Corrigé DS n°1

Rem : Un certain nombre de calculs ne sont pas détaillés dans le corrigé (il s'agit de calculs matriciels élémentaires). Mais il fallait évidemment les faire lors du D.S, et ne pas se contenter du mot "évident" ...

PARTIE I :

1) $\mathbb{H}$ sous-anneau de $(\mathcal{M}_2(\mathbb{C}),+,\times)$

Il fallait vérifier : • $1_{\mathcal{M}_2(\mathbb{C})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$

• $\forall (M_1,M_2) \in \mathbb{H}^2$, $M_1 - M_2 \in \mathbb{H}$ et $M_1 M_2 \in \mathbb{H}$

ce qui est facile.

---

2) • $\mathbb{H}$ s.e.v. de $(\mathcal{M}_2(\mathbb{C}),+,.)$ ($\mathbb{R}$-e.v)

Il fallait vérifier : $\mathbb{H} \neq \emptyset$ et
$\forall (\lambda_1,\lambda_2) \in \mathbb{R}^2$, $\forall (M_1,M_2) \in \mathbb{H}^2$, $\lambda_1 M_1 + \lambda_2 M_2 \in \mathbb{H}$

ce qui est facile. (en utilisant : $\lambda \in \mathbb{R} \Leftrightarrow \lambda = \bar{\lambda}$)

(N.B : Comme on a déjà démontré que $(\mathbb{H},+)$ est un ss-gpe de $(\mathcal{M}_2(\mathbb{C}),+)$, on pouvait se contenter de vérifier : $\forall \lambda \in \mathbb{R}$, $\forall M \in \mathbb{H}$, $\lambda . M \in \mathbb{H}$)

• φ isomorphisme de $\mathbb{R}$-espaces vectoriels

car : $\forall (\lambda_1,\lambda_2) \in \mathbb{R}^2$, $\forall (M_1,M_2) \in \mathbb{H}^2$, $\varphi(\lambda_1 M_1 + \lambda_2 M_2) = \lambda_1 \varphi(M_1) + \lambda_2 \varphi(M_2)$ (calcul simple)

et : $\forall M \in \mathbb{H}$, $\exists ! (z,z') \in \mathbb{C}^2$ tq $M = \varphi(z,z')$ (par définition de φ !) donc φ bijective

---

3) a) • (E,I,J,K) est libre car, si $(a,b,c,d) \in \mathbb{R}^4$, $aE + bI + cJ + dK = 0 \Rightarrow a=b=c=d=0$ (facile)

• D'après ce qui précède, $\mathbb{H}$ est $\mathbb{R}$-isomorphe au $\mathbb{R}$-e.v. $\mathbb{C}^2$; or $\dim_{\mathbb{R}} \mathbb{C}^2 = 4$, donc $\dim \mathbb{H} = 4 = \mathrm{card}(\{E,I,J,K\})$. D'après un th. célèbre du cours, (E,I,J,K) sera une base de $\mathbb{H}$.

• On pouvait aussi directement montrer que $\{E,I,J,K\}$ est génératrice de $\mathbb{H}$, car, si $M = \begin{pmatrix} z & z' \\ -\bar{z}' & \bar{z} \end{pmatrix} \in \mathbb{H}$, avec $z = a+ib$, $z' = c+id$ ($(a,b,c,d) \in \mathbb{R}^4$), il est facile de vérifier que $M = aE + bI + cJ + dK$.

---

b) On peut montrer que $G = \{E,I,J,K,-E,-I,-J,-K\}$ est un sous-groupe du groupe $GL_2(\mathbb{C})$ (ens. des matrices inversibles de $\mathcal{M}_2(\mathbb{C})$). En effet :

• $G \subset GL_2(\mathbb{C})$ car $\det E$, $\det I$, $\det J$, $\det K$ sont non nuls, donc les élts de G sont bien des matrices inversibles.

