Devoir sur table n° 3

(corrigé)

Table des matières

1 Commentaires

Ce devoir est une compilation des sujets suivants :

— Mathématiques I commune aux trois ENS, année 2007, filière MP (pour la partie II) ;

— Mathématiques I du concours X-ENS, année 2023, filière MP (pour les deux autres parties).

J'ai retiré tout ce qui ne concerne pas le théorème des quatre carrés dans la première source d'inspiration, et tout ce qui a attrait à la topologie et la géométrie dans la seconde.

Le devoir parcourt deux des trois propriétés les plus souvent étudiées lorsqu'on parle de l'ensemble $\mathbb{H}$ des quaternions :

— il est en un certain sens le « plus petit » corps non commutatif contenant $\mathbb{R}$, et le corps servant de modèle à beaucoup d'autres corps non commutatifs : le livre *Les corps non commutatifs* d'André Blanchard est la référence sur ce sujet ;

— il permet de démontrer le théorème des quatre carrés, ce qui est une conséquence remarquable puisque son énoncé semble, *a priori*, se restreindre à l'ensemble des entiers naturels ;

— il permet d'imiter la géométrie dans le plan complexe : en effet, grâce aux calculs avec les quaternions, on peut faire de la géométrie en dimension 4... et 3 !

Noter qu'en classes préparatoires, un corps est par définition commutatif, donc parler de corps non commutatif peut surprendre. Cette hypothèse est rajoutée dans le programme pour vous éviter des contorsions (et peut-être pour s'adapter à l'usage anglo-saxon...), car les corps non commutatifs sont pleins de subtilités échappant même aux mathématiciens rompus. Un exemple de subtilité : on ne peut pas factoriser un polynôme à coefficients dans un corps non commutatif même en connaissant toutes ses racines, et cela implique notamment qu'il peut avoir plus de racines que son degré. Par exemple le polynôme $X^2 + 1_H \in \mathbb{H}[X]$ admet pour racines distinctes : $\pm I$, $\pm J$, $\pm K$. Cela dépasse très largement son degré.

Le « plus petit corps » non commutatif contenant $\mathbb{R}$. C'est un théorème dû à Frobenius : les seuls corps contenant $\mathbb{R}$ et étant de dimension finie sur $\mathbb{R}$ (le sujet du devoir affaiblit cette condition) sont $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$. Si l'on décrète qu'un corps doit être commutatif, on remarque que le seul corps non trivial à contenir $\mathbb{R}$ tout en étant de dimension finie est $\mathbb{C}$. En fait, cela pourrait être démontré sans effort dès que l'on sait que $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$. En effet, si K est un corps commutatif contenant $\mathbb{R}$, et de dimension finie sur $\mathbb{R}$, alors pour tout $x \in K$, le corps $\mathbb{R}(x)$ – le plus petit corps contenant $\mathbb{R}$ et x – est de dimension finie sur $\mathbb{R}$ puisqu'il est inclus dans K qui est de dimension finie, donc grâce à un résultat classique (présent dans vos feuilles d'exercices du chapitre IV) on sait que x est annulé par un polynôme réel non nul. Or les racines des polynômes réels (non nuls) sont des nombres complexes, donc : $x \in \mathbb{C}$. Ceci vaut pour tout $x \in K$, d'où : $\mathbb{R} \subseteq K \subseteq \mathbb{C}$, et un argument dimensionnel implique : $K \in \{\mathbb{R}, \mathbb{C}\}$. C'est très classique et c'est ainsi qu'on raisonne au début de la troisième partie. C'est donc le cas non commutatif qui donne tout son mérite au théorème de Frobenius.

Il est intéressant de remarquer qu'un corps vérifiant les hypothèses de son théorème ne peut pas être de dimension 3 : c'est à mettre en rapport avec l'ambition originelle de Hamilton (voir plus bas)

et le théorème des quatre carrés qui n'a pas d'analogue avec trois carrés : on ne pouvait pas imiter la stratégie du théorème des quatre carrés en introduisant un surcorps de dimension 3.

Le raisonnement de Frobenius est basé sur le *principe de conjugaison*, déjà mentionné en plusieurs endroits (commentaires du devoir des vacances, ou dans le cours du chapitre III avec S_n). À savoir : le premier objectif de Frobenius est de montrer que si K est un corps contenant $\mathbb{R}$ (et de dimension finie sur $\mathbb{R}$), et différent de $\mathbb{R}$, alors il contient au moins une racine carrée de -1 ; c'est la partie facile si j'ose dire, puisqu'elle découle de manipulations algébriques bêtes et méchantes (on montre qu'il y a au moins une racine carrée de nombre strictement négatif, et après bricolage cela donne une racine carrée de -1). Soit K est de dimension 2, et dans ce cas le morphisme envoyant $i \in \mathbb{C}$ sur une racine carrée de -1 dans K est un morphisme, injectif comme tout morphisme de corps, et bijectif par égalité dimensionnelle, donc K est isomorphe à $\mathbb{C}$; soit K n'est pas de dimension 2, et on veut montrer qu'il existe d'autres racines carrées de -1, qui jouent le rôle de $\pm j$ et $\pm k$ dans $\mathbb{H}$. Si l'on y parvient, alors il n'est plus très difficile de montrer que K et $\mathbb{H}$ sont isomorphes.

L'idée de Frobenius est de chercher les éléments dans K qui devraient jouer l'analogue de j et k. Trouver un seul des deux suffit : si l'on trouve l'analogue de j, il suffit d'utiliser la relation $k = ij$ pour avoir l'analogue du dernier élément. On trouve l'analogue de j par conjugaison : cela tient au fait que dans $\mathbb{H}$, les éléments i et j anti-commutent au sens où l'on a : $ij = -ji$, ou encore : $iji^{-1} = j$. L'élément j est donc un point fixe de l'automorphisme intérieur $x \mapsto ixi^{-1}$, et c'est ainsi que par analogie, on étudie les points fixes de l'automorphisme semblable dans K pour trouver j parmi ses points fixes (le problème fait étudier $x \mapsto ixi$ à la place, mais il n'y a pas de raison conceptuelle particulière).

Le théorème des quatre carrés. La stratégie derrière le théorème des quatre carrés de Lagrange s'inspire de raisonnements arithmétiques antérieurs : on put déjà constater le succès du recours à des anneaux plus grands que $\mathbb{Z}$ pour résoudre des problèmes (résolution de $x^2 + y^2 = z^2$ en passant par l'équation $(x + iy)(x - iy) = z^2$ dans $\mathbb{Z}[i]$, ou de $x^3 + y^3 = z^3$ en passant par l'équation $(x + y)(x + jy)(x + j^2y) = z^3$ dans $\mathbb{Z}[j]$: idée due à Euler). Ce genre d'idée permet aussi d'obtenir le théorème des deux carrés de Fermat, en vérité démontré par Euler, et plus tard par d'autres mathématiciens *via* d'autres démonstrations : on montre que les nombres premiers $p > 2$ pouvant s'écrire sous la forme $p = x^2 + y^2$, avec x et y entiers, sont forcément congrus à 1 modulo 4 et réciproquement (le sens direct est facile, le sens réciproque est très savant et nécessite de manière plus ou moins implicite de raisonner dans $\mathbb{Z}[i]$), et on en déduit ensuite à quelle condition nécessaire et suffisante un entier naturel non nul s'écrit comme une somme de deux carrés. La clé est la propriété de stabilité par multiplication, provenant de l'identité :

$$\forall (a, b, c, d) \in \mathbb{Z}^4, \quad (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

On en déduit que si n est un produit de nombres premiers congrus à 1 modulo 4 et de carrés de nombres premiers congrus à 3 modulo 4, alors n s'écrit comme une somme de deux carrés.

D'où sort cette identité monstrueuse ? La trouve-t-on par un coup de chance, et doit-on la retenir bêtement par cœur ? Je ne sais pas comment l'a trouvée Diophante, mais en tout cas je sais comment le mathématicien moderne peut la retrouver aisément et s'en inspirer ailleurs : en utilisant le fait que $a^2 + b^2$ soit le module au carré de $a + ib \in \mathbb{C}$. L'identité ci-dessus découle alors trivialement de la multiplicativité du module :

$$(a^2+b^2)(c^2+d^2) = |a+ib|^2 \cdot |c+id|^2 = |(a+ib)(c+id)|^2 = |(ac-bd)+i(ad+bc)|^2 = (ac-bd)^2+(ad+bc)^2.$$

Si l'on veut généraliser cette identité en vue de démontrer un théorème des trois carrés (ou quatre, sachant qu'il ne sert à rien de chercher un théorème des cinq carrés ou plus, au vu de ce qu'on démontre dans ce sujet : pourquoi ?), c'est possible à moindre frais dès lors que nous avons un analogue des nombres complexes et du module au carré, préservant la propriété de multiplicativité. Rien de plus

facile... Si l'on connaît les quaternions. Si, pour tout quaternion $a+bi+cj+dk$, on considère la multiplication par son conjugué $a-bi-cj-dk$, on obtient une fonction multiplicative à valeurs réelles, qui joue le même rôle que le module au carré d'un nombre complexe :

$$(a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2,$$

et sa propriété de multiplicativité permet de montrer que l'ensemble des entiers s'écrivant comme somme de quatre carrés est stable par multiplication :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) = {}& (ap+bq+cr+ds)^2 + (aq-bp-cs+dr)^2 \\ & + (ar+bs-cp-dq)^2 + (as-br+cq-dp)^2.\end{aligned}$$

Notons qu'on a mentionné ci-dessus, en parlant du théorème de Frobenius, qu'on ne pouvait pas trouver de surcorps de $\mathbb{R}$ de dimension 3. À cet égard, on comprend qu'on ne peut pas étudier les sommes de trois carrés par les mêmes arguments : un produit de deux sommes de trois carrés n'est pas forcément une somme de trois carrés :

$$(a^2+b^2+c^2)(p^2+q^2+r^2) = (ap+bq+cr)^2 + (aq-bp)^2 + (ar-cp)^2 + (br-cq)^2.$$

C'est donc une étude difficile (mais qui a une réponse définitive), qui nécessite une compréhension fine des *formes quadratiques* sur $\mathbb{Q}$.

