MPSI

Mathématiques
Devoir surveillé 07

Samedi 9 mars – 8h-12h

- Durée : 4 heures.
- Le sujet est constitué d'un seul problème. Les parties A et B sont **communes aux deux classes**. La partie C est **réservée aux MPSI1**, les parties D et E sont **réservées aux MPSI2.**
- Toute calculatrice ou appareil électronique est interdit.
- La présentation et le soin apporté aux réponses seront pris en compte dans la notation. **Encadrez, soulignez vos résultats** et **numérotez vos pages**.
- Lorsque vous utilisez le résultat d'une question précédente, **donnez le numéro de la question utilisée.**
- À tout moment, vous pouvez admettre le résultat d'une question pour pouvoir continuer : il suffit de le préciser clairement sur la copie.
- Si vous voyez ce qui semble être une erreur d'énoncé, indiquez-le sur la copie.
- Laissez de la place dans une marge à gauche pour pouvoir noter plus facilement le devoir.
- Une réponse fausse, si elle ne laisse pas paraître de calculs intermédiaires, compte 0 points ; avec calculs intermédiaires elle peut rapporter quelques points.

♫ Bon courage ! ♫

Racines carrées

Ce problème permet d'aborder divers avatars de la notion de racine carrée. Les parties sont largement indépendantes. Dans tout ce problème, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.
La partie A. est centrée sur des considérations d'analyse, et notamment d'analyse asymptotique.
La partie B., quant à elle, s'intéresse aux polynômes qui sont des carrés d'autres polynômes, en utilisant un point de vue analytique, puis un point de vue arithmétique. On notera que la question 10. sera à utiliser dans les autres parties.
Ensuite, des parties d'algèbre linéaire font le lien entre polynômes et algèbre, de deux manières différentes :

- la partie C., réservée aux MPSI1, s'intéresse à la possibilité d'écrire une matrice comme un carré d'une autre matrice.
- réservées aux MPSI2, les parties D. et E. permettent de déterminer l'éventuelle existence d'une racine carrée d'un endomorphisme et, en particulier, de l'endomorphisme de dérivation.

A. Un peu d'analyse

A-I. Questions préliminaires

Soit f une fonction définie sur un intervalle I contenant 0, $n \in \mathbb{N}$. On suppose que f admet un développement limité à l'ordre n, et, plus précisément, que $f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + o(x^n)$.

1. $\boxed{\text{COURS}}$ Soit P un polynôme à coefficients dans $\mathbb{K}$. Donner les coefficients de P^2.

2. Démontrer que $f(x)^2 \underset{x\to 0}{=} \sum_{k=0}^{n} b_k x^k + o(x^n)$, où l'on précisera l'expression de b_k pour tout k.

3. $\boxed{\text{COURS}}$ Donner le développement limité à l'ordre n de $\sqrt{1+h}$ au voisinage de 0. On laissera les coefficients sous forme d'un produit.

> **Correction.** On sait que $\sqrt{1+h} \underset{h\to 0}{=} \sum_{k=0}^{n} \frac{\prod_{i=0}^{k-1}\left(\frac{1}{2}-i\right)}{k!} h^k + o(h^n)$.

A-II. Étude d'une fonction

On note I l'intervalle $\left]-\infty, \frac{1}{4}\right[$. On veut dans cette partie déterminer toutes les fonctions $f : \mathrm{I} \to \mathbb{R}$ continues sur I vérifiant la relation

$$\forall x \in \mathrm{I} \quad x f^2(x) - f(x) + 1 = 0 \quad (\star)$$

4. Préciser $f(0)$ pour une telle fonction. et montrer qu'il existe une fonction $\epsilon : \mathrm{I}\backslash\{0\} \to \{-1, 1\}$ vérifiant $\forall x \in \mathrm{I}\backslash\{0\} \quad f(x) = \dfrac{1+\epsilon(x)\sqrt{1-4x}}{2x}$

Correction. Si f est une telle fonction, en évaluant en 0 dans $(\star)$, on obtient $f(0) = 1$. De plus, pour x dans $\mathrm{I}\backslash\{0\}$ fixé, $f(x)$ est solution d'une équation du second degré, de discriminant égal à $\boxed{1-4x>0}$, d'où

$$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x} = \frac{1+\epsilon(x)\sqrt{1-4x}}{2},$$

où $\epsilon(x) = 1$ ou -1.

On note, pour tout x dans $\mathrm{I}\backslash\{0\}$, $g(x) = \dfrac{1-\sqrt{1-4x}}{2x}$.

5. Démontrer que g est prolongeable par continuité en 0. Donner la valeur de son prolongement par continuité en 0, et démontrer la dérivabilité de ce prolongement par continuité. On notera également g la fonction ainsi prolongée.

Correction. On lit la question et on sait, par avance, que l'on devra obtenir un développement limité de g à l'ordre 1 : vu que l'on divise par x, on va faire un dl de $\sqrt{1-4x}$ à l'ordre 2

$$\sqrt{1-4x} \underset{x\to 0}{=} 1-2x-\frac{1}{8}(-4x)^2+o(x) \underset{x\to 0}{=} 1-2x-2x^2+o(x^2)$$

Ainsi,

$$\begin{aligned} g(x) &\underset{x\to 0}{=} \frac{1-(1-2x-2x^2+o(x^2))}{x} \\ &\boxed{\underset{x\to 0}{=} 1+x+o(x).} \end{aligned}$$

Ainsi, g est prolongeable par continuité en 0, en posant $\boxed{g(0)=1}$. Ce prolongement est dérivable (car g admet un développement limité à l'ordre 1 en 0), et $\boxed{g'(0)=1}$.

