Préparation à l'agrégation interne de mathématiques — Université Grenoble-Alpes
2020-2021

Écrit blanc d'algèbre

durée : 6h

Introduction

Dans ce problème, on s'intéresse aux sommes de carrés d'éléments dans un anneau commutatif. On voit en particulier des formules pour le produit de deux sommes de n carrés pour $n = 1$, 2, 4 et 8, et on démontre qu'il n'existe pas de formule analogue pour les autres valeurs de n, ce qui constitue un théorème établi par Hurwitz en 1898. La démonstration de ce résultat introduit des algèbres de matrices qui sont des corps, commutatifs et non commutatifs.

On appelle $\mathbb{R}$-algèbre tout $\mathbb{R}$-espace vectoriel $\mathbb{A}$ muni d'une opération interne, nommée multiplication ou produit, vérifiant les propriétés suivantes : cette multiplication est associative, possède un élément neutre noté 1_A ($\mathbb{A}$ est donc un anneau pour l'addition et le produit), et vérifie la propriété de distributivité :

$$\forall a \in \mathbb{A}, \forall b \in \mathbb{A}, \forall c \in \mathbb{A}, \quad a(b+c) = ab + ac, \quad (b+c)a = ba + ca$$

ainsi que :

$$\forall a \in \mathbb{A}, \forall b \in \mathbb{A}, \forall \lambda \in \mathbb{R}, \quad a(\lambda b) = (\lambda a)b = \lambda(ab).$$

Si cette multiplication est commutative, l'algèbre est dite commutative.

Dans ce problème, les $\mathbb{R}$-algèbres seront simplement appelées algèbres. *Lorsqu'on ne précise pas, la dimension d'une algèbre sera toujours sa dimension en tant que $\mathbb{R}$-espace vectoriel.*

Une sous-algèbre d'une algèbre $\mathbb{A}$ est un sous-ensemble de $\mathbb{A}$ qui est lui-même une algèbre (pour les mêmes opérations) et qui possède les mêmes éléments neutres que $\mathbb{A}$. Pour que $\mathbb{B}$ soit une sous-algèbre de $\mathbb{A}$, il suffit que ce soit un sous-espace vectoriel et un sous-anneau de $\mathbb{A}$.

On appelle morphisme d'algèbre entre deux algèbres $\mathbb{A}$ et $\mathbb{B}$, toute application linéaire f de $\mathbb{A}$ dans $\mathbb{B}$ qui est un morphisme d'anneau, c'est-à-dire qui vérifie :

$$\forall u \in \mathbb{A}, \ \forall a' \in \mathbb{A}, \ f(aa') = f(a)f(a') \text{ et } f(1_A) = 1_B.$$

Un morphisme d'algèbre qui est une bijection est appelé isomorphisme d'algèbre. On vérifie alors que son application réciproque est également un morphisme d'algèbre. On dira que deux algèbres sont isomorphes s'il existe un isomorphisme d'algèbre entre les deux.

Dans tout le problème, n désigne un entier strictement positif. Les ensembles $\mathcal{M}_n(\mathbb{R})$, resp. $\mathcal{M}_n(\mathbb{C})$, de matrices carrées à n lignes et n colonnes et à coefficients réels, resp. complexes, sont des algèbres pour les opérations habituelles. Leur élément neutre pour le produit est la matrice identité, notée I_n.

Si A est une matrice de $\mathcal{M}_n(\mathbb{C})$, on note $\overline{A}$ la matrice dont les coefficients sont les conjugués des coefficients de A.

Si E est un espaces vectoriel sur $\mathbb{R}$, resp. sur $\mathbb{C}$, l'ensemble $\mathrm{End}(E)$ des endomorphismes de E est une algèbre et pour toute base $\mathcal{B}$ de E, l'application qui à un endomorphisme de E lui associe sa matrice dans $\mathcal{B}$ est un isomorphisme d'algèbre de $\mathrm{End}(E)$ dans $\mathcal{M}_n(\mathbb{R})$, resp. $\mathcal{M}_n(\mathbb{C})$.

