Devoir Maison n° 7 : corrigé

MPSI Lycée Camille Jullian

27 janvier 2025

Problème : autour des quaternions.

I. Le groupe des quaternions, vision matricielle.

1. On calcule sans difficulté $I^2 = J^2 = K^2 = -\mathbf{1}$ (avec les merveilleuses notations imposées), $IJ = K$, donc $IJK = K^2 = -\mathbf{1}$, $JI = -K$ et enfin $JK = I$.
2. Si on ne veut pas trop se fatiguer, c'est un sous-groupe du groupe multiplicatif $GL_2(\mathbb{C})$ constitué des matrices inversibles de $\mathcal{M}_2(\mathbb{C})$. En effet, il contient la matrice identité $\mathbf{1}$, est stable par produit (on en a calculé la plupart à la question 1, les résultats des quelques produits restants seront de toute façon donnés dans le tableau qui va suivre). Et surtout, les inverses de chaque élément appartiennent bien à l'ensemble puisque I, J et K ont pour inverse leur opposé d'après les calculs de carrés effectués ci-dessus. Bien entendu, ce groupe n'est absolument pas commutatif, puisqu'on a déjà vu que IJ et JI donnent des résultats opposé. Le tableau tant attendu (on donne dans la case le résultat du produit de l'élément de la ligne, à gauche, par celui de la colonne, à droite) :

$\times$	$\mathbf{1}$	$-\mathbf{1}$	I	$-I$	J	$-J$	K	$-K$
$\mathbf{1}$	$\mathbf{1}$	$-\mathbf{1}$	I	$-I$	J	$-J$	K	$-K$
$-\mathbf{1}$	$-\mathbf{1}$	$\mathbf{1}$	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	$-\mathbf{1}$	$\mathbf{1}$	K	$-K$	$-J$	J
$-I$	$-I$	I	$\mathbf{1}$	$-\mathbf{1}$	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	$-\mathbf{1}$	$\mathbf{1}$	I	$-I$
$-J$	$-J$	J	K	$-K$	$\mathbf{1}$	$-\mathbf{1}$	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	$-\mathbf{1}$	$\mathbf{1}$
$-K$	$-K$	K	$-J$	J	I	$-I$	$\mathbf{1}$	$-\mathbf{1}$

3. En exploitant l'indication de l'énoncé, on a :
   - un seul sous-groupe à un élément, constitué de $\mathbf{1}$.
   - un seul sous-groupe à deux élements : $\{\mathbf{1}, -\mathbf{1}\}$ (en effet, un tel sous-groupe contient nécessairement l'élément neutre, et un deuxième élément dont le carré doit être égal à $\mathbf{1}$, ce qui n'est le cas que pour $-\mathbf{1}$).
   - trois sous-groupes à quatre éléments : $\{\mathbf{1}, -\mathbf{1}, I, -I\}$, $\{\mathbf{1}, -\mathbf{1}, J, -J\}$ et $\{\mathbf{1}, -\mathbf{1}, K, -K\}$ (si un tel sous-groupe contient l'un des éléments I, J, ou K, il contient son carré $-\mathbf{1}$, et son opposé obtenue en le multipliant par $-\mathbf{1}$, ce qui fait déjà quatre éléments, on ne peut donc pas en ajouter d'autres, et les trois ensembles donnés sont bien stables par produit et passage à l'inverse).
   - évidemment, un sous-groupe à huit éléments, $\mathbb{H}_8$ tout entier.
4. On doit vérifier les choses suivantes :
   - $\mathbb{H}$ contient la matrice nulle, ce qui est le cas pour $a = b = c = d = 0$.
   - $\mathbb{H}$ est stable par passage à l'opposé, ce qui est trivial (on remplace simplement a, b, c et d par leurs opposés).