En résumé : l'ensemble des nombres s'écrivant comme somme de quatre entiers au carré est stable par multiplication. Or on sait que tout entier naturel non nul est produit de nombres premiers. Ainsi, pour savoir quels entiers sont somme de quatre carrés, il suffit de traiter la question pour les nombres premiers : c'est l'objet de la majorité des questions de la deuxième partie, où l'on démontre que *tout* nombre premier peut s'écrire ainsi ! La démonstration repose sur le principe de descente infinie : on montre qu'il existe un entier m tel que mp soit somme de quatre carrés (on y parvient par du dénombrement modulo p, illustrant par ailleurs un intérêt de raisonner dans $\mathbb{Z}/p\mathbb{Z}$: faire de la combinatoire dans un ensemble fini), et on donne un algorithme permettant de diminuer la taille de l'entier m tant qu'il est strictement supérieur à 1. L'algorithme doit s'arrêter sinon on aurait une contradiction, si bien qu'on finit par rencontrer le cas $m=1$.

On montre en passant que l'équation $\bar{x}^2+\bar{y}^2=-\bar{1}$ admet toujours une solution dans $\mathbb{Z}/p\mathbb{Z}$. En fait, on a mieux : l'application $(\bar{x},\bar{y}) \mapsto \bar{a}\bar{x}^2+\bar{b}\bar{y}^2$ est surjective de $(\mathbb{Z}/p\mathbb{Z})^2$ dans $\mathbb{Z}/p\mathbb{Z}$ pour tous $\bar{a}$ et $\bar{b}$ non nuls, et cela se démontre exactement de la même manière que dans le sujet. Cela s'étend à davantage que deux variables, et à d'autres corps finis que $\mathbb{Z}/p\mathbb{Z}$.

Il peut paraître surprenant qu'on puisse obtenir un résultat sur $\mathbb{N}$ en raisonnant d'abord dans $\mathbb{Z}/p\mathbb{Z}$ pour tout p, puisque la projection naturelle $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est très loin d'être injective. Le principe de Hasse-Minkowski donne de la hauteur à cette stratégie : *sous de bonnes hypothèses*, une équation de degré 2 (en plusieurs variables) a une solution rationnelle si et seulement si elle admet une solution modulo p pour tout nombre premier p, ainsi que dans $\mathbb{R}$. Une démonstration de ce principe nécessite les corps p-adiques et dépasse donc largement le cadre du programme.

Application à la géométrie. C'est pour des considérations géométriques que les quaternions ont été inventés (découverts ?) par Hamilton. Il cherchait en effet à faire de la géométrie en dimension 3 de la même manière que les nombres complexes le permettent dans le plan, en introduisant un nouveau nombre j (vérifiant lui aussi $j^2=-1$, et qui représentait dans l'esprit de Hamilton un vecteur directeur du troisième axe d'un repère orthonormé de $\mathbb{R}^3$) ainsi qu'une multiplication sur l'ensemble des nombres de la forme $a+bi+cj$. Il a très longtemps buté sur la définition de cette multiplication (et pour cause : le théorème de Frobenius nous enseigne que cet espoir était vain). En calculant :

$$(a+bi+cj)(d+ie+jf) = (ad-be-cf)+(ae+bd)i+(af+cd)j+(bf+ce)ij,$$

il se demandait ce que devait valoir ij. Comme $i^2 = j^2 = -1$, il semblait qu'on devait avoir : $(ij)^2 = 1$, et donc poser $ij = 1$ ou $ij = -1$ (notons que ce raisonnement présuppose que i et j commutent). Mais dans ces deux cas, on ne préservait pas la propriété de multiplicativité de la norme. C'est pour y remédier qu'il se résolut à songer que i et j ne devaient pas commuter (pensée très originale à l'époque, moins pour nous qui avons l'habitude des anneaux non commutatifs avec les matrices par exemple). En posant $ij = -ji = k$, tous ses problèmes furent résolus, mais ceci eut un prix : augmenter la dimension de l'espace dans lequel travailler, puisque $(1, i, j, k)$ engendre un espace de dimension 4 au lieu de 3.

Il ne suffit pas de décréter une table de multiplication pour qu'elle existe : c'est par les matrices qu'on obtient une construction rigoureuse de ces quaternions (c'est parfois ainsi que sont définis les nombres complexes également).

Hamilton raconte lui-même qu'il eut cette idée lors d'une promenade avec sa femme sur un pont de Dublin appelé *Broom Bridge* (éclair de génie qui fut cependant le fruit d'une longue gestation). Il grava la table de multiplication des nombres 1, i, j et k sur le pont.

Bien que l'ensemble $\mathbb{H} = \mathrm{Vect}_{\mathbb{R}}((1, i, j, k))$ des quaternions soit de dimension 4, il permet malgré tout de faire de la géométrie en dimension 3. Par exemple : si on considère les « quaternions purs », c'est-à-dire les quaternions de la forme $bi + cj + dk$, alors le produit de $bi + cj + dk$ par $qi + rj + sk$ correspond au produit vectoriel des vecteurs (b, c, d) par (q, r, s) dans $\mathbb{R}^3$, moins leur produit scalaire. Ou encore : il existe un isomorphisme entre le groupe des quaternions de module 1 et le groupe des rotations de $\mathbb{R}^3$. Le détail apparaît dans le sujet originel de 2023 où j'ai puisé mon inspiration, parmi les questions que j'ai supprimées.

Pour l'anecdote : j'ai découvert *a posteriori* (donc cela n'a pas conditionné mon choix du sujet) que l'on a fêté les cent quatre-vingts ans de la découverte des quaternions par Hamilton, ce lundi 16 octobre 2023.

Ce qu'on retiendra en bref. Tout quaternion non nul est inversible : $\mathbb{H}$ est un « corps non commutatif ». Le groupe quaternionique fournit un exemple de groupe non cyclique ni commutatif dont tous les sous-groupes stricts sont cycliques. Stabilité par multiplication de l'ensemble des sommes de quatre carrés. Décompte des carrés dans $\mathbb{Z}/p\mathbb{Z}$. L'application $(\bar{x}, \bar{y}) \mapsto \bar{a}\bar{x}^2 + \bar{b}\bar{y}^2$ est une surjection de $(\mathbb{Z}/p\mathbb{Z})^2$ dans $\mathbb{Z}/p\mathbb{Z}$. Méthode de descente infinie. Irréductibilité du polynôme minimal. Construction d'un isomorphisme d'algèbres en utilisant le fait qu'il préserve les solutions aux équations polynomiales.

Questions faciles ou classiques à retravailler

— PREMIÈRE PARTIE : toutes les questions ;

— DEUXIÈME PARTIE : questions 8 à 10, question 12 ;

— TROISIÈME PARTIE : questions 20 et 21.

2 Corrigé

Première partie

1. Pour montrer que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$, il suffit de noter que c'est l'image de l'application $\mathbb{R}$-linéaire $(z_1, z_2) \mapsto Z(z_1, z_2)$ définie sur $\mathbb{C}^2$. De plus Z est clairement injective, donc elle induit un isomorphisme de $\mathbb{C}^2$ dans son image $\mathbb{H}$. On en déduit que l'image par Z de toute base de $\mathbb{C}^2$ est une base de $\mathbb{H}$; or une base évidente de $\mathbb{C}^2$ est $((1,0), (i,0), (0,1), (0,i))$. En prenant l'image par Z de cette base, on obtient la base $(Z(1,0), Z(i,0), Z(0,1), Z(0,i)) = (E, I, -J, K)$ de $\mathbb{H}$. D'où le résultat : (E, I, J, K) est une base de $\mathbb{H}$.

Questions à se poser, réflexes à acquérir. Remarquer la plus-value notable de passer par une application linéaire injective pour préserver des propriétés (ici : montrer à peu de frais qu'un ensemble est un espace vectoriel et en donner une base). On gagne du temps lorsqu'on reconnaît l'image ou le noyau d'une application linéaire.

2. La question précédente démontre que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$. Pour montrer que $\mathbb{H}$ est une sous-$\mathbb{R}$-algèbre de $\mathrm{M}_2(\mathbb{C})$, il suffit donc de démontrer la stabilité par produit, qui découle directement de l'identité facile à vérifier :

$$\forall (z_1, z_2, z_1', z_2') \in \mathbb{C}^4, \quad Z(z_1, z_2)Z(z_1', z_2') = Z(z_1 z_1' - \overline{z_2} z_2', z_2 z_1' + \overline{z_1} z_2') \in \mathbb{H}. \tag{1}$$

De plus $\mathbb{H}$ est stable par $Z \mapsto Z^*$, puisque :

$$\forall (z_1, z_2) \in \mathbb{C}^2, \quad Z(z_1, z_2)^* = \begin{pmatrix} \overline{z_1} & \overline{z_2} \\ -z_2 & z_1 \end{pmatrix} = Z(\overline{z_1}, -z_2) \in \mathbb{H}. \tag{2}$$

On peut aussi remarquer que :

$$E^* = E, \quad I^* = -I, \quad J^* = -J, \quad K^* = -K,$$

pour étendre ensuite le résultat de stabilité à tout élément de $\mathbb{H}$ par linéarité.

Questions à se poser, réflexes à acquérir.
- Pourquoi un sous-espace vectoriel d'une algèbre, stable par produit, est bien une algèbre ?
- De la même manière que j'ai justifié la stabilité par $Z \mapsto Z^*$ juste en raisonnant sur une base, pouvais-je en faire autant pour montrer la stabilité par produit ?