Une matrice réelle ou complexe est dite *scalaire* si elle est de la forme λI_n, où λ est réel ou complexe. Une matrice diagonale est une matrice dont tous les éléments non diagonaux sont nuls. Les ensembles de matrices scalaires et de matrices diagonales forment des sous-algèbres de $\mathcal{M}_n(\mathbb{R})$ et $\mathcal{M}_n(\mathbb{C})$.

Un anneau dans lequel tout élément non nul admet un inverse pour le produit s'appelle un *anneau à divisions*. On dit que c'est un *corps non commutatif* lorsqu'il n'est pas commutatif, c'est un corps s'il est commutatif.

La partie I étudie des sous-algèbres de $\mathcal{M}_n(\mathbb{R})$ et s'intéresse celles qui sont des anneaux à divisions. Cette partie est indépendante des parties suivantes. La partie II étudie des familles de symétries dans un espace vectoriel complexe. La partie III introduit l'algèbre des quaternions. Pour l'essentiel cette partie est indépendante de la partie II. Dans la partie IV, on établit le théorème de Hurwitz en utilisant les parties II et III. Dans la partie V, on démontre le théorème des quatre carrés en s'appuyant sur la partie III.

Remarque typographique : dans cet énoncé, la lettre i désigne le nombre complexe de carré -1 et ne doit pas être confondu avec la lettre i désignant un indice.

Partie I – Des algèbres de matrices réelles

Soit A une matrice non scalaire de $\mathcal{M}_2(\mathbb{R})$. Jusqu'à la question 5, on note $\mathbb{A}$ l'ensemble

$$\mathbb{A} = \{M \in \mathcal{M}_2(\mathbb{R}) \ / \ \exists (a,b) \in \mathbb{R}^2,\ M = aI_2 + bA\}$$

1. Montrer que $A^2 - \mathrm{tr}\,(A)A + \det(A)I_2 = 0$.
2. En déduire que $\mathbb{A}$ est une algèbre commutative de dimension deux, sous-algèbre de $\mathcal{M}_2(\mathbb{R})$.
3. (a) Montrer que $\mathbb{A}$ contient une matrice B telle que $B^2 = -I_2$ si, et seulement si, $(\mathrm{tr}\,A)^2 < 4\det A$.
   (b) Vérifier qu'alors I_2 et B forment une base de $\mathbb{A}$ et en déduire un isomorphisme d'algèbre entre A et le corps $\mathbb{C}$ des nombres complexes.
4. On suppose que A est non scalaire et vérifie $(\mathrm{tr}\,A)^2 = 4\det A$. Déterminer toutes les matrices M de $\mathbb{A}$ telles que $M^2 = 0$ et montrer que $\mathbb{A}$ n'est pas un corps.
5. On suppose que A est telle que $(\mathrm{tr}\,A)^2 > 4\det A$. Montrer que $\mathbb{A}$ est isomorphe à l'algèbre des matrices diagonales réelles. Est-ce que $\mathbb{A}$ est un corps ?

Soit maintenant $\mathbb{A}$ une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$. On s'intéresse à quelques cas où on peut affirmer que $\mathbb{A}$ est, ou n'est pas, un anneau à divisions.

6. (a) On suppose que $\mathbb{A}$ contient une matrice non scalaire A qui a une valeur propre réelle λ. Montrer que $\mathbb{A}$ ne peut pas être un anneau à divisions. *On utilisera une matrice bien choisie de* $\mathbb{A}$.

(b) En déduire que si $\mathbb{A}$ contient une matrice diagonalisable ou trigonalisable non scalaire, elle ne peut pas être un anneau à divisions.