- $\underline{X \text{ est interne de } G}$ car : $\forall X \in G$, $EX = X$ et $I^2 = -I$, $J^2 = -J$, $K^2 = -K$
et $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, $IK = -J$.
- $\underline{\text{Si } X \in G,\ X^{-1} \in G}$ car : $I^{-1} = -I$, $J^{-1} = -J$, $K^{-1} = -K$, $E^{-1} = E$.

---

4) a) • s est $\mathbb{R}$-linéaire : il suffit de vérifier que : $\forall (\lambda_1, \lambda_2) \in \mathbb{R}^2$, $\forall (M_1, M_2) \in \mathbb{H}^2$,
on a : $s(\lambda_1 M_1 + \lambda_2 M_2) = \lambda_1 s(M_1) + \lambda_2 s(M_2)$

• $s \circ s = id_{\mathbb{H}}$ est immédiat. On en déduit que s est bijective (et $s^{-1} = s$)

Donc s est un automorphisme du $\mathbb{R}$-ev $\mathbb{H}$.

b) Calcul... (et question sans intérêt pour la suite)

c) • si $M = \begin{pmatrix} z & z' \\ -\bar{z}' & \bar{z} \end{pmatrix} \in \mathbb{H}$, $tr(M) = z + \bar{z}$ et $-M + tr(M) E = \begin{pmatrix} -z & -z' \\ \bar{z}' & -\bar{z} \end{pmatrix} + \begin{pmatrix} z+\bar{z} & 0 \\ 0 & z+\bar{z} \end{pmatrix} = s(M)$

• On a déjà vu que s est une application linéaire involutive, donc il s'agit d'une symétrie du $\mathbb{R}$-e.v $\mathbb{H}$ (cf cours)

• Il s'agit de la symétrie p.r. à $Inv(s)$ et de direction $Opp(s)$, avec :

$M \in Opp(s) \iff s(M) = -M \iff tr(M) = 0 \iff z + \bar{z} = 0$

et $M \in Inv(s) \iff s(M) = M \iff M = \frac{tr(M)}{2}(E)$

Or, il est facile de vérifier que $E \in Inv(s)$; donc $Vect(E) \subset Inv\, s$
et que $I, J, K \in Opp(s)$; donc $Vect(I, J, K) \subset Opp\, s$

Puisque $\mathbb{H} = Inv \oplus Opp\, s$, on a donc nect : $Inv(s) = Vect\, E$ et $Opp(s) = Vect(I, J, K)$

Ainsi, $\underline{s \text{ est la symétrie p.r. à } \mathbb{R}.E, \text{ de direction } Vect(I,J,K)}$

[Rem : une autre façon de démontrer ce résultat consistait à remarquer que, si $M = aE + bI + cJ + dK$ avec $(a,b,c,d) \in \mathbb{R}^4$, alors $s(M) = aE - bI - cJ - dK$].

d) On trouve facilement, si $M = \begin{pmatrix} z & z' \\ -\bar{z}' & \bar{z} \end{pmatrix}$: $M s(M) = s(M) M = (|z|^2 + |z'|^2) E$

Donc, si $M \neq 0$, on a $(z, z') \neq (0,0)$ et $|z|^2 + |z'|^2 \neq 0$, et il s'ensuit que M est inversible (à droite et à gauche) d'inverse $\underline{M^{-1} = \frac{1}{|z|^2 + |z'|^2} M}$. ($M^{-1} \in \mathbb{H}$ car $|z|^2 + |z'|^2 \in \mathbb{R}^*$)

e) On en déduit :

• $\mathbb{H}$ est une $\mathbb{R}$-algèbre (cf. 1°/ et 2°/)

• $\mathbb{H}$ est un corps (non commutatif)

---

5) Questions faciles pour qui connaît la déf. d'un morphisme d'algèbres...