3. Soit $(z_1, z_2) \in \mathbb{C}^2$ tel que : $Z = Z(z_1, z_2)$. On a :

$$ZZ^* \overset{(2)}{=} Z(z_1, z_2)Z(\overline{z_1}, -z_2) \overset{(1)}{=} Z(\underbrace{z_1\overline{z_1} + \overline{z_2}z_2}_{=|z_1|^2+|z_2|^2}, \underbrace{z_2\overline{z_1} - \overline{z_1}z_2}_{=0}) = \left(|z_1|^2 + |z_2|^2\right) E,$$

soit donc, avec les notations de l'énoncé :

$$\forall Z \in \mathbb{H}, \quad ZZ^* = \mathrm{N}(Z)E. \tag{3}$$

Or on remarque que si $\mathrm{N}(Z(z_1, z_2)) = 0$, alors $z_1 = z_2 = 0$ (en utilisant le fait qu'une somme de réels positifs soit nulle seulement si chaque terme est nul), et donc $Z(z_1, z_2) = 0_{\mathbb{H}}$, la réciproque étant évidente. Autrement dit :

$$\forall Z \in \mathbb{H}, \quad (\mathrm{N}(Z) = 0 \iff Z = 0_{\mathbb{H}}).$$

En particulier, si Z est un élément non nul de $\mathbb{H}$, alors $\mathrm{N}(Z) \neq 0$, et donc l'égalité ci-dessus équivaut à :

$$Z \cdot \left(\frac{1}{\mathrm{N}(Z)} Z^*\right) = E.$$

On en déduit que Z admet un inverse à droite dans $\mathbb{H}$, mais aussi dans $\mathrm{M}_2(\mathbb{C})$ (rappelons que E est la matrice identité : ainsi l'inversibilité est équivalente dans ces deux anneaux). Dans $\mathrm{M}_2(\mathbb{C})$, un inverse à droite est aussi un inverse à gauche, donc Z est inversible dans $\mathrm{M}_2(\mathbb{C})$ et $\mathbb{H}$ et on a :

$$\forall Z \in \mathbb{H} \setminus \{0_{\mathbb{H}}\}, \quad Z^{-1} = \frac{1}{\mathrm{N}(Z)} Z^*.$$

On a donc montré : $\mathbb{H}^\times = \mathbb{H} \setminus \{0_{\mathbb{H}}\}$ (l'inclusion directe est triviale et l'inclusion réciproque était l'objectif de cette question).

Questions à se poser, réflexes à acquérir.
- Puisque $\mathbb{H}$ n'est pas une algèbre commutative, pourquoi pouvais-je malgré tout regrouper $\frac{1}{\mathrm{N}(Z)}$ et Z^*, après avoir divisé (3) par $\mathrm{N}(Z)$?
- Le calcul de l'inverse ne rappelle-t-il pas quelque chose de connu ?
- Revoir pourquoi, dans $\mathrm{M}_n(\mathbb{C})$, un inverse à droite est aussi un inverse à gauche. Et dans $\mathrm{M}_{n,p}(\mathbb{C})$?

4. Posons : $Z = aE + bI + cJ + dK$, avec $(a,b,c,d) \in \mathbb{R}^4$. Comme $Z' \mapsto ZZ'$ et $Z' \mapsto Z'Z$ sont linéaires, elles coïncident sur $\mathbb{H}$ si et seulement si elles coïncident sur une base de $\mathbb{H}$. On en déduit que $ZZ' = Z'Z$ pour tout $Z' \in \mathbb{H}$ si et seulement si :

$$ZE = EZ, \quad ZI = IZ, \quad ZJ = JZ, \quad ZK = KZ,$$

si et seulement si, d'après les règles de calcul admises dans l'énoncé :

$$\left\{\begin{array}{rcl} aI - bE - cK + dJ &=& aI - bE + cK - dJ, \\ aJ + bK - cE - dI &=& aJ - bK - cE + dI, \\ aK - bJ + cI - dE &=& aK + bJ - cI - dE, \end{array}\right.$$

si et seulement si, en identifiant les coordonnées dans la base (E,I,J,K) :

$$-c = c, \quad d = -d, \quad b = -b,$$

si et seulement si : $b = c = d = 0$, si et seulement si : $Z = aE \in \mathbb{R}_{\mathbb{H}}$. On a montré :

$$Z \in \mathbb{R}_{\mathbb{H}} \iff \forall Z' \in \mathbb{H}, \quad ZZ' = Z'Z.$$

Questions à se poser, réflexes à acquérir.
- Observer l'économie d'avoir montré un résultat en raisonnant sur une base.
- On remarque que la ligne $ZK = KZ$ est obsolète pour conclure : était-ce prévisible ?

5. Le fait que G soit un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \cdot)$ est relativement immédiat. L'inclusion est claire (on a $I \cdot (-I) = \mathrm{I}_2$ et de même avec J et K, ce qui prouve l'inversibilité de toutes les matrices en présence), et la stabilité par produit vient des identités suivantes, qui sont admises par l'énoncé et procèdent d'un calcul matriciel sans mystère :

$$(\pm I)^2 = (\pm J)^2 = (\pm K)^2 = -\mathrm{I}_2, \quad IJ = K,\ JK = I,\ KI = J, \quad JI = -K,\ KJ = -I,\ IK = -J.$$

On obtient les autres produits *via* une multiplication par $-\mathrm{I}_2$. La stabilité par inversion découle des premières identités ci-dessus, qui impliquent : $I^{-1} = -I \in G$, etc. Ainsi G est un sous-ensemble non vide de $\mathrm{GL}_2(\mathbb{C})$, stable par produit et inverse, donc c'est un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \cdot)$.

Déterminons les sous-groupes de G. On commence par obtenir explicitement des sous-groupes en considérant les sous-groupes engendrés par un ou deux éléments. On montre aisément que E est d'ordre 1, $-E$ d'ordre 2, et $\pm I$, $\pm J$, $\pm K$ d'ordre 4 (et il n'y a pas d'autre élément). Cela fournit déjà les sous-groupes :

$$\{E\}, \quad \langle -E\rangle = \{-E, E\}, \quad \langle \pm I\rangle = \{I, -E, -I, E\},$$

$$\langle \pm J\rangle = \{J, -E, -J, E\}, \quad \langle \pm K\rangle = \{K, -E, -K, E\}.$$

Montrons qu'il n'y a pas d'autre sous-groupe strict : soit H un sous-groupe de G. Par le théorème de Lagrange, son cardinal divise 8, donc il est égal à 1, 2, 4 ou 8. Les cas 1 et 8 sont triviaux (on a $H = \{E\}$ ou $H = G$). S'il est de cardinal 2, alors il contient un élément non trivial qui doit

être d'ordre 2, et c'est donc $-E$. On en déduit : $-E \in H$, puis : $\langle -E\rangle \subseteq H$. En comparant les cardinaux : $H = \langle -E\rangle$.

Si H est de cardinal 4, alors ses éléments sont d'ordre 1 ou 2 ou 4. Mais ils ne peuvent pas tous être d'ordre 1 ou 2 (vu qu'il n'y a que E et $-E$ à avoir ces ordres : c'est insuffisant pour donner H), donc il doit contenir un élément d'ordre 4, disons I par exemple. On a alors : $\langle I\rangle \subseteq H$, puis en comparant les cardinaux : $H = \langle I\rangle$. De même si H contient J ou K plutôt que I.

On a traité toutes les possibilités de cardinaux, donc la liste des sous-groupes est complète. On observe notamment que les sous-groupes stricts de G sont tous cycliques, mais G ne l'est pas puisqu'il n'est même pas commutatif : on a $IJ = K$ et $JI = -K$, or : $K \neq -K$.

Remarque. Le théorème de Lagrange étant hors programme (hormis dans le cas de l'ordre d'un élément qui divise le cardinal du groupe), il faut le redémontrer lorsqu'on traite cette question. Je rappelle que pour cela, on introduit la relation d'équivalence définie sur G par : $\forall (g, g') \in G^2$, $g \sim g' \iff g' \in gH$, et on note que les classes d'équivalence sont toutes de la forme gH avec $g \in G$, donc en bijection avec H (une bijection évidente entre H et gH étant $h \mapsto gh$, de réciproque $h \mapsto g^{-1}h$). Il reste à écrire : $G = \bigsqcup_{\bar{g}\in G/H} gH$, et à comparer les cardinaux, pour obtenir le théorème de Lagrange.

Questions à se poser, réflexes à acquérir.
- Ce que j'ai fait là est-il généralisable, voire un *algorithme* permettant de trouver tous les sous-groupes d'un groupe donné ?
- Justifier avec et sans calcul que $\langle I\rangle$ et $\langle -I\rangle$ sont égaux (de même avec J et K).

6. Soit $(Z, Z') \in \mathbb{H}^2$. On a, d'après (3) :

$$\mathrm{N}(ZZ')E = ZZ'(ZZ')^*,$$

or : $(ZZ')^* = Z'^*Z^*$ (conséquence directe des propriétés de la conjugaison complexe et de la transposition), donc :

$$\mathrm{N}(ZZ')E = ZZ'Z'^*Z^* \overset{(3)}{=} Z(\mathrm{N}(Z')E)Z^*,$$

et comme : $\mathrm{N}(Z')E \in \mathbb{R}_{\mathbb{H}}$, d'après la question précédente $\mathrm{N}(Z')E$ commute avec Z^*, donc :

$$\mathrm{N}(ZZ')E = ZZ^*\mathrm{N}(Z')E = \mathrm{N}(Z)E \cdot \mathrm{N}(Z')E = \mathrm{N}(Z)\mathrm{N}(Z')E.$$

On en déduit :

$$\mathrm{N}(ZZ') = \mathrm{N}(Z)\mathrm{N}(Z'),$$

d'où le résultat.

Questions à se poser, réflexes à acquérir. Pourquoi serait-il plus délicat de montrer cette propriété de multiplicativité directement, partant de la définition ? À comparer avec le module d'un nombre complexe.

7. Soit $(x, y, z, t) \in \mathbb{R}^4$. On a par définition de N :

$$\mathrm{N}\left(xE + yI + zJ + tK\right) = \mathrm{N}\left(Z(x + iy, -z + it)\right) = |x + iy|^2 + |-z + it|^2 = x^2 + y^2 + z^2 + t^2,$$

d'où le résultat.

Deuxième partie

8. Notons f le morphisme de l'énoncé. Soit $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Alors :

$$\bar{x} \in \ker(f) \iff \bar{x}^2 = \bar{1} \iff \bar{x}^2 - \bar{1} = \bar{0} \iff (\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0},$$

et comme p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre (et même un corps, comme le rappelle l'énoncé), donc l'égalité précédente équivaut à $\bar{x}-\bar{1}=\bar{0}$ ou $\bar{x}+\bar{1}=\bar{0}$. On en déduit :

$$\bar{x}\in\ker(f)\iff \bar{x}=\bar{1}\text{ ou }\bar{x}=-\bar{1},$$

donc $\ker(f)=\{-\bar{1},\bar{1}\}$. Une preuve élémentaire ne passant pas par la théorie des anneaux, passe par le lemme d'Euclide : si p divise $x^2-1=(x-1)(x+1)$, alors p divise $x-1$ ou $x+1$.