(c) Montrer que si $\mathbb{A}$ est intègre, c'est-à-dire si :

$$\forall A \in \mathbb{A}, \forall B \in \mathbb{A},\ AB = 0 \ \Rightarrow\ A = 0 \text{ ou } B = 0\,,$$

alors $\mathbb{A}$ est un anneau à divisions. *On utilisera un morphisme bien choisi.*

Partie II – Symétries vectorielles complexes

Dans cette partie, on considère un espace vectoriel E de dimension finie $n \geqslant 1$ sur le corps $\mathbb{C}$ des nombres complexes.

Soient F et G deux sous-espaces supplémentaires de E (i.e. $E = F \oplus G$). On appelle symétrie (vectorielle) de E par rapport à F parallèlement à G l'endomorphisme s de E défini par :

$$\forall (x, y) \in F \times G,\ s(x + y) = x - y.$$

Pour tout endomorphisme u de E, on pose $F_u = \operatorname{Ker}(u - \mathrm{id}_E)$ et $G_u = \operatorname{Ker}(u + \mathrm{id}_E)$.

• Symétries et involutions

7. Soient F et G deux sous-espaces supplémentaires de E et s la symétrie par rapport à F parallèlement à G.

   (a) Montrer que $F = F_s$ et $G = G_s$.

   (b) Montrer que $s \circ s = \mathrm{id}_E$. En déduire que s est un automorphisme de E.

   (c) Déterminer les valeurs propres et les sous-espaces propres de s. On discutera selon les sous-espaces F et G.

8. Soit s un endomorphisme de E tel que $s \circ s = \mathrm{id}_E$. Montrer que s est une symétrie.

• Couples de symétries qui anticommutent

9. Soient s et t deux symétries de E qui anticommutent, c'est-à-dire telles que $s \circ t + t \circ s = 0$.

   (a) Prouver les égalités $t(F_s) = G_s$ et $t(G_s) = F_s$.

   (b) En déduire que F_s et G_s ont la même dimension et que n est pair.

• H-systèmes

On appelle H-système d'endomorphismes de E toute famille finie de symétries de E qui anticommutent deux à deux, c'est-à-dire toute famille finie $(S_1, \ldots, S_p)$ d'endomorphismes de E tels que

$$\begin{cases} \forall i & S_i \circ S_i &=& \mathrm{id}_E \\ \forall i \neq j & S_i \circ S_j + S_j \circ S_i &=& 0 \end{cases}$$

De même, on appelle H-système de matrices de taille n toute famille finie $(A_1, \ldots, A_p)$ de matrices de $\mathcal{M}_n(\mathbb{C})$ telles que

$$\begin{cases} \forall i & A_i^2 &=& \mathrm{id}_E \\ \forall i \neq j & A_i A_j + A_j A_i &=& 0 \end{cases}$$

Dans les deux cas, p est appelé longueur du H-système.

10. Montrer que la longueur p d'un H-système d'endomorphismes de E est majorée par n^2.
11. Montrer que l'existence d'un H-système $(S_1, \dots, S_p)$ de E équivaut à l'existence d'un H-système de matrices de taille n. En déduire que la longueur d'un H-système de E ne dépend que de la dimension n de E et pas de l'espace E.

On note $p(n)$ le plus grand entier p tel que E admet un H-système de longueur p.

12. Si n est un entier impair, que peut-on dire de $p(n)$?

- **Majoration de $p(n)$**

13. On suppose ici que n est pair et on pose $n = 2m$. On considère :
    - un H-système $(S_1, \dots, S_p, T, U)$ de E,
    - le sous-espace $E_0 = F_T = \operatorname{Ker}(T - \mathrm{id})$,
    - pour $j \in [\![1, p]\!]$, l'endomorphisme $R_j = \mathrm{i}\, U \circ S_j$ de E.

    (a) Montrer que, pour tout $j \in [\![1, p]\!]$, le sous-espace E_0 est stable par R_j.

    (b) Pour tout $j \in [\![1, p]\!]$, on note s_j l'endomorphisme de E_0 induit par R_j. Montrer que $(s_1, \dots, s_p)$ est un H-système de E_0.