PARTIE 2 :

Préliminaire

- l'écriture $\sum_{k\in\mathbb{N}} p_k a^k$ a un sens car :
  - (p_k) est à support fini
  - si $a \in \mathcal{A}$, $a^k \in \mathcal{A}$ et $p_k a^k \in \mathcal{A}$ car $p_k \in \mathbb{K}$ et $\mathcal{A}$ est une $\mathbb{K}$-algèbre
  - la somme d'élts de $\mathcal{A}$ est un élt de $\mathcal{A}$.
- φ_a est un morphisme de $\mathbb{K}$-algèbres car :
  - $\varphi_a(1_{\mathbb{K}[X]}) = 1_{\mathcal{A}}$ (car $a^0 = 1_{\mathcal{A}}$)
  - Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k\in\mathbb{N}} p_k X^k$ $Q = \sum_{k\in\mathbb{N}} q_k X^k$, et soient $\lambda, \mu \in \mathbb{K}$.

Les règles de calcul ds la $\mathbb{K}$-algèbre $\mathcal{A}$ et dans $\mathbb{K}[X]$ donnent :

$$\varphi_a(\lambda P + \mu Q) = \sum_{k\in\mathbb{N}} (\lambda p_k + \mu q_k) a^k = \lambda \sum_{k\in\mathbb{N}} p_k a^k + \mu \sum_{k\in\mathbb{N}} q_k a^k = \lambda \varphi_a(P) + \mu \varphi_a(Q)$$

et, si $R = PQ$: $R = \sum_{k\in\mathbb{N}} r_k X^k$ avec $r_k = \sum_{i+j=k} p_i q_j$

$$\varphi_a(PQ) = \sum_{k\in\mathbb{N}} r_k a^k = \sum_{k\in\mathbb{N}} \Big(\sum_{i+j=k} p_i q_j \Big) a^k = \sum_{i\in\mathbb{N}} p_i a^i \cdot \sum_{j\in\mathbb{N}} q_j a^j = \varphi_a(P)\,\varphi_a(Q)$$

(car les a^i et les a^j commutent !)

PARTIE 2.A

1) $\mathcal{A}$ étant de dimension finie, la famille $\{a^k, k \in \mathbb{N}\}$ est liée.
C'est à dire qu'il existe une famille $(\lambda_k)_{k\in\mathbb{N}}$ d'élts de $\mathbb{C}$, à support fini et non tous nuls telle que $\sum_{k\in\mathbb{N}} \lambda_k a^k = 0$.
Si $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$, alors $P \in \mathbb{C}[X]$, P est non nul, et $P(a) = 0$.

2) Il existe $\lambda \in \mathbb{C}$ et des $\alpha_i \in \mathbb{C}$ (non nécessairement distincts) tels que

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

En utilisant le fait que φ_a est un morphisme, on en déduit :

$$P(a) = \lambda \prod_{i=1}^{n} (a - \alpha_i \cdot 1_A)$$

Or $P(a) = 0$ et $\mathcal{A}$ est intègre : il existe donc i tel que $a - \alpha_i 1_A = 0$, soit $a = \alpha_i \cdot 1_{\mathcal{A}}$

3) Il est facile de vérifier que l'application $\begin{array}{l}\mathbb{C} \to \mathcal{A}\\ \alpha \mapsto \alpha \cdot 1_{\mathcal{A}}\end{array}$ est un isomorphisme d'algèbres.

PARTIE 2.B.

1) Soit $a \in \mathcal{A}$, $a \neq 0$. L'application $\varphi : \begin{array}{l}\mathcal{A} \to \mathcal{A}\\ x \mapsto ax\end{array}$ (on a bien $ax \in \mathcal{A}$!)
est (facile) $\mathbb{R}$-linéaire (en utilisant les règles de calcul usuelles dans une algèbre)

De plus, φ est injective car : $x \in \operatorname{Ker}\varphi \Rightarrow ax = 0 \Rightarrow x = 0$ car $\mathcal{A}$ intègre

Le $\mathbb{R}$-e.v. $\mathcal{A}$ étant de dimension finie, on en déduit que φ est bijective.