6. Montrer que ϵ est continue, prolongeable par continuité sur I tout entier, et en déduire finalement $f = g$.

Correction. On sait que pour tout x dans $\mathrm{I}\backslash\{0\}$,

$$\epsilon(x) = \frac{2xf(x)-1}{\sqrt{1-4x}}$$

Cette fonction est continue sur $\mathrm{I}\backslash\{0\}$ et admet une limite finie en 0, égale à -1. La fonction ϵ est donc prolongeable par continuité en 0
Mais alors ϵ est **continue**, **à valeurs dans** $\{-1,1\}$, donc ϵ est constante : si ce n'était pas le cas, on disposerait de deux réels $x \neq y$ dans I vérifiant $\epsilon(x) = 1$ et $\epsilon(y) = -1$ donc, par continuité de ϵ et par le théorème des valeurs intermédiaires, on disposerait d'un réel z de I vérifiant $\epsilon(z) = 0$, absurde.

Donc ϵ est constante, égale à sa limite en 0, c'est-à-dire égale à -1.
Donc pour tout x dans I, $f(x) = \dfrac{1-\sqrt{1-4x}}{2x} = g(x)$, d'où le résultat désiré.

7. Démontrer que g admet un développement limité à tout ordre en 0 et que, si $n \in \mathbb{N}$,

$$g(x) \underset{x\to 0}{=} c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + o(x^n),$$

où, pour tout k dans $[\![0, n]\!]$ $c_k = \dfrac{1}{k+1}\dbinom{2k}{k}$.

Correction. On calcule déjà le développement limité en 0 de $\sqrt{1-4x}$ à l'ordre $n+1$:

$$\begin{aligned}\sqrt{1-4x} &\underset{x\to 0}{=} 1 + \sum_{k=1}^{n+1} \frac{1}{k!} \prod_{i=0}^{k-1} \left(\frac{1}{2} - i\right)(-4x)^k + o(x^{n+1}) \\ &\underset{x\to 0}{=} 1 + \sum_{k=1}^{n} \frac{1}{k!} \prod_{i=0}^{k-1} \frac{1-2i}{2}(-4x)^k + o(x^n)\end{aligned}$$

Or,

$$\begin{aligned}\prod_{i=0}^{k-1} \frac{1-2i}{2} &= (-1)^k \frac{1}{2^k} \prod_{i=0}^{k-1}(2i-1) \\ &= (-1)^k \frac{1}{2^k}(-1) \times 1 \times 3 \times 5 \times \cdots \times (2(k-1)-1) \\ &= -(-1)^k \frac{1}{2^k} \frac{(2k-2)!}{2 \times 4 \times \cdots \times (2k-2)} \\ &= -(-1)^k \frac{1}{2^k} \frac{(2k-2)!}{2^k(k-1)!} \\ &= -(-1)^k \frac{1}{4^k} \frac{(2k-2)!}{(k-10!}\end{aligned}$$

Donc

$$\begin{aligned}\sqrt{1-4x} &\underset{x\to 0}{=} 1 - \sum_{k=1}^{n+1} \frac{1}{k!}(-1)^k \frac{1}{4^k} \frac{(2k-2)!}{(k-1)!}(-4x)^k + o(x^{n+1}) \\ &\underset{x\to 0}{=} 1 - \sum_{k=1}^{n+1} \frac{1}{k!} \frac{(2k-2)!}{(k-1)!} x^k + o(x^{n+1}) \\ &\underset{x\to 0}{=} 1 - \sum_{k=1}^{n+1} \frac{1}{k} \binom{2k-2}{k-1} x^k + o(x^{n+1}).\end{aligned}$$

Ainsi,

$$\begin{aligned} g(x) &\underset{x\to 0}{=} \frac{1-\left(1-\sum_{k=1}^{n+1}\frac{1}{k}\binom{2k-2}{k-1}x^k+o(x^{n+1})\right)}{x} \\ &\underset{x\to 0}{=} \sum_{k=1}^{n+1}\frac{1}{k}\binom{2k-2}{k-1}x^{k-1}+o(x^n) \\ &\boxed{\underset{x\to 0}{=} \sum_{k=0}^{n}\frac{1}{k+1}\binom{2k}{k}x^k+o(x^n)} \end{aligned}$$

B. Racines carrées de polynômes

B-I. Valuation d'un polynôme

Si $P = \sum_{k=0}^{d} a_k X^k$ est un polynôme dans $\mathbb{C}[X]$, on définit la valuation de P, notée $\mathrm{val}(P)$, comme

$$\mathrm{val}(P) = \min\{k \in [\![0, d]\!],\ a_k \neq 0\}.$$

Par convention, on dit que $\mathrm{val}(0_{\mathbb{C}[X]}) = +\infty$. Soient P et Q deux polynômes.

8. Si on note $p = \mathrm{val}(P)$, démontrer que $P(x) \underset{x\to 0}{\sim} a_p x^p$. En déduire que, pour n dans $\mathbb{N}$, $P(x) \underset{x\to 0}{=} o(x^n)$ si, et seulement si X^{n+1} divise P.

Correction. Comme $p = \mathrm{val}(P)$, on peut écrire $P(X) = \sum_{k=p}^{d} a_k X^k$. Ainsi, comme $a_p \neq 0$ et comme $\boxed{\sum_{k=p+1}^{d} a_k x^k \underset{x\to 0}{=} o(x^p)}$, on en déduit que $\boxed{\mathrm{P(x)} \underset{x\to 0}{\sim} a_p x^p}$.

Ainsi, $P(x) \underset{x\to 0}{=} o(x^n)$ si et seulement si $x^p \underset{x\to 0}{=} o(x^n)$, donc si et seulement si $p > n$, i.e. si et seulement si $\mathrm{val}(P) \geqslant n+1$. Ceci est équivalent au fait que X^{n+1} divise P.

9. Soient P et Q deux polynômes non nuls. Donner, en le démontrant, un lien entre $\mathrm{val}(P+Q)$, $\mathrm{val}(P)$ et $\mathrm{val}(Q)$. Faire de même pour $\mathrm{val}(PQ)$.