Remarque importante. On a : $\bar{1}\neq-\bar{1}$, car p est un nombre premier impair (cela interviendra de manière décisive dans la question suivante). En effet, l'égalité $\bar{1}=-\bar{1}$ équivaut à $\bar{2}=\bar{0}$, et donc au fait que p divise 2. C'est impossible car $p\geqslant 3$.

Remarque. Dans $\mathbb{Z}/8\mathbb{Z}$, l'équation $\bar{x}^2=\bar{1}$ admet pour solutions *tous* les éléments impairs de l'anneau, c'est-à-dire 1, -1, 3 et -3. Il y a donc bien plus de solutions en général et il est crucial de comprendre l'importance de la primalité de p.

Questions à se poser, réflexes à acquérir.

— Pouvait-on observer, autrement que par le calcul bête et méchant, le fait que 8 divise x^2-1 pour tout x impair ?

— Arriverait-on de même à résoudre $\bar{x}^k=\bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$? (La réponse à cette question permet de comprendre l'un des intérêts de la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$.)

9. On rappelle que f désigne le morphisme de la question précédente. Par le théorème d'isomorphisme, les groupes $(\mathbb{Z}/p\mathbb{Z})^\times/\ker(f)$ et $\mathrm{im}(f)$ sont isomorphes, et ils ont donc même cardinal. C'est-à-dire :

$$\mathrm{card}\,(\mathrm{im}(f))=\frac{\mathrm{card}\,(\mathbb{Z}/p\mathbb{Z})^\times)}{\mathrm{card}(\ker(f))}\overset{(q.\,8)}{=}\frac{p-1}{\mathrm{card}(\{-\bar{1},\bar{1}\})}=\frac{p-1}{2}.$$

Or : $\mathrm{im}(f)=\{\bar{a}\in(\mathbb{Z}/p\mathbb{Z})^\times\mid\exists\bar{x}\in(\mathbb{Z}/p\mathbb{Z})^\times,\ \bar{a}=\bar{x}^2\}=\{\bar{a}\in\mathbb{Z}/p\mathbb{Z}\mid\exists\bar{x}\in\mathbb{Z}/p\mathbb{Z},\ \bar{a}=\bar{x}^2\}\setminus\{\bar{0}\}$ (on note que $\bar{0}$ est effectivement dans ce dernier ensemble, puisque : $\bar{0}=\bar{0}^2$). Donc :

$$\mathrm{card}\left(\left\{\bar{a}\in\mathbb{Z}/p\mathbb{Z}\mid\exists\bar{x}\in\mathbb{Z}/p\mathbb{Z},\ \bar{a}=\bar{x}^2\right\}\right)=\mathrm{card}(\mathrm{im}(f))+\mathrm{card}(\{\bar{0}\})=\frac{p-1}{2}+1=\frac{p+1}{2}.$$

Démonstration n'utilisant pas le théorème d'isomorphisme. On utilise le fait que deux éléments ont même carré si et seulement s'ils sont opposés, par un argument d'intégrité déjà utilisé à la question précédente : $\bar{x}_1^2=\bar{x}_2^2\iff(\bar{x}_1-\bar{x}_2)(\bar{x}_1+\bar{x}_2)=\bar{0}\iff\bar{x}_1=\pm\bar{x}_2$. On en déduit que si, pour tout $\bar{y}$ dans l'image de f, on note $\bar{x}_y$ et $-\bar{x}_y$ ses deux antécédents, alors : $(\mathbb{Z}/p\mathbb{Z})^\times=\bigsqcup_{\bar{y}\in\mathrm{im}(f)}\{\bar{x}_y,-\bar{x}_y\}$. Comparer les cardinaux donne alors le résultat, étant donné que $\bar{x}_y\neq-\bar{x}_y$ pour tout $\bar{y}\in\mathrm{im}(f)$ (si ce n'était pas le cas, multiplier par l'inverse de $\bar{x}_y$ donnerait : $\bar{1}=-\bar{1}$, ce qui est faux pour $p>2$).

Si l'on y regarde bien, j'ai implicitement redémontré le théorème d'isomorphisme ci-dessus.

Remarque. Si $p=2$, alors tout élément de $\mathbb{Z}/2\mathbb{Z}$ est un carré : $\bar{0}^2=\bar{0}$, et : $\bar{1}^2=\bar{1}$.

Questions à se poser, réflexes à acquérir.

— Pourquoi être passé par $(\mathbb{Z}/p\mathbb{Z})^\times$ d'abord ? Ne pouvait-on pas immédiatement adapter la stratégie de ces deux dernières questions à $\mathbb{Z}/p\mathbb{Z}$?

— Pourquoi passer par le noyau ? Ne pouvait-on pas dénombrer le cardinal de l'image directement ? Reconnaître là une stratégie fréquente, notamment en algèbre linéaire.

10. Posons : $X=\{\bar{a}\in\mathbb{Z}/p\mathbb{Z}\mid\exists\bar{x}\in\mathbb{Z}/p\mathbb{Z},\ \bar{a}=\bar{x}^2\}$, et : $Y=\left\{\bar{b}\in\mathbb{Z}/p\mathbb{Z}\mid\exists\bar{y}\in\mathbb{Z}/p\mathbb{Z},\ \bar{b}=-\bar{1}-\bar{y}^2\right\}$. On veut montrer : $X\cap Y\neq\emptyset$. Nous allons y parvenir par une minoration du cardinal de $X\cap Y$. On connaît en effet le cardinal de X (qui vaut $\frac{p+1}{2}$ par la question précédente), et le cardinal de Y lui est égal puisque l'application :

$$g:\begin{cases}X&\to&Y\\ \bar{a}&\mapsto&-\bar{1}-\bar{a}\end{cases}$$

est correctement définie et admet pour réciproque l'application $\bar{b} \mapsto -\bar{1}-\bar{b}$: elle est donc bijective et préserve les cardinaux. On a donc, par la formule de Moivre :

$$\mathrm{card}(X \cap Y) = \mathrm{card}(X) + \mathrm{card}(Y) - \mathrm{card}(X \cup Y) = 2\frac{p+1}{2} - \mathrm{card}(X \cup Y),$$

et comme $X \cup Y$ est inclus dans $\mathbb{Z}/p\mathbb{Z}$, on a : $\mathrm{card}(X \cup Y) \leqslant p$. On en déduit :

$$\mathrm{card}(X \cap Y) \geqslant (p+1) - p = 1,$$

d'où : $X \cap Y \neq \emptyset$, ce qu'il fallait démontrer.

Questions à se poser, réflexes à acquérir.

— Le rôle de $-\bar{1}$ est-il important ? Ne peut-on pas le remplacer par n'importe quelle classe modulo p ? Se demander, dans les questions qui suivent, ce qui motiva son choix.

— Interpréter ce qu'il fallut démontrer comme un résultat de surjectivité, en le généralisant.

11. La question précédente assure l'existence de $(x, y) \in \mathbb{Z}^2$ tel que : $\bar{x}^2 = -\bar{1}-\bar{y}^2$. Mieux : un système complet de représentants de $\mathbb{Z}/p\mathbb{Z}$ étant $[\![-\frac{p-1}{2}, \frac{p-1}{2}]\!]$, on peut supposer : $(x, y) \in [\![-\frac{p-1}{2}, \frac{p-1}{2}]\!]^2$. De plus, quitte à changer x en $-x$, ou y en $-y$ (leurs carrés sont égaux), on peut supposer que x et y sont des entiers naturels inférieurs ou égaux à $\frac{p-1}{2}$. Alors :

$$\bar{x}^2 = -\bar{1} - \bar{y}^2 \iff p \mid x^2 + y^2 + 1 \iff \exists m \in \mathbb{Z},\ x^2 + y^2 + 1 = mp.$$

Le premier prédicat étant vrai, le dernier aussi. Il reste à justifier que l'on a : $m \in [\![1, p-1]\!]$, et c'est là qu'apparaît l'intérêt de s'être ramené à $(x, y) \in [\![0, \frac{p-1}{2}]\!]^2$. Étant donné que : $1 + x^2 + y^2 \geqslant 1$, il est immédiat que : $m > 0$, donc : $m \geqslant 1$. En outre, on a :

$$mp = 1 + |x|^2 + |y|^2 \leqslant 1 + \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 = \frac{p^2 - 2p + 3}{2},$$

donc :

$$m \leqslant \frac{p}{2} - 1 + \frac{3}{2p} \overset{(p\geqslant 3)}{\leqslant} \frac{p}{2} - 1 + \frac{1}{2} = \frac{p-1}{2} < \frac{p}{2} < p,$$

d'où le résultat : $m \in [\![1, p-1]\!]$.

Questions à se poser, réflexes à acquérir.

— Comprendre pourquoi, si je ne fais pas la réduction de x et y du début de question, on NE peut PAS démontrer que $0 < m < p$ et résoudre la question.

— Il semble qu'il n'apparaisse nulle part le fait que x et y soient positifs, dans cette démonstration. Pourquoi m'y suis-je ramené ?

— Pouvait-on démontrer que $m < p$ sans développer mochement la quantité $1 + 2\left(\frac{p-1}{2}\right)^2$?

12. Pour alléger les notations, notons $\mathbb{H}_\mathbb{Z}$ le sous-ensemble de $\mathbb{H}$ constitué des matrices de la forme $x_1E + x_2I + x_3J + x_4K$, avec x_1, x_2, x_3 et x_4 des *entiers relatifs*. Les règles de multiplication de E, I, J et K permettent de se convaincre aisément que $\mathbb{H}_\mathbb{Z}$ est stable par produit, et c'est la clé pour traiter cette question. Il est en effet utile de remarquer que l'on a, pour tout $t \in \mathbb{N}$:

$$\begin{aligned}
t \in \mathcal{N}^4 &\iff \exists (x_1, x_2, x_3, x_4) \in \mathbb{N}^4, \quad t = x_1^2 + x_2^2 + x_3^2 + x_4^2 \\
&\iff \exists (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4, \quad t = x_1^2 + x_2^2 + x_3^2 + x_4^2 && (x_i^2 = (-x_i)^2) \\
&\iff \exists (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4, \quad t = \mathrm{N}\left(x_1E + x_2I + x_3J + x_4K\right) && (q.\ 7) \\
&\iff \exists Z \in \mathbb{H}_\mathbb{Z}, \quad t = \mathrm{N}(Z).
\end{aligned}$$

Montrons alors que $\mathcal{N}^4$ est stable par multiplication. Soit $(a,b) \in (\mathcal{N}^4)^2$. D'après l'équivalence ci-dessus, il existe Z et Z' dans $\mathbb{H}_\mathbb{Z}$ tels que : $a = \mathrm{N}(Z)$, et : $b = \mathrm{N}(Z')$. Alors, d'après ce qu'on a démontré dans la question 6, on a :

$$ab = \mathrm{N}(Z)\mathrm{N}(Z') = \mathrm{N}(ZZ') \in \mathcal{N}^4,$$

parce que $ZZ' \in \mathbb{H}_\mathbb{Z}$. D'où le résultat.

