Devoir sur table n° 3

18/10/2023, 13h45–17h45

Définitions.

On dit qu'une structure $(A, +, \times, \cdot)$ est une $\mathbb{R}$-*algèbre* si elle induit une structure d'anneau $(A, +, \times)$ et d'espace vectoriel $(A, +, \cdot)$, telles que pour tout $\lambda \in \mathbb{R}$ et tout $(a, b) \in A^2$, on ait : $(\lambda \cdot a) \times b = \lambda \cdot (a \times b) = a \times (\lambda \cdot b)$. Par commodité, on note simplement A une telle $\mathbb{R}$-algèbre, les lois étant implicites.

Si A est une $\mathbb{R}$-algèbre, on dit que B est une *sous-*$\mathbb{R}$*-algèbre* de A si B est un sous-$\mathbb{R}$-espace vectoriel de A stable par la loi de composition interne $(a, b) \mapsto a \times b$.

On admet que $\mathrm{M}_2(\mathbb{C})$ est une $\mathbb{R}$-algèbre.

Deux $\mathbb{R}$-algèbres A et B sont dites *isomorphes* s'il existe une bijection $\mathbb{R}$-linéaire $f : A \to B$ telle que : $\forall (x, y) \in A^2,\ f(xy) = f(x)f(y)$. Autrement dit : c'est à la fois un isomorphisme de $\mathbb{R}$-espaces vectoriels et d'anneaux.

Soit A une $\mathbb{R}$-algèbre et soit $e \in A$ l'élément unité de A pour la multiplication. On notera $\mathbb{R}_A$ la sous-algèbre $\{ae \mid a \in \mathbb{R}\}$ de A. Un élément x de A est dit *inversible* s'il existe $y \in A$ tel que : $xy = yx = e$. On note $A^\times$ l'ensemble des éléments inversibles de A. On admet que $A^\times$ est un groupe pour la multiplication.

Notations.

Pour tout $(z_1, z_2) \in \mathbb{C}^2$, on note : $Z(z_1, z_2) = \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix}$. Soit $\mathbb{H} = \{Z(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\} \subseteq \mathrm{M}_2(\mathbb{C})$ l'ensemble des *quaternions*. On définit :

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

On admet que ces matrices vérifient les relations suivantes dans $\mathrm{M}_2(\mathbb{C})$:

$$I^2 = J^2 = K^2 = -E, \quad IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J.$$

On veillera à ne pas confondre l'élément i de $\mathbb{C}$ et la matrice I de $\mathbb{H} \subseteq \mathrm{M}_2(\mathbb{C})$, ni la matrice I avec la matrice identité E.

On définit une application $\mathrm{N} : \mathbb{H} \to \mathbb{R}$ par : $\mathrm{N}(Z(z_1, z_2)) := |z_1|^2 + |z_2|^2$.

Objectif.

L'objectif de ce problème est d'étudier dans une **première partie** les propriétés de base de $\mathbb{H}$, qui est un exemple fameux de « corps non commutatif » (on parle plutôt d'algèbre à division, puisqu'un corps est normalement commutatif par définition). Nous utilisons cet ensemble de quaternions pour démontrer un théorème d'arithmétique en **deuxième partie** (tout entier naturel est somme de quatre entiers au carré), et en **troisième partie** nous démontrons une sorte de théorème d'unicité de $\mathbb{H}$, parfois formulé en ces termes : les seuls corps, commutatifs ou non, contenant $\mathbb{R}$ en étant de dimension finie sur $\mathbb{R}$, sont à isomorphisme près : $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$. Nous le reformulerons en temps voulu.

Première partie

Pour toute matrice $A = ((a_{i,j}))_{1 \leqslant i,j \leqslant 2} \in \mathrm{M}_2(\mathbb{C})$, on note : $A^* = ((\overline{a_{j,i}}))_{1 \leqslant i,j \leqslant 2}$.

