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

Corrigé de l'écrit blanc d'algèbre

Partie I – Des algèbres de matrices réelles

1. Le polynôme caractéristique de la matrice A est $X^2 - \operatorname{tr}(A)X + \det(A)$ et le théorème de Cayley-Hamilton dit que ce polynôme annule A, ce qui répond à la question.

   Remarque. — Le fait que le polynôme caractéristique d'un matrice $A \in \mathcal{M}_2(\mathbb{K})$ est $X^2 - \operatorname{tr}(A)X + \det(A)$ est à connaître. Cela peut se montrer par le calcul à partir d'une matrice quelconque, mais se retient plus facilement en se plaçant sur un corps algébriquement clos ($\mathbb{C}$ pour une matrice réelle). Sur un tel corps le polynôme caractéristique est scindé, la matrice est trigonalisable, de valeurs propres λ_1, λ_2, le polynôme caractéristique est $(X-\lambda_1)(X-\lambda_2)$, la trace $\lambda_1+\lambda_2$ et le déterminant $\lambda_1\lambda_2$.

2. Par définition, $\mathbb{A}$ est le sous-espace vectoriel engendré par I_2 et A donc c'est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$. De plus $\mathbb{A}$ contient I_2 et $\mathbb{A}$ est stable pour le produit car $A^2 \in \operatorname{vect}(I_2, A)$. Donc $\mathbb{A}$ est une sous-algèbre de $\mathcal{M}_2(\mathbb{R})$. $\mathbb{A}$ est commutative car les polynômes en A commutent deux à deux. Comme A n'est pas une matrice scalaire, (I_2, A) est une famille libre et par conséquent une base du $\mathbb{R}$-espace vectoriel $\mathbb{A}$.

3. (a) Supposons qu'il existe une matrice $B = aI_2 + bA \in \mathbb{A}$ telle que $B^2 = -I_2$. Alors toute valeur propre λ de B vérifie $\lambda^2 = -1$ donc B ne possède pas de valeur propre réelle. On en déduit que A ne possède pas non plus de valeur propre réelle (car μ valeur propre de A implique[1] $a + b\mu$ valeur propre de B). Le polynôme caractéristique de A n'a donc pas de racine réelle donc son discriminant $\Delta = (\operatorname{tr} A)^2 - 4\det A$ est strictement négatif.

   Réciproquement, supposons que $\Delta = (\operatorname{tr} A)^2 - 4\det A < 0$. On a $0 = A^2 - \operatorname{tr}(A)A + \det(A) = (A - \frac{\operatorname{tr}(A)}{2} I_2)^2 - \frac{\Delta}{4} I_2$. Donc la matrice $B = \frac{2}{\sqrt{-\Delta}}\left(\left(-\frac{\operatorname{tr} A}{2}\right) I_2 + A\right) \in \mathbb{A}$ vérifie $B^2 = -I_2$.

   (b) On suppose que $B \in \mathbb{A}$ est telle que $B^2 = -I_2$. Alors B n'est pas une matrice scalaire (car si $\lambda \in \mathbb{R}$, $(\lambda I_2)^2 = \lambda^2 I_2 \neq -I_2$) donc (I_2, B) est une famille libre de $\mathbb{A}$. Comme $\mathbb{A} = \operatorname{vect}\{I_2, A\}$ on en déduit que $\mathbb{A}$ est un $\mathbb{R}$-espace vectoriel de dimension deux et que (I_2, B) en est une base.

   Définissons alors f comme l'unique application linéaire entre les $\mathbb{R}$-espaces vectoriels $\mathbb{A}$ et $\mathbb{C}$ telle que $f(I_2) = 1$ et $f(B) = i$. Alors f est un isomorphisme d'espaces vectoriels car elle envoie une base de $\mathbb{A}$ sur une base de $\mathbb{C}$. De plus $f(I_2) = 1$. Enfin, si $M = xI_2 + yB$ et $M' = x'I_2 + y'B$ sont deux éléments de $\mathbb{A}$, $MM' = xx'I_2 + (xy' + x'y)B + yy'B^2 = (xx' - yy')I_2 + (xy' + x'y)B$ donc

   $$f(MM') = (xx' - yy')f(I_2) + (xy' + x'y)f(B) = (xx' - yy') + i(xy' + x'y)$$

   et

   $$f(M)f(M') = (x + iy)(x' + iy') = (xx' - yy') + i(xy' + x'y)$$

1. Il est important de savoir que, d'une manière générale, la trigonalisation dans $\mathbb{C}$ montre que pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$ et tout polynôme P, on a $\operatorname{Sp}(P(A)) = P(\operatorname{Sp}(A))$.

On a donc $f(MM') = f(M)f(M')$ ce qui achève de montrer que f est un isomorphisme d'algèbres entre $\mathbb{A}$ et $\mathbb{C}$.

4. D'après le calcul fait en question 3 et A étant non scalaire, si $M = aI_2 + bA$, la condition $M^2 = 0$ équivaut à $\begin{cases} a^2 - b^2 \det A = 0 \\ 2ab + b^2 \mathrm{tr}\, A = 0 \end{cases}$ c'est-à-dire à

$$b = a = 0 \qquad \text{ou} \qquad \begin{cases} a = -\frac{b}{2}\mathrm{tr}\, A \\ b^2\left(\frac{1}{4}(\mathrm{tr}\, A)^2 - \det A\right) = 0 \end{cases}$$

soit encore, compte-tenu de l'hypothèse $(\mathrm{tr}\, A)^2 = 4 \det A$, à $a = -\frac{b}{2}\mathrm{tr}\, A$.

Conclusion : Si A n'est pas une matrice scalaire et vérifie $(\mathrm{tr}\, A)^2 = 4 \det A$, les solutions de $M^2 = 0$ dans $\mathbb{A}$ sont les matrices de la forme $b\left(-\frac{\mathrm{tr}\, A}{2} I_2 + A\right)$ avec $b \in \mathbb{R}$. Comme A est non scalaire, la matrice $-\frac{\mathrm{tr}\, A}{2} I_2 + A$ est non nulle, de carré nul, donc non inversible, par conséquent $\mathbb{A}$ n'est pas un corps.

Remarques. — 1) Pour justifier que $\mathbb{A}$ n'est pas un corps, il ne suffit pas de dire qu'il existe une matrice non nulle non inversible, même si cela paraît évident (il existe des situations où un résultat faux semble évident). Il faut *toujours* donner un contre-exemple pour convaincre. Remarquez qu'ici ça nécessite l'hypothèse A non scalaire.

2) Dans cette question on peut également raisonner sur le discriminant du polynôme caractéristique de la manière suivante. Si $(\mathrm{tr}\, A)^2 = 4 \det A$, alors le polynôme caracéristique de A possède une racine double réelle. La matrice A est non diagonalisable sinon elle serait scalaire, mais elle est trigonalisable. Donc il existe $P \in \mathrm{GL}_2(\mathbb{R})$ telle que $PAP^{-1} = \lambda I_2 + N$ avec[2] $N = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}$, $\alpha \in \mathbb{R}^*$, et, par identification de la trace, $\lambda = \frac{\mathrm{tr}\,(A)}{2}$. Une matrice M de $\mathbb{A}$ est donc de la forme $M = aI_2 + bA = P^{-1}((a + b\frac{\mathrm{tr}\,(A)}{2})I_2 + bN)P$. En remarquant que la matrice N est nilpotente, on a alors $M^2 = P^{-1}((a + b\frac{\mathrm{tr}\,(A)}{2})^2 I_2 + 2(a + b\frac{\mathrm{tr}\,(A)}{2})N)P$. On trouve que $M^2 = 0$ si et seulement si $a + b\frac{\mathrm{tr}\,(A)}{2} = 0$.

5. Si $(\mathrm{tr}\, A)^2 > 4 \det A$ le discriminant du polynôme caractéristique de A est strictement positif donc χ_A possède deux racines réelles distinctes *i.e.* A possède deux valeurs propres réelles distinctes ce qui implique sa diagonalisabilité dans $\mathcal{M}_2(\mathbb{R})$.