Questions à se poser, réflexes à acquérir.

— Pourquoi passer de $\mathbb{N}^4$ à $\mathbb{Z}^4$? Ne suffisait-il pas de définir $\mathbb{H}_\mathbb{N}$ plutôt ?

— C'est LA grande idée de cette démonstration, qui ne se généraliserait pas à une somme de trois carrés par exemple. En saisir tout le sel ! Et réfléchir à au moins une autre propriété dont on montrerait la stabilité par multiplication semblablement.

13. D'après la question 11, il existe un entier $m \in [\![1, p-1]\!]$ et deux entiers naturels x et y tels que :

$$mp = 1 + x^2 + y^2 = 1^2 + x^2 + y^2 + 0^2 \in \mathcal{N}^4,$$

d'où le résultat.

14. Si m est pair alors, en utilisant la formule de développement du carré d'une somme, on a :

$$(x_1 + x_2 + x_3 + x_4)^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \bmod 2 \equiv mp \bmod 2 \equiv 0 \cdot p \bmod 2 \equiv 0 \bmod 2,$$

et comme $\mathbb{Z}/2\mathbb{Z}$ est un corps, il est intègre et on en déduit :

$$x_1 + x_2 + x_3 + x_4 \equiv 0 \bmod 2.$$

Par conséquent, $x_1 + x_2 + x_3 + x_4$ est un entier pair et c'est la somme de quatre entiers, donc soit ces quatre entiers sont pairs, soit les quatre sont impairs, soit deux sont pairs et deux sont impairs. On va effectuer une distinction de cas :

— **premier cas :** ils ont tous la même parité ; on les réordonne de façon croissante :

$$0 \leqslant x_{i_4} \leqslant x_{i_3} \leqslant x_{i_2} \leqslant x_{i_1},$$

et l'application $\sigma : j \mapsto i_j$ est clairement une permutation de S_4 telle que les entiers $x_{\sigma(1)} \pm x_{\sigma(2)}$, $x_{\sigma(3)} \pm x_{\sigma(4)}$ soient tous positifs et pairs ;

— **second cas :** deux sont pairs et deux sont impairs ; il existe deux indices distincts i_1 et i_2 tels que x_{i_1}, x_{i_2} soient pairs et deux autres indices distincts i_3, i_4 tels que x_{i_3}, x_{i_4} soient impairs ; on définit alors $\sigma \in S_4$ par :

$$\sigma(1) = \begin{cases} i_1 & \text{si} \quad x_{i_1} \geqslant x_{i_2} \\ i_2 & \text{si} \quad x_{i_1} < x_{i_2} \end{cases}, \quad \sigma(2) = \begin{cases} i_2 & \text{si} \quad x_{i_1} \geqslant x_{i_2} \\ i_1 & \text{si} \quad x_{i_1} < x_{i_2} \end{cases},$$

et :

$$\sigma(3) = \begin{cases} i_3 & \text{si} \quad x_{i_3} \geqslant x_{i_4} \\ i_4 & \text{si} \quad x_{i_3} < x_{i_4} \end{cases}, \quad \sigma(4) = \begin{cases} i_4 & \text{si} \quad x_{i_3} \geqslant x_{i_4} \\ i_3 & \text{si} \quad x_{i_3} < x_{i_4} \end{cases}.$$

et les entiers $x_{\sigma(1)} \pm x_{\sigma(2)}$, et $x_{\sigma(3)} \pm x_{\sigma(4)}$ sont tous positifs et pairs.

Puisque $\frac{x_{\sigma(1)} \pm x_{\sigma(2)}}{2}$ et $\frac{x_{\sigma(3)} \pm x_{\sigma(4)}}{2}$ sont des entiers positifs, on a :

$$\begin{aligned} &\left(\frac{x_{\sigma(1)} + x_{\sigma(2)}}{2}\right)^2 + \left(\frac{x_{\sigma(1)} - x_{\sigma(2)}}{2}\right)^2 + \left(\frac{x_{\sigma(3)} + x_{\sigma(4)}}{2}\right)^2 + \left(\frac{x_{\sigma(3)} - x_{\sigma(4)}}{2}\right)^2 \\ &= \frac{1}{2}\left(x_{\sigma(1)}^2 + x_{\sigma(2)}^2 + x_{\sigma(3)}^2 + x_{\sigma(4)}^2\right) \\ &= \frac{1}{2}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right) \\ &= \frac{mp}{2} \in \mathcal{N}^4, \end{aligned}$$

d'où le résultat.

Remarque. La relation : $\left(\sum_{i=1}^{4} x_i\right)^2 \equiv \sum_{i=1}^{4} x_i^2 \bmod 2$ se généralise. Pour tout p premier et tout corps K contenant $\mathbb{Z}/p\mathbb{Z}$, on a : $\forall (x,y) \in K^2$, $(x+y)^p = x^p + y^p$. Autrement dit : l'application $x \mapsto x^p$ est un morphisme de corps de K dans lui-même. Vous trouverez des éléments de démonstration dans vos feuilles d'exercices du chapitre IV.

Questions à se poser, réflexes à acquérir.

- Vérifier le développement au carré de la somme de quatre entiers. Aurait-on eu une identité analogue avec un autre exposant ou un autre module ? À mettre en parallèle de la remarque ci-dessus.
- Vérifier rigoureusement qu'une somme de quatre entiers est paire si et seulement s'ils sont tous de même parité, ou deux pairs et deux impairs.
- Comment définit-on la permutation σ ? C'est surtout pour le second cas, et pour sa distinction de cas, que la question se pose.

15. Procédons par l'absurde en supposant m_0 pair. Alors $\dfrac{m_0}{2}$ est un entier positif non nul et d'après la question précédente on a : $\dfrac{m_0}{2}p = \dfrac{m_0 p}{2} \in \mathcal{N}^4$. Par minimalité de m_0, on a : $m_0 \leqslant \dfrac{m_0}{2}$, ce qui équivaut à : $m_0 = 0$. C'est absurde puisque l'on a : $m_0 \geqslant 1$. Ce raisonnement par l'absurde montre donc que m_0 est impair.

16. Pour tout $i \in [\![1,4]\!]$, soit b_i l'entier le plus proche de $\dfrac{x_i}{m_0}$ (dans le cas où il y a deux choix possibles, b_i peut être n'importe lequel des deux). L'expression explicite de b_i ne sera pas utile pour la suite. Tout ce qui importe est que l'on ait :

$$\forall i \in [\![1,4]\!], \quad \left|\frac{x_i}{m_0} - b_i\right| \leqslant \frac{1}{2}.$$

S'il existe $i \in [\![1,4]\!]$ tel que : $\left|\dfrac{x_i}{m_0} - b_i\right| = \dfrac{1}{2}$, alors :

$$\frac{x_i}{m_0} - b_i = \pm\frac{1}{2} \iff \pm\frac{m_0}{2} = x_i - b_i m_0 \iff m_0 = \pm 2(x_i - b_i m_0) \in 2\mathbb{Z},$$

ce qui est faux par la question précédente, donc : $\forall i \in [\![1,4]\!]$, $\left|\dfrac{x_i}{m_0} - b_i\right| < \dfrac{1}{2}$. On en déduit :

$$\forall i \in [\![1,4]\!], \quad |x_i - b_i m_0| < \frac{m_0}{2}.$$

Posons alors : $\forall i \in [\![1,4]\!]$, $y_i = x_i - b_i m_0$. On doit encore montrer que les y_i vérifient :

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2, \quad \text{et :} \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m_0.$$

Faisons. Comme : $\forall i \in [\![1,4]\!]$, $y_i \equiv x_i \bmod m_0$, on a :

$$\sum_{i=1}^{4} y_i^2 \equiv \sum_{i=1}^{4} x_i^2 \bmod m_0 \equiv m_0 p \bmod m_0 \equiv 0 \bmod m_0,$$

et la majoration $|y_i| < \dfrac{m_0}{2}$ justifiée ci-dessus donne :

$$\sum_{i=1}^{4} y_i^2 < \sum_{i=1}^{4} \left(\frac{m_0}{2}\right)^2 = m_0^2.$$

Montrons enfin : $0 < \sum_{i=1}^{4} y_i^2$, en raisonnant par l'absurde. Si : $\sum_{i=1}^{4} y_i^2 = 0$, alors, comme c'est une somme de nombres positifs, on a : $\forall i \in [\![1,4]\!]$, $y_i = 0$. Par définition des y_i, cela donne : $\forall i \in [\![1,4]\!]$, $x_i = b_i m_0$, donc :

$$m_0 p = \sum_{i=1}^{4} x_i^2 = m_0^2 \sum_{i=1}^{4} b_i^2,$$

et en divisant par m_0 on obtient : $p = m_0 \sum_{i=1}^{4} b_i^2$. C'est un produit d'entiers naturels égal à un nombre premier p. Ce n'est possible que si : $m_0 \in \{1, p\}$, ce qui est absurde par hypothèse sur m_0 (il est inférieur à $p-1$, et on l'a supposé différent de 1). On a donc montré : $0 < \sum_{i=1}^{4} y_i^2$, et les trois conditions de l'énoncé sont bien satisfaites par les y_i.

Questions à se poser, réflexes à acquérir.

— Se demander ce qui nous a conduit à définir b_i ainsi.

— Sauriez-vous expliciter b_i ? Cet « entier le plus proche » est-il défini de manière unique ?