1. Montrer que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$, et que (E, I, J, K) est une $\mathbb{R}$-base de $\mathbb{H}$.
2. Montrer que $\mathbb{H}$ est une sous-$\mathbb{R}$-algèbre de $\mathrm{M}_2(\mathbb{C})$ stable par l'application $Z \mapsto Z^*$.
3. Soit $Z \in \mathbb{H}$. Calculer ZZ^* et en déduire que tout élément non nul de $\mathbb{H}$ est inversible.
4. Soit $Z \in \mathbb{H}$. Montrer que $Z \in \mathbb{R}_{\mathbb{H}}$ si et seulement si $ZZ' = Z'Z$ pour tout $Z' \in \mathbb{H}$.

5. Soit $G = \{E, -E, I, -I, J, -J, K, -K\}$. Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, et que les sous-groupes stricts de G sont tous cycliques. Est-ce que G est lui-même cyclique ?
6. Montrer que l'on a $\mathrm{N}(ZZ') = \mathrm{N}(Z)\mathrm{N}(Z')$ pour tout $(Z, Z') \in \mathbb{H}^2$.
7. Montrer que pour tout $(x, y, z, t) \in \mathbb{R}^4$ on a :

$$\mathrm{N}\left(xE + yI + zJ + tK\right) = x^2 + y^2 + z^2 + t^2.$$

Deuxième partie

Soit p un nombre premier impair. On sait que $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est-à-dire : $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

8. Déterminer le noyau du morphisme de groupes :

$$\left\{ \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ \bar{x} & \mapsto & \bar{x}^2 \end{array} \right. .$$

9. En déduire le cardinal de son image et le cardinal de l'ensemble :

$$\left\{\bar{a} \in \mathbb{Z}/p\mathbb{Z} \mid \exists x \in \mathbb{Z}/p\mathbb{Z},\ \bar{a} = \bar{x}^2\right\}.$$

10. Montrer :

$$\left\{\bar{a} \in \mathbb{Z}/p\mathbb{Z} \mid \exists \bar{x} \in \mathbb{Z}/p\mathbb{Z},\ \bar{a} = \bar{x}^2\right\} \cap \left\{\bar{b} \in \mathbb{Z}/p\mathbb{Z} \mid \exists \bar{y} \in \mathbb{Z}/p\mathbb{Z},\ \bar{b} = -\bar{1} - \bar{y}^2\right\} \neq \emptyset.$$

11. Montrer qu'il existe $(x, y) \in \mathbb{N}^2$ et $m \in [\![1, p-1]\!]$ tels que : $1 + x^2 + y^2 = mp$.

Dans le reste de cette partie, on note :

$$\mathcal{N}^4 = \left\{t \in \mathbb{N} \ \mid \ \exists (x_1, x_2, x_3, x_4) \in \mathbb{N}^4,\ t = x_1^2 + x_2^2 + x_3^2 + x_4^2\right\}.$$

L'objectif des questions suivantes est de démontrer le théorème des quatre carrés.

12. Montrer que $\mathcal{N}^4$ est stable par multiplication, c'est-à-dire :

$$\forall (a, b) \in \left(\mathcal{N}^4\right)^2, \quad ab \in \mathcal{N}^4.$$

On rappelle que p est un nombre premier impair.

13. Montrer qu'il existe $m \in [\![1, p-1]\!]$ tel que mp appartienne à $\mathcal{N}^4$.

On note m_0 le plus petit entier strictement positif tel que : $m_0 p \in \mathcal{N}^4$.

14. Soit m un entier pair tel qu'il existe $(x_1, x_2, x_3, x_4) \in \mathbb{N}^4$ avec : $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Montrer qu'il existe une permutation σ de S_4 telle que les entiers :

$$x_{\sigma(1)} + x_{\sigma(2)}, \quad x_{\sigma(1)} - x_{\sigma(2)}, \quad x_{\sigma(3)} + x_{\sigma(4)} \quad \text{et} \quad x_{\sigma(3)} - x_{\sigma(4)}$$

soient tous les quatre pairs et positifs. En déduire : $\frac{mp}{2} \in \mathcal{N}^4$.

