Devoir surveillé $n°01$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

•••••••••

Exercice I

1. (a) Pour $n=0$, $A^0=1=0\times 1+0\times\sqrt{2}$. Supposons que A^n peut s'écrire sous la forme $p_n+q_n\sqrt{2}$ où p_n et q_n sont des entiers naturels et montrons que $A^{n+1}=p_{n+1}+q_{n+1}\sqrt{2}$ où p_{n+1} et q_{n+1} sont des entiers naturels. On a

$$\begin{aligned} A^{n+1} &= A^n\times A \\ &= (p_n+q_n\sqrt{2})(1+\sqrt{2}) \\ &= (p_n+2q_n\sqrt{2})+(p_n+q_n)\sqrt{2} \\ &= p_{n+1}+q_{n+1}\sqrt{2} \end{aligned}$$

avec $p_{n+1}=p_n+2q_n$ et $q_{n+1}=p_n+q_n$. Comme p_n et q_n sont des entiers, alors (p_{n+1},q_{n+1}) est un couple des entiers naturels.
Par le principe de récurrence, pour chaque $n\in\mathbb{N}$, il existe un couple des entiers (p_n,q_n) tel que $A^n=p_n+q_n\sqrt{2}$.

(b) Supposons que $m+n\sqrt{2}=p+q\sqrt{2}$. Alors on a aussi $(m-p)+(n-q)\sqrt{2}=0$. Si $n\neq q$, alors $\sqrt{2}=\dfrac{m-p}{n-q}\in\mathbb{Q}$ ce qui est faux. Donc nécessairement $n-q=0-$ et $m-p=0$, soit encore $m=p$ et $n=q$.

2. $(p_0,q_0)=(1,0)$ et $(p_1,q_1)=(1,1)$.

3. D'après la première question $p_{n+1}=p_n+2q_n$ et $q_{n+1}=p_n+q_n$.

4. On a

$$p_{n+2}=p_{n+1}+2q_{n+1}=p_{n+1}+2(p_n+q_n)=2p_{n+1}+p_n$$

et

$$q_{n+2}=p_{n+1}+q_{n+1}=p_n+2q_n+q_{n+1}=2q_{n+1}+q_n.$$

5. L'équation caractéristique associée au deux relations linéaires s'écrit : $r-2r-1=0$, dont les racines sont $1+\sqrt{2}$ et $1-\sqrt{2}$, donc il existe des réels $\alpha,\beta,\gamma,\delta$ tels que $p_n=\alpha(1+\sqrt{2})^n2+\beta(1-\sqrt{2})^n$ et $q_n=\gamma(1+\sqrt{2})^n2+\delta(1-\sqrt{2})^n$. Les conditions initiales montre que $\alpha=\beta=\dfrac{1}{2}$ et $\gamma=\delta=$. D'où :

$$\forall n\in\mathbb{N},\ \ p_n=\frac{1}{2}\left[(1+\sqrt{2})^n+(1-\sqrt{2})^n\right]$$

et

$$\forall n\in\mathbb{N},\ \ q_n=\frac{1}{2}\left[(1+\sqrt{2})^n+(1-\sqrt{2})^n\right].$$

Exercice II

1. On a clairement $\mathbb{Z}_\alpha\subset\mathbb{C}$ et $1=1+\alpha 0\in\mathbb{Z}_\alpha$. Soit $z,z'\in\mathbb{Z}_\alpha$ avec $z=p+q\alpha$ et $z'=p'+q'\alpha$ avec $p,p',q,q'\in\mathbb{Z}$, on a :

$$z-z'=(p+q\alpha)-(p'+q'\alpha)=(p-p')+(q-q')\alpha\in\mathbb{Z}_\alpha$$

car $p-p'$ et $q-q'$ sont des entiers relatifs de plus

$$zz'=(p+q\alpha)(p'+q'\alpha)=pp'+(pq'+p'q)\alpha+qq'\alpha^2$$

or d'après (1) $\alpha^2=b\alpha-c$, d'où

$$zz'==pp'-qq'c+(pq'+p'q+qq'b)\alpha$$

Par conséquent $(\mathbb{Z}_\alpha,+,.)$ est un anneau.

2. Soit $z = p + q\alpha = 0$. Si $q \neq 0$, alors $\alpha = \dfrac{-p}{q} \in \mathbb{C} \setminus \mathbb{Q}$, car α est une racine de (1) et $\triangle = b^2 - 4c < 0$. Donc nécessairement $q = 0$ et par conséquent $p = 0$.