Soit B une matrice diagonale semblable à A et P une matrice inversible telle que $B = P^{-1}AP$. La conjugaison $M \mapsto P^{-1}MP$ est un automorphisme de l'algèbre $\mathcal{M}_2(\mathbb{R})$ (composé de deux isomorphismes l'algèbre $\mathcal{M}_2(\mathbb{R}) \to \mathrm{End}(\mathbb{R}^2) \to \mathcal{M}_2(\mathbb{R})$), qui en restriction à $\mathbb{A}$ donne un isomorphisme d'algèbre de $\mathbb{A}$ dans $\mathbb{B} = \mathrm{vect}\{I_2, B\}$. Or $\mathbb{B}$ est égal à l'espace $\mathcal{D}_2(\mathbb{R})$ des matrices carrées diagonales d'ordre 2 : en effet $\mathbb{B} \subset \mathcal{D}_2(\mathbb{R})$ et $\dim_{\mathbb{R}}(\mathbb{B}) = 2 = \dim_{\mathbb{R}}(\mathcal{D}_2(\mathbb{R}))$ (car $\left(E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$ est une base de $\mathcal{D}_2(\mathbb{R})$).

Dans ce cas, $\mathbb{A}$ n'est pas un corps car si h désigne un isomorphisme de $\mathbb{A}$ sur $\mathbb{B} = \mathcal{D}_2(\mathbb{R})$, $h^{-1}(E_{11})$ et $h^{-1}(E_{22})$ sont deux éléments non nuls de $\mathbb{A}$ dont le produit est nul, donc qui sont non inversibles (diviseurs de 0).

6. (a) Soit $A \in \mathbb{A}$ non scalaire et possédant une valeur propre réelle λ. Alors $A - \lambda I_n$ appartient à $\mathbb{A}$ (car $\mathbb{A}$ est stable par combinaisons linéaires et contient A et I_n), $A - \lambda I_n$ est non inversible dans $\mathcal{M}_2(\mathbb{R})$ (car λ est valeur propre de A) donc dans $\mathbb{A}$, et n'est pas la matrice nulle (car A n'est pas scalaire) ce qui prouve que $\mathbb{A}$ n'est pas un anneau à division.

2. notez que c'est la décomposition de Dunford de la matrice

(b) Toute matrice trigonalisable (*a fortiori* diagonalisable) de $\mathcal{M}_n(\mathbb{R})$ a un polynôme caractéristique scindé sur $\mathbb{R}$ donc possède au moins une valeur propre réelle. Par suite, d'après (a), si $\mathbb{A}$ contient une matrice non scalaire trigonalisable, $\mathbb{A}$ n'est pas un anneau à division.

(c) On suppose $\mathbb{A}$ intègre et $A \in \mathbb{A} \setminus \{0\}$. L'application $\Phi_A : X \mapsto AX$ est un endomorphisme de $\mathbb{A}$. De plus, $\mathbb{A}$ étant intègre et A étant non nulle, $\operatorname{Ker} \varphi_A = \{0\}$ donc φ_A est injectif. Comme φ_A est un endomorphisme d'un espace vectoriel de dimension finie, on en déduit que φ_A est un isomorphisme. En particulier, φ_A est surjective donc il existe $B \in \mathbb{A}$ telle que $\varphi_A(B) = I_n$. La matrice A possède donc un inverse à droite, donc est inversible d'inverse B appartenant à $\mathbb{A}$. Tout élément non nul de $\mathbb{A}$ possède donc un inverse dans $\mathbb{A}$ donc $\mathbb{A}$ est un anneau à division.

Remarque. — La preuve de ce résultat est la même que la preuve du résultat suivant : tout anneau commutatif fini intègre est un corps. La finitude est essentielle à la preuve, dans ce résultat l'hypothèse algèbre de dimension finie remplace l'hypothèse anneau fini.

Partie II – Symétries vectorielles complexes

• Symétries et involutions

7. (a) On cherche F_s : c'est l'ensemble des $x = y + z \in E$ avec $(y, z) \in F \times G$ tels que $s(x) = x$, c'est-à-dire tels que $y - z = y + z$. Ceci équivaut à $x = y \in F$, donc $F = F_s$.
On démontre de même que $G = G_s$.

(b) Soit $x = y + z \in E$, avec $(y, z) \in F \times G$. Alors

$$s(s(x)) = s(y - z) = y - (-z) = y + z = x,$$

donc $s \circ s = \mathrm{id}_E$. L'existence de $u \in \mathcal{L}(E)$ telle que $u \circ s = s \circ u = \mathrm{id}_E$ (avec $u = s$) prouve que s est un automorphisme de E (de réciproque s).

Remarque : Comme E est de dimension finie, on aurait pu se contenter d'une seule des deux égalités $u \circ s = \mathrm{id}_E$ ou $s \circ u = \mathrm{id}_E$.

(c) Si $F = E$, alors $G = \{0\}$ et $s = \mathrm{id}_E$, qui n'a qu'une seule valeur propre (c'est 1) et un seul sous-espace propre (c'est E).
Si $F = \{0\}$, alors $G = E$ et $s = -\mathrm{id}_E$, qui n'a qu'une seule valeur propre (c'est -1) et un seul sous-espace propre (c'est E).
Sinon, s possède deux valeurs propres (ce sont 1 et -1) et les deux sous-espaces propres sont respectivement F et G.

8. Soient $F = F_s$, $G = G_s$. Soit $x \in E$. Notons $y = \frac{1}{2}(x + s(x))$ et $z = \frac{1}{2}(x - s(x))$. On a $x = y + z$, et comme $s \circ s = \mathrm{id}_E$, on a $s(y) = \frac{1}{2}(s(x) + x) = y$, donc $y \in F$, et $s(z) = \frac{1}{2}(s(x) - x) = -z$, donc $z \in G$. Ceci montre que $E = F + G$ et comme F et G sont en somme directe en tant qu'espaces propres de s, cela donne $E = F \oplus G$. De plus en reprenant les notations ci-dessus, $s(x) = s(y) + s(z) = y - z$, ce qui montre que s est la symétrie vectorielle de E par rapport à F parallèlement à G.

Remarque. — La preuve ci-dessus est classique et élémentaire. En invoquant le polynôme annulateur $X^2 - 1$ scindé à racine simple de s, on obtient directement que s est diagonalisable avec un spectre contenu dans $\{-1, 1\}$, donc est une symétrie.

• **Couples de symétries qui anticommutent**

9. (a) Soit $x \in t(F_s)$: il existe donc $x' \in F_s$ tel que $x = t(x')$. Pour démontrer que $x \in G_s$, il suffit de vérifier que $s(x) = -x$. Or $s(x) = s(t(x')) = -t(s(x'))$ car t et s anticommutent, et $s(x') = x'$ car $x' \in F_s$. Finalement, on a bien $s(x) = -t(x') = -x$, et on a prouvé que

$$t(F_s) \subset G_s.$$

Le même calcul (en remplaçant la valeur propre 1 par la valeur propre -1) montre que $t(G_s) \subset F_s$.

Pour démontrer les inclusions réciproques, on applique t à la première inclusion, ce qui donne $(t \circ t)(F_s) \subset t(G_s)$, c'est-à-dire $F_s \subset t(G_s)$, et on conclut que $F_s = t(G_s)$. On montre de même que $G_s = t(F_s)$.

(b) La conservation des dimensions des sous-espaces vectoriels par un automorphisme montre que $\dim F_s = \dim G_s$, et comme $E = F_s \oplus G_s$, on a $\dim E = 2 \dim F_s$ qui est paire.