Correction. On a les formules $\mathrm{val}(P+Q) \geqslant \min(\mathrm{val}(P), \mathrm{val}(Q))$ et $\mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q)$. En effet, on a l'équivalence

$$p = \mathrm{val}(P) \Leftrightarrow 0 \text{ est de multiplicité } p \text{ dans } P.$$

Ainsi, si on note $p = \mathrm{val}(P)$, $q = \mathrm{val}(Q)$ et $m = \min(p, q)$, alors X^m divise P et Q donc X^m divise $P+Q$. Donc la multiplicité de 0 dans $P+Q$ est supérieure ou égale à

m, c'est-à-dire que $\boxed{\mathrm{val}(P+Q) \geqslant m = \min(p,q)}$. De même, 0 est de multiplicité $p+q$ dans $P \times Q$ donc $\boxed{\mathrm{val}(PQ) = p+q = \mathrm{val}(P) + \mathrm{val}(Q)}$.

Application. On note $(s_k)_{k\in\mathbb{N}}$ la suite des coefficients du développement limité de $\sqrt{1+x}$ en 0. Soit $n \in \mathbb{N}$ et $S_n(X) = \sum_{k=0}^{n} s_k X^k$.

10. Démontrer qu'il existe un polynôme R de $\mathbb{R}[X]$ tel que $1+X = S_n(X)^2 + X^{n+1}R(X)$.
On pourra utiliser la question 8.

Correction. Par définition du développement limité à l'ordre n, on sait que $\sqrt{1+h} \underset{h\to 0}{=} S_n(h) + o(h^n)$.
On en déduit que $1+h \underset{h\to 0}{=} S_n(h)^2 + o(h^n)$ (développement limité d'un produit). (Remarque : en fait, on pourrait même garder la troncature à l'ordre n de $S_n(h)$.)
Mais alors si $P = 1+X-S_n$, on vient de démontrer que $P(h) \underset{h\to 0}{=} o(h^n)$, donc X^{n+1} divise $1+X-S_n(X)^2$. D'où le résultat désiré.

B-II. Détermination pratique de la racine d'un polynôme

Soit P un polynôme **à coefficients réels**, ne s'annulant pas en 0. On veut démontrer que P est un carré si et seulement si les trois propositions suivantes sont simultanément vérifiées :

(a) son degré d est pair,

(b) $P(0) > 0$,

(c) il existe un polynôme $\boxed{Q \in \mathbb{R}_{d/2}[X]}$ vérifiant $\sqrt{P(h)} \underset{h\to 0}{=} Q(h) + o(h^d)$.

Dans ce cas on aura $Q^2 = P$.

11. Démontrer que si P est le carré d'un autre polynôme, alors les propositions (a),(b),(c) sont vraies.

Correction. On suppose qu'il existe Q vérifiant $P = Q^2$. Alors

- $\deg(P)$ est pair, égal à $2\deg(Q)$,
- $P(0) = Q(0)^2 > 0$,
- $Q(0) \neq 0$ et, quitte à multiplier par -1, on peut supposer $Q(0) > 0$. Mais alors

$$Q(x) \underset{x\to 0}{\longrightarrow} Q(0) > 0,$$

donc, au voisinage de 0, $Q(x) > 0$. Ainsi, au voisinage de 0,

$$\sqrt{P(x)} = \sqrt{Q(x)^2} = Q(x) \underset{x\to 0}{=} Q(x) + o(x^d),$$

car $\deg(Q) < d$.

[Remplacer simplement par « démontrer la réciproque] On suppose désormais que les propositions (a), (b), (c) sont vraies. On écrit $d = 2n$ et

$$P(X) = \alpha^2 + a_1 X + \cdots + a_{2n} X^{2n},\ \text{où } \alpha \in \mathbb{R}_+^*.$$

12. Vérifier que $P(x) > 0$ au voisinage de 0 et démontrer qu'il existe un polynôme Q (que l'on ne cherchera pas à exprimer) de degré n vérifiant

$$\sqrt{P(h)} \underset{h\to 0}{=} Q(h) + o(h^n)$$

> **Correction.** On sait que $P(x) \underset{x\to 0}{\longrightarrow} P(0) = \alpha^2 > 0$, donc P est positif au voisinage de 0. Ainsi,
> $$\sqrt{P(x)} = \alpha\sqrt{1 + \frac{a_1}{\alpha}x + \cdots + \frac{a_{2n}}{\alpha}x^n} \underset{x\to 0}{=} \alpha(1 + R(x) + o(x^n)),$$
> où R est un polynômde de degré n, qui est la partie régulière du développement limité de $\sqrt{1 + \frac{a_1}{\alpha}x + \cdots + \frac{a_{2n}}{\alpha}x^n}$ en 0. Ainsi, en posant $\boxed{Q = \alpha(1 + R)}$, on a le résultat.

13. Démontrer que si $\sqrt{P(h)} \underset{h\to 0}{=} Q(h) + o(h^d)$, alors $Q^2 = P$. *On pourra utiliser la question 8..*

> **Correction.** Si $\sqrt{P(h)} \underset{h\to 0}{=} Q(h) + o(h^d)$, alors $P(h) \underset{h\to 0}{=} Q(h)^2 + o(h^d)$, donc, par la question 8., X^{d+1} divise $P - Q^2$. Or, $\deg(P - Q^2) \leqslant d$, donc $P - Q^2 = 0_{\mathbb{R}[X]}$, ce qui permet d'écrire que $\boxed{P = Q^2}$.

14. Dans le cas où $P(0) = 0$, énoncer une condition nécessaire et suffisante pour que P soit un carré, similaire aux conditions (a), (b), (c). On ne demande pas de la démontrer. *Cette CNS fera intervenir la notion de valuation.*

> **Correction.** Une CNS peut être la suivante
> (a) P est de degré d pair et de valuation p paire,
> (b) le terme devant le coefficient de degré p de P est strictement positif,
> (c) il existe un polynôme Q de degré $n = p/2$ vérifiant $\sqrt{P(h)} \underset{h\to 0}{=} Q(h) + o(h^d)$.
>
> On prouverait cette proposition de la même manière, en écrivant juste $P = X^p R$ et en appliquant les questions précédentes à R.