15. Montrer que m_0 est impair.

On suppose que $m_0 \neq 1$. On se donne $(x_1, x_2, x_3, x_4) \in \mathbb{N}^4$ tel que : $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

16. Montrer qu'il existe des entiers b_1, b_2, b_3 et b_4 tels que les entiers donnés par $y_i = x_i - b_i m_0$ pour $i \in [\![1,4]\!]$ satisfassent les trois conditions suivantes :
    - pour tout $i \in [\![1,4]\!]$, on a : $|y_i| < \dfrac{1}{2} m_0$;
    - on a : $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2$;
    - on a : $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m_0$.

On note : $m_1 = \dfrac{y_1^2+y_2^2+y_3^2+y_4^2}{m_0}$.

17. Montrer qu'il existe $(z_1,z_2,z_3,z_4) \in \mathbb{N}^4$ tel que l'on ait :
    — l'égalité : $z_1^2+z_2^2+z_3^2+z_4^2 = m_0^2 m_1 p$;
    — pour tout $i \in [\![1,4]\!]$, la congruence : $z_i \equiv 0 \bmod m_0$.
    Indication : on pourra considérer le produit $(x_1E+x_2I+x_3J+x_4K)(y_1E-y_2I-y_3J-y_4K)$.
18. Montrer : $m_0 = 1$.
19. Montrer : $\mathbb{N} = \mathcal{N}^4$.

Troisième partie

Soient A une $\mathbb{R}$-algèbre et e son élément neutre. Dans cette partie, on identifiera $\mathbb{R}_A$ avec $\mathbb{R}$, et on notera (abusivement) a l'élément ae de A pour $a \in \mathbb{R}$. On dit que A est *algébrique* si pour tout $x \in A$ il existe un entier $n \in \mathbb{N}\setminus\{0\}$ et $(a_i)_{0\leqslant i\leqslant n-1} \in \mathbb{R}^n$ tels que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

On dit que A est *sans diviseur de zéro* si $xy \neq 0$ pour tout $(x,y) \in (A\setminus\{0\})^2$. Dans cette partie, nous allons montrer le théorème F ci-dessous.

Théorème F. Une $\mathbb{R}$-algèbre algébrique et sans diviseur de zéro est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$.

Soit A une $\mathbb{R}$-algèbre algébrique et sans diviseur de zéro.

20. Montrer que $x^2 \in \mathbb{R}+\mathbb{R}x$ pour tout $x \in A$.
    Indication : introduire le polynôme de $\mathbb{R}[X]$ *unitaire et de degré minimal ayant* x *pour racine, et montrer qu'il est de degré au plus* 2.
21. Montrer que si $x \in A\setminus\mathbb{R}$, alors $\mathbb{R}+\mathbb{R}x$ est une $\mathbb{R}$-algèbre isomorphe à $\mathbb{C}$.

On suppose que A n'est pas isomorphe à une des algèbres $\mathbb{R}$ ou $\mathbb{C}$.

22. Montrer qu'il existe $i_A \in A$ tel que : $i_A^2 = -1$.

On fixe par la suite un élément i_A de A tel que : $i_A^2 = -1$. On note : $U = \mathbb{R}+\mathbb{R}i_A$, et on définit l'application :

$$T : \begin{cases} A & \to & A \\ x & \mapsto & i_A x i_A \end{cases}.$$

On note $\mathrm{id} : A \to A$ l'application identité de A.

23. Montrer : $\forall (x,y) \in A^2$, $T(xy) = -T(x)T(y)$.
24. Calculer $T^2 = T\circ T$ et en déduire : $A = \ker(T-\mathrm{id}) \oplus \ker(T+\mathrm{id})$.
25. Montrer : $\ker(T+\mathrm{id}) = U$, et en déduire : $\ker(T-\mathrm{id}) \neq \{0\}$.

On fixe $\beta \in \ker(T-\mathrm{id})\setminus\{0\}$.

26. Montrer que l'application $x \mapsto \beta x$ envoie $\ker(T-\mathrm{id})$ dans $\ker(T+\mathrm{id})$. En déduire que $\beta^2 \in U$ et que : $\ker(T-\mathrm{id}) = \beta U$.
27. Montrer : $\beta^2 \in]-\infty,0[$.
28. Démontrer le théorème F.