En particulier : $\exists a' \in \mathcal{A}$ tq $\varphi(a') = 1_{\mathcal{A}}$ soit $aa' = 1$. $\mathcal{A}$ étant commutative, on a donc $aa' = a'a = 1$, et a est inversible.

Tout élt non nul de $\mathcal{A}$ étant inversible, on en déduit que $(\mathcal{A}, +, \times)$ est un corps.

2°) a) • il existe bien $x_0 \in \mathcal{A}$, tel que $x_0 \notin \mathbb{R}.1_{\mathcal{A}}$: sinon, on aurait $\mathcal{A} = \mathbb{R}.1_{\mathcal{A}}$ et $\mathcal{A}$ serait de dimension 1, ce qui est exclu par l'énoncé

• Il n'existe donc pas $\lambda \in \mathbb{R}$ tq $x_0 = \lambda 1_A$ donc $(1, x_0)$ est libre

b) En raisonnant comme dans 2.A.1, on obtient qu'il existe un polynôme $P \in \mathbb{R}[X]$, non nul, tel que $P(a) = 0$. La décomposition de P en facteurs irréductibles de $\mathbb{R}[X]$ peut s'écrire : $P = \lambda . \prod_{i=1}^{n} (X - \alpha_i) \prod_{j=1}^{m} Q_j$, où $\lambda, \alpha_i \in \mathbb{R}$, Q_j poly. irréductib de degré 2.

On a alors : $\lambda \prod_{i=1}^{n} (x_0 - \alpha_i 1_{\mathcal{A}}) \prod_{j=1}^{m} Q_j(x_0) = 0$.

Or $x_0 - \alpha_i 1_{\mathcal{A}} \neq 0$ pour tout i (car $x_0 \notin \mathbb{R}.1_{\mathcal{A}}$), et $\mathcal{A}$ est intègre, donc il existe j tel que $Q_j(x_0) = 0$.

c) En notant $Q_j = X^2 + pX + q$, avec $p^2 - 4q < 0$, on a : $x_0^2 + px_0 + q.1_{\mathcal{A}} = 0_{\mathcal{A}}$

soit $\left(x_0 + \frac{p}{2}\right)^2 = \frac{p^2 - 4q}{4} . 1_{\mathcal{A}} = \frac{4q - p^2}{4} (-1_{\mathcal{A}})$.

En posant $y_0 = \frac{2}{\sqrt{4q - p^2}} \left(x_0 + \frac{p}{2}\right)$, on trouve bien $\underline{y_0^2 = -1_{\mathcal{A}}}$

3°) a) • θ morphisme injectif de $\mathbb{R}$-algèbres : facile

• donc, d'après le cours, $\mathbb{C}$ corps $\Rightarrow \theta(\mathbb{C})$ sous-corps de $\mathcal{A}$.

b) Pour vérifier que $\mathcal{A}$ est bien une $\mathbb{K}$-algèbre, puisque l'on sait déjà que $(\mathcal{A}, +, \times)$ est un anneau, il suffit en fait de vérifier que :

- $\forall \lambda \in \mathbb{K}, \forall x \in \mathcal{A}$, $\lambda x \in \mathcal{A}$: cela découle de $\mathbb{K} \subset \mathcal{A}$
- $\forall \lambda \in \mathbb{K}, \forall (x, y) \in \mathcal{A}^2$ $\lambda(xy) = x(\lambda y) = (\lambda x) y$: cela découle du fait que $\mathcal{A}$ est <u>commutative</u>

(c'est <u>ici</u> que sert cette hypothèse !)