- $\mathbb{H}$ est stable par somme, ce qui est également trivial : $(a\mathbf{1}+bI+cJ+dK)+(a'\mathbf{1}+b'I+c'J+d'K)=(a+a')\mathbf{1}+(b+b')I+(c+c')J+(d+d')K\in\mathbb{H}$.
- la stabilité par produit est en fait également triviale, le calcul est juste très pénible : à l'aide des produits calculés pour obtenir la loi de groupe de $\mathbb{H}_8$, $(a\mathbf{1}+bI+cJ+dK)\times(a'\mathbf{1}+b'I+c'J+d'K)=aa'+ab'I+ac'J+ad'K+ba'I-bb'\mathbf{1}+bc'K-bd'J+ca'J-cb'K-cc'\mathbf{1}+cd'I+da'K+db'J-dc'I-dd'\mathbf{1}=(aa'-bb'-cc'-dd')\mathbf{1}+(ab'+ba'+cd'-dc')I+(ac'-bd'+ca'+db')J+(ad'+bc'-cb'+da')K\in\mathbb{H}$.

II. L'algèbre des quaternions.

1. Puisque $ij=-ji$, on peut par exemple constater que $(i+j)^2=i^2+ij+ji+j^2=i^2+j^2=-1-1=-2$. On peut donc prendre $\frac{1}{\sqrt{2}}(i+j)$ comme « racine carrée » de -1 (il y en a plein d'autres).
2. D'après l'horrible formule obtenue à la dernière question de la première partie, si $x\in\mathbb{R}$, alors $x\times(a+bi+cj+dk)=xa+xbi+xcj+xdk$, et de même pour le produit dans l'autre sens, donc x commute effectivement avec tout le monde. Supposons maintenant que $q=a+bi+cj+dk$ ne soit **pas** réel. Alors on a par exemple $b\neq 0$, et si c'est le cas q ne commute pas avec j : $qj=-c-di+aj+bk$ ne peut pas être égal à $jq=-c+di+aj-bk$. Remaqu'on d'ailleurs que q ne commutera pas non plus avec j si $d\neq 0$. Enfin, si $c\neq 0$, c'est avec i ou k que q ne commutera pas (calcule extrêmement similaire). Les seuls quaternions pouvant commuter avec tout le monde sont donc les réels.
3. La première propriété est complètement triviale. la deuxième aussi : $a-bi-cj-dk+a'-b'i-c'i-d'k=a+a'-(b+b')i-(c+c')j-(d+d')k$. C'est nettement moins sympathique pour le produit : avec les notations évidentes, $\overline{q'}\times\overline{q}=(a'-b'i-c'j-d'k)(a-bi-cj-dk)=aa'-ba'i-ca'j-da'k-ab'i-bb'+cb'k-db'j-ac'j-bc'k-cc'+dc'i-ad'k+bd'j-cd'i-dd'=(aa'-bb'-cc'-dd')+(dc'-ba'-ab'-cd')i+(bd'-db'-ca'-ac')j+(cb'-da'-bc'-ad')k=\overline{qq'}$.
4. Encore un calcul passionnant : $q\times\overline{q}=(a+bi+cj+dk)(a-bi-cj-dk)=a^2-abi-acj-adk+abi+b^2+bck+bdj+acj-bck+c^2-cdi+adk-bdj+cdi+d^2=a^2+b^2+c^2+d^2\in\mathbb{R}^+$. Le calcul dans l'autre sens est identique (on peut aussi utiliser le fait que le conjugué de $\overline{q}$ est q et simplement appliquer la formule obtenue à $\overline{q}$, ce qui donne le même résultat $a^2+b^2+c^2+d^2$).
5. Le calcul précédent montre que $|\overline{q}|=|q|$. Pour l'autre formule, on peut ruser : $|qq'|=\sqrt{qq'\overline{qq'}}=\sqrt{q(q'\overline{q'})\overline{q}}=\sqrt{|q'|^2q\overline{q}}=\sqrt{|q'|^2|q|^2}=|q|\times|q'|$. La seule chose qu'on a fait commuter dans ce calcul est le réel $|q'|^2$, ce qu'on a le droit de faire.
6. Par définition, $q\times\overline{q}=|q|^2$. Comme le membre de droite de cette égalité est un réel non nul (car $q\neq 0\Rightarrow a^2+b^2+c^2+d^2\neq 0$), on peut le faire passer de l'autre côté (on a le droit de diviser des quaternions par des réels sans ambiguîté, par contre une division de quaternions n'a aucun sens à cause de la non cummutativité du produit) : $q\times\frac{\overline{q}}{|q|^2}=1$. De même, $\frac{\overline{q}}{|q|^2}\times q=1$, donc q est inversible et $q^{-1}=\frac{\overline{q}}{|q|^2}$. C'est exactement la même formule que pour les nombres complexes.
7. On sait déjà que l'ensemble $\mathbb{H}$ est muni de deux lci associatives (non, il n'y a rien à prouver, rappelons qu'initialement les opérations sont simplement issues de la somme et du produit matriciel dont on connaît déjà l'associativité !). L'addition est commutative, 0 est élément neutre pour la somme et 1 pour le produit (pour cette dernière affirmation vérifier la formule explicite obtenue pour le produit des quaternions). Tout quaternion $q=a+bi+cj+dk$ admet un opposé qui est simplement $-q=-a-bi-cj-ck$, et on vient de prouver que tout quaternion non nul est inversible. On a bien tous les élements pour affirmer que $\mathbb{H}$ est un corps non commutatif.

