Corrigé de Centrale PC 2014 maths 2

L'étude des structures algébriques n'est plus au programme de la filière PC depuis que ce problème a été posé. Il faut donc adapter ce corrigé (et l'énoncé correspondant) si on souhaite le donner en PC ou en PSI. Plus sagement, il faut sans doute se contenter de le poser en MP. Par ailleurs, on a choisi de résoudre les questions de nature algorithmique (partie IV) en Python.

Partie I – Symétries vectorielles

I.A Symétries et involutions

I.A.1 (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.

I.A.2 (a) Pour commencer, les sous-ensembles F et G sont des sous-espaces vectoriels de E en tant que noyaux d'endomorphismes de E.

Ensuite, soit $x \in E$. On cherche $(y, z) \in F \times G$ tel que $x = y + z$.

- Analyse. Si tel est le cas, alors $\frac{1}{2}(x + s(x)) = \frac{1}{2}(y + z + y - z) = y$ et $\frac{1}{2}(x - s(x)) = \frac{1}{2}(y + z - (y - z)) = z$.
- Synthèse. Soient $y = \frac{1}{2}(x+s(x))$ et $z = \frac{1}{2}(x-s(x))$. On a bien $x = y+z$, et comme $s \circ s = \mathrm{id}_E$, on en déduit que $s(y) = \frac{1}{2}(s(x) + x) = y$, donc $y \in F$, et $s(z) = \frac{1}{2}(s(x) - x) = -z$, donc $z \in G$.

On a démontré que

$$E = F \oplus G.$$

(b) On démontre que s est la symétrie vectorielle de E par rapport à F parallèlement à G. On sait déjà que F et G sont supplémentaires d'après la question précédente. Comme $F = \mathrm{Ker}(s - \mathrm{id}_E)$ et $G = \mathrm{Ker}(s + \mathrm{id}_E)$, on a, par linéarité,

$$\forall (y, z) \in F \times G, \quad s(y + z) = y - z,$$

ce qui achève de caractériser la symétrie annoncée.

I.B Couples de symétries qui anticommutent

I.B.1 (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

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

De la même manière, on 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 $G_s = t(F_s)$. Finalement,

$$t(F_s) = G_s \quad \text{et} \quad t(G_s) = F_s.$$

(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

$$\dim E = 2 \dim F_s \quad \text{est nécessairement paire.}$$

Remarque. — Il n'y a pas de question I.B.2

I.C H-systèmes

I.C.1 On va démontrer 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 donc $(\lambda_1, \dots, \lambda_p) \in \mathbb{C}^p$ 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 résultats obtenus, on trouve

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

On en déduit que $\lambda_j = 0$ (l'espace E n'est pas nul, donc id_E n'est pas la fonction nulle…), et ceci pour tout $j \in [\![1, p]\!]$, ce qui achève la preuve.

I.C.2 Dans cette question, on fixe une base $\mathcal{B}$ quelconque de E, et on utilise implicitement le fait que l'application $u \in \mathcal{L}(E) \mapsto \mathrm{mat}_{\mathcal{B}}(u) \in \mathcal{M}_n(\mathbb{C})$ 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.

I.C.3 Si $(S_1, \dots, S_p)$ est un H-système de E avec $p \geqslant 2$, alors il est clair que (S_1, S_2) est aussi un H-système de E. En appliquant la question I.B.1.b, on en déduit que n est pair.

Par contraposition, si n est impair, un éventuel H-système de E est de longueur 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 conclut que

$$n \text{ impair } \implies p(n) = 1.$$

I.D Majoration de p(n)

I.D.1 Attention : dans l'énoncé comme dans ce corrigé, les symboles i et i désignent respectivement un indice servant à décrire les H-systèmes, et un des deux nombres complexes dont le carré vaut -1. La différence entre les deux est d'ordre typographique : les indices sont en italiques, le nombre complexe en romain.

(a) On rappelle le théorème du cours suivant : 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 $R_j = \mathrm{i}\, U \circ S_j$.

(b) On vérifie les deux conditions (il est formellement incorrect de mener les calculs directement sur les endomorphismes U, S_i et S_j, car ce sont des fonctions définies sur E tout entier, alors que s_i n'est définie que sur E_0).

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

(c) D'après la question I.B.1b, la dimension de E_0 vaut $m = \frac{n}{2}$ et, comme $(s_1, \dots, s_p)$ 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 $(S_1, \dots, S_p, U, T)$ est un H-système maximal de E [c'est-à-dire de longueur $p(n)$], on a $p + 2 = p(n) = p(2m)$. On conclut que

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

I.D.2 On raisonne par récurrence sur $d \in \mathbb{N}$.