17. On a : $(x_1 + x_2 I + x_3 J + x_4 K)(y_1 - y_2 I - y_3 J - y_4 K) \in \mathbb{H}$. Notons $(z_1, z_2, z_3, z_4) \in \mathbb{R}^4$ les coordonnées de cet élément de $\mathbb{H}$ dans la base (E, I, J, K), de sorte que :

$$(x_1 E + x_2 I + x_3 J + x_4 K)(y_1 E - y_2 I - y_3 J - y_4 K) = z_1 E + z_2 I + z_3 J + z_4 K.$$

D'après les questions 6 et 7, on a :

$$\begin{aligned}
\sum_{i=1}^{4} z_i^2 &= \mathrm{N}((x_1 + x_2 I + x_3 J + x_4 K)(y_1 - y_2 I - y_3 J - y_4 K)) && (q.\,7)\\
&= \mathrm{N}(x_1 + x_2 I + x_3 J + x_4 K)\mathrm{N}(y_1 - y_2 I - y_3 J - y_4 K)) && (q.\,6)\\
&= \left(\sum_{i=1}^{4} x_i^2\right)\left(\sum_{i=1}^{4} y_i^2\right) && (q.\,7)\\
&= (m_0 p)(m_0 m_1)\\
&= m_0^2 m_1 p.
\end{aligned}$$

Montrons à présent les relations de congruence : $\forall i \in [\![1,4]\!]$, $z_i \equiv 0 \bmod m_0$. Si l'on développe le produit $(x_1 E + x_2 I + x_3 J + x_4 K)(y_1 E - y_2 I - y_3 J - y_4 K)$ et qu'on utilise la liberté de la famille (E, I, J, K), on observe que l'on a :

$$\left\{\begin{array}{rcl}
z_1 &=& \sum\limits_{i=1}^{4} x_i y_i,\\
z_2 &=& -x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3,\\
z_3 &=& -x_1 y_3 + x_2 y_4 + x_3 y_1 - x_4 y_2,\\
z_4 &=& -x_1 y_4 - x_2 y_3 + x_3 y_2 + x_4 y_1.
\end{array}\right.$$

Cela démontre déjà que les z_i sont entiers (on pouvait aussi le déduire de la stabilité par produit de $\mathbb{H}_\mathbb{Z}$, défini dans la résolution de la question 12). En utilisant les relations de congruence démontrées dans la question précédente : $\forall i \in [\![1,4]\!]$, $y_i \equiv x_i \bmod m_0$, et ces quatre égalités, on trouve :

$$\left\{\begin{array}{rcl}
z_1 &\equiv& \sum\limits_{i=1}^{4} x_i^2 \equiv 0 \bmod m_0,\\
z_2 &\equiv& -x_1 x_2 + x_2 x_1 + x_3 x_4 - x_4 x_3 \equiv 0 \bmod m_0,\\
z_3 &\equiv& -x_1 y_3 + x_2 x_4 + x_3 x_1 - x_4 x_2 \equiv 0 \bmod m_0,\\
z_4 &\equiv& -x_1 y_4 - x_2 x_3 + x_3 x_2 + x_4 x_1 \equiv 0 \bmod m_0.
\end{array}\right.$$

Pour les trois dernières congruences, le fait d'obtenir 0 mod m_0 est évident (les termes se simplifient deux à deux). Pour la première, on utilise le fait que : $\sum_{i=4} x_i^2 = m_0 p$. D'où le résultat (pour se ramener à des entiers naturels, il suffit de changer z_i en $|z_i|$, qui vérifie les mêmes conditions).

Questions à se poser, réflexes à acquérir.
— Vérifier le calcul que j'ai omis.
— Dans le cas complexe, que donne le calcul analogue $(x_1+x_2i)(y_1-y_2i)$ de *concret* géométriquement ?

18. Puisque pour tout $i \in [\![1,4]\!]$, l'entier m_0 divise z_i, on sait que $\left|\frac{z_i}{m_0}\right|$ est un entier positif, et on a :

$$\sum_{i=1}^{4} \left|\frac{z_i}{m_0}\right|^2 = \frac{1}{m_0^2}\sum_{i=1}^{4} z_i^2 = m_1 p, \quad \text{or :} \quad m_1 = \frac{1}{m_0}\sum_{i=1}^{4} y_i^2 < \frac{m_0^2}{m_0} = m_0.$$

Par conséquent, on a : $m_1 p \in \mathcal{N}^4$, avec m_1 un entier naturel *non nul* (car $\sum_{i=1}^{4} y_i^2 > 0$) strictement plus petit que m_0, ce qui contredit la minimalité de m_0. Impossible ! Donc l'hypothèse $m_0 \neq 1$ est absurde, ce qui entraîne : $m_0 = 1$. D'où le résultat.

Remarque. Le raisonnement de ces dernières questions suit le « principe de descente infinie ». C'est un raisonnement par l'absurde consistant à produire une suite strictement décroissante d'entiers naturels (vérifiant une propriété donnée), ce qui est bien sûr impossible. Il apparaît souvent en arithmétique pour montrer l'INexistence de solutions à une équation.

19. Les questions 13 à 18 montrent que tout nombre premier impair p est une somme de quatre carrés d'entiers naturels, et c'est aussi le cas de 2 (puisque : $2 = 1^2 + 1^2 + 0^2 + 0^2$), donc $p \in \mathcal{N}^4$ pour tout p nombre premier. Or $\mathcal{N}^4$ est stable par multiplication d'après la question 12, et tout entier naturel non nul est produit de nombres premiers, donc : $\mathbb{N}\setminus\{0\} \subseteq \mathcal{N}^4$. De plus on a évidemment : $0 \in \mathcal{N}^4$, puisque : $0 = \sum_{i=1}^{4} 0^2$, donc finalement : $\mathbb{N} \subseteq \mathcal{N}^4$. L'inclusion réciproque étant évidente, on a démontré le théorème des quatre carrés : $\mathbb{N} = \mathcal{N}^4$.

Troisième partie

20. La résolution de cette question anticipe légèrement sur le chapitre IV où l'on explicite les idéaux de $K[X]$, mais vous vous convaincrez qu'on peut aisément s'en passer : au lieu d'utiliser la minimalité de π_x au sens de la relation de divisibilité, il suffit d'utiliser sa minimalité au sens du degré.
Soit $x \in A$. Alors l'ensemble :

$$\{P \in \mathbb{R}[X] \mid P(x) = 0_A\}$$

est un idéal de $\mathbb{R}[X]$, non réduit à $0_{\mathbb{R}[X]}$ puisque A est algébrique (donc il existe bien $P \in \mathbb{R}[X]$ non nul tel que $P(x) = 0_A$), donc il admet un générateur $\pi_x \in \mathbb{R}[X]$ non nul. Puisque l'on a :

$$\{P \in \mathbb{R}[X] \mid P(x) = 0_A\} = (\pi_x),$$

alors en particulier :

$$\forall P \in \mathbb{R}[X], \quad (P(x) = 0_A \iff \pi_x | P)\,.$$

Montrons que π_x est de degré au plus 2 ; nous en déduirons aisément le résultat voulu.
Cela revient à démontrer que π_x est irréductible : en effet, on sait que les seuls polynômes irréductibles sur $\mathbb{R}[X]$ sont de degré 1 ou 2. Or, si π_x n'était pas irréductible, il existerait des polynômes non constants $P_1, P_2 \in \mathbb{R}[X]$ tels que : $\pi_x = P_1 P_2$. En évaluant cette égalité en x, on aurait : $\pi_x(x) = 0_A = P_1(x)P_2(x)$. Or $P_1(x) \in A$ et $P_2(x) \in A$, et A est supposé sans diviseur de zéro, donc $P_1(x)P_2(x) = 0_A$ n'est possible que si $P_1(x) = 0_A$ ou $P_2(x) = 0_A$: d'après

l'équivalence ci-dessus, π_x diviserait soit P_1 soit P_2, ce qui est impossible pour des raisons de degré. Par l'absurde, on a montré que π_x est un polynôme irréductible de $\mathbb{R}[X]$, et il est donc de degré 1 ou 2.

Déduisons-en : $x^2 \in \mathbb{R}+\mathbb{R}x$. Pour cela, il suffit d'effectuer la division euclidienne de X^2 par π_x, ce qui est possible puisque π_x est non nul : il existe $(Q,R) \in \mathbb{R}[X]^2$ tel que : $X^2 = \pi_x Q + R$, avec : $\deg(R) \leqslant \deg(\pi_x) - 1 \leqslant 1$. En évaluant cette égalité en x, on obtient : $x^2 = \pi_x(x)Q(x) + R(x) = R(x) \in \mathbb{R} + \mathbb{R}x$: d'où le résultat.

Questions à se poser, réflexes à acquérir.

— Adapter la démonstration sans recours aux idéaux.

— Pourquoi, à la lecture de l'énoncé, on *pouvait penser* à introduire le polynôme minimal sans indication ? Comment pouvait-on formuler de manière équivalente le résultat à montrer : $x^2 \in \mathbb{R}+\mathbb{R}x$, de sorte à l'interpréter naturellement en termes de polynôme annulateur ?

— Pourquoi ai-je introduit une division euclidienne de X^2 par π_x, au lieu de simplement écrire $\pi_x(x) = 0$ pour ensuite isoler x^2 dans cette égalité ?

21. Soit $x \in A \setminus \mathbb{R}$. Pour construire l'isomorphisme demandé, l'idée est de trouver un antécédent de i dans $\mathbb{R}+\mathbb{R}x$ (il suffit en effet de définir une application linéaire sur une base, donc sur $(1,i)$ par exemple). Comme un isomorphisme conserve tout ce qui est relatif à la structure de $\mathbb{R}$-algèbre, cet antécédent doit être une racine carrée de -1 dans A. C'est ce que nous allons chercher à construire dans ce qui suit.