• **H-systèmes**

10. On va montrer qu'un H-système $(S_1, \dots, S_p)$ est une famille libre de $\mathcal{L}(E)$, ce qui établira que

$$p \leqslant \dim \mathcal{L}(E) = n^2.$$

Soit $(\lambda_1, \dots, \lambda_p) \in \mathbb{C}^p$ tel que $\sum_{i=1}^p \lambda_i S_i = 0$. On fixe $j \in \{1, \dots, p\}$. En composant à droite et à gauche l'égalité précédente par S_j, puis en ajoutant les deux égalités obtenues, on obtient

$$\sum_{1 \leqslant i \leqslant p,\, i \neq j} \lambda_i (S_i \circ S_j + S_j \circ S_i) + 2\lambda_j (S_j \circ S_j) = 2\lambda_j \,\mathrm{id}_E = 0.$$

On en déduit que $\lambda_j = 0$, et ceci pour tout $j \in [\![1, p]\!]$, ce qui achève la preuve.

11. Soit $\mathcal{B}$ une base quelconque de E. Il est rappelé dans l'énoncé que l'application $u \in \mathrm{End}(E) \mapsto \mathrm{mat}_{\mathcal{B}}\, u \in \mathcal{M}_n(\mathbb{C})$ est un (iso)morphisme d'algèbres.

Si $(S_1, \dots, S_p)$ est un H-système d'endomorphismes de E, alors la famille de leurs matrices sur $\mathcal{B}$ est un H-système de $\mathcal{M}_n(\mathbb{C})$. Réciproquement, si $(A_1, \dots, A_p)$ est un H-système de matrices de $\mathcal{M}_n(\mathbb{C})$, la famille des endomorphismes dont les A_i sont les matrices sur $\mathcal{B}$ est un H-système de E.

La longueur maximale d'un H-système de E est donc la longueur maximale d'un H-système de $\mathcal{M}_n(\mathbb{C})$. Cette longueur maximale ne dépend donc pas de E, mais seulement de n.

12. Si $(S_1, \dots, S_p)$ est un H-système de E avec $p \geqslant 2$, alors (S_1, S_2) est aussi un H-système de E et d'après la question 9.b, on en déduit que n est pair.

Supposons n est impair. Un H-système de E est donc de longueur au plus 1. Par ailleurs, toute famille (S) composée d'une unique symétrie vectorielle de E est un H-système ($S^2 = \mathrm{id}_E$ et il n'y a pas de deuxième condition).

On a montré que si n est impair, alors $p(n) = 1$.

• **Majoration de $p(n)$**

13. (a) On rappelle que si deux endomorphismes f et g de E commutent, alors les sous-espaces propres de l'un sont stables par l'autre. On l'applique à $f = U \circ S_j$ et $g = T$ et au sous-espace propre $E_0 = \mathrm{Ker}\,(T - \mathrm{id}_E)$ de $g = T$: c'est possible car

$$\begin{aligned} f \circ g = (U \circ S_j) \circ T = U \circ (S_j \circ T) = U \circ (-T \circ S_j) = -(U \circ T) \circ S_j, \\ = -(-T \circ U) \circ S_j = T \circ (U \circ S_j) = g \circ f. \end{aligned}$$

On conclut que E_0 est stable par $R_j = \mathrm{i}\,U \circ S_j$.

Remarque. — En utilisant $E_0 = F_T$ et la question 9(a), on obtenait rapidement le résultat (sans remarquer que T et $U \circ S_j$ commutent).

(b) On vérifie les deux conditions d'un H-système :

— Pour tout $i \in [\![1, p]\!]$ et tout $x \in E_0$, comme $U^2 = S_j^2 = \mathrm{id}_E$, on a

$$\begin{aligned} s_j^2(x) &= [\mathrm{i}^2 (U \circ S_i)^2](x) = -[U \circ (S_i \circ U) \circ S_i](x), \\ &= -[U \circ (-U \circ S_j) \circ S_j](x) = [(U \circ U) \circ (S_j \circ S_j)](x) = x, \end{aligned}$$

et on conclut que $s_j^2 = \mathrm{id}_{E_0}$.

— Pour tout $(i, j) \in [\![1, p]\!]^2$ tel que $i \neq j$ et tout $x \in E_0$, on a

$$\begin{aligned} (s_i \circ s_j + s_j \circ s_i)(x) &= \mathrm{i}^2 [(U \circ S_i) \circ (U \circ S_j) + (U \circ S_j) \circ (U \circ S_i)](x), \\ &= -[(U \circ U) \circ (S_i \circ S_j) + (U \circ U) \circ (S_j \circ S_i)](x), \\ &= -[S_i \circ S_j + S_j \circ S_i](x) = 0, \end{aligned}$$

car S_i et S_j anticommutent. On conclut que $s_i \circ s_j + s_j \circ s_i = 0$.

Finalement, $(s_1, \ldots, s_p)$ est un H-système de E_0.

(c) D'après la question 9(b), la dimension de E_0 vaut $m = \frac{n}{2}$ et, comme $(s_1, \ldots, s_p)$ est un H-système de E_0, on a $p \leqslant p(m)$, donc

$$p + 2 \leqslant p(m) + 2.$$

Si l'on suppose maintenant que $(S_1, \ldots, S_p, U, T)$ est un H-système de E de longueur $p(n)$, on a $p + 2 = p(n) = p(2m)$. On conclut que

$$p(2m) \leqslant p(m) + 2.$$

14. On raisonne par récurrence sur $d \in \mathbb{N}$.

— Si $d = 0$, alors $n = m$ est impair, et on sait d'après la question 12 que $p(n) = 1$, qui vérifie bien l'inégalité $p(n) \leqslant 2d + 1 = 1$.

— Si la majoration est établie pour un entier $d \in \mathbb{N}$, on considère un entier n de la forme $2^{d+1}m$ avec m impair. Alors $n = 2n'$ avec $n' = 2^d m$. La question précédente, puis l'hypothèse de récurrence, permettent d'écrire que

$$p(n) = p(2m') \leqslant p(m') + 2 = p(2^d m) + 2 \leqslant (2d + 1) + 2 = 2(d + 1) + 1.$$

C'est la majoration attendue au rang $d + 1$.

• Construction de H-systèmes maximaux

15. On va montrer que $(A_1, \ldots, A_{N+2})$ est un H-système de matrices de $\mathcal{M}_{2n}(\mathbb{C})$, ce qui prouvera, par définition de la fonction p, que

$$p(2n) \geqslant N + 2.$$

— Soit $j \in [\![1, N]\!]$. On calcule

$$A_j^2 = \begin{pmatrix} a_j^2 & 0 \\ 0 & (-a_j)^2 \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} = I_{2n},$$
$$A_{N+1}^2 = \begin{pmatrix} I_n^2 & 0 \\ 0 & I_n^2 \end{pmatrix} = I_{2n} \quad \text{et} \quad A_{N+2}^2 = \begin{pmatrix} -(\mathrm{i}I_n)^2 & 0 \\ 0 & -(\mathrm{i}I_n)^2 \end{pmatrix} = I_{2n}.$$

— On fixe deux entiers distincts i et j dans $[\![1, N]\!]$. Alors

$$A_i A_j + A_j A_i = \begin{pmatrix} a_i a_j + a_j a_i & 0 \\ 0 & -a_i a_j - a_j a_i \end{pmatrix} = 0.$$

On fixe un entier $j \in [\![1, n]\!]$. Alors

$$A_j A_{N+1} + A_{N+1} A_j = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0, \quad A_j A_{N+2} + A_{N+2} A_j = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$
$$A_{N+1} A_{N+2} + A_{N+2} A_{N+1} = \begin{pmatrix} -\mathrm{i}I_n^2 + \mathrm{i}I_n^2 & 0 \\ 0 & \mathrm{i}I_n^2 - \mathrm{i}I_n^2 \end{pmatrix} = 0,$$

ce qui achève la preuve de ce que $(A_1, \ldots, A_{N+2})$ est un H-système de matrices complexes de taille $2n$.

16. On va démontrer, par récurrence sur la valuation 2-adique $d \in \mathbb{N}$ de n, que $p(n) \geqslant 2d + 1$. Cette minoration, jointe à la majoration de la question 14, prouvera que

$$p(n) = 2d + 1.$$

— Si $d = 0$, on a déjà démontré que $p(n) = 1 = 2d + 1$.