III. Entiers d'Hamilton.

1. C'est un sous-ensemble de $\mathbb{H}$ qui contient les deux neutres 0 et 1. Il est par ailleurs stable par passage à l'opposé de façon évidente (si les quatre coefficients a, b, c et d sont entiers, leurs opposés aussi, et s'ils sont demi-entiers de même), et stable par somme sans difficulté (si les deux quaternions sont tous les deux « demi-entiers » ou tous les deux « vraiment entiers », leur somme sera entière, et si un seul des deux est demi-entier, on conservera une somme demi-entière). Le calcul est nettement plus pénible pour le produit, distinguons plusieurs cas, en notant $q = a + bi + cj + dk$ et $q' = a' + b'i + c'j + d'k$:

   - si q et q' ont des coordonnées entières, celles de qq' seront entières en reprenant la formule explicite de la dernière question de la partie I.
   - si q a des coordonnées entières mais q' des coordonnées demi-entières, on pose $e' = a' + \frac{1}{2}$, $f' = b' + \frac{1}{2}$, $g' = c' + \frac{1}{2}$ et $h' = d' + \frac{1}{2}$ (qui sont donc tous les quatre entiers), puis on calcule la première coordonnée de qq' : $aa' - bb' - cc' - dd' = ae' - bf' - cg' - dh' - \frac{a-b-c-d}{2}$. Ce nombre est entier **ou** demi-entier selon la parité de l'entier $a-b-c-d$. Un calcul quasi-identique montre qu'il en sera de même pour les trois dernières coordonnées du produit, cette fois-ci en fonction de la parité des entiers $a+b+c-d$, $a-b+c+d$ et $a+b-c+d$. Il faut donc que les quatre entiers $a-b-c-d$, $a+b+c-d$, $a-b+c+d$ et $a+b-c+d$ aient tous la même partié pour avoir $hh' \in \mathbb{Z}_{\mathbb{H}}$. Or, c'est le cas puisque leurs différences sont toutes des doubles d'entiers, donc paires (par exemple $(a+b+c-d)-(a-b+c+d) = 2(b-d)$).
   - le cas où c'est q' qui est à coordonnées entières et q à coordonnées demi-entières se traite exactement de la même façon que le précédent.
   - enfin, si q et q' sont tous les deux à coordonnées demi-entières, avec des notations identiques à celle du calcul précédent, $aa'-bb'-cc'-dd' = \left(e-\frac{1}{2}\right)\left(e'-\frac{1}{2}\right) - \left(f-\frac{1}{2}\right)\left(f'-\frac{1}{2}\right) - \left(g-\frac{1}{2}\right)\left(g'-\frac{1}{2}\right) - \left(h-\frac{1}{2}\right)\left(h'-\frac{1}{2}\right) = ee' - ff' - gg' - hh' - \frac{e-f-g-h}{2} - \frac{e'-f'-g'-h'}{2} + 1$. Cette première coordonnée du produit est entièr ou demi-entièr selon la parité de $e-f-g-h+e'-f'-g'-h'$. À part le fait qu'on fait intervenir encore plus de variables que précédemment, le principe est le même, les trois autres coordonnées feront intervenir des entiers de parité identiques (car ayant des différences avec celui-ci qui sont des doubles d'entiers), ce qui prouve qu'on aura toujours $qq' \in \mathbb{Z}_{\mathbb{H}}$.