3. (a) En prenant $z = p + q\alpha$ et $z' = p' + q'\alpha$ on a montré que

$$zz' = pp' - qq'c + (pq' + p'q + qq'b)\alpha$$

En développant f il vient

$$f(zz') = (pp' - cqq')^2 + b(pp' - cqq')(pq' + qp' + bqq') + c(pq' + qp' + bqq')^2$$

et par ailleurs

$$f(z)f(z') = (p^2 + bpq + cq^2)(p'^2 + bp'q' + cq'^2)$$

On vérifie alors aisément par soustraction que :

$$\forall z, z \in \mathbb{Z}_\alpha, \quad f(zz') = f(z)f(z').$$

(b) Si $z = 0$, par définition $f(z) = 0$. Supposons maintenant $f(z) = 0$, alors $p^2 + bpq + cq^2 = 0$, donc si $q \neq 0$, $\left(\dfrac{p}{q}\right)^2 + b\left(\dfrac{p}{q}\right) + c = 0$. Donc $\dfrac{p}{q}$ est une racine réelle non complexe de l'équation du second degré $t^2 + bt + c = 0$ et donc nécessairement $\triangle = (-b)^2 - 4c \geq 0$ ce qui est absurde, donc nécessairement $q = 0$ et puis $p = 0$, ainsi $z = 0$.

4. (a) Cours

(b) Soit $z \in G_\alpha$, notons z^{-1} l'inverse de z, on a :

$$f(zz^{-1}) = f(1) = f(z)f(z^{-1}) = 1 \ \ (\text{car} \ \ f(1) = 1)$$

Or $f(z), f(z^{-1}) \in \mathbb{Z}^+$, donc nécessairement $f(z) = 1$, d'où $f(G_\alpha) \subset \{\ 1\ \}$ et comme $f(1) = 1$. D'où $f(G_\alpha) = \{\ 1\ \}$.

(c) Soit $z = p + q\alpha \in G_\alpha$, on a :

$$f(z) = f(p + q\alpha) \Rightarrow p^2 + bpq + cq^2 = 1$$

Donc p est une racine de l'équation du second degré $t^2 + bqt + (cq^2 - 1) = 0$ donc son discriminant $\triangle = (bq)^2 - 4(cq^2 - 1) \geq 0$ ou encore $q^2(b^2 - 4c) \geq -4$ ce qui équivalent à $q^2(4c - b^2) \leq 4$.

(d) Soit $z = p + q\alpha \in G_\alpha$, alors nécessairement $3q^2 \leq 4$. Ainsi on a trois choix pour $q = -1, 0$ et 1. On cherche les éléments inversibles :

- Si $q = -1$, alors $f(p + q\alpha) = p^2 + p + 1 = 1$, donc $p = 0$ ou $p = -1$ convient.
- Si $q = 0$ alors $f(p + q\alpha) = p^2 = 1$, donc $p = 1$ ou $p = -1$ conviennent.
- Si $q = 1$ alors $f(p + q\alpha) = p^2 - p + 1 = 1$ donc $p = 0$ ou $p = 1$ conviennent.

Donc l'ensemble des éléments inversibles est :

$$G_\alpha = \{\ -\alpha, -1 - \alpha, 1, -1, \alpha, 1 + \alpha\ \}.$$

5. Il est clair que cet ensemble est un sous-anneau de $(\mathbb{C}, +, .)$. Donc il suffit de montrer que tous les éléments de $\mathbb{Q}_\alpha^* = \mathbb{Q}_\alpha \setminus \{0\}$ sont inversibles par la loi $(.)$.
Soient w et w' de $\mathbb{Q}_\alpha$ tels que $ww' = 1$. On a d'après les calculs précédents le système :

$$\begin{cases} vv' - cuu' &= 1 \\ uv' + (bu + v)u' &= 0 \end{cases}$$

On obtient les solutions :

$$\begin{cases} u' &= \dfrac{-u}{v^2 + vbu + cu^2} \\ v' &= \dfrac{bu + v}{v^2 + vbu + cu^2} \end{cases}$$

qui existent, sont rationnels et unique puisqu'on a démontrer que le dénominateur est strictement positif.
On vérifie que l'élément $w' = u' + \alpha v'$ convient et donc tous les éléments sont inversibles.

6. On peut vérifier facilement que $\mathbb{Q}_\alpha$ est un sous-espace vectoriel de $\mathbb{C}$, de plus la famille $(1, \alpha)$ est une famille génératrice et libre, donc $\dim_{\mathbb{Q}}(\mathbb{Q}_\alpha) = 2$.

Problème

1. On a $\mathrm{Im}(A) = \mathrm{Im}(EA) \subset \mathrm{Im}(E)$, donc $\mathrm{rg}(A) = \mathrm{rg}(EA) \leq \mathrm{rg}(E)$. De même $\mathrm{Im}(E) = \mathrm{Im}(AA') \subset \mathrm{Im}(A)$, donc $\mathrm{rg}(E) \leq \mathrm{rg}(A)$. Finalement $\forall A \in G$, $\mathrm{rg}(A) = \mathrm{rg}(E) = r$.