— Si la minoration est établie pour un entier $d \in \mathbb{N}$, on considère un entier n de la forme $2^{d+1}m$ avec m impair. Alors $n = 2n'$ avec $n' = 2^d m$. L'hypothèse de récurrence affirme l'existence d'un H-système $(a_1, \ldots, a_N)$ de matrices complexes de taille n', avec $N = 2d+1$. La question précédente montre alors que

$$p(n) = p(2n') \geqslant N + 2 = (2d + 1) + 2 = 2(d + 1) + 1.$$

C'est la minoration attendue au rang $d + 1$.

17. Pour $n = 1$, les matrices de taille n sont des nombres complexes parenthésés, et voici les deux seuls H-systèmes de longueur $p(1) = 1$:

$$(1) \quad \text{et} \quad (-1).$$

On applique ensuite deux fois la construction de la question 15 à partir du H-système (1), pour obtenir un H-système en dimension 2 de longueur $p(2) = 3$:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix},$$

ainsi qu'un H-système en dimension 4 de longueur $p(4) = 5$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathrm{i} & 0 & 0 \\ -\mathrm{i} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\mathrm{i} \\ 0 & 0 & \mathrm{i} & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \mathrm{i} & 0 \\ 0 & 0 & 0 & \mathrm{i} \\ -\mathrm{i} & 0 & 0 & 0 \\ 0 & -\mathrm{i} & 0 & 0 \end{pmatrix}.$$

Partie III – Quaternions et sommes de carrés

- **Le « corps » des quaternions**

18. (a) La dimension de $\mathcal{C}$ sur $\mathcal{M}_2(\mathbb{C})$ vaut 8 et que

$$(E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}, \mathrm{i}E_{1,1}, \mathrm{i}E_{1,2}, \mathrm{i}E_{2,1}, \mathrm{i}E_{2,2})$$

en est une base ($E_{i,j}$ est la matrice élémentaire dont le terme en position (i,j) vaut 1 et les autres zéro).

(b) Si l'on écrit $a = \alpha + \mathrm{i}\beta$ et $b = \gamma + \mathrm{i}\delta$ avec $(\alpha, \beta, \gamma, \delta) \in \mathbb{R}^4$, on a

$$M(a,b) = \begin{pmatrix} \alpha + \mathrm{i}\beta & -\gamma - \mathrm{i}\delta \\ \gamma - \mathrm{i}\delta & \alpha - \mathrm{i}\beta \end{pmatrix} = \alpha e + \beta J + \gamma I + \delta K.$$

Ceci prouve que $\mathbb{H} = \mathrm{Vect}_{\mathbb{R}}(e, I, J, K)$, et en particulier que c'est un sous-espace vectoriel réel de $\mathcal{M}_2(\mathbb{C})$. Par ailleurs, il est aisé de vérifier que la famille (e, I, J, K) est libre, donc que c'est une base de $\mathbb{H}$. L'espace vectoriel $\mathbb{H}$ est donc de dimension 4 (sur $\mathbb{R}$).

$\mathbb{H}$ contient le neutre pour la multiplication e. Montrons que $\mathbb{H}$ est stable par multiplication, ce qui achèvera de montre que $\mathbb{H}$ est une sous-algèbre de $\mathcal{M}_2(\mathbb{C})$.

Soit $(a,b,c,d) \in \mathbb{C}^4$. On a :

$$\begin{aligned} M(a,b)M(c,d) &= \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & -d \\ \bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & -ad - b\bar{c} \\ \bar{b}c + \bar{a}\bar{d} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix}, \\ &= M(ac - b\bar{d}, ad + b\bar{c}). \end{aligned}$$

Le résultat appartient à $\mathbb{H}$, donc $\mathbb{H}$ est stable par multiplication.

19. On sait déjà que $\mathbb{H}$ est un anneau (sous-anneau de $\mathcal{M}_2(\mathbb{C})$).

Pour tous $a, b \in \mathbb{C}$, on a $\det M(a,b) = a\bar{a} + b\bar{b} = |a|^2 + |b|^2 = 0$ si et seulement si $a = b = 0$, c'est-à-dire si et seulement si $M(a,b)$ est la matrice nulle. Ceci prouve que

$$\mathbb{H} \setminus \{0\} \subset \mathrm{GL}_2(\mathbb{C}).$$

La partie $\mathbb{H}\setminus\{(0)\}$ de $\mathrm{GL}_2(\mathbb{C})$ est stable par inverse car on vérifie facilement avec la formule établie pour la question 18(b) que

$$\forall (a,b) \in \mathbb{C}^2 \setminus \{(0,0)\}, \quad [M(a,b)]^{-1} = M\left(\frac{\bar{a}}{|a|^2 + |b|^2}, -\frac{b}{|a|^2 + |b|^2}\right).$$

Cela montre que $\mathbb{H}$ est un anneau à division. Il n'est pas commutatif car $K = IJ \neq JI = -K$.

20. (a) Voici la table, où l'on place le produit AB à l'intersection de la ligne A et de la colonne B :

$\times$	e	I	J	K
e	e	I	J	K
I	I	$-e$	K	$-J$
J	J	$-K$	$-e$	I
K	K	J	$-I$	$-e$

(b) On note $\mathcal{S} = (\mathrm{i}I, \mathrm{i}J, \mathrm{i}L)$ le système étudié.

— La table ci-dessus montre que, si $L \in \{I, J, K\}$, alors $L^2 = -e = -I_2$, et on en déduit que $(\mathrm{i}L)^2 = I_2$, donc que les éléments de $\mathcal{S}$ sont des symétries vectorielles.

— On constate aussi que les éléments I, J et K de $\mathbb{H}$ anticommutent deux à deux. Cette propriété n'est pas modifiée quand on les multiplie par le nombre i.

On conclut que $\mathcal{S}$ est un H-système de $\mathcal{M}_2(\mathbb{C})$.

• **Conjugaison et normes**

21. (a) Avec les notations de l'énoncé, si l'on pose $a = x + \mathrm{i}z$ et $b = y - \mathrm{i}t$, on a :

$$q = xe + yI + zJ + tK = \begin{pmatrix} x+\mathrm{i}z & -y+\mathrm{i}t \\ y+\mathrm{i}t & x-\mathrm{i}z \end{pmatrix} = M(a,b),$$
$$q^* = xe - yI - zJ - tK = \begin{pmatrix} x-\mathrm{i}z & y-\mathrm{i}t \\ -y-\mathrm{i}t & x+\mathrm{i}z \end{pmatrix} = {}^t\overline{M(a,b)}.$$

On a montré que $q^* = {}^t\overline{q}$.

(b) Pour tout $(q, r) \in \mathbb{H}^2$, on a :

$$(qr)^* = {}^t(\overline{qr}) = {}^t(\overline{q}\,\overline{r}) = {}^t\overline{r}\,{}^t\overline{q} = r^*q^*.$$

(c) Pour tout $q \in \mathbb{H}$ on a :

$$q^{**} = {}^t\Big({}^t\overline{\overline{q}}\Big) = {}^t\big({}^t\overline{\overline{q}}\big) = {}^t\big({}^tq\big) = q.$$

La $\mathbb{R}$–linéarité de $q \mapsto q^*$ est évidente, et le fait que $q^{**} = q$ montre que $q \mapsto q^*$ est une involution de $\mathbb{H}$, en particulier une bijection. C'est donc un automorphisme du $\mathbb{R}$–espace vectoriel $\mathbb{H}$.

Remarques. — C'est un automorphisme involutif de $\mathbb{H}$, c'est-à-dire une symétrie vectorielle de $\mathbb{H}$, par rapport à la droite $\mathrm{Vect}_{\mathbb{R}}(e)$ et parallèlement à l'hyperplan $\mathrm{Vect}_{\mathbb{R}}(I, J, K)$. L'application $q \mapsto q^*$ est appelée la conjugaison dans $\mathbb{H}$, et q^* est appelé le conjugué du quaternion q. Cette analogie entre complexes et quaternions est mise à profit à la question 22(b).