    (c) En déduire $p(2m) \leqslant p(m) + 2$.
14. Montrer que si $n = 2^d m$ avec m impair, alors $p(n) \leqslant 2d + 1$.

- **Construction de H-systèmes maximaux**

15. Soient $N = p(n)$ et $(a_1, \dots, a_N)$ un H-système de matrices de taille n, c'est-à-dire tel que

$$\forall i,\ a_i^2 = \mathrm{id}_E \quad \text{et} \quad \forall i \neq j,\ a_i a_j + a_j a_i = 0.$$

    En considérant les matrices suivantes de $\mathcal{M}_{2n}(\mathbb{C})$ écrites par blocs

$$A_j = \begin{pmatrix} a_j & 0 \\ 0 & -a_j \end{pmatrix} (j \in [\![1, N]\!]) \quad A_{N+1} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \quad A_{N+2} = \begin{pmatrix} 0 & \mathrm{i}I_n \\ -\mathrm{i}I_n & 0 \end{pmatrix},$$

    montrer que $p(2n) \geqslant N + 2$.
16. Déterminer $p(n)$ en fonction de l'unique entier $d \in \mathbb{N}$ tel que n s'écrive $n = 2^d m$ avec m impair.
17. Écrire, pour chacun des entiers $n = 1, 2, 4$, un H-système de matrices de taille n de longueur $p(n)$.

Partie III – Quaternions et sommes de carrés

Pour $(a, b) \in \mathbb{C}^2$, on désigne par $M(a, b)$ la matrice carrée complexe :

$$M(a, b) = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}).$$

Une matrice de la forme $M(a,b)$ sera appelée un *quaternion*. On considèrera en particulier les quaternions suivant :

$$e = I_2 = M(1,0),\ I = M(0,1),\ J = M(\mathrm{i},0),\ K = M(0,\mathrm{i})$$

et on notera :

$$\mathbb{H} = \{M(a,b) \,|\, (a,b) \in \mathbb{C}^2\}$$

le sous-ensemble de $\mathcal{M}_2(\mathbb{C})$ constitué des quaternions.

On veillera à ne pas confondre la matrice $I = M(0,1)$ et la matrice unité $I_2 = e = M(1,0)$.

• Le « corps » des quaternions

18. (a) Donner, sans justification, une base et la dimension de l'algèbre $\mathcal{M}_2(\mathbb{C})$ (sur le corps $\mathbb{R}$).
    (b) Montrer que $\mathbb{H}$ est une sous-algèbre de $\mathcal{M}_2(\mathbb{C})$, en donner une base et la dimension (sur le corps $\mathbb{R}$).
19. Montrer que $(\mathbb{H}, +, \times)$ est un corps non commutatif.
20. (a) Calculer les produits deux à deux des matrices e, I, J, K. On présentera les résultats dans une table à double entrée et les calculs ne sont pas demandés.
    (b) En déduire que $(\mathrm{i}I, \mathrm{i}J, \mathrm{i}K)$ est un H-système de $\mathcal{M}_2(\mathbb{C})$.

• Conjugaison et normes

On a montré que tout élément $q \in \mathbb{H}$ s'écrit de manière unique $q = xe + yI + zJ + tK$ avec $x, y, z, t \in \mathbb{R}$.

Pour tous $x, y, z, t \in \mathbb{R}$ et $q = xe + yI + zJ + tK \in \mathbb{H}$, on pose $q^* = xe - yI - zJ - tK \in \mathbb{H}$ et $N(q) = x^2 + y^2 + z^2 + t^2 \in \mathbb{R}_+$.