2. L'énoncé était légèrement buggué pour cette question, q doit bien sûr appartenir à $\mathbb{Z}_{\mathbb{H}}$ pour que la question ait un sens, et surtout c'est $|q|^2$ qui est entier naturel et pas $|q|$. Si q est à coordonnées entières, la propriété est évidente ($|q|^2 = a^2 + b^2 + c^2 + d^2$ est une somme d'entiers naturels). Et s'il est à coordonnées demi-entières, on reprend les notations de la question précédente pour calculer $\left(e-\frac{1}{2}\right)^2 + \left(f-\frac{1}{2}\right)^2 + \left(g-\frac{1}{2}\right)^2 + \left(h-\frac{1}{2}\right)^2 = e^2 + f^2 + g^2 + h^2 - e - f - g - h + 1$ qui est un entier naturel (le résultat ne peut pas être négatif puisque, sous sa forme initiale, il est égal à la somme de quatre carrés de nombres réels).
3. Le carré de la norme d'un entier de Hamilton étant entière, on doit donc avoir $|q|^2 \in \mathbb{N}$ et $|q^{-1}|^2 \in \mathbb{N}$. Or, $|q| \times |q^{-1}| = |1| = 1$. Un produit de deux entiers naturels qui est égal à 1, ça ne peut se produire que si $|q|^2 = |q^{-1}|^2 = 1$, donc $|q| = 1$ (la norme étant toujours un réel positif, rappelons-le en passant). Réciproquement, si $|q| = 1$, on a tout simplement $q^{-1} = \overline{q}$ (cf question $II.6$) qui est aussi un entier de Hamilton.
4. On distingue deux possibilités :

   - si q a des coordonnées entières, elles doivent vérifier d'après la question précédente $a^2 + b^2 + c^2 + d^2 = 1$, ce qui n'est possible que si trois des quatre coordonnées sont nulles. On

trouve donc huit premières unités : ± 1, $\pm i$, $\pm j$ et $\pm k$.

- si q a des coordonnées demi-entières, le carré de ces coordonnées sera de la forme $\frac{p}{4}$, avec p entier naturel. La seule façon d'avoir une somme de ces carrés égale à 1 est que chacun de ces quatre carrés soit égal à $\frac{1}{4}$, donc chaque coordonnée égale à $\pm\frac{1}{2}$. Cela nous donne les seize unités manquantes : tous les quaternions de la forme $\pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$ conviennent (et il y en a bien $2^4 = 16$, on choisit le signe de chaque coordonnée indépendamment les unes des autres).

5. (a) Soit donc q un quaternion quelconque, si on considère indépendamment chacune des coordonnées de q, elle est à une distance au maximum $\frac{1}{4}$ de l'entier ou du demi-entier le plus proche (par exemple si $a = \frac{1}{4}$, a est à distance $\frac{1}{4}$ à la fois de l'entier 0 et du demi-entier $\frac{1}{2}$. Si les quatres « plus proches » sont tous entiers, ou tous demi-entiers, on les regroupe pour donner un entier de Hamilton qui vérifie $|q-e|^2 \leqslant 4 \times \left(\frac{1}{4}\right)^2 = \frac{1}{4}$. Ce sera par exemple le cas de $q = \frac{1}{4} - \frac{1}{4}i + \frac{5}{4}j - \frac{5}{4}k$, pour lequel $e = j - k$ convient. Mais s'il y a un mélange d'entiers et de demi-entiers parmi les plus proches, c'est un peu plus compliqué. Le pire cas est celui où deux plus proches sont entiers et les deux autres demi-entiers, par exemple lorsque $q = \frac{1}{5} - \frac{1}{5}i + \frac{3}{5}j - \frac{3}{5}k$ (les plus proches valant ici respectivement 0, 0, $\frac{1}{2}$ et $-\frac{1}{2}$). Mais même dans ce cas, en prenant les quatre **entiers** les plus proches des coordonnées, la distance entre les coordonnées et ces entiers vaut au maximum $\frac{1}{4}$ pour celles qui avaient déjà un plus proche qui était entier, mais $\frac{1}{2}$ pour celles qui avaient un plus proche demi-entier. Dans notre exemple, on prendra ainsi $e = j - k$. On peut alors majorer $|q-e|^2$ par $2 \times \frac{1}{16} + 2 \times \frac{1}{4} = \frac{5}{8}$, ce qui prouve la propriété demandée.