(d) Soient $(x, y, z, t) \in \mathbb{R}^4$, $(a, b) = (x + \mathrm{i}z, y - \mathrm{i}t) \in \mathbb{C}^2$ et $q = M(a, b)$. Alors les calculs de la question 18(b) montrent que

$$qq^* = M(a,b)\,{}^tM(\bar{a},\bar{b}) = M(a\bar{a} + b\bar{b}, -a\bar{\bar{b}} + b\bar{\bar{a}}) = M(|a|^2 + |b|^2, 0) = N(q)e.$$

Remarque – On peut aussi mener un calcul à partir de la table et du H-système de la question 20 :

$$\begin{aligned} qq^* &= (xe + yI + zJ + tK)(xe - yI - zJ - tK), \\ &= x^2e - xyI - xzJ - xtK + yxI - y^2I^2 - yzIJ - ytIK \\ &\qquad + zxJ - zyJI - z^2J^2 - ztJK + txK - tyKI - tzKJ - t^2K^2, \\ &= (x^2 + y^2 + z^2 + t^2)e - yz(IJ + JI) - yt(IK + KI) - zt(JK + KJ), \\ &= N(q)e. \end{aligned}$$

Soit $(q, r) \in \mathbb{H}^2$. On calcule $(qr)(qr)^*$ de deux manières : d'une part, la relation ci-dessus montre que ce produit vaut $N(qr)e$. D'autre part, la question 21(b) donne

$$\begin{aligned} (qr)(r^*q^*) = q(rr^*)q^* = q(N(r)e)q^* = N(r)qq^* = N(r)N(q)e, \\ = N(q)N(r)e. \end{aligned}$$

Comme $N(qr)$ et $N(q)N(r)$ sont des nombres et que e est un vecteur non nul d'un espace vectoriel, l'égalité $N(qr)e = N(q)N(r)e$ entraîne l'égalité $N(qr) = N(q)N(r)$, ce qui conclut.

22. (a) Par linéarité de la trace, on obtient

$$\operatorname{tr}(q) = \operatorname{tr}(xe + yI + zJ + tK) = 2x.$$

(b) On appelle *quaternion réel* (respectivement *quaternion pur*) un quaternion de la forme xe avec x réel (respectivement $yI + zJ + tK$ avec y, z, t réels), et on note $\mathbf{R}$ et $\mathbf{P}$ les sous-ensembles formés des quaternions réels et des quaternions purs respectivement.
Il est clair que $\mathbf{R}$ et $\mathbf{P}$ sont deux sous-espaces vectoriels supplémentaires de $\mathbb{H}$, donc que l'égalité de deux quaternions équivaut à l'égalité de leurs parties réelles et de leurs parties pures (appellations évidentes). D'après la question précédente et la définition du conjugué, la partie réelle et la partie pure de $q \in \mathbb{H}$ sont données par

$$\operatorname{Re}(q) = \frac{\operatorname{tr}(q)}{2}e = \frac{q + q^*}{2} \quad \text{et} \quad \operatorname{Pur}(q) = \frac{q - q^*}{2}.$$

Comme la trace vérifie $\forall (A, B) \in (\mathcal{M}_n(\mathbb{K}))^2$, $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, les traces de $u := qr - rq$ et de $v := q^*r^* - r^*q^*$ sont nulles, donc ces deux quaternions ont la même partie réelle. Enfin, comme $v = -u^*$, on a

$$\operatorname{Pur}(v) = \frac{v - v^*}{2} = \frac{-u^* + u^{**}}{2} = \frac{u - u^*}{2} = \operatorname{Pur}(u).$$

Les quaternions u et v sont donc égaux.

(c) On applique la question précédente à $q = acb^*$ et $r = d$, en écrivant l'égalité sous la forme $qr + r^*q^* = q^*r^* + rq$. On obtient le résultat attendu :

$$(acb^*)d + d^*(acb^*)^* = (acb^*)^*d^* + d(acb^*).$$

On utilise ensuite la relation $\forall q \in \mathbb{H}$, $qq^* = N(q)e$ et son corollaire $\forall (q, r) \in \mathbb{H}^2$, $qrr^*q^* = qq^*rr^*$, et on l'applique au membre de droite de l'inégalité à démontrer (les termes soulignés

se simplifient en vertu de la relation ci-dessus) :

$$\begin{aligned}
&[N(ac-d^*b)+N(bc^*+da)]e\\
&\quad=(ac-d^*b)(ac-d^*b)^*+(bc^*+da)(bc^*+da)^*,\\
&\quad=(ac-d^*b)(c^*a^*-b^*d)+(bc^*+da)(cb^*+a^*d^*),\\
&\quad=aa^*cc^*\underline{-(acb^*)d-d^*(acb^*)^*}+bb^*dd^*\\
&\qquad\qquad+bb^*cc^*\underline{+(acb^*)^*d^*+d(acb^*)}+aa^*dd^*,\\
&\quad=aa^*cc^*+bb^*dd^*+bb^*cc^*+aa^*dd^*,\\
&\quad=(aa^*+bb^*)(cc^*+dd^*)=\big[\big(N(a)+N(b)\big)\big(N(c)+N(d)\big)\big]\,e.
\end{aligned}$$

On en déduit que pour tous les quaternions a, b, c et d :

$$(N(a)+N(b))(N(c)+N(d))=N(ac-d^*b)+N(bc^*+da).$$

Partie IV – Un théorème de Hurwitz

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

23. (a) Dans la suite x,y,z,t,x',y',z',t' désigne des réels quelconques.

— Pour $n=1$, l'application

$$B_1\colon (x,y)\in\mathbb{R}^2\mapsto xy$$

est bilinéaire, et comme la norme euclidienne canonique sur $\mathbb{R}^1$ est la valeur absolue, on a bien $\|B_1(x,y)\|=\|x\|\,\|y\|$, c'est-à-dire $|xy|=|x|\,|y|$.

— Pour $n=2$, l'application

$$B_2\colon ((x,y),(x',y'))\in(\mathbb{R}^2)^2\mapsto(xx'-yy',xy'+x'y)\in\mathbb{R}^2$$

est bilinéaire. Elle a été déduite de la loi de multiplication des nombres complexes

$$(x+\mathrm{i}y)(x'+\mathrm{i}y')=(xx'-yy')+\mathrm{i}(xy'+x'y).$$

Comme la norme euclidienne d'un vecteur de $\mathbb{R}^2$ est aussi le module de son affixe complexe, on obtient

$$\begin{aligned}
\|B_2(X,Y)\|^2&=(xx'-yy')^2+(xy'+x'y)^2=|(x+\mathrm{i}y)(x'+\mathrm{i}y')|^2,\\
&=|x+\mathrm{i}y|^2|x'+\mathrm{i}y'|^2=(x^2+y^2)(x'^2+y'^2)=\|X\|^2\|Y\|^2,
\end{aligned}$$

où $X=(x,y)$ et $Y=(x',y')$.

Remarque. — Cette formule admet la conséquence arithmétique suivante : le produit de sommes de 2 carrés d'entiers est une somme de 2 carrés d'entiers. Par exemple, $(1^2+2^2)(3^2+4^2)=5^2+10^2$.

— Pour $n=4$, l'application

$$B_4\colon ((x,y,z,t),(x',y',z',t'))\in(\mathbb{R}^4)^2\mapsto\begin{pmatrix}xx'-yy'-zz'-tt'\\xy'+yx'+zt'-tz'\\xz'+zx'+ty'-yt'\\xt'+tx'+yz'-zy'\end{pmatrix}\in\mathbb{R}^4$$

est bilinéaire (les coordonnées de $B_4(X,Y)$ sont des formes bilinéaires en X, Y). Elle a été déduite de la loi de multiplication des quaternions

$$\begin{aligned}(xe+yI+zJ+tK)(x'e+y'I+z'J+t'K)\\ =(xx'-yy'-zz'-tt')e+(xy'+yx'+zt'-tz')I\\ +(xz'+zx'+ty'-yt')J+(xt'+tx'+yz'-zy')K.\end{aligned}$$

Comme *le carré* de la norme euclidienne d'un vecteur (x,y,z,t) de $\mathbb{R}^4$ est aussi la norme $N(q)$ de son quaternion associé $q = xe+yI+zJ+tK$, on obtient comme dans le cas $n=2$ l'égalité $\|B_4(X,Y)\|^2 = \|X\|^2\|Y\|^2$, où $X=(x,y,z,t)$ et $Y=(x',y',z',t')$. Cette égalité s'écrit de manière détaillée

$$\begin{aligned}(x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2)\\ =(xx'-yy'-zz'-tt')^2+(xy'+yx'+zt'-tz')^2\\ +(xz'+zx'+ty'-yt')^2+(xt'+tx'+yz'-zy')^2.\end{aligned}$$

Remarque. — Cette formule admet la conséquence arithmétique suivante : le produit de deux sommes de 4 carrés d'entiers est une somme de 4 carrés d'entiers. Par exemple, $(1^2+2^2+3^2+4^2)(5^2+6^2+7^2+8^2) = 60^2+12^2+30^2+24^2$.