B-III. Factorisation en puissances croissantes

15. Démontrer qu'un polynôme $P \in \mathbb{C}[X]$ est scindé à racines simples si et seulement si $P \wedge P' = 1$.

> **Correction.** P est scindé à racines simples si et seulement si P et P' n'ont pas de racine en commun (une racine de P est multiple si elle est aussi racine de P'), c'est-à-dire, étant donnée la décomposition en produit d'irréductibles, si et seulement si $P \wedge P' = 1$.

16. Déterminer une condition nécessaire et suffisante sur $P \in \mathbb{C}[X]$ pour qu'il existe un entier $k \geqslant 1$ tel que P divise $(P')^k$.

Correction. **Condition nécessaire.** Supposons qu'il existe $k \geqslant 1$ tel que P divise $(P')^k$. Alors les racines de P sont toutes racines de P'. Ceci signifie que toutes les racines de P sont multiples.
Condition suffisante. Supposons que toutes les racines de P soient multiples. Alors on $P = K.\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$, avec $(\alpha_1, \dots, \alpha_r)$ deux à deux distincts, et $(m_1, \dots, m_r)$ r entiers supérieurs où égaux à 2. Ainsi, si $m = \max(m_1, \dots, m_r)$, comme $(\alpha_1, \dots, \alpha_r)$ sont racines de P', elles sont racines de $(P')^m$ de multiplicité au moins m. Donc P divise $(P')^m$.
La CNS rechercée est donc « P est à racines toutes multiples ».

On veut démontrer que tout polynôme unitaire admet une unique factorisation en puissances croissantes, c'est-à-dire que pour tout polynôme unitaire P, il existe un unique entier s, un unique s-uplet de polynômes $(P_1, \dots, P_s)$, unitaires, tous à racines simples, premiers entre eux deux à deux, tels que

$$P = P_1 P_2^2 P_3^3 \dots P_s^s, \text{ et } P_s \neq 1.$$

Par exemple, si $P(X) = X^4(X-1)(X-\pi)^2(X-2)(X-5)^4$, alors on posera $P_1 = (X-1)(X-2)$, $P_2 = (X-\pi)$, $P_3 = 1$ et $P_4 = X(X-5)$. On aura bien $P = P_1 P_2^2 P_3^3 P_4^4$, et (P_1, P_2, P_3, P_4) premiers entre eux deux à deux.

17. Démontrer que tout polynôme unitaire de $\mathbb{C}[X]$ admet une factorisation en puissances croissantes. On en admet l'unicité.
Si la décomposition de P en puissances croissantes est $P = P_1 P_2^2 \dots P_s^s$, exprimer $P_1 \dots P_s$ à l'aide des racines de P.

Correction. Soit $P \in \mathbb{C}[X]$, unitaire. Alors, comme P est scindé, on écrit

$$P(X) = \prod_{k=1}^{r}(X-\alpha_k)^{m_k},$$

où $\alpha_1, \dots, \alpha_r$ sont deux à deux distincts et $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$. On note alors $s = \max(m_1, \dots, m_r)$ la plus grande des multiplicités, et on pose, pour $i \in [\![1, s]\!]$

$$\boxed{P_i = \prod_{\substack{1 \leqslant k \leqslant r \\ m_k = i}} (X-\alpha_k)}$$

Ainsi, P_i est le produit des facteurs irréductibles $(X-\alpha)$ où α est racine de multiplicité i dans P. On a alors directement

$$P_i^i = \prod_{\substack{1 \leqslant k \leqslant r \\ m_k = i}} (X-\alpha_k)^i == \prod_{\substack{1 \leqslant k \leqslant r \\ m_k = i}} (X-\alpha_k)^{m_k},$$

et donc

$$P = P_1 P_2^2 \dots P_s^s.$$

En particulier,

$$\boxed{P_1 \dots P_s = \prod_{k=1}^{r}(X - \alpha_k).}$$

Obtenir cette factorisation semble nécessiter de connaître la décomposition de P en produit de polynômes irréductibles, question difficile à résoudre. Nous allons proposer un algorithme, basé sur un calcul de pgcd, permettant de déterminer la factorisation de P en puissances croissantes.

On part de P un polynôme unitaire, $P_1 P_2^2 P_3^3 \dots P_s^s$ sa factorisation en puissances croissantes.

18. Démontrer que le pgcd D de P et P' est $D = P_2 P_3^2 \dots P_s^{s-1}$. On note Q le polynôme vérifiant $P = DQ$.

Correction. Comme $P = P_1 P_2^2 \dots P_s^s$, on en déduit que

$$\begin{aligned} P' &= \sum_{i=1}^{s} i P_i' P_i^{i-1} \prod_{\substack{1 \leqslant j \leqslant s \\ j \neq i}} P_j^j \\ &= (P_1^{1-1} P_2^{2-1} \dots P_s^{s-1}) \left(\sum_{i=1}^{s} i P_i' \prod_{\substack{1 \leqslant j \leqslant s \\ j \neq i}} P_j \right) \\ &= D \times R, \end{aligned}$$

en posant $D = P_2 P_3^2 \dots P_s^{s-1}$ et $S = \sum_{i=1}^{s} i P_i' \prod_{\substack{1 \leqslant j \leqslant s \\ j \neq i}} P_j$.

Or, si α est une racine de P, on dispose de i tel que α est racine de P_i, alors $S(\alpha) = i P_i'(\alpha) \prod_{j \neq i} P_j(\alpha) \neq 0$. Ainsi, R n'a aucune racine en commun avec P. On en déduit donc que $\boxed{P \wedge P' = D}$.