   (b) On applique la propriété précédente à $e_1 \times e_2^{-1}$ pour trouver un entier de Hamilton q tel que $|e_1 e_2^{-1} - q| \leqslant \frac{5}{8} < 1$. On pose alors $r = e_1 - qe_2$ (de façon à bien avoir $e_1 = qe_2 + r$), et on a $r \times e_2^{-1} = e_1 e_2^{-1} - q$, donc $|r \times e_2^{-1}| < 1$, donc $|r| \times |e_2^{-1}| < 1$, d'où $|r| < |e_2|$ d'après les propriétés de la norme. Le couple (q, r) vérifie donc les hypothèses demandées. Le couple n'a aucune raison d'être unique. Il suffit de trouver e_1 et e_2 pour lesquels le produit $e_1 \times e_2^{-1}$ est à une distance strictement inférieure à 1 de deux entiers de Hamilton distincts. Par exemple, si $e_2 = 1 + i + j + k$, alors $e_2^{-1} = \frac{\overline{e_2}}{|e_2|^2} = \frac{1 - i - j - k}{4}$. On prend bêtement $e_1 = 1$, et l'inverse qu'on vient de calculer est à distance $\frac{1}{4}$ de 0, mais aussi de $\frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j - \frac{1}{2}k$, ce qui permet de construire deux divisions distinctes de e_1 par e_2 (je vous laisse finir le détail des calculs si vous êtes motivés).

6. Déjà, un nombre qui n'est pas premier au sens classique du terme n'a aucune chance d'être premier au sens de Hamilton (par exemple $6 = 2 \times 3$, et ni 2 ni 3 ne sont des unités de Hamilton, donc 6 n'est pas premier). Il ne reste donc qu'à vérifier les nombres premiers inférieurs à 20, ce qui est légèrement laborieux (non, il n'y a pas à ma connaissance de méthode évidente regroupant tous les cas) :

   - on peut factoriser 2 sous la forme $2 = (1+i)(1-i)$, donc 2 n'est pas premier (même pas besoin de quaternions ici, les complexes classiques suffisent).
   - $3 = (1+i+j)(1-i-j)$, puisqu'en notant $q = 1+i+j$, $q \times \overline{q} = |q|^2 = 1+1+1 = 3$.

- $5 = (2+i)(2-i)$, le lecteur attentif remarquant que tout entier qui est somme de deux carrés va être traité de la même façon.
- $7 = (2+i+j+k)(2-i-j-k)$, encore une histoire d'utilisation de conjugué.
- $11 = (3+i+j)(3-i-j)$.
- $13 = (3-2i)(3+2i)$.
- $17 = (4+i)(4-i)$.
- $19 = (3+3i+j)(3-3i-j)$ (plein d'autres possibilités ici).

On remarquera qu'on n'a même pas eu besoin d'exploiter les demi-entiers pour trouver les décompositions. En fait, un théorème classique connu sous le nom de théorème des quatre carrés de Lagrange stipule que tout entier naturel peut s'écrire comme somme de quatre carrés d'entiers, ce qui prouve qu'aucun entier autre que 1 ne peut être un entier premier de Hamilton. D'ailleurs, la démonstration la plus classique du théorème utilise... les quaternions !