21. (a) Pour tout $q \in \mathbb{H}$, trouver une relation matricielle entre q^* et q.
    (b) En déduire que, pour tout $(q,r) \in \mathbb{H}^2, (qr)^* = r^*q^*$.
    (c) Montrer que $q^{**} = q$ pour tout $q \in \mathbb{H}$ et que $q \mapsto q^*$ est un automorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{H}$.
    (d) Pour $q \in \mathbb{H}$, exprimer qq^* à l'aide de $N(q)$. En déduire la relation valable pour tout $(q,r) \in \mathbb{H}^2$

$$N(qr) = N(q)N(r)$$

22. (a) Soient $(x,y,z,t) \in \mathbb{R}^4$ et $q = xe + yI + zJ + tK$. Exprimer la trace de la matrice $q \in \mathcal{M}_2(\mathbb{C})$ en fonction du réel x.
    (b) En déduire que, pour tout $(q,r) \in \mathbb{H}^2$, $qr - rq = q^*r^* - r^*q^*$.
    (c) Soient a, b, c, d des quaternions. Établir la relation $(acb^*)d + d^*(acb^*)^* = (acb^*)^*d^* + d(acb^*)$ et en déduire l'identité $(N(a) + N(b))(N(c) + N(d)) = N(ac - d^*b) + N(bc^* + da)$.

Partie IV – Un théorème de Hurwitz

Soit un entier naturel $n \geqslant 1$. On munit $\mathbb{R}^n$ du produit scalaire usuel et de la norme euclidienne usuelle définis, pour tout $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{R}^n$, par

$$(X|Y) = \sum_{k=1}^{n} x_k y_k \quad \text{et} \quad \|X\| = \sqrt{\sum_{k=1}^{n} x_k^2}$$

L'objet de cette partie est d'étudier l'existence d'une application bilinéaire $B_n \colon (\mathbb{R}^n)^2 \to \mathbb{R}^n$ vérifiant

$$\forall X, Y \in \mathbb{R}^n, \quad \|B_n(X,Y)\| = \|X\| \, \|Y\| \qquad (IV.1).$$

- **Des formules pour $\mathbf{n = 1, 2, 4, 8}$**

23. (a) Montrer l'existence d'une application bilinéaire B_n vérifiant (IV.1) lorsque n est l'un des entiers 1, 2, 4. *Pour $n = 2$ (respectivement 4) on pourra considérer le produit de deux nombres complexes (respectivement de deux quaternions).*

    (b) En utilisant la question 22, montrer, pour $n = 8$, l'existence d'une application bilinéaire vérifiant (IV.1). On ne demande pas d'expliciter une application bilinéaire B_8, mais seulement de prouver son existence.

- **Le théorème de Hurwitz**

Dans la suite on suppose que $n \geqslant 3$ et qu'il existe une application bilinéaire B telle que

$$\forall X, Y \in \mathbb{R}^n, \quad \|B(X,Y)\| = \|X\| \, \|Y\|.$$

Soit $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$ et, pour $i \in [\![1, n]\!]$, soit u_i l'endomorphisme de $\mathbb{R}^n$ défini par

$$\forall X \in \mathbb{R}^n, \quad u_i(X) = B(X, e_i)$$

La matrice de u_i dans la base canonique de $\mathbb{R}^n$ sera notée A_i.

24. (a) Prouver que, pour tout $X \in \mathbb{R}^n$, on a

$$\forall Y = (y_1, \ldots, y_n) \in \mathbb{R}^n, \quad \sum_{i,j=1}^{n} y_i y_j (u_i(X)|u_j(X)) = \|X\|^2 \sum_{i=1}^{n} y_i^2$$

    (b) En déduire que les endomorphismes u_i vérifient les relations

$$\forall i, j = 1, \ldots, n, \ \forall X \in \mathbb{R}^n \quad \|u_i(X)\| = \|X\| \text{ et } (i \neq j \Rightarrow (u_i(X)|u_j(X)) = 0)$$

    et plus généralement, $\forall i, j = 1, \ldots, n$, $\forall X, X' \in \mathbb{R}^n$:

$$(u_i(X)|u_i(X')) = (X|X') \text{ et } (i \neq j \Rightarrow (u_i(X)|u_j(X')) + (u_j(X)|u_i(X')) = 0).$$

    (c) Prouver que les matrices A_j vérifient les relations :

$$\forall i, j = 1, \ldots, n, \quad {}^t A_i A_i = I_n \text{ et } (i \neq j \Rightarrow {}^t A_i A_j + {}^t A_j A_i = 0).$$

25. Pour $j = 1, \ldots, n-1$ on note S_j la matrice complexe $S_j = \mathrm{i}\, {}^t A_n A_j$.

    (a) Prouver que $(S_1, \ldots, S_{n-1})$ est un H-système.