19. Démontrer qu'alors P_1 est le quotient de Q par $D \wedge Q$.

Correction. On a alors $Q = P_1 \dots P_s$ et, comme $P_1, \dots, P_s$ sont premiers entre eux deux à deux, $D \wedge Q = P_2 \dots P_s$.
Ainsi, P_1 est bien le quotient de Q par $D \wedge Q$!

20. Comment déterminer ensuite P_2, P_3, etc. ? En quoi cette factorisation peut permettre une méthode effective (algorithmique) permettant de déterminer si un polynôme est un carré ?

Correction. On refait le même algorithme sur $Q = P_2 P_3^2 \dots P_s^{s-1}$ pour déterminer P_2, puis on peut itérer de la sorte.

On obtient donc tous les polynômes $P_1, \dots, P_s$. Alors

$$P = P_1 P_2^2 \dots P_s^s.$$

Si pour tout i impair, on a $P_i = 1$, cela signifie que P est un produit de polynômes à des puissances paires, donc P est un carré.
L'algorithme que l'on vient de présenter est effectif, car calculer un pgcd peut se faire via l'algorithme d'Euclide, qui n'a besoin que de divisions euclidiennes, divisions que l'on peut faire en connaissant simplement les coefficient des polynômes.

C. (MPSI1) Racines carrées de matrices

Si $P(X) = \sum_{k=0}^{d} a_k X^k$ est un polynôme, si M est une matrice carrée de taille n, on note $P(M)$ la matrice $\sum_{k=0}^{d} a_k M^k$. On rappelle que $M^0 = \mathrm{I}_n$.

Le but de cette partie est de savoir, étant donnée une matrice M, s'il existe une matrice N vérifiant $N^2 = M$; une question supplémentaire sera de savoir si, de plus, N peut être exprimée comme un polynôme en M.

C-I. Quelques manipulations

On considère la matrice $M = \begin{pmatrix} 3 & 1 \\ -4 & -1 \end{pmatrix}$, et le polynôme $P(X) = \frac{1}{2}X + \frac{1}{2}$

21. Calculer $P(M)$ et vérifier que $P(M)^2 = M$.

Correction. On calcule

$$P(M) = \frac{1}{2}M + \frac{1}{2}\mathrm{I}_2 = \begin{pmatrix} 2 & 1/2 \\ -2 & 0 \end{pmatrix}.$$

Ainsi, on a

$$P(M)^2 = \begin{pmatrix} 2 & 1/2 \\ -2 & 0 \end{pmatrix}^2 = \begin{pmatrix} 3 & 1 \\ -4 & -1 \end{pmatrix}$$

C-II. Cas d'une matrice diagonalisable

Soit $M \in \mathscr{M}_n(\mathbb{C})$. On suppose qu'il existe une matrice inversible B et une matrice diagonale D à coefficients deux à deux distincts vérifiant $M = BDB^{-1}$. On note

$$D = \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix}, \text{ où } (\lambda_1, \dots, \lambda_n) \text{ sont deux à deux distincts.}$$

22. Démontrer que pour tout polynôme P,

$$P(M) = B \begin{pmatrix} P(\lambda_1) & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n) \end{pmatrix} B^{-1}$$

Correction. Soit P dans $\mathbb{C}[X]$, $P(X) = \sum_{k=0}^{d} a_k X^k$. Alors

$$\begin{aligned} P(M) &= \sum_{k=0}^{d} a_k M^k \\ &= \sum_{k=0}^{d} a_k (BDB^{-1})^k \\ &= \sum_{k=0}^{d} a_k B D^k P^{-1}, \end{aligned}$$

d'où le résultat désiré.

On note, pour tout i dans $[\![1, n]\!]$, δ_i une racine carrée de λ_i.

23. $\boxed{\text{COURS}}$ Donner l'unique polynôme P de $\mathbb{C}[X]$ de degré inférieur ou égal à $n-1$ vérifiant, pour tout i dans $[\![1, n]\!]$, $P(\lambda_i) = \delta_i$. Déterminer (en refaisant la preuve) l'ensemble

$$\{Q \in \mathbb{C}[X],\ \forall i \in [\![1, n]\!],\ Q(\lambda_i) = \delta_i\}.$$

Correction. Soit $(L_0, \dots, L_n)$ la base d'interpolation de Lagrange associée à $(\lambda_1, \dots, \lambda_n)$. Alors si $P = \sum_{k=0}^{n} \delta_k L_k$, P est de degré inférieur ou égal à n et vérifie, pour tout k, $P(\lambda_k) = \delta_k$.
Soit ensuite $Q \in \mathbb{C}[X]$. Alors on a les équivalences

$$\begin{aligned} (\forall i \in [\![1, n]\!],\ Q(\lambda_i) = \delta_i) &\Leftrightarrow (\forall i \in [\![1, n]\!],\ Q(\lambda_i) = P(\lambda_i)) \\ &\Leftrightarrow (\forall i \in [\![1, n]\!],\ (Q-P)(\lambda_i) = 0) \\ &\Leftrightarrow (\lambda_1, \dots, \lambda_n) \text{ sont racines de } Q-P \\ &\Leftrightarrow \prod_{k=1}^{n} (X - \lambda_k) \text{ divise } Q-P \text{ (car } (\lambda_1, \dots, \lambda_n) \text{ sont 2 à 2 distinctes.} \\ &\Leftrightarrow \exists A \in \mathbb{C}[X],\ Q - P = A \times \prod_{k=1}^{n} (X - \lambda_k). \end{aligned}$$

L'ensemble recherché est donc

$$\boxed{\left\{ P + A \times \prod_{k=1}^{n} (X - \lambda_k),\ A \in \mathbb{C}[X] \right\}}$$

