Corrigé du devoir surveillé n°4

Exercice 1.

Soit $A = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 3 & -1 \\ -4 & 8 & -3 \end{pmatrix}$.

1. Calculer A^2+A puis en déduire un polynôme annulateur de A. Est-ce le polynôme minimal de A ?
2. Montrer que A est inversible en exhibant son inverse.
3. Calculer A^n pour $n \in \mathbb{N}^*$.

Correction.

1. On a $A^2+A = 2I_3$ donc $A^2+A-2I_3 = 0_3$ d'où $P = X^2+X-2$ est un polynôme annulateur de A. Comme A n'est pas de la forme αI_3, aucun polynôme de degré 1 n'annule A d'où $\deg(\pi_A) \geq 2$. Or $\pi_A | P$ et π_A et P sont unitaire donc $\pi_A = P$.
2. On pose $B = \frac{1}{2}(A+I_3)$. Alors on a :
$$AB = \frac{1}{2}(A^2+A) = \frac{1}{2}(2I_3) = I_3$$
donc A est inversible et $A^{-1} = B = \frac{1}{2}(A+I_3)$.
3. Soit $n \in \mathbb{N}$. On effectue la division euclidienne de X^n par $\pi_A = X^2+X-2 = (X-1)(X+2)$: il existe $Q, R \in \mathbb{R}[X]$ tels que $\deg(R) < \deg(\pi_A) = 2$. Ainsi, il existe $a_n, b_n \in \mathbb{R}$ tels que $R = a_nX + b_n$.
De plus, on a, en evaluant l'égalité $X^n = \pi_A Q + R$ en 1 et -2 :
$$\begin{cases} 1 = a_n + b_n \\ (-2)^n = -2a_n + b_n \end{cases} \Leftrightarrow \begin{cases} a_n = \frac{1}{3}(1-(-2)^n) \\ b_n = \frac{1}{3}(2+(-2)^n) \end{cases}$$
Ainsi, on a :
$$A^n = R(A) = a_nA + b_nI_3 = \frac{1}{3}\left((1-(-2)^n)A + (2+(-2)^n)I_3\right).$$

Exercice 2.

On dit qu'un polynôme $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{C}[X]$ de degré $n \in \mathbb{N}$ (donc $P \neq 0$) est **réciproque** si :
$$\text{pour tout } k \in [\![0,n]\!],\ a_{n-k} = a_k$$
Par exemple, $P = 1+X+X^2+X^3$ et $Q = 7-2X+7X^2$ sont des polynômes réciproques.

1. Soit $P \in \mathbb{C}[X]$ de degré n. Démontrer que P est réciproque si et seulement si $P(X) =$

$X^n P\left(\frac{1}{X}\right)$.

2. Montrer qu'un produit de polynômes réciproques est réciproque.
3. On suppose que P et Q sont réciproques et que $Q|P$. Démontrer que $\frac{P}{Q}$ est réciproque.
4. Soit $P \in \mathbb{C}[X]$ un polynôme réciproque.
   (a) Démontrer que si α est une racine de P, alors $\alpha \neq 0$ et α^{-1} est une racine de P.
   (b) Démontrer que si 1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
   (c) Démontrer que si le degré de P est impair, alors -1 est racine de P.
   (d) Démontrer que si P est de degré pair et si -1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
5. Démontrer que tout polynôme réciproque de $\mathbb{C}[X]$ de degré $2n$ se factorise en

$$P = a_{2n}(X^2 + b_1 X + 1)\dots(X^2 + b_n X + 1).$$

Que peut-on dire si le degré de P est impair ?

Correction.

1. Soit $P = a_n X^n + \cdots + a_0$, alors

$$X^n P\left(\frac{1}{X}\right) = a_0 X^n + \cdots + a_n.$$

Ainsi, si P est réciproque, on a bien $X^n P(1/X) = P(X)$. Réciproquement, si $X^n P(1/X) = P(X)$, alors on a nécessairement $a_0 = a_n$, $a_1 = a_{n-1}$, etc... Donc P est réciproque.

2. Soient P et Q réciproques, de degrés respectifs n et m. Alors

$$X^n P(1/X) = P(X) \text{ et } X^m Q(1/X) = Q(X).$$

On en déduit que

$$X^{n+m}(PQ)(1/X) = X^n P(1/X) X^m Q(1/X) = P(X)Q(X) = (PQ)(X).$$

Ainsi, d'après la question précédente, PQ est réciproque.

3. Le raisonnement est complètement identique, en utilisant le quotient au lieu du produit !
4. (a) Puisque P est réciproque, $a_0 = a_n \neq 0$ et donc $P(0) = a_0 \neq 0$. D'autre part, si α est racine de P, alors la relation $P(\alpha) = \alpha^n P(\alpha^{-1})$ prouve que α^{-1} est aussi racine de P.
   (b) Dérivons la relation de la première question. On trouve, pour tout $x \neq 0$,

$$P'(x) = nx^{n-1}P(1/x) - x^{n-2}P'(1/x).$$

On évalue en 1, et on trouve

$$P'(1) = -P'(1)$$

et donc $P'(1) = 0$. On en déduit que 1 est racine au moins double.

   (c) On utilise encore le résultat de la première question, et on remarque que $P(-1) = -P(-1)$ puisque le degré de P est impair. Donc $P(-1) = 0$.

(d) On raisonne exactement comme deux questions plus haut.