    (b) En déduire qu'on a l'inégalité $p(n) \geqslant n - 1$ où $p(n)$ est défini dans la partie II.

26. Prouver que n est élément de $\{1, 2, 4, 8\}$.

Partie V – Sommes de carrés dans un anneau

27. Soit $(A, +, \times)$ un anneau commutatif. Pour $p \in \mathbb{N}^*$, on note $C_p(A)$ l'ensemble des sommes de p carrés d'éléments de A.

    Prouver que pour tout anneau A, les ensembles $C_p(A)$ sont stables pour la multiplication lorsque p vaut 1, 2, 4 ou 8. *On pourra utiliser les formes bilinéaires B_p définies dans la partie IV.*

• Le théorème des quatre carrés

On note $\mathbb{G} = \{xe + yI + zJ + tK \,|\, x, y, z, t \in \mathbb{Z}\}$ l'ensemble des quaternions « entiers ».

28. (a) Montrer que $\mathbb{G}$ est un sous-groupe de $\mathbb{H}$ pour l'addition et qu'il est stable par multiplication.
    (b) Montrer que pour tout $q \in \mathbb{H}$, il existe $\mu \in \mathbb{G}$ tel que $N(q - \mu) \leqslant 1$.
    (c) Quel est l'ensemble des $q \in \mathbb{H}$ tels que $\forall \mu \in \mathbb{G},\ N(q - \mu) \geqslant 1$?

29. Soit p un nombre premier impair. Pour tout entier $r \in \mathbb{Z}$, on note $\varphi(r)$ le reste de la division euclidienne de r^2 par p. On a donc $0 \leqslant \varphi(r) \leqslant p - 1$ et $r^2 - \varphi(r) \in p\mathbb{Z}$.
    (a) Montrer que la restriction de φ à $\{0, \ldots, \frac{p-1}{2}\}$ est injective.
    (b) On considère les ensembles $X = \{p - \varphi(r) \,|\, 0 \leqslant r \leqslant \frac{p-1}{2}\}$ et $Y = \{\varphi(s) + 1 \,|\, 0 \leqslant s \leqslant \frac{p-1}{2}\}$. Montrer que X et Y sont inclus dans $\{1, \ldots, p\}$ et que leur intersection est non vide. En déduire qu'il existe $u, v \in \{0, \ldots, \frac{p-1}{2}\}$ et $m \in \{1, \ldots, p-1\}$ tels que $u^2 + v^2 + 1 = mp$.

30. On suppose encore que p est un nombre premier impair. Justifier qu'il existe $m \in \{1, \ldots, p-1\}$ et $\mu = xe + yI + zJ + tK \in \mathbb{H} \setminus \{0\}$ tels que $N(\mu) = mp$. On choisit m minimal et on suppose que $m > 1$.
    (a) Montrer que si m était pair, un nombre pair des entiers x, y, z, t serait impair et aboutir à une contradiction. *On pourra écrire* $(\frac{x-y}{2})^2 + (\frac{x+y}{2})^2 = \frac{x^2+y^2}{2}$.
    (b) On suppose m impair. Montrer qu'il existe $\nu \in \mathbb{G}$ tel que $N(\mu - m\nu) < m^2$.
    (c) Prouver que $\mu' = \frac{1}{m}\mu(\mu - m\nu)^*$ est dans $\mathbb{G} \setminus \{0\}$ et que $N(\mu')$ est un multiple de p strictement inférieur à mp. Conclure.

31. Montrer que tout entier naturel est somme de quatre carrés d'entiers.

Fin de l'énoncé.