24. Démontrer qu'alors $P(M)^2 = M$.

Correction. On en déduit alors que

$$\begin{aligned}
P(M)^2 &= B \begin{pmatrix} P(\lambda_1) & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n) \end{pmatrix} B^{-1} \times B \begin{pmatrix} P(\lambda_1) & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n) \end{pmatrix} B^{-1} \\
&= B \begin{pmatrix} P(\lambda_1)^2 & & (0) \\ & \ddots & \\ (0) & & P(\lambda_n)^2 \end{pmatrix} B^{-1} \\
&= B \begin{pmatrix} \delta_1^2 & & (0) \\ & \ddots & \\ (0) & & \delta_n^2 \end{pmatrix} B^{-1} = B \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix} B^{-1} = M
\end{aligned}$$

25. Comment adapter le résultat précédent au cas où $(\lambda_1, \dots, \lambda_n)$ ne sont pas deux à deux distincts ?

Correction. Si $(\lambda_1, \dots, \lambda_n)$ ne sont pas deux à deux distincts, il faut que l'on choisisse, lorsque $\lambda_i = \lambda_j$, la **même** racine carrée, et de prendre le polynôme interpolateur associé aux racines distinctes et, avec, comme valeurs, les racines carrées ainsi choisies.

C-III. Un deuxième cas particulier

Dans cette partie, on suppose que $M = \mathrm{I}_n + A$, où A vérifie $A^p = 0_n$, avec $p \in \mathbb{N}^*$.

26. Démontrer qu'il existe $P \in \mathbb{C}[X]$ vérifiant $P(A)^2 = \mathrm{I}_n + A = M$, puis en déduire qu'il existe $Q \in \mathbb{C}[X]$ vérifiant $Q(M)^2 = M$. *On pourra utiliser la question 10.*

Correction. Par la question 10., on sait que l'on dispose de Q tel que $1+X = S_{p-1}(X)^2 + X^pQ(X)$. On en déduit alors que

$$\mathrm{I}_n + A = S_{p-1}(A)^2 + A^pQ(A) = S_{p-1}(A)^2 = S_{p-1}(M - \mathrm{I}_n)$$

En posant $\boxed{Q = S_{p-1}(X-1)}$, on obtient le résultat voulu.

27. À titre d'exemple, faire le lien entre la question précédente et l'exemple de la question 21.

Correction. Dans la question 21., on considère $M = \begin{pmatrix} 3 & 1 \\ -4 & -1 \end{pmatrix}$. Or, si $A = M - \mathrm{I}_2$, $A = \begin{pmatrix} 2 & 1 \\ -4 & -2 \end{pmatrix}$, et $\boxed{A^2 = 0_2}$.

Ainsi, on considère $S_1(X) = 1 + \frac{1}{2}X$, et $Q = S_1(X-1) = \frac{1}{2}X + \frac{1}{2}$.

On pose alors $N = Q(M) = \dfrac{1}{2}M + \dfrac{1}{2}\mathrm{I}_2 = \begin{pmatrix} 2 & 1/2 \\ -2 & 0 \end{pmatrix}$. Alors $Q(M)^2 = M$.

C-IV. Cas quelconque – un exemple

Nous allons, dans un cas particulier, chercher à résoudre le problème de la recherche d'une racine carrée dans un cas qui n'est pas traité par les parties précédentes. On considère

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

28. Calculer, pour k dans $\mathbb{N}^*$, A^k.

Correction. On calcule $A^2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ et on montre, par récurrence, que pour tout k, $\boxed{A^k = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4^k \end{pmatrix}}$.

29. Soit P un polynôme de $\mathbb{C}[X]$, Démontrer que

$$P(A) = \begin{pmatrix} P(1) & P'(1) & 0 \\ 0 & P(1) & 0 \\ 0 & 0 & P(4) \end{pmatrix}$$

Correction. On écrit $P(X) = \displaystyle\sum_{k=0}^{n} a_k X^k$. Ainsi,

$$
\begin{aligned}
P(A) &= \sum_{k=0}^{n} a_k A^k \\
&= \sum_{k=0}^{n} \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4^k \end{pmatrix} \\
&= \begin{pmatrix} \sum_{k=0}^{n} a_k & \sum_{k=0}^{n} k a_k & 0 \\ 0 & \sum_{k=0}^{n} a_k & 0 \\ 0 & 0 & \sum_{k=0}^{n} a_k 4^k \end{pmatrix} \\
&= \begin{pmatrix} P(1) & P'(1) & 0 \\ 0 & P(1) & 0 \\ 0 & 0 & P(4) \end{pmatrix}.
\end{aligned}
$$

30. Déterminer un polynôme P vérifiant $P(1) = 1$, $P'(1) = \frac{1}{2}$, $P(4) = 2$ et en déduire que $P(A)^2 = A$.

Correction. Comme $P(1) = 1$ et $P'(1) = \frac{1}{2}$, il est naturel, par la formule de Taylor, de chercher P sous la forme

$$P(X) = 1 + \frac{1}{2}(X-1) + c(X-1)^2$$

Mais comme on veut $P(4) = 2$, il faut

$$1 + \frac{3}{2} + 9c = 2,$$

c'est-à-dire $c = -\frac{1}{18}$. On pose donc

$$\boxed{P(X) = 1 + \frac{1}{2}(X-1) - \frac{1}{18}(X-1)^2.}$$

On en déduit alors que

$$\boxed{P(A) = \begin{pmatrix} 1 & 1/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ et donc } P(A)^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.}$$

D. (MPSI2) Racines carrées d'endomorphismes

Soit E un $\mathbb{C}$-espace vectoriel. Si $P(X) = \sum_{k=0}^{d} a_k X^k$, si φ est un endomorphisme de E, on note $P(\varphi)$ l'endomorphisme $\sum_{k=0}^{d} a_k \varphi^k$, où l'on a défini

$$\varphi^k = \underbrace{\varphi \circ \cdots \circ \varphi}_{k \text{ fois}}, \text{ et, par convention, } \varphi^0 = \mathrm{Id}_E.$$

La question que l'on se pose est la suivante : étant donné un endomorphisme φ de E, existe-t-il un endomorphisme ψ de E vérifiant $\psi^2 = \varphi$? Peut-on, de plus, imposer que ψ soit un polynôme en φ ?