- Si $d = 0$, alors $n = m$ est impair, et on sait d'après la question I.C.3 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 $d + 1$.

I.E Construction de H-systèmes maximaux

I.E.1 On va montrer que $(A_1, \dots, A_{N+2})$ 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 $(A_1, \dots, A_{N+2})$ est un H-système de matrices complexes de taille $2n$.

I.E.2 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 I.D.2, 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 $(a_1, \dots, a_N)$ 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 $d + 1$.

I.E.3 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 I.E.1 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 II – Quaternions et sommes de carrés

II.A Le « corps » des quaternions

II.A.1 (a) On affirme sans justification que la dimension de $\mathcal{C}$ sur $\mathbb{R}$ 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 $\mathcal{C}$. Par ailleurs, il est aisé de vérifier que la famille (e, I, J, K) est libre, donc que c'est une base de $\mathbb{H}$.

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

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

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

II.A.2 Tout d'abord, $\det M(a, b) = a\bar{a} + b\bar{b} = |a|^2 + |b|^2$ est nul si et seulement si $a = b = 0$, c'est-à-dire dans le cas où $M(a, b)$ est la matrice nulle. Ceci prouve que

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

La partie $\mathbb{H}$ de $\mathrm{GL}_2(\mathbb{C})$ est non vide (elle contient $e = I_2$), stable par produit d'après la question II.A.1.c, et stable par inverse car on vérifie facilement grâce à la même question que

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

C'est donc un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$. Il n'est pas commutatif car $K = IJ \neq JI = -K$.

II.A.3 (a) On ne détaille pas les calculs. 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 $\mathcal{C} = \mathcal{M}_2(\mathbb{C})$.

II.B Conjugaison et normes

II.B.1 (a) Avec les notations de l'énoncé, si l'on pose $a = x + \mathrm{i}z$ et $b = y - \mathrm{i}t$,

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

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

On obtient bien le résultat attendu, en notant $\overline{A}$ la matrice dont les éléments sont les conjugués de ceux de A (on utilisera librement cette notation dans la suite du problème).

(b) On vérifie aisément que $\overline{A \times B} = \overline{A} \times \overline{B}$ pour toutes matrices complexes multipliables (cela résulte de ce que la conjugaison dans $\mathbb{C}$ est un morphisme pour l'addition et la multiplication dans $\mathbb{C}$). Par ailleurs, le cours affirme que la transposition est un antimorphisme multiplicatif, c'est-à-dire que ${}^t(A \times B) = {}^tB \times {}^tA$ toutes matrices complexes multipliables. Il en résulte que

$$\forall (q,r) \in \mathbb{H}^2, \quad (qr)^* = {}^t(\overline{qr}) = {}^t(\overline{q}\,\overline{r}) = {}^t\overline{r}\,{}^t\overline{q} = r^*q^*.$$

(c) Le résultat vient de ce que la conjugaison dans $\mathbb{C}$ et la transposition sont deux involutions, et aussi du fait qu'elles commutent, c'est-à-dire de l'égalité $\forall A \in \mathcal{M}_{n,p}(\mathbb{K})$, ${}^t\,\overline{A} = \overline{{}^tA}$. Alors

$$\forall q \in \mathbb{H}, \quad q^{**} = {}^t\Big(\overline{{}^t\overline{q}}\Big) = {}^t\big({}^t\overline{\overline{q}}\big) = {}^t\big({}^tq\big) = q.$$

Ensuite, 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 $\mathbb{H}$, donc une bijection de $\mathbb{H}$: c'est donc un automorphisme du $\mathbb{R}$–espace vectoriel $\mathbb{H}$.

Remarques. — C'est même 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 II.B.2.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 la question II.A.1.c montre que

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

On peut aussi mener un calcul à partir de la table et du H-système de la question II.A.3 :

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

On calcule ensuite $(qr)(qr)^*$ de deux manières : d'une part, la relation ci-dessus montre que ce produit vaut $N(qr)e$. D'autre part, la question II.B.1.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

$$\forall (q,r) \in \mathbb{H}^2, \quad N(qr) = N(q)N(r).$$

II.B.2 (a) Par linéarité de la trace, on obtient

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

(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

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

Comme la trace vérifie $\forall (A,B) \in (\mathcal{M}_n(\mathbb{K}))^2$, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, 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

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

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) :

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

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 III – Un théorème de Hurwitz

III.A Des formules pour n = 1, 2, 4, 8

III.A.1 Dans cette question, on omet les quantificateurs universels devant les nombres réels $x, y, z \ldots$

- 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 $Y = (x',y')$. Elle 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 (l'expression des composantes de $B_4(X,Y)$ le montre). Elle a été déduite de la loi de multiplication des quaternions

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

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

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

Elle 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, $(1^2 + 2^2 + 3^2 + 4^2)(5^2 + 6^2 + 7^2 + 8^2) = 60^2 + 12^2 + 30^2 + 24^2$.