2. (a) Soit $x \in \mathrm{Im}(E) \cap \ker(E)$. Si $x = Ey$ avec $y \in \mathbb{R}^n$ alors $Ex = E^2y$ Comme $E^2 = E$, $x = Ey = Ex = 0$, donc $\mathrm{Im}(E) \cap \ker(E) = \{0\}$. On sait que $\dim \mathrm{Im}(E) + \dim \ker(E) = \dim(\mathbb{R}^n)$ (théorème du rang) ceci montre que $\mathbb{R}^n = \mathrm{Im}(E) \oplus \ker(E)$.

(b) Comme $E^2 = E$, $E|_{\mathrm{Im}\,E}$ est l'application identique de $\mathrm{Im}(E)$. Donc si $r < n$, soit $(e_1, e_2, ..., e_r)$ une base de $\mathrm{Im}(E)$ et $(e_{r+1}, ..., e_n)$ une base de $\ker(E)$. Alors $(e_1, e_2, ..., e_n)$ est une base de $\mathbb{R}^n$, dans cette base, E a pour matrice $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$
Si $r = n$, $E = I_n$.

(c) Montrons que $\ker(A) = \ker(E)$, en effet :

$$Ex = 0 \Rightarrow AEx = 0 \Rightarrow Ax = 0$$

et

$$Ax = 0 \Rightarrow A'Ax = 0 \Rightarrow Ex = 0$$

donc $\ker(A) = \ker(E)$ et on a vu $\mathrm{Im}(A) = \mathrm{Im}(E)$. Donc dans la base $(e_1, e_2, ..., e_n)$ A a donc pour matrice $\begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}$ et $A_1 \in \mathbf{GL}_r(\mathbb{R})$ puisque A est de rang r.
Soit alors $P \in \mathbf{GL}_n(\mathbb{R})$ et G_r un sous-groupe de $\mathbf{GL}_r(\mathbb{R})$, les sous-groupes G de matrices de rang r sont de la forme :

$$G = \left\{ P^{-1} \begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix} P \ \text{ où } \ A_1 \in G_r \right\}$$

3. (a)

(i)⇒(ii) Si $A \in G$, alors $A^2 \in G$ et donc $\mathrm{rg}(A^2) = \mathrm{rg}(A)$.

(ii)⇒(iii) On a toujours $\mathrm{Im}(A^2) \subset \mathrm{Im}(A)$, si de plus $\mathrm{rg}(A) = \mathrm{rg}(A^2)$, alors $\mathrm{Im}(A^2) = \mathrm{Im}(A)$.

(iii)⇒(iv) On a toujours $\ker(A) \subset \ker(A^2)$, si de plus $\mathrm{Im}(A^2) = \mathrm{Im}(A)$, alors $\mathrm{rg}(A^2) = \mathrm{rg}(A)$ et $\dim \ker(A) = \dim(\ker(A^2))$, donc $\ker(A^2) = \ker(A)$.

(iv)⇒(v) Soit $x = Ay \in \ker(A) \cap \mathrm{Im}(A)$, alors $Ax = A^2y = 0$, comme $\ker(A) = \ker(A^2)$, $Ay = 0 = x$, donc $\ker(A) \cap \mathrm{Im}(A) = \{0\}$, comme $\dim \mathrm{Im}(A) + \dim \ker(A) = \dim \mathbb{R}^n$, $\mathbb{R}^n = \mathrm{Im}(A) \oplus \ker(A)$.

(v)⇒(i) Si $\mathbb{R}^n = \mathrm{Im}(A) \oplus \ker(A)$, alors $A|_{\mathrm{Im}(A)}$ est injectif donc bijectif, et dans une base adaptée à la décomposition, A a pour matrice $\begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}$ où A_1 est inversible. A appartient alors au groupe

$$G = \left\{ \begin{pmatrix} A_1^m & 0 \\ 0 & 0 \end{pmatrix} \,\middle|\, m \in \mathbb{Z} \right\}$$

(b) Soit $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ alors $A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\ker(A^2) \neq \ker(A)$. A ne saurait donc appartenir à aucun groupe multiplicatif de $\mathscr{M}_2(\mathbb{R})$.

(c) Soit $X \in \mathscr{M}_n(\mathbb{R})$ telle que $AX = XA$, $X^2A = X$ et $A^2X = A$. Alors $A^2x = 0$ entraine $XA^2x = 0$ et donc $A^2Xx = Ax = 0$, donc $\ker(A) = \ker(A^2)$ et les cinq propriétés sont vérifiées.
Réciproquement, si on prend $X = A'$, on voit que X vérifie les trois conditions précédentes.