(b) On convient que la notation $\underbrace{x,y,z,t}_{q}$ signifie que le quaternion q vaut $xe+yI+zJ+tK$. Si $q\in\mathbb{H}$ est donné, il est théoriquement possible, mais parfois pénible en pratique, d'expliciter ses composantes sur la $\mathbb{R}$-base (e,I,J,K). Dans ce cas, on se contentera d'écrire $\underbrace{\cdots\cdots}_{q}$.

Pour $n=8$, l'application

$$B_8\colon((\underbrace{x,y,z,t}_{a},\underbrace{x',y',z',t'}_{b}),(\underbrace{u,v,w,s}_{c},\underbrace{u',v',w',s'}_{d}))\in(\mathbb{R}^8)^2\mapsto(\underbrace{\cdots\cdots}_{ac-d^*b}\ \underbrace{\cdots\cdots}_{bc^*+da})\in\mathbb{R}^8$$

est bilinéaire[3] et elle vérifie $\|B_8(X,Y)\|^2 = \|X\|^2\|Y\|^2$. En effet, $\|X\|^2 = N(a)+N(b)$ si X est décrit par les quaternions a et b, et $\|Y\|^2 = N(c)+N(d)$ si Y est décrit par les quaternions c et d. L'égalité attendue vient de la formule $(N(a)+N(b))(N(c)+N(d)) = N(ac-d^*b)+N(bc^*+da)$ de la question 22(c).

Remarque. —Cette formule admet la conséquence arithmétique suivante : le produit de deux sommes de 8 carrés d'entiers est une somme de 8 carrés d'entiers.

Jusqu'à maintenant, le problème nous a fait comprendre que la formule des 2 carrés

$$(x^2+y^2)(x'^2+y'^2) = (xy-x'y')^2+(xy'+x'y)^2$$

est la traduction d'une relation portant sur la module des nombres complexes.

Ensuite, le problème expose une nouvelle structure algébrique, le corps (non commutatif) $\mathbb{H}$ des quaternions, muni d'une norme qui conduit à la formule des 4 carrés d'Euler :

$$\begin{aligned}(x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2) = (xx'-yy'-zz'-tt')^2\\ +(xy'+yx'+zt'-tz')^2+(xz'+zx'+ty'-yt')^2+(xt'+tx'+yz'-zy')^2,\end{aligned}$$

3. La distributivité du produit des quaternions sur leur somme montre que, lorsque c et d sont fixés, les applications $(a,b)\mapsto ac-d^*b$ et $(a,b)\mapsto bc^*+da$ sont linéaires, ce qui justifie la linéarité à gauche de B_8. On procède de même pour la linéarité à droite.

Finalement, on vient de démontrer (potentiellement) la formule des 8 carrés, en évitant d'explorer la structure algébrique correspondante, la $\mathbb{R}$-algèbre non associative $\mathbb{O}$ des octonions (ou octaves de Cayley). Le paragraphe suivant nous montre que cette histoire s'arrête là. Pour se faire peur, voici la formule des 8 carrés, tirée de `https://fr.wikipedia.org/wiki/Identit\'e_des_huit_carr\'es_de_Degen` :

$$\begin{aligned}
&(a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2+a_8^2)\times(b_1^2+b_2^2+b_3^2+b_4^2+b_5^2+b_6^2+b_7^2+b_8^2)\\
&=(a_1b_1-a_2b_2-a_3b_3-a_4b_4-a_5b_5-a_6b_6-a_7b_7-a_8b_8)^2\\
&\quad+(a_1b_2+a_2b_1+a_3b_4-a_4b_3+a_5b_6-a_6b_5-a_7b_8+a_8b_7)^2\\
&\quad+(a_1b_3-a_2b_4+a_3b_1+a_4b_2+a_5b_7+a_6b_8-a_7b_5-a_8b_6)^2\\
&\quad+(a_1b_4+a_2b_3-a_3b_2+a_4b_1+a_5b_8-a_6b_7+a_7b_6-a_8b_5)^2\\
&\quad+(a_1b_5-a_2b_6-a_3b_7-a_4b_8+a_5b_1+a_6b_2+a_7b_3+a_8b_4)^2\\
&\quad+(a_1b_6+a_2b_5-a_3b_8+a_4b_7-a_5b_2+a_6b_1-a_7b_4+a_8b_3)^2\\
&\quad+(a_1b_7+a_2b_8+a_3b_5-a_4b_6-a_5b_3+a_6b_4+a_7b_1-a_8b_2)^2\\
&\quad+(a_1b_8-a_2b_7+a_3b_6+a_4b_5-a_5b_4-a_6b_3+a_7b_2+a_8b_1)^2.
\end{aligned}$$

- **Le théorème de Hurwitz**

24. (a) On traduit la formule $\|B(X,Y)\|^2=\|X\|^2\|Y\|^2$ en utilisant la linéarité à droite de B et la définition de la norme :

$$\begin{aligned}
\|B(X,Y)\|^2&=\left(B\left(X,\sum_{i=1}^n y_ie_i\right)\middle|B\left(X,\sum_{j=1}^n y_je_j\right)\right)\\
&=\sum_{i=1}^n\sum_{j=1}^n y_iy_j\,(B(X,e_i)|B(X,e_j))\\
&=\sum_{i=1}^n\sum_{j=1}^n y_iy_j(u(e_i)|u(e_j))=\|X\|^2\sum_{i=1}^n y_i^2.
\end{aligned}$$

(b) — En appliquant la formule ci-dessus à $Y=e_i$, $i\in\{1,...,n\}$, on obtient

$$\forall X\in\mathbb{R}^n,\quad (u_i(X)|u_i(X))=\|u_i(X)\|^2=\|X\|^2.$$

C'est la première relation demandée.

Soient i et j des entiers distincts entre 1 et n. En appliquant la formule ci-dessus à Y défini par $y_i=y_j=1$ et $y_k=0$ pour tout $k\notin\{i,j\}$, on obtient, compte-tenu de la symétrie du produit scalaire : $\|u_i(X)\|^2+\|u_j(X)\|^2+2(u_i(X)|u_j(X))=2\|X\|^2$. Comme on sait déjà que $\|u_k(X)\|^2=\|X\|^2$ pour tout k, on en déduit que

$$\forall X\in\mathbb{R}^n,\quad (u_i(X)|u_j(X))=0.$$

C'est la deuxième relation demandée.

— Le cours affirme qu'un automorphisme orthogonal d'un espace préhilbertien réel est caractérisé par plusieurs conditions équivalentes, dont la conservation de la norme et la conservation du produit scalaire. La première relation démontrée ci-dessus signifie que l'endomorphisme u_k conserve la norme, c'est donc un élément de $\mathrm{GO}(\mathbb{R}^n)$, donc il conserve le produit scalaire :

$$\forall (X,X')\in(\mathbb{R}^n)^2,\quad (u_k(X)|u_k(X'))=(X|X').$$

Enfin, soient i et j des entiers distincts entre 1 et n. En appliquant relation $(u_i(X)|u_j(X)) = 0$ à $X + X'$ au lieu de X et en développant par bilinéarité, on obtient

$$\forall (X, X') \in (\mathbb{R}^n)^2, \quad (u_i(X)|u_j(X')) + (u_i(X')|u_j(X)) = 0.$$

(c) Pour tous $i, j \in [\![1, n]\!]$, les applications $(X, X') \mapsto (u_i(X)|u_i(X'))$ et $(X, X') \mapsto (u_i(X)|u_j(X'))+(u_i(X')|u_j(X))$ sont des formes bilinéaires sur $\mathbb{R}^n$, de matrices dans la base canonique ${}^tA_iA_i$ et ${}^tA_iA_j + {}^tA_jA_i$. Le résultat de cette question est donc la traduction matricielle du résultat de la question précédente.