D-I. Cas d'un endomorphisme diagonalisable

Soit $(e_1, \dots, e_n)$ une base de E, $(\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$, deux à deux distincts, φ un endomorphisme de E tel que pour tout i dans $[\![1, n]\!]$, $\varphi(e_i) = \lambda_i e_i$.

21. COURS Démontrer qu'un tel φ est unique.

Correction. Soit ψ un autre endomorphisme de E vérifiant, pour tout i dans $[\![1, n]\!]$, $\psi(e_i) = \lambda_i e_i$.
Alors φ et ψ coïncident sur une base, donc ils sont égaux.

22. Soit $i \in [\![1, n]\!]$. Démontrer que pour tout k dans $\mathbb{N}$, $\varphi^k(e_i) = \lambda_i^k e_i$ et que, si $P \in \mathbb{C}[X]$,

$$P(\varphi)(e_i) = P(\lambda_i) e_i.$$

Correction. Déjà, par récurrence, $\varphi^k(e_i) = \lambda_i^k e_i$ pour tous k et i. Notons ensuite $P(X) = \sum_{k=0}^{d} a_k X^k$. Alors

$$\begin{aligned} P(\varphi)(e_i) &= \sum_{k=0}^{d} a_k \varphi^k(e_i) \\ &= \sum_{k=0}^{d} a_k \lambda_i^k e_i \\ &\boxed{= P(\lambda_i) e_i.} \end{aligned}$$

On note, pour tout i, δ_i une racine carrée de λ_i.

23. COURS Donner l'unique polynôme P de $\mathbb{C}[X]$ de degré inférieur ou égal à $n-1$ vérifiant, pour tout i dans $[\![1, n]\!]$, $P(\lambda_i) = \delta_i$. Déterminer alors l'ensemble

$$\{Q \in \mathbb{C}[X],\ \forall i \in [\![1, n]\!],\ Q(\lambda_i) = \delta_i\}.$$

Correction. Soit $(L_0, \dots, L_n)$ la base d'interpolation de Lagrange associée à $(\lambda_1, \dots, \lambda_n)$. Alors si $P = \displaystyle\sum_{k=0}^{n} \delta_k L_k$, P est de degré inférieur ou égal à n et vérifie, pour tout k, $P(\lambda_k) = \delta_k$.
Soit ensuite $Q \in \mathbb{C}[X]$. Alors on a les équivalences

$$\begin{aligned}
(\forall i \in [\![1, n]\!],\ Q(\lambda_i) = \delta_i) &\Leftrightarrow (\forall i \in [\![1, n]\!],\ Q(\lambda_i) = P(\lambda_i)) \\
&\Leftrightarrow (\forall i \in [\![1, n]\!],\ (Q - P)(\lambda_i) = 0) \\
&\Leftrightarrow (\lambda_1, \dots, \lambda_n) \text{ sont racines de } Q - P \\
&\Leftrightarrow \prod_{k=1}^{n} (X - \lambda_k) \text{ divise } Q - P \text{ (car } (\lambda_1, \dots, \lambda_n) \text{ sont 2 à 2 distinctes.} \\
&\Leftrightarrow \exists A \in \mathbb{C}[X],\ Q - P = A \times \prod_{k=1}^{n} (X - \lambda_k).
\end{aligned}$$

L'ensemble recherché est donc

$$\boxed{\left\{ P + A \times \prod_{k=1}^{n} (X - \lambda_k),\ A \in \mathbb{C}[X] \right\}}$$

24. Démontrer qu'alors, si $\psi = P(\varphi)$, on a $\psi \circ \psi = \varphi$.

Correction. On pose $\psi = P(\varphi)$. Soit $i \in [\![1, n]\!]$. Alors

$$\psi(e_i) = P(\varphi)(e_i) = P(\lambda_i) e_i = \delta_i e_i.$$

Ainsi,

$$\psi^2(e_i) = \delta_i^2 e_i = \lambda_i e_i = \boxed{\varphi(e_i)}$$

$\boxed{\text{Les endomorphismes } \psi^2 \text{ et } \varphi \text{ coïncident sur une base, ils sont donc égaux.}}$

25. Comment adapter le résultat précédent au cas où $(\lambda_1, \dots, \lambda_n)$ ne sont pas deux à deux distincts ?

Correction. Si $(\lambda_1, \dots, \lambda_n)$ ne sont pas deux à deux distincts, il faut que l'on choisisse, lorsque $\lambda_i = \lambda_j$, la **même** racine carrée, et de prendre le polynôme interpolateur associé aux racines distinctes et, avec, comme valeurs, les racines carrées ainsi choisies.

26. À titre d'exemple, on considère E un $\mathbb{C}$-espace vectoriel, (e_1, e_2, e_3) une base de E, et φ la symétrie par rapport à $\mathrm{Vect}(e_1)$, parallèlement à $\mathrm{Vect}(e_2, e_3)$.
Déterminer un polynôme P tel que si $\psi = P(\varphi)$, alors $\psi \circ \psi = \varphi$ (on ne demande pas de forme développée).

Correction. Nous sommes dans le cadre de cette partie, car $\varphi(e_1) = -e_1$, $\varphi(e_2) = e_2$ et $\varphi(e_3) = e_3$. On a donc $\lambda_1 = -1$, $\lambda_2 = \lambda_3 = 1$. On prend donc $\delta_1 = i$, $\delta_2 = \delta_3 = 1$, et on considère P le polynôme de $\mathbb{C}_1[X]$ valant i en -1 et 1 en 1. On aura alors $P(\varphi)^2 = \varphi$.