III.A.2 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[1] 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 $\|Y\|^2 = N(c) + N(d)$

1. 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.

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 II.B.2.c.

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

Remarque. — 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 :

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

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/Identité_des_huit_carrés_de_Degen` :

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

III.B Le théorème de Hurwitz

III.B.1 (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 qui est le k-ième vecteur de la base canonique (il vérifie $\|Y\|=1$ et $y_iy_j=0$ sauf si $i=j=k$), on obtient

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

C'est la première relation (au carré et au nom de l'indice près).
Soient k et ℓ des entiers distincts entre 1 et n. En appliquant la formule ci-dessus à Y défini par $y_k=y_\ell=1$ et $y_i=0$ pour tout $i\notin\{k,\ell\}$, on obtient, compte-tenu de la symétrie du produit scalaire : $\|u_k(X)\|^2+\|u_\ell(X)\|^2+2(u_k(X)|u_\ell(X)) = 2\|X\|^2$. Comme on sait déjà que $\|u_i(X)\|^2=\|X\|^2$ pour tout i, on en déduit que

$$\forall X\in\mathbb{R}^n,\quad (u_k(X)|u_\ell(X)) = 0.$$

C'est la deuxième relation (aux noms des indices près).

• 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 $\mathrm{O}(\mathbb{R}^n)$, 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 k et ℓ des entiers distincts entre 1 et n. En appliquant relation $(u_k(X)|u_\ell(X))=0$ à $X+X'$ au lieu de X et en développant par bilinéarité, on obtient

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

(c) On sait qu'un endomorphisme est un automorphisme orthogonal si et seulement si sa matrice dans une base orthonormale est une matrice orthogonale. La base canonique étant orthonormale, on déduit de ce résultat du cours et de la question précédente que $A_k\in\mathrm{O}_n(\mathbb{R})$ pour tout k, c'est-à-dire que

$$\forall k\in[\![1,n]\!],\quad {}^tA_kA_k = I_n.$$

On sait aussi que, pour le produit scalaire canonique de $\mathbb{R}^n$, on a $\forall (X,X')\in(\mathbb{R}^n)^2$, $(X|X') = {}^tXX'$. La relation $\forall (X,X')\in(\mathbb{R}^n)^2$, $(u_k(X)|u_\ell(X'))+(u_\ell(X)|u_k(X'))=0$ se traduit donc par

$$\forall (X,X')\in(\mathbb{R}^n)^2,\quad {}^tX({}^tA_kA_\ell+{}^tA_\ell A_k)X' = 0.$$

Si v est l'endomorphisme de $\mathbb{R}^n$ de matrice ${}^tA_kA_\ell+{}^tA_\ell A_k$ dans la base canonique, la relation ci-dessus signifie que $\forall (X,X')\in(\mathbb{R}^n)^2$, $(X|v(X'))=0$. Or dans un espace préhilbertien réel, le seul vecteur orthogonal à tous les vecteurs X est le vecteur nul. On a donc $\forall X'\in\mathbb{R}^n$, $v(X')=0$, donc v est l'endomorphisme nul, donc ses matrices sont nulles, donc

$$\forall (k,\ell)\in[\![1,n]\!]^2,\quad k\neq\ell\Rightarrow {}^tA_kA_\ell+{}^tA_\ell A_k = 0.$$

III.B.2 (a)

- D'une part, en utilisant le fait que A_n et A_j sont orthogonales et la relation ${}^tA_nA_j + {}^tA_jA_n = 0$, on obtient

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

- D'autre part, 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 $p(n)$.