25. (a) — En utilisant le fait que A_n et A_j sont orthogonales et la relation ${}^tA_nA_j + {}^tA_jA_n = 0$, on obtient

$$S_j^2 = \mathrm{i}^2({}^tA_nA_j\,{}^tA_nA_j) = -\mathrm{i}^2({}^tA_jA_n\,{}^tA_nA_j) = {}^tA_jI_nA_j = {}^tA_jA_j = I_n.$$

— Si j et k sont deux entiers distincts entre 1 et $n-1$, on obtient de même

$$\begin{aligned} S_j \circ S_k + S_k \circ S_j &= \mathrm{i}^2({}^tA_nA_j\,{}^tA_nA_k + {}^tA_nA_k\,{}^tA_nA_j), \\ &= -\mathrm{i}^2({}^tA_jA_n\,{}^tA_nA_k + {}^tA_kA_n\,{}^tA_nA_j), \\ &= {}^tA_jA_k + {}^tA_kA_j = 0. \end{aligned}$$

On conclut que $(S_1, \ldots, S_{n-1})$ est un H-système de $\mathcal{M}_n(\mathbb{C})$.

(b) L'inégalité $n - 1 \leqslant p(n)$ résulte de la définition même de $p(n)$.

26. Ecrivons $n = 2^d m$ avec $d \in \mathbb{N}$ et m entier naturel impair. D'après la question 16, on a $p(n) = 2d+1$. On a montré (en supposant l'existence de l'application bilinéaire B) que $n - 1 \leqslant p(n)$, donc $2^d m \leqslant 2d + 2$, c'est-à-dire $m \leqslant 2^{-d}(2d + 2) = 2^{1-d}(d + 1)$. Or l'application $f : x \mapsto 2^{-x}(2x + 2)$ admet un maximum en $x = \frac{1}{\ln 2} - 1 \approx 0.4$. Comme $f(3) = 1$, on a $f(d) \leq 1$ pour tout $d \geq 3$. Comme m est non nul, cela impose que $d \in \{0, 1, 2, 3\}$. De plus m est inférieur à la plus grande valeur prise par f sur $\{0, 1, 2, 3\}$, qui vaut 2. Comme m est un nombre impair, on a $m = 1$. Cela montre que $n = 1$, 2, 4 ou 8.

Remarque. — C'est le théorème de Hurwitz, qui affirme qu'il ne peut exister de formules des n carrés, au sens où on l'a exposé plus haut, que si $n = 1$, 2, 4 ou 8.

Partie V – Sommes de carrés dans un anneau

27. On remarque que les applications bilinéaires B_p, précédemment définies sur $(\mathbb{R}^p)^2$ et à valeurs dans $\mathbb{R}^p$, peuvent en fait être définies sur $(A^p)^2$ et à valeurs dans A^p, car leurs coefficients sont uniquement les nombres réels $1_\mathbb{R}$ et $-1_\mathbb{R}$. Il suffit de les remplacer par les éléments 1_A et -1_A de l'anneau A pour obtenir des applications notées B_p^A. Par exemple, B_2^A est définie par

$$\forall ((x, y), (x', y')) \in (A^2)^2, \quad B_2^A((x, y), (x', y')) = (xx' - yy', xy' + x'y).$$

Les formules des p carrés établies plus haut pour des nombres réels restent valables pour les éléments de A, car leur validité ne dépend que des propriétés d'anneau commutatif. On se contente

d'illustrer cette affirmation dans le cas $p = 2$, par un calcul qui met en lumière la commutativité, puisqu'il fait appel, notamment, à la formule du binôme dans A et aux relations $(\alpha\beta)^2 = \alpha^2\beta^2$:

$$\begin{aligned}(xy - x'y')^2 + (xy' + x'y)^2 &= x^2y^2 + x'^2y'^2 - 2xyx'y' + x^2y'^2 + x'^2y^2 + 2xy'x'y,\\ &= x^2y^2 + x'^2y'^2 + x^2y'^2 + x'^2y^2 = (x^2 + y^2)(x'^2 + y'^2).\end{aligned}$$

Comme indiqué plus haut, ces formules des p carrés pour $p \in \{1, 2, 4, 8\}$ signifient que le produit de deux sommes de p carrés dans A est une somme de p carrés dans A, c'est-à-dire que $C_p(A)$ est stable par la multiplication.

- **Le théorème des quatre carrés**

28. (a) On sait que $(\mathbb{Z}^4, +)$ et $(\mathbb{H}, +)$ sont des groupes (le premier en tant que produit de groupes, le second en tant que groupe additif d'un espace vectoriel). L'application $\varphi\colon (x, y, z, t) \in \mathbb{Z}^4 \mapsto xe + yI + zJ + tK \in \mathbb{H}$ est, à l'évidence, un morphisme de groupes, donc son image $\mathbb{G}$ est un sous-groupe de $(\mathbb{H}, +)$.

La stabilité de $\mathbb{G}$ par le produit résulte des formules de la question 23 (expression de B_4) donnant les coordonnées sur la base (E, I, J, K) du produit de deux quaternions, et du fait que $+$ et $\times$ sont des lois internes à $\mathbb{Z}$.

(b) Si $q = xe + yI + zJ + tK \in \mathbb{H}$ on choisit des entiers relatifs x', y', z', t' distants de moins de $\frac{1}{2}$ de x, y, z, t respectivement, et on pose $\mu_q = x'e + y'I + z'J + t'K \in \mathbb{G}$. Alors

$$N(q - \mu_q) = (x - x')^2 + (y - y')^2 + (z - z')^2 + (t - t')^2 \leqslant \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

(c) On remarque que si l'une des composantes x, y, z, t de $q \in \mathbb{H}$ n'est pas un demi-entier (i.e. un nombre de la forme $n + \frac{1}{2}$ avec $n \in \mathbb{Z}$), la majoration ci-dessus est stricte : $N(q - \mu_q) < 1$.

Réciproquement, si toutes les composantes de $q = xe + yI + zJ + tK$ sont des demi-entiers, les 16 quaternions entiers

$$\mu = \left(x \pm \frac{1}{2}\right)e + \left(y \pm \frac{1}{2}\right)I + \left(z \pm \frac{1}{2}\right)J + \left(t \pm \frac{1}{2}\right)K \in \mathbb{G}$$

les plus proches de q vérifient $N(q - \mu) = 1$, et les autres vérifient

$$N(q - \mu) \geqslant \left(\frac{3}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 3 > 1.$$

En conclusion, l'ensemble des $q \in \mathbb{H}$ tels que $\forall \mu \in \mathbb{G}\,, N(q - \mu) \geqslant 1$ sont les quaternions « demi-entiers », c'est-à-dire ceux sont les 4 composantes sont des demi-entiers.

29. (a) Soit $(r, s) \in [\![1, \frac{p-1}{2}]\!]^2$ tel que $\varphi(r) = \varphi(s)$. Alors p divise

$$(r^2 - \varphi(r)) - (s^2 - \varphi(s)) = r^2 - s^2 = (r - s)(r + s),$$

donc p divise l'un des deux facteurs $r - s$ ou $r + s$. Comme $2 \leqslant r + s \leqslant p - 1$, il ne divise pas $r + s$, donc il divise $r - s$. Mais comme $|r - s| \leqslant \frac{p-1}{2}$, et comme zéro est le seul multiple de p dans l'intervalle d'entiers $[\![0, \frac{p-1}{2}]\!]$, il faut que $r = s$.

