme d'Euclide vu au lycée pour trouver le pgcd de deux entiers. Pour effectuer des divisions euclidiennes successives efficaces nous nous rappellerons la méthode décrite dans la solution de l'exercice précédent...

**1)** Faisons la division euclidienne de $A$ par $B$ en commençant par éliminer le plus haut degré dans $A$ avec $B$

$$\begin{aligned} A &= 2X^2(X^2 - 7X + 5) + 14X^3 - 10X^2 - 17X^3 + 31X^2 - 15X = 2X^2B - 3X^3 + 21X^2 - 15X \\ &= 2X^2B - 3X(X^2 - 7X + 5) - 21X^2 + 15X + 21X^2 - 15X = (2X^2 - 3X)B. \end{aligned}$$

Ainsi $B$ divise $A$ et donc $PGCD(A,B) = B$.

**2)** Faisons la division euclidienne de $A$ par $B$ en commençant par éliminer le plus haut degré dans $A$ avec $B$

$$\begin{aligned} A &= X(X^4 + 2X^3 - X - 2) - 2X^4 + X^2 + 2X + X^4 - 6X^3 - X^2 - X + 6 = XB - X^4 - 6X^3 + X + 6 \\ &= XB - (X^4 + 2X^3 - X - 2) - 4X^3 + 4. \end{aligned}$$

Comme $\deg(-4X^3 + 4) < \deg(B)$ nous venons de faire la division euclidienne de $A$ par $B$. Nous enchaînons alors avec celle de $B$ par $R_1 = -4X^3 + 4$.

$$B = -\frac{1}{4}X(-4X^3 + 4) + X + 2X^3 - X - 2 = -\frac{1}{4}XR_1 + 2X^3 - 2 = -\frac{1}{4}XR_1 - \frac{1}{2}R_1 = \left(-\frac{1}{4}X - \frac{1}{2}\right)R_1.$$

Le reste de cette division euclidienne étant nul nous trouvons donc que $R_1$ est associé au pgcd de $A$ et $B$ qui est unitaire. Ainsi $PGCD(A,B) = \frac{1}{\text{coef dominant de } R_1} R_1 = X^3 - 1$.

## Exercice 11 : *Divisibilité abstraite*

Les deux questions sont indépendantes mais porte chacune sur un problème de divisibilité moins concret que les exemples explicites ci-dessus.

1) Soient $p$ et $q$ deux entiers positifs tels que $p|q$. Montrer que $X^p - 1|X^q - 1$.

2) Prenons $P$ un polynôme de $\mathbb{R}[X]$. Montrer que

$$P(X) - X|P(P(X) - P(X).$$

**Solution.** Dans des questions générales sur les polynômes nous n'avons pas énormément de choix possibles pour démarrer. Soit nous parlons degré et racines (voir polynômes dérivés si les racines sont multiples), soit nous écrivons $P = \sum_{k=0}^{d} a_k X^k$ et nous regardons ce que l'on obtient.

**1)** On nous donne deux entiers positifs tels que $p|q$. Cela signifie que

$$\exists k \in \mathbb{N}, \quad q = pk.$$

Remplaçons donc $q$ pour faire apparaître $p$ dans notre polynôme $X^q - 1$.

$$X^q - 1 = X^{pk} - 1 = (X^p)^k - 1$$

Nous voyons donc des termes de la forme $a^k - b^k$ là où nous voudrions voir apparaître $a - b$. Nous savons que cela est possible car

$$\forall k \in \mathbb{N}^*, \quad a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right) = (a-b)\sum_{l=0}^{k-1} a^l b^{k-1-l}.$$

Ainsi

$$X^q - 1 = (X^p - 1)\left(\sum_{l=0}^{k-1} (X^p)^l\, 1^{k-1-l}\right) = (X^p - 1)\left(\sum_{l=0}^{k-1} (X^p)^l\right).$$

Comme $\sum_{l=0}^{k-1} (X^p)^l$ est un polynôme nous avons donc bien $X^p - 1|X^q - 1$.

**2)** Ici on nous parle d'un polynôme $P$ général donc nous ne pouvons pas faire grand chose à part écrire que $P = \sum_{k=0}^{d} a_k X^k$. Regardons alors $P(P(X)) - P(X)$ et essayons d'y faire apparaître $P(X) - X$...

$$P(P(X)) - P(X) = \sum_{k=0}^{d} a_k (P(X))^k - \sum_{k=0}^{d} a_k X^k = \sum_{k=0}^{d} a_k \left[(P(X))^k - X^k\right]$$

Nous voyons donc des termes de la forme $a^k - b^k$ là où nous voudrions voir apparaître $a - b$. Nous savons que cela est possible car

$$\forall k \in \mathbb{N}^*, \quad a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right) = (a-b)\sum_{l=0}^{k-1} a^l b^{k-1-l}.$$

Comme ici

$$\sum_{k=0}^{d} a_k \left[(P(X))^k - X^k\right] = \sum_{k=1}^{d} a_k \left[(P(X))^k - X^k\right]$$

nous pouvons bien utiliser la formule et obtenir

$$P(P(X)) - P(X) = \sum_{k=0}^{d} a_k (P(X) - X)\left(\sum_{l=0}^{k-1} P(X)^l X^{k-1-l}\right) = (P(X) - X)\left[\sum_{k=0}^{d} a_k \left(\sum_{l=0}^{k-1} P(X)^l X^{k-1-l}\right)\right].$$

Comme $\sum_{k=0}^{d} a_k \left(\sum_{l=0}^{k-1} P(X)^l X^{k-1-l}\right)$ est bien un polynôme de $\mathbb{K}[X]$ il vient bien que $P(X) - X$ divise $P(P(X)) - P(X)$.