On a : $x^2 \in \mathbb{R}+\mathbb{R}x$, d'après la question précédente. Soit, donc, $(a,b) \in \mathbb{R}^2$ tel que : $x^2 = b + ax$. On peut classiquement réécrire cette égalité ainsi :

$$\left(x - \frac{a}{2}\right)^2 = \frac{4b-a^2}{4}.$$

On a : $4b - a^2 < 0$, sinon on aurait : $x = \frac{a}{2} \pm \frac{\sqrt{4b-a^2}}{2} \in \mathbb{R}$, ce qui est faux par hypothèse (le fait que $u^2 = v^2$ implique $u = \pm v$ ne va pas de soi, et est faux si u et v ne commutent pas ; on utilise de plus le fait que A soit sans diviseur de zéro : ainsi $u^2 - v^2 = (u+v)(u-v) = 0$ implique $u+v = 0$ ou $u-v = 0$, l'identité remarquable étant valable si et seulement si $uv = vu$). Ainsi : $a^2 - 4b > 0$, ce qui permet d'écrire :

$$\left(\frac{2x-a}{\sqrt{a^2-4b}}\right)^2 = -1.$$

Posons : $x' = \dfrac{2x-a}{\sqrt{a^2-4b}}$, qui est un élément de A car $x \in A$, $\mathbb{R} \subseteq A$, et A est stable par produit et somme en tant qu'algèbre. Considérons l'application $\mathbb{R}$-linéaire de $\mathbb{C}$ dans $\mathbb{R}+\mathbb{R}x$ définie sur la $\mathbb{R}$-base $(1,i)$ de $\mathbb{C}$ par :

$$f(1) = 1, \quad f(i) = x'.$$

Montrons que f est un isomorphisme de $\mathbb{R}$-algèbres. Comme c'est une application $\mathbb{R}$-linéaire, il suffit de vérifier qu'elle est multiplicative et bijective.

Montrons qu'elle est multiplicative : soient $z = \alpha + i\beta \in \mathbb{C}$ et $z' = \alpha' + i\beta' \in \mathbb{C}$, avec $(\alpha,\beta,\alpha',\beta') \in \mathbb{R}^4$. On a d'une part, par $\mathbb{R}$-linéarité :

$$\begin{aligned} f(zz') = f(\alpha\alpha' - \beta\beta' + i(\alpha\beta' + \alpha'\beta)) &= (\alpha\alpha' - \beta\beta')f(1) + (\alpha\beta' + \alpha'\beta)f(i) \\ &= (\alpha\alpha' - \beta\beta') + (\alpha\beta' + \alpha'\beta)x', \end{aligned}$$

et d'autre part, par un calcul analogue :

$$f(z)f(z') = f(\alpha+i\beta)f(\alpha'+i\beta') = (\alpha + x'\beta)(\alpha' + x'\beta') = (\alpha\alpha' + \beta\beta'x'^2) + (\alpha\beta' + \alpha'\beta)x'.$$

Or, par construction : $x'^2 = -1$, d'où :

$$f(z)f(z') = (\alpha\alpha' - \beta\beta') + (\alpha\beta' + \alpha'\beta)x' = f(zz'),$$

donc f est multiplicative. On en déduit aisément qu'elle est de noyau réduit à 0_A : en effet, si $z \in \mathbb{C}^*$ vérifie : $f(z) = 0_A$, alors on a : $0_A = f(z)f\left(\frac{1}{z}\right) = f(1) = 1$, ce qui est absurde. Par conséquent seul $z = 0$ vérifie $f(z) = 0_A$, donc f est injective. Il reste à montrer qu'elle est surjective : soit $(a, b) \in \mathbb{R}^2$, montrons que $a + bx \in \mathbb{R} + \mathbb{R}x$ admet un antécédent par f. Nous avons :

$$x' = f(i) \iff \frac{2x - a}{\sqrt{a^2 - 4b}} = f(i) \iff x = \frac{\sqrt{a^2 - 4b}}{2}f(i) + \frac{a}{2} = f\left(\frac{i\sqrt{a^2 - 4b} + a}{2}\right),$$

ce qui montre que x admet $\frac{i\sqrt{a^2-4b}+a}{2}$ pour antécédent. Cela nous permet d'en déduire que l'application $\mathbb{R}$-linéaire de $\mathbb{R} + \mathbb{R}x$ dans $\mathbb{C}$ définie sur la $\mathbb{R}$-base $(1, x)$ de $\mathbb{R} + \mathbb{R}x$ par :

$$g(1) = 1, \quad g(x) = \frac{i\sqrt{a^2 - 4b} + a}{2}$$

vérifie : $f \circ g = \mathrm{id}_{\mathbb{R}+\mathbb{R}x}$ (c'est vrai sur une base, donc c'est vrai partout), donc f est surjective.
Ainsi il existe bien un morphisme de $\mathbb{R}$-algèbres bijectif de $\mathbb{C}$ dans $\mathbb{R}+\mathbb{R}x$, donc ces deux algèbres sont isomorphes.

Remarque. Nous n'avons pas démontré que $(1, x)$ est une $\mathbb{R}$-base de $\mathbb{R}+\mathbb{R}x$. Faisons-le à présent. C'est une famille génératrice par définition de $\mathbb{R} + \mathbb{R}x$, il suffit donc de montrer qu'elle est libre : soit $(\alpha, \beta) \in \mathbb{R}^2$ tel que : $\alpha+\beta x = 0_A$. Si $\beta \neq 0$, alors : $x = -\frac{\alpha}{\beta} \in \mathbb{R}$, ce qui est faux par hypothèse. Donc $\beta = 0$, et il en résulte aisément $\alpha = 0$.

Remarque. Il découle de cette question que tout élément non nul de A est inversible : si $x \in \mathbb{R}^*$ alors c'est trivial car $\frac{1}{x} \in \mathbb{R}^* \subseteq A$, et si $x \in A\setminus\mathbb{R}$ alors $\mathbb{R}+\mathbb{R}x$ est isomorphe en tant que $\mathbb{R}$-algèbre à $\mathbb{C}$. Or tout élément non nul de $\mathbb{C}$ admet un inverse, donc par cet isomorphisme c'est aussi le cas de x, d'où le résultat.

Une autre démonstration, très instructive et qui n'utilise pas l'isomorphisme avec $\mathbb{C}$: il découle de la question précédente que l'application $y \mapsto xy$ est un endomorphisme de $\mathbb{R} + \mathbb{R}x$, qui est de dimension finie puisqu'il admet une famille génératrice finie (à savoir $(1, x)$). Elle est de plus injective puisque $\mathbb{R} + \mathbb{R}x$ n'admet pas de diviseur de zéro (et $x \neq 0$), donc surjective par un argument dimensionnel : soit y un antécédent de 1 par cet endomorphisme. Alors $xy = 1$, donc x est inversible à droite. Le même argument avec l'endomorphisme $y \mapsto yx$ montre que x est inversible à gauche. On en déduit classiquement que x est inversible.

Questions à se poser, réflexes à acquérir.

- Comprendre la stratégie de construction de f, qui est la même pour la plupart des isomorphismes de corps construits.
- Est-ce que g est nécessairement un morphisme d'algèbres, étant donné que f en est un ?
- Réfléchir à un allègement substantiel de la vérification que f est multiplicative, en décrivant autrement les éléments de $\mathbb{R} + \mathbb{R}x$ (d'une manière plus compliquée en apparence).
- Un autre argument permet d'obtenir la bijectivité de f : lequel ? Se souvenir qu'elle est linéaire *et* que c'est un morphisme d'anneaux (presque de corps).

22. L'élément x' de la question précédente répond à la question. Nous proposons une façon de faire pour le candidat qui aurait proposé un autre isomorphisme entre $\mathbb{R} + \mathbb{R}x$ et $\mathbb{C}$.
Soit $x \in A \setminus \mathbb{R}$. Un tel élément existe, puisque A n'est pas isomorphe à $\mathbb{R}$ par hypothèse. Alors d'après la question précédente, il existe un isomorphisme de $\mathbb{R}$-algèbres, noté f, de $\mathbb{R} + \mathbb{R}x$ dans $\mathbb{C}$. Posons : $i_A = f^{-1}(i) \in A$. Alors, f étant un isomorphisme de $\mathbb{R}$-algèbres, f^{-1} aussi et on a :

$$i_A^2 = \left(f^{-1}(i)\right)^2 = f^{-1}(i^2) = f^{-1}(-1) = -1,$$

d'où le résultat.

Questions à se poser, réflexes à acquérir. Revoir là une illustration que les isomorphismes préservent tout ce qui est relatif à la structure.

23. Soit $(x,y) \in A^2$. Comme $i_A^2 = -1$, on a :

$$T(xy) = i_A xy i_A = i_A x(-i_A^2) y i_A = -i_A x i_A i_A y i_A = -T(x)T(y),$$

d'où le résultat.

24. Soit $x \in A$. On a :

$$T^2(x) = T(T(x)) = i_A T(x) i_A = i_A(i_A x i_A) i_A = i_A^2 x i_A^2 = (-1)^2 x = x,$$

donc : $T^2 = \mathrm{id}$. Or T est clairement $\mathbb{R}$-linéaire, donc c'est une symétrie de A. On en déduit : $A = \ker(T - \mathrm{id}) \oplus \ker(T + \mathrm{id})$.

Remarque. Il nous sera plusieurs fois utile de remarquer la propriété suivante. Soit $(\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2$. Alors :

$$\forall (x,y) \in \ker(T - \varepsilon_1 \mathrm{id}) \times \ker(T - \varepsilon_2 \mathrm{id}), \quad xy \in \ker(T + \varepsilon_1\varepsilon_2 \mathrm{id}). \tag{4}$$

Supposons en effet que $(x,y) \in \ker(T - \varepsilon_1 \mathrm{id}) \times \ker(T - \varepsilon_2 \mathrm{id})$, et utilisons la question 23. On a :

$$T(xy) = -T(x)T(y) = -\varepsilon_1 x \varepsilon_2 y = -\varepsilon_1\varepsilon_2 xy,$$

donc $xy \in \ker(T + \varepsilon_1\varepsilon_2 \mathrm{id})$ comme annoncé.

Questions à se poser, réflexes à acquérir. Pourquoi puis-je « changer » de place ε_1 et ε_2, alors que A n'est *a priori* pas commutative ?

25. Remarque préliminaire : en appliquant la question 21 à U, et du fait qu'un isomorphisme conserve tout ce qui est relatif à la structure, on obtient immédiatement que U est commutatif (car $\mathbb{C}$ l'est) et qu'une $\mathbb{R}$-base de U est $(1, i_A)$.