D-II. Un deuxième cas particulier

On suppose que $\varphi = \mathrm{Id}_E + \psi$, où ψ vérifie $\psi^p = 0_{\mathscr{L}(E)}$, pour un certain $p \in \mathbb{N}^*$.

27. Démontrer qu'il existe un polynôme P tel que $P(\varphi)^2 = \varphi$.

Correction. Par la question 10., on sait que l'on dispose de Q tel que $1+X = S_{p-1}(X)^2 + X^p Q(X)$. On en déduit alors que

$$\mathrm{Id}_E + \psi = S_{p-1}(\psi)^2 + \psi^p Q(\psi) = S_{p-1}(\psi)^2 = S_{p-1}(\varphi - \mathrm{Id}_E)$$

En posant $\boxed{Q = S_{p-1}(X-1)}$, on obtient le résultat voulu.

E. (MPSI2) Racines carrées de la dérivation

28. On considère ici un espace vectoriel E admettant une base de cardinal n, et on considère u un endomorphisme nilpotent de E, c'est-à-dire qu'il existe un entier $k_0 \geqslant 1$ tel que $u^{k_0} = 0$. On appelle indice de nilpotence de u le plus petit entier k tel que $u^k = 0$.

(a) Montrer l'existence de l'indice de nilpotence. On le note p.

Correction. La partie $\{k \in \mathbb{N},\ u^k = 0_{\mathscr{L}(E)}\}$ est une partie de $\mathbb{N}$, non vide car k_0 appartient à cette partie, donc elle admet un plus petit élément.

(b) On veut montrer ici que p est inférieur ou égal à n. Pour cela, on considère un vecteur x appartenant à $E \setminus \ker(u^{p-1})$. Montrer que la famille $(x, u(x), \dots, u^{p-1}(x))$ est libre, puis conclure.

Correction.

- Déjà, montrons la liberté de la famille $(x, u(x), \dots, u^{p-1}(x))$: soit $(\lambda_0, \dots, \lambda_{p-1}) \in \mathbb{K}^p$ vérifiant

$$\sum_{k=0}^{p-1} \lambda_k u^k(x) = 0_E$$

On démontre alors par récurrence sur $k \in [\![0, p-1]\!]$ que $\lambda_k = 0$.
Initialisation. On compose l'égalité précédente par u^{p-1} pour obtenir

$$\sum_{i=0}^{p-1} \lambda_i u^{p+i-1}(x) = 0_E$$

Pour $i \geqslant 1$, $u^{p+i-1} = 0_{\mathscr{L}(E)}$, donc l'égalité devient $\lambda_0 u^{p-1}(x) = 0_E$. Comme $u^{p-1}(x) \neq 0_E$, on en déduit que $\boxed{\lambda_0 = 0}$.
Hérédité. Soit $k \in [\![1, p-1]\!]$ tel que $\lambda_0 = \cdots = \lambda_{k-1} = 0$. Alors

$$\sum_{i=k}^{p-1} \lambda_k u^i(x) = 0_E$$

On compose l'égalité précédente par u^{p-1-k} pour obtenir

$$\sum_{i=k}^{p-1} \lambda_k u^{i+p-1-k}(x) = 0_E$$

Mais pour $i \geqslant k+1$, $u^{i+p-1-k} = 0_{\mathscr{L}(E)}$, donc $\lambda_k u^{p-1}(x) = 0_E$. Comme $u^{p-1}(x) \neq 0_E$, on en déduit que $\boxed{\lambda_k = 0}$.
D'où l'hérédité et le résultat : $(\lambda_0, \dots, \lambda_{p-1}) = (0, \dots, 0)$ et la famille est libre.
- Ensuite, par le lemme technique de la fin du chapitre d'algèbre linéaire, comme $(x, \dots, u^{p-1}(x))$ est une famille de p vecteurs dans un espace engendré par n vecteurs, $\boxed{p \leqslant n}$ (sinon, la famille serait liée).

Pour tout entier naturel n non nul, on note $E_n = \mathbb{R}_n[X]$ et on note Δ l'endomorphisme de dérivation de E_n.
On cherche ici à montrer qu'il n'existe pas d'endomorphisme $u \in \mathcal{L}(E_n)$ vérifiant $u^2 = \Delta$ et on raisonne par l'absurde en supposant qu'il existe un tel endomorphisme u de E.

29. Vérifier que Δ est nilpotent et préciser son indice de nilpotence p. Vérifier également que u est nilpotent.

Correction.

- On sait que pour tout polynôme P de degré inférieur ou égal à n, $P^{(n+1)} = 0_{\mathbb{R}_n[X]}$, c'est-à-dire que $\Delta^{n+1}(P) = 0_{E_n}$. Donc Δ est nilpotent.
  De plus, $\Delta^n(X^n) = n!$ Donc $\Delta^n \neq 0_{\mathscr{L}(E_n)}$, donc $\boxed{\Delta \text{ est nilpotent d'indice } n+1.}$
- De même, $u^{2(n+1)} = \Delta^{n+1} = 0_{\mathscr{L}(E)}$ donc u est aussi nilpotent.

30. En déduire une contradiction dans le cas où n est impair.

Correction. Si n est impair, notons $m = \dfrac{n+1}{2}$. Alors

$$\boxed{\Delta^m = u^{2m} = u^{n+1} = 0_{\mathscr{L}(E_n)}}$$

car l'indice de nilpotence de u est inférieur ou égal à $n+1$. Ceci est absurde car $m < n+1$ et l'indice de nilpotence de Δ est $n+1$.

31. Démontrer le résultat annoncé quand n est pair.

Correction. Si n est pair, on note $m = \dfrac{n}{2}$. Alors

$$\boxed{\Delta^{m+1} = u^{2m+2} = u^{n+2} = 0_{\mathscr{L}(E_n)}.}$$

Donc, nécessairement, $m + 1 \geqslant n + 1$, donc $\dfrac{n}{2} \geqslant n$, absurde sauf si $n = 0$, ce qui est exclu.