III.B.3 On étudie la fonction $f\colon x \in \mathbb{R}_+ \mapsto 2^{1-x}(x+1)$. Ell est dérivable avec $\forall x \in \mathbb{R}_+$, $f'(x) = 2^{1-x}(1-(x+1)\ln 2)$. Si $a = \frac{1}{\ln 2} - 1 \approx 0.4$, son tableau de variation est le suivant :

x	0		a		$+\infty$
$f'(x)$		$+$	0	$-$	
$f(x)$	2	$\nearrow$		$\searrow$	0

Comme $f(3) = 2^{1-3}(3+1) = 1$, on en déduit que $f(x) \geqslant 1 \iff x \leqslant 3$.
On passe ensuite au raisonnement principal, qui reprend les notations et les résultats de la partie I : si on écrit n sous la forme $2^d m$ avec $d \in \mathbb{N}$ et m entier naturel impair, alors $p(n) = 2d+1$. On en déduit les implications suivantes :

$$n-1 \leqslant p(n) \Rightarrow 2^d m \leqslant 2d+2 \Rightarrow m \leqslant f(d) \Rightarrow 1 \leqslant f(d) \Rightarrow d \in \{0,1,2,3\}.$$

Par conséquent, $m \leqslant \max(f(0), f(1), f(2), f(2)) = 2$. Comme m est impair, il ne reste qu'une seule valeur possible : $m = 1$. Dans ce cas, $n = 2^d$ avec $d \in \{0,1,2,3\}$, donc

$$n \in \{1,2,4,8\}.$$

Ceci constitue 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 IV – Représentation des parties de $\mathbb{N}$ et quelques algorithmes

IV.A La commande `print(carres(10))` donne $[1,1,0,0,1,0,0,0,0,1,0]$.

```
def carres(N):
    C = (N+1)*[0]
    i = 0
    while i**2 <= N:
        C[i**2] = 1
        i = i+1
    return(C)
```

IV.B La commande `print(Eratosthene(10))` renvoie $[1,0,1,1,0,1,0,1,0,0,0]$.

```
def Eratosthene(N):
    C = (N+1)*[1]
    C[1] = 0
    i = 2
    while i <= N:
        multiple = 2*i
        while multiple <= N:
            C[multiple] = 0
            multiple = multiple+i
        i = i+1
    return(C)
```

IV.C La commande `print(somme(carres(10),Eratosthene(10),10))` renvoie $[1,1,1,1,1,1,1,1,1,1,0]$, ce qui signifie que les nombres entiers de 0 à 9 sont tous la somme d'un carré et d'un nombre premier (ou sont eux-mêmes des carrés), mais pas 10.

```
def somme(A,B,N):
    C = (N+1)*[0]
    for i in range(N+1):
        for j in range(N-i+1):
            if A[i]*B[j] == 1:
                C[i+j] = 1
    return(C)
```

IV.D La commande `print(quatrecarres(1000))` renvoie `True` : tous les entiers plus petits que 1000 sont des sommes de 4 carrés d'entiers.

```
def quatrecarres(N):
    C = carres(N)
    resultat = carres(N)
    for k in range(3):
        resultat = somme(resultat,C,N)
    test = 1
    for i in range(N+1):
        test = test*resultat[i]
    if test == 1:
        return(True)
    else:
        return(False)
```

Partie V – Sommes de carrés dans un anneau

V.A 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

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

D'un point de vue typographique, le passage de $\mathbb{R}^p$ à A^p est totalement transparent… 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

$$C_p(A) \text{ est stable par la multiplication.}$$

V.B Le théorème des quatre carrés

V.B.1 (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 III.A.1 (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) On commence par justifier le résultat suivant.

Lemme. — Pour tout nombre réel u, il existe un entier relatif u' distant de u de moins de $\frac{1}{2}$:

$$\forall u \in \mathbb{R}, \quad \exists m \in \mathbb{Z}, \quad |u - u'| \leqslant \frac{1}{2}.$$

On pose pour cela $n = \lfloor u \rfloor \in \mathbb{Z}$ (partie entière de u). Comme $n \leqslant u < n+1$, on pose $u' = n$ si $u \leqslant n + \frac{1}{2}$, et $u' = n+1$ sinon ; il convient.

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) Dans le lemme ci-dessus, on remarque que si $u \neq n + \frac{1}{2}$, alors $|u-u'| < \frac{1}{2}$. Par conséquent, si l'une des composantes x, y, z, t de q 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.

V.B.2 (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.

V.B.3 Avec les notations de la question précédente, le quaternion entier $\mu = ue + vI + 1\,J + 0\,K$ 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 V.B.1.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

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

V.B.4 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 III.A.1, 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.

Bibliographie

Les nombres : Leur histoire, leur place et leur rôle de l'Antiquité aux recherches actuelles, Ouvrage collectif, Vuibert, 1998.