On a démontré que φ est injective sur $[\![1, \frac{p-1}{2}]\!]$.

(b) La propriété caractéristique d'un reste dans une division par p (il appartient à $[\![0, p-1]\!]$) montre que X et Y sont inclus dans $\{1, \dots, p\}$.
La question précédente montre que X et Y sont tous deux de cardinal $\frac{p+1}{2}$. La formule du crible $\mathrm{Card}(X \cup Y) = \mathrm{Card}(X) + \mathrm{Card}(Y) - \mathrm{Card}(X \cap Y)$ et l'inclusion $X \cup Y \subset [\![1, p]\!]$ montrent alors que

$$\frac{p+1}{2} + \frac{p+1}{2} - \mathrm{Card}(X \cap Y) = p + 1 - \mathrm{Card}(X \cap Y) \leqslant p.$$

On en déduit que $\mathrm{Card}(X \cap Y) \geqslant 1$, c'est-à-dire que

$$X \cap Y \neq \emptyset.$$

On note h un élément de $X \cap Y$. Il existe alors u et v dans $[\![0, \frac{p-1}{2}]\!]$ tels que $h = p - \varphi(u) = \varphi(v) + 1$. Comme $p \geqslant 3$ (c'est un nombre premier impair), on en déduit notamment que

$$\varphi(u) + \varphi(v) = p - 1 \geqslant 2.$$

On note k et ℓ les quotients des divisions euclidiennes de u^2 et v^2 par p. Si l'on pose $m = 1 + k + \ell$, on a

$$u^2 + v^2 + 1 = kp + \varphi(u) + \ell p + \varphi(v) + 1 = (k + \ell + 1)p = mp.$$

Comme $0 \leqslant k = \frac{u^2 - \varphi(u)}{p}$ et $0 \leqslant \ell = \frac{v^2 - \varphi(v)}{p}$, on peut encadrer m de la manière suivante :

$$\begin{aligned} 1 \leqslant m = k + \ell + 1 &\leqslant \frac{u^2 + v^2 - \varphi(u) - \varphi(v)}{p} + 1, \\ &\leqslant \frac{2(\frac{p-1}{2})^2 - 2 + p}{p} = \frac{(p-1)^2 - 4 + 2p}{2p} = \frac{p^2 - 3}{p} = p - \frac{3}{p} \leqslant p - 1, \end{aligned}$$

la dernière majoration provenant de l'hypothèse $p \geqslant 3$ (il n'y a rien de trop...). Cela établit le résultat attendu.

30. Avec les notations de la question précédente, le quaternion entier $\mu = ue + vI + J$ convient.

(a) Si m est pair, ce que l'on écrit $m = 2m'$ avec $m' \in \mathbb{N}^*$, alors $x^2 + y^2 + z^2 + t^2$ est pair. Comme n^2 possède la même parité que n pour tout $n \in \mathbb{Z}$, il faut qu'un nombre pair, disons k, des entiers x, y, z et t soit impair. On montre qu'une incompatibilité se produit pour chaque valeur de k.

— Si $k = 0$, il existe $\mu' \in \mathbb{G} \setminus \{0\}$ tel que $\mu = 2\mu'$, et alors $N(\mu) = 4N(\mu') = mp = 2m'p$, donc $N(q') = m'p$ avec $1 \leqslant m' < m$, donc m ne serait pas minimal.

— Si $k = 2$, on suppose que x et y sont impairs et que z et t sont pairs, ce que l'on écrit $z = 2z'$ et $t = 2t'$ avec z' et t' entiers (le raisonnement serait le même dans les autres cas). Alors $x' = \frac{x-y}{2}$ et $y' = \frac{x+y}{2}$ sont des entiers relatifs et on a $N(\mu) = 2x'^2 + 2y'^2 + 4z'^2 + 4t'^2 = 2m'p$ donc $x'^2 + y'^2 + 2z'^2 + 2t'^2 = m'p$ avec (x', y', z', t') quadruplet d'entiers non nul. Enfin, l'identité $2z'^2 + 2t'^2 = (z' - t') + (z' + t')^2$ conduit à

$$x'^2 + y'^2 + (z' - t') + (z' + t') = m'p,$$

où le quadruplet $(x', y', z' - t', z' + t') \in \mathbb{Z}^4$ est non nul, et $1 \leqslant m' < m$, donc m ne serait pas minimal.

— Si $k = 4$, les nombres $x' = \frac{x-y}{2}$, $y' = \frac{x+y}{2}$, $z' = \frac{z-t}{2}$ et $t' = \frac{z+t}{2}$ sont entiers et $\mu' := x'e + y'I + z'J + t'K \in \mathbb{G}$ est *non nul*. Comme $N(\mu) = 2x'^2 + 2y'^2 + 2z'^2 + 2t'^2 = 2m'p$, on a

$$N(\mu') = x'^2 + y'^2 + z'^2 + t'^2 = m'p.$$

avec $1 \leqslant m' < m$, donc m ne serait pas minimal.

(b) Si m est impair, le quaternion $\frac{\mu}{m}$ n'est pas un quaternion demi-entier, sinon $\frac{x}{m}$ serait de la forme $n + \frac{1}{2}$ avec $n \in \mathbb{Z}$, donc on aurait $2(x - mn) = m$, ce qui est impossible puisque m est impair. La question 28(c) montre qu'il existe un quaternion $\nu \in \mathbb{G}$ tel que $N(\frac{\mu}{m} - \nu) < 1$, ce qui entraîne

$$N(\mu - m\nu) < m^2.$$

(c) Comme la conjugaison est un morphisme de corps, comme $\mu\mu^* = N(\mu)e = mpe$, et comme $\mathbb{G}$ est stable par multiplication, on obtient

$$\mu' = \frac{1}{m}(\mu\mu^* - m\mu\nu^*) = pe + \mu\nu^* \in \mathbb{G}.$$

Si $\mu - m\nu$ était nul, on aurait $\nu = \frac{\mu}{m} \in \mathbb{G} \setminus \{0\}$ et $N(\mu) = m^2 N(\nu) = mp$, donc $mN(\nu) = p$. Le nombre entier m diviserait le nombre premier p avec $3 \leqslant m \leqslant p - 1$: c'est impossible. Comme $\mathbb{H} \setminus \{0\}$ est formé de matrices inversibles, on déduit, de la non nullité de μ et de $\mu - m\nu$, la non nullité de $\mu' = \frac{1}{m}\mu(\mu - m\nu)^*$.
Enfin,

$$N(\mu') = \frac{1}{m^2}N(\mu)N(\mu - m\nu) = \frac{pN(\mu - m\nu)}{m}$$

appartient à $\mathbb{N}$ car $\mu' \in \mathbb{G}$. Il en résulte que m divise le produit $pN(\mu - m\nu)$. Comme p est premier et $1 \leqslant m \leqslant p - 1$, il faut que m divise $N(\mu - m\nu)$. On pose $m' = \frac{N(\mu - m\nu)}{m}$, qui est strictement plus petit que m et qui vérifie $N(\mu') = m'p$, ce qui contredit la minimalité de m. Cela achève le raisonnement par l'absurde consistant à supposer $m > 1$: on a donc établi que $m = 1$, c'est-à-dire que, pour tout nombre premier p impair, il existe $(x, y, z, t) \in \mathbb{Z}^4$ tel que

$$x^2 + y^2 + z^2 + t^2 = p.$$

31. D'une part, $0 = 0^2 + 0^2 + 0^2$ et $1 = 1^2 + 0^2 + 0^2 + 0^2$.
D'autre part, soit un entier $n \geqslant 2$. Il se décompose en produit de facteurs premiers, qui s'écrivent tous comme somme de 4 carrés (question précédente pour les premiers impairs, et $2 = 1^2 + 1^1 + 0^2 + 0^2$). D'après la question 23, le produit de deux sommes de 4 carrés est une somme de 4 carrés, et cela se généralise aisément par récurrence sur n à un produit de n sommes de 4 carrés. On en déduit le théorème de Lagrange : tout nombre entier naturel est la somme de 4 carrés d'entiers.

Fin du corrigé.