c) $\mathbb{K}$ étant isomorphe à $\mathbb{C}$, $\mathbb{K}[X]$ est isomorphe à $\mathbb{C}[X]$, et on peut donc, comme dans 2.A.2, en déduire que, pour tout $a \in \mathcal{A}$, il existe $\alpha \in \mathbb{K}$ tq $a = \alpha$

soit $\boxed{\mathcal{A} = \mathbb{K}}$

1°) Cela se démontre presque comme 2.B.1 ; mais ici, $\mathcal{A}$ n'étant pas supposé commutative, il faut considérer les deux applications $x \mapsto ax$ et $x \mapsto xa$.
(cf. une dém. similaire vue en cours)

2°) Il suffit de vérifier, en utilisant les règles de calcul dans la $\mathbb{R}$-algèbre $\mathcal{A}$, que :

$$\begin{cases} \sigma(1_{\mathcal{A}}) = 1_{\mathcal{A}} \ ; \ \forall (x,y) \in \mathcal{A}^2, \ \sigma(x+y) = \sigma(x) + \sigma(y) \text{ et } \sigma(xy) = \sigma(x)\sigma(y) \\ \forall x \in \mathcal{A}, \ \forall \lambda \in \mathbb{R}, \ \sigma(\lambda x) = \lambda \sigma(x). \end{cases}$$

Enfin : $\forall x \in \mathcal{A}$, $\sigma[\sigma(x)] = u(uxu^{-1})u^{-1} = u^2 x (u^2)^{-1} = (-1_{\mathcal{A}})\, x\, (-1_{\mathcal{A}}) = x$
d'où $\sigma^2 = Id_{\mathbb{H}}$. σ est donc involutive, et, par suite, bijective.

3°) CF. COURS : σ automorphisme involutif de $\mathbb{R}$-e.v $\Rightarrow$ σ est une symétrie p.r. à $\mathcal{A}'$ de direction $\mathcal{A}''$.

4°) a) • Soient $x, y \in \mathcal{A}'$ et $\lambda, \mu \in \mathbb{R}$. Alors :

$\sigma(\lambda x + \mu y) = \lambda \sigma(x) + \mu \sigma(y) = \lambda x + \mu y$ donc $\lambda x + \mu y \in \mathcal{A}'$

$\sigma(xy) = \sigma(x)\sigma(y) = xy$ donc $xy \in \mathcal{A}'$.

Enfin, $\sigma(1_{\mathcal{A}}) = 1_{\mathcal{A}}$ d'où $1_{\mathcal{A}} \in \mathcal{A}'$: $\mathcal{A}'$ est une sous-algèbre de $\mathcal{A}$.

b) $1_{\mathcal{A}} \in \mathcal{A}'$ et $u \in \mathcal{A}'$ $\Rightarrow$ $\mathrm{Vect}(1_{\mathcal{A}}, u) = \mathbb{K}$ est inclus dans $\mathcal{A}'$.

c) Si $x \in \mathcal{A}'$, $\sigma(x) = x$ soit $ux = xu$. Ainsi u commute avec tous les élts de $\mathcal{A}'$, donc tous les élts de $\mathbb{K}$ commutent avec ceux de $\mathcal{A}'$. On en déduit alors, comme dans 2.B.3.b, que $\mathcal{A}'$ est une $\mathbb{K}$-algèbre.

$\mathbb{K}$ étant isomorphe à $\mathbb{C}$, on démontre alors, comme dans 2.B.3.c., $\mathcal{A}' = \mathbb{K}$.

5°) a) Si $\mathcal{A}''$ était réduit à $\{0\}$, on aurait $\mathcal{A} = \mathcal{A}' = \mathbb{K}$; $\mathcal{A}$ serait alors commutative, ce qui est exclu par l'énoncé.

Il existe donc $z_0 \neq 0$, $z_0 \in \mathcal{A}''$.

b) • Soit $x \in \mathcal{A}'$: $\sigma(xz_0) = \sigma(x)\sigma(z_0) = x.(-z_0) = -xz_0$, donc $xz_0 \in \mathcal{A}''$

D'où $\mathcal{A}' z_0 \subset \mathcal{A}''$.