(d) Soit $Y \in \mathscr{M}_n(\mathbb{R})$ vérifiant les trois conditions précédentes. D'une part, $AXAY = (AXA)Y = AY$. D'autre part, $AXAY = (AX)(AY) = (XA)(YA) = X(AYA) = XA$. Conclusion : $AY = XA$. D'où $X = XAX = XXA = XAY = AYY = YAY = Y$.

(e) Si X existe, alors $\ker(A)$ et $\mathrm{Im}(A)$ sont stables par X puisque X et A commutent et $X|_{\ker(A)} = 0$ puisque $X^2A = X$.
Si A s'écrit dans une base sous la forme $\begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}$ où $A_1 \in \mathbf{GL}_r(\mathbb{R})$, alors X s'écrit $\begin{pmatrix} X_1 & 0 \\ 0 & 0 \end{pmatrix}$. $X_1 = X|_{\mathrm{Im}(A)}$ est injectif car $A^2X = A$ donc bijectif.
Finalement, de $A_1^2X_1 = A_1$, on tire $X_1 = A_1^{-1}$. Ceci montre que X est unique et égal à A'.
Pour A fixé, A' est donc entièrement caractérisé par les trois conditions de 3.c, et ne dépend pas du groupe G auquel A appartient.

4. (a) Soit $B = \begin{pmatrix} B_1 & B_2 \\ 0 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{R})$ avec $B_1 \in \mathbf{GL}_r(\mathbb{R})$. $B^2 = \begin{pmatrix} B_1^2 & B_1B_2 \\ 0 & 0 \end{pmatrix}$. B est de rang r puisque le rang d'une matrice est l'ordre maximal de sous-matrices inversibles et que, clairement, B_1 est une telle sous-matrice. Donc $\mathrm{rg}(B) = r = \mathrm{rg}(B^2)$ et par conséquent B appartient à un groupe multiplicatif de matrices G. Si on prend $E = \begin{pmatrix} I_r & B_1^{-1}B_2 \\ 0 & 0 \end{pmatrix}$, alors on vérifie que $BE = EB = B$. E sera donc l'élément neutre de G. Cherchons B' de la forme $B' = \begin{pmatrix} C_1 & C_2 \\ 0 & 0 \end{pmatrix}$. Les calculs précédentes montrent qu'on doit avoir : $C_1 = B_1^{-1}$ et $C_2 = (B_1^{-1})^2B_2$.
Réciproquement, si on considère $B' = \begin{pmatrix} B_1^{-1} & (B_1^{-1})^2B_2 \\ 0 & 0 \end{pmatrix}$ alors on a les relations $BB' = B'B$, $B'^2B = B'$ et $B^2B' = B$.

(b) Comme A est de rang 2, on se place dans une base où A est de la forme $\begin{pmatrix} a & b & \lambda \\ c & d & \mu \\ 0 & 0 & 0 \end{pmatrix}$ où $A_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible.
Il est clair que $\mathrm{Im}(A) = \mathrm{Vect}(v_1, v_2)$ avec $v_1 = \begin{pmatrix} 1 & 2 & 0 \end{pmatrix}$ et $v_2 = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}$. Si on choisit $v_3 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$, on voit bien que (v_1, v_2, v_3) est une base de $\mathbb{R}^3$. On a $Av_1 = Ae_1 + 2Ae_2 + Ae_3 = \begin{pmatrix} 6 & 12 & 1 \end{pmatrix} = v_1 + 5v_2$, $Av_2 = Ae_1 + 2Ae_2 = \begin{pmatrix} 5 & 10 & 1 \end{pmatrix} = v_1 + 4v_2$ et $Av_3 = Ae_2 = 2v_2$. Donc A est semblable à la matrice $B = \begin{pmatrix} 1 & 1 & 0 \\ 5 & 4 & 2 \\ 0 & 0 & 0 \end{pmatrix}$, plus précisément on a : $B = P^{-1}AP$ avec $P = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. D'après la question précédente, $B' = \begin{pmatrix} B_1^{-1} & (B_1^{-1})^2B_2 \\ 0 & 0 \end{pmatrix}$ avec $B_1 = \begin{pmatrix} 1 & 1 \\ 5 & 4 \end{pmatrix}$ et $B_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$. D'après des calculs, on trouve $B' = \begin{pmatrix} -4 & 1 & -10 \\ 5 & -1 & 12 \\ 0 & 0 & 0 \end{pmatrix}$ et par conséquent $A' = PB'P^{-1} = \begin{pmatrix} -4 & 2 & 1 \\ -8 & 4 & 2 \\ 21 & -10 & -5 \end{pmatrix}$

●●●●●●●●●