Pour alléger les notations, posons : $K = \ker(T + \mathrm{id})$. Montrons d'abord que $U \subseteq K$. Comme T est $\mathbb{R}$-linéaire et U admet pour $\mathbb{R}$-base $(1, i_A)$, il suffit de montrer : $T(1) = -1$, $T(i_A) = -i_A$. On a d'une part : $T(1) = i_A \cdot 1 \cdot i_A = i_A^2 = -1$, et d'autre part :

$$T(i_A) = i_A i_A i_A = i_A^2 i_A = -i_A,$$

d'où le résultat : $U \subseteq K$. Montrons l'inclusion réciproque. Soit $z \in K$. Comme K est inclus dans A, on a aussi : $z \in A$, ce qui permet d'appliquer la question 20 : soit $(a,b) \in \mathbb{R}^2$ tel que : $z^2 = b + az$. Cette égalité peut se réécrire :

$$\left(z - \frac{a}{2}\right)^2 - \frac{4b - a^2}{4} = 0_A.$$

Notons $\delta \in U$ une racine carrée de $\dfrac{4b-a^2}{4} \in \mathbb{R} \subseteq U$ dans U. Il en existe car U est une $\mathbb{R}$-algèbre isomorphe à $\mathbb{C}$, et tout élément admet une racine carrée dans $\mathbb{C}$. L'égalité précédente implique :

$$\left(\left(z - \frac{a}{2}\right) - \delta\right)\left(\left(z - \frac{a}{2}\right) + \delta\right) = 0_A.$$

Pour que cette identité remarquable soit valable, encore faut-il que δ et $z - \frac{a}{2}$ commutent. Si δ est réel alors c'est trivial, et sinon on a : $\delta = \pm i_A \sqrt{a^2 - 4b}$. Or le fait que z soit dans K implique,

par définition : $i_A z i_A = -z$, c'est-à-dire (en multipliant par $-i_A$ à gauche de chaque membre de l'égalité) : $z i_A = i_A z$, ce qui assure que z et δ commutent après multiplication par $\pm\sqrt{a^2-4b} \in \mathbb{R}$. Chaque membre de ce produit est dans A, puisque A contient z et U, et est stable par somme et produit. Comme A est sans diviseur de zéro, on en déduit que ce produit est nul si et seulement si l'un des deux termes est nul. Cela donne donc :

$$z = \frac{a}{2} \pm \delta \in U,$$

d'où le résultat : $K \subseteq U$. Ayant démontré la double inclusion, on a : $K = U$, ce qu'il fallait démontrer.

On en déduit que si : $\ker(T - \mathrm{id}) = \{0_A\}$, alors par la question précédente : $A = U \simeq \mathbb{C}$. C'est absurde par hypothèse sur A, donc $\ker(T - \mathrm{id}) \neq \{0_A\}$.

Questions à se poser, réflexes à acquérir. Comprendre pourquoi, si l'on ne détaille pas comme on l'a fait la démonstration que $z = \frac{a}{2} \pm \delta$, on peut très vite tomber sur une absurdité très perturbante et contre-intuitive dans cette question. Cette préoccupation est liée à la suivante : pourquoi ai-je estimé utile de préciser que U est commutatif ? Où cela intervient-il ?

26. Soit $\varepsilon \in \{-1,1\}$, et soit $x \in \ker(T - \varepsilon\mathrm{id})$. Alors βx appartient à $\ker(T + \varepsilon\mathrm{id})$ par l'identité (4) démontrée en remarque dans la résolution de la question 24 (on a en effet $\beta \in \ker(T - \mathrm{id})$). Ainsi l'application $m_\beta : x \mapsto \beta x$ envoie $\ker(T - \mathrm{id})$ dans $U = \ker(T + \mathrm{id})$, et elle envoie aussi $U = \ker(T + \mathrm{id})$ dans $\ker(T - \mathrm{id})$. On en déduit, par composition, que $(m_\beta)^2 : x \mapsto \beta^2 x$ induit une application de U dans lui-même. En prenant $x = 1$ (qui appartient bien à U, comme on l'a montré dans la question précédente), on a donc : $\beta^2 = \beta^2 \cdot 1 \in U$.

Déduisons-en : $\ker(T - \mathrm{id}) = \beta U$. Pour cela, on note que l'application $m_{\beta|U} : U \to \ker(T - \mathrm{id})$ est injective parce que $U \subseteq A$ est sans diviseur de zéro par hypothèse sur A, donc : $\dim_{\mathbb{R}}(U) \leqslant \dim_{\mathbb{R}}(\ker(T - \mathrm{id}))$. Par le même argument, appliqué à $m_{\beta|\ker(T-\mathrm{id})}$, on a : $\dim_{\mathbb{R}}(\ker(T - \mathrm{id})) \leqslant \dim_{\mathbb{R}}(U)$. Donc : $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(\ker(T - \mathrm{id}))$. Ainsi $m_{\beta|U} : U \to \ker(T - \mathrm{id})$ est une application linéaire et injective entre deux espaces vectoriels de même dimension, donc elle est surjective. Autrement dit : $\ker(T - \mathrm{id}) = m_{\beta|U}(U) = \beta U$. D'où le résultat.

Questions à se poser, réflexes à acquérir. Peut-on avoir la bijectivité de $m_{\beta|U}$ directement, par exemple par construction d'une réciproque ?

27. On sait que $\beta^2 \in U = \mathbb{R} + \mathbb{R}i_A$, mais on a aussi $\beta^2 \in \mathbb{R} + \mathbb{R}\beta$ d'après la question 20. Soit, donc, $(a,b,c,d) \in \mathbb{R}^4$ tel que :

$$\beta^2 = a + b i_A = c + d\beta.$$

On a alors :

$$(a - c) + b i_A = d\beta.$$

Or $(a - c) + b i_A \in U$ et $d\beta \in \ker(T - \mathrm{id})$. Comme U et $\ker(T - \mathrm{id})$ sont en somme directe, cela implique : $a - c + b i_A = d\beta = 0_A$. Comme $\beta \neq 0_A$, ceci implique : $d = 0$. Ainsi $\beta^2 = c \in \mathbb{R}$. Ce ne peut pas être égal à un réel positif ou nul, sinon on aurait, du fait que $\sqrt{c} \in \mathbb{R}$ et β commutent : $\beta = \pm\sqrt{c}$ (on a déjà expliqué l'importance de la commutation dans les questions 21 et 25). Donc β serait dans U, ce qui est impossible encore par un argument de somme directe. Ainsi c est strictement négatif, donc : $\beta^2 \in]-\infty,0[$.

28. Rappelons que $\ker(T + \mathrm{id}) = U = \mathbb{R} + \mathbb{R}i_A$, et on sait que l'application $m_\beta : x \mapsto \beta x$ induit un isomorphisme de U dans $\ker(T - \mathrm{id})$: il transforme donc une $\mathbb{R}$-base de U en une $\mathbb{R}$-base de $\ker(T - \mathrm{id})$; on en déduit que $(m_\beta(1), m_\beta(i_A)) = (\beta, \beta i_A)$ est une $\mathbb{R}$-base de $\ker(T - \mathrm{id})$. Le

fait que β soit dans $\ker(T-\mathrm{id})$ implique : $\beta i_A = -i_A\beta$, donc $(\beta, -\beta i_A) = (\beta, i_A\beta)$ est aussi une $\mathbb{R}$-base de $\ker(T-\mathrm{id})$. Comme :

$$A = \ker(T-\mathrm{id}) \oplus \ker(T+\mathrm{id}),$$

on en déduit qu'une $\mathbb{R}$-base de A est : $(1, i_A, \beta, i_A\beta)$. Nous allons l'utiliser pour conclure.
On a montré l'existence de $\lambda < 0$ tel que : $\beta^2 = \lambda$. Posons : $j_A = \frac{\beta}{\sqrt{-\lambda}}$ (cette définition est faite de sorte que $j_A^2 = -1$), et : $k_A = i_A j_A$. Alors $(1, i_A, j_A, k_A)$ est une $\mathbb{R}$-base de A (nous n'avons fait que multiplier les deux derniers vecteurs de la base précédente par des scalaires non nuls), et l'application $\mathbb{R}$-linéaire $f : A \to \mathbb{H}$ définie sur cette base par :

$$f(1) = E, \quad f(i_A) = I, \quad f(j_A) = J, \quad f(k_A) = K$$

est bijective (puisqu'elle transforme une base de A en une base de $\mathbb{H}$). Il reste à vérifier qu'elle est un morphisme de $\mathbb{R}$-algèbres, c'est-à-dire : $\forall (x,y) \in A^2$, $f(xy) = f(x)f(y)$. Par $\mathbb{R}$-linéarité, on se convainc qu'il suffit de le vérifier pour les éléments d'une base. Or c'est bien le cas puisque :

$$\begin{aligned}
&i_A^2 = j_A^2 = k_A^2 = -1,\\
&i_A j_A = k_A,\ j_A i_A = -k_A,\ j_A k_A = i_A,\ k_A j_A = -i_A,\ k_A i_A = j_A,\ i_A k_A = -j_A,
\end{aligned}$$

tandis que leurs images par f vérifient exactement les mêmes identités d'après ce qui fut admis dans l'énoncé. La vérification de toutes ces identités est relativement aisée grâce à tout ce qui précède (dès qu'on a démontré l'une des identités de la seconde ligne, la première découlant de la définition de k_A, une multiplication adéquate à gauche et à droite de chaque membre de l'égalité donne l'identité suivante ; de plus n'oublions pas que j_A et k_A sont dans $\ker(T-\mathrm{id})$, ce qui signifie exactement que $j_A i_A = -i_A j_A$ et $k_A i_A = -i_A k_A$). Faisons seulement la vérification pour k_A^2, qui est la seule non triviale de la liste ; on a : $k_A^2 = i_A j_A i_A j_A = T(j_A) j_A = j_A j_A = j_A^2 = -1$.
Ceci étant dit : f est un isomorphisme de $\mathbb{R}$-algèbres entre A et $\mathbb{H}$, ce qui démontre que si A n'est pas isomorphe à $\mathbb{R}$ ou $\mathbb{C}$, alors A est isomorphe à $\mathbb{H}$. En bref : A est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, ce qui démontre le théorème F.

Questions à se poser, réflexes à acquérir.

— Vérifier tout ce que j'affirme sur la vérification que $f(xy) = f(x)f(y)$ et ce qui suit.

— Est-ce que cette démonstration nécessite *a priori* de savoir que $\mathbb{C}$ et $\mathbb{H}$ existent, ou bien elle aurait justement permis de les définir ?