• Récip^t., soit $x \in \mathcal{A}''$. $z_0 \neq 0$ donc z_0 inversible ($\mathcal{A}$ corps) et on a :

$\sigma(xz_0^{-1}) = \sigma(x)\sigma(z_0)^{-1} = -x.(-z_0)^{-1} = xz_0^{-1}$

donc $xz_0^{-1} \in \mathcal{A}'$, d'où $x \in \mathcal{A}' z_0$.

On a donc $\mathcal{A}'' = \mathcal{A}' z_0$

[On pouvait en déduire $\dim_{\mathbb{R}} \mathcal{A}'' = \dim_{\mathbb{R}} \mathcal{A}' = 2$, d'où $\dim_{\mathbb{R}} \mathcal{A} = 4$].

6°/ $z_0 \neq 0 \in \mathcal{A}''$, donc $z_0 \notin \mathcal{A}'$ et, a fortiori, $z_0 \notin \mathbb{R}$. La même démonstration qu'en 2.B.2 montre qu'il existe $p, q \in \mathbb{R}$ tq $z_0^2 + p z_0 + q.1_{\mathcal{A}} = 0$ avec $p^2 - 4q < 0$

On a alors $\sigma(z_0)^2 + p\sigma(z_0) + q.1_{\mathcal{A}} = 0$

d'où $z_0^2 - p z_0 + q.1_{\mathcal{A}} = 0$ (car $z_0 \in \mathcal{A}'' \Rightarrow \sigma(z_0) = -z_0$)

d'où $z_0^2 + q.1_{\mathcal{A}} = 0$.

Or $q > 0$ (car $p^2 - 4q < 0$), donc $v = \frac{1}{\sqrt{q}} z_0$ est bien t.q. $v \in \mathcal{A}''$ et $v^2 = -1_{\mathcal{A}}$.

7°/ • On sait déjà que $(1_{\mathcal{A}}, u)$ est une base du $\mathbb{R}$-e.v. $\mathcal{A}'$.

• On a : $uv \in \mathcal{A}''$ (car $\sigma(uv) = \sigma(u)\sigma(v) = u.(-v) = -uv$)

et (v, uv) est libre (car $\lambda v + \mu uv = 0 \Rightarrow (\lambda.1_A + \mu u)v = 0$

$\Rightarrow \lambda.1_A + \mu u = 0$ car $\mathcal{A}$ intègre et $v \neq 0$

$\Rightarrow \lambda = \mu = 0$ car $(1_{\mathcal{A}}, u)$ est libre)

Or on a vu ci-dessus que $\dim \mathcal{A}'' = 2$, donc (v, uv) est une base de $\mathcal{A}''$.

Donc, puisque $\mathcal{A} = \mathcal{A}' \oplus \mathcal{A}''$, $(1_A, u, v, w)$ est une base de $\mathcal{A}$.

8°/ On a $u^2 = v^2 = -1_A$ et $uv = -vu$ (car $v \in \mathcal{A}'' \Rightarrow uvu^{-1} = -v$)

d'où $w^2 = uvuv = u(-uv)v = -u^2v^2 = -1_A$.

Puis $uw = u^2 v = -v$; etc..

On trouve facilement la table de multiplication suivante :

	1	u	v	w
1	1	u	v	w
u	u	-1	w	$-v$
v	v	$-w$	-1	u
w	w	v	$-u$	-1

qui est "semblable" à celle de $\{E, I, J, K\}$ dans $\mathbb{H}$.

Il est alors facile d'en déduire que l'application

$$f : \mathbb{H} \longrightarrow \mathcal{A}$$

$$aE + bI + cJ + dK \longmapsto a1_{\mathcal{A}} + bu + cv + dw \qquad (a,b,c,d) \in \mathbb{R}^4$$

est un isomorphisme de $\mathbb{R}$-algèbres.