5. On va procéder par récurrence sur n, le cas $n = 1$ étant trivial. Supposons donc que le résultat a été démontré pour tout polynôme réciproque de degré $2n$, et prouvons-le pour un polynôme réciproque P de degré $2n + 2$. Soit α une racine de P. Alors, on sait que $\alpha \neq 0$ et que α^{-1} est aussi racine de P. Si $\alpha \neq 1, -1$, $\alpha^{-1} \neq \alpha$ et on peut factoriser P par $(X-\alpha)(X-\alpha^{-1})$. Or, il est facile de vérifier que $(X-\alpha)(X-\alpha^{-1})$ s'écrit $(X^2+b_{n+1}X+1)$. D'autre part, si $\alpha = 1$ ou $\alpha = -1$, alors α est racine de multiplicité au moins deux, et on peut factoriser par $(X-\alpha)^2$. Un tel polynôme s'écrit encore $(X^2+b_{n+1}X+1)$. Donc, dans tous les cas, en notant $Q = X^2 + b_{n+1}X + 1$, on a $Q|P$ et P, Q réciproques. On en déduit que $\frac{P}{Q}$ est réciproque, de degré $2n$, donc par l'hypothèse de récurrence s'écrit

$$\frac{P}{Q} = a_{2n+2}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

On remultiplie par Q, et on a bien prouvé que le résultat est vrai au rang $n+1$. Si maintenant P est réciproque de degré impair $2n + 1$, alors -1 est racine de P et P se factorise par le polynôme réciproque $Q = X + 1$. Donc $\frac{P}{Q}$ est réciproque de degré pair $2n$, donc s'écrit $a_{2n+1}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1)$. Ainsi, tout polynôme réciproque de degré impair $2n + 1$ se factorise en

$$P = a_{2n+1}(X + 1)(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

Exercice 3.

On rappelle les notations suivantes : pour $n \in \mathbb{N}^*$,

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad \text{et} \quad \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}.$$

On pose :

$$G = \{z \in \mathbb{C} \mid \exists p \in \mathbb{Z},\ z^{2^p} = 1\}.$$

1. Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$ puis montrer que $\mathbb{U}_n$ est cyclique.
2. Montrer que G est un sous-groupe de $\mathbb{U}$.
3. a. Montrer que $\{n \in \mathbb{N}^* \mid \mathbb{U}_n \subset G\}$ est infini.

   b. En déduire que G est infini.
4. On suppose par l'absurde que G est monogène.

   a. Montrer qu'il existe $p \in \mathbb{N}$ tel que $G \subset \mathbb{U}_{2^p}$.

   b. En déduire une contradiction et conclure.
5. Montrer que tout sous-groupe fini de G est cyclique.

Correction.

1. Soit $n \in \mathbb{N}^*$.
   Pour tout $z \in \mathbb{U}_n$, on a $|z|^n = |z^n| = 1$. Comme $|z|$ est un réel positif et que l'équation

$x^n = 1$ admet 1 pour unique solution sur $\mathbb{R}_+$, on a $|z| = 1$. Par suite $z \in \mathbb{U}$.
On a donc $\mathbb{U}_n \subset \mathbb{U}$. Montrons que $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

— 1 est l'élément neutre de $(\mathbb{U}, \times)$ et on a $1^n = 1$ donc $1 \in \mathbb{U}_n$

— Soit $z_1, z_2 \in \mathbb{U}_n$. Alors $z_1^n = 1$ et $z_2^n = 1$ d'où :

$$\left(z_1 z_2^{-1}\right)^n = \left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1.$$

Donc $z_1 z_2^{-1}$ appartient à $\mathbb{U}_n$.

Ainsi, par la caractérisation des sous-groupes, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$. Montrons que $\mathbb{U}_n$ est cyclique. Tout d'abord, d'après le cours, $\mathbb{U}_n$ étant l'ensemble des racines n-ième de l'unité, on a :

$$\mathbb{U}_n = \left\{e^{i\frac{2k\pi}{n}} \mid k \in \mathbb{Z}\right\} = \left\{e^{i\frac{2k\pi}{n}} \mid k \in [\![0, n-1]\!]\right\}$$

donc $\mathbb{U}_n$ est fini de cardinal n et on a :

$$\left\langle e^{i\frac{2\pi}{n}} \right\rangle = \left\{\left(e^{i\frac{2\pi}{n}}\right)^k \mid k \in \mathbb{Z}\right\} = \left\{e^{i\frac{2k\pi}{n}} \mid k \in \mathbb{Z}\right\} = \mathbb{U}_n.$$

Ainsi, U_n est un groupe monogène fini et donc, par définition, cyclique.

2. Soit $z \in G$. ALors il existe $p \in \mathbb{Z}$ tel que $z^{2^p} = 1$ donc on a $|z|^{2^p} = |z^{2^p}| = 1$. Comme $|z|$ est un réel positif et que l'équation $x^n = 1$ admet 1 pour unique solution sur $\mathbb{R}_+$, on a $|z| = 1$. Par suite $z \in \mathbb{U}$.
On a donc $G \subset \mathbb{U}$. Montrons que G est un sous-groupe de $\mathbb{U}$.

— 1 est l'élément neutre de $(\mathbb{U}, \times)$ et on a $1^{2^0} = 1^1 = 1$ donc $1 \in G$

— Soit $z_1, z_2 \in G$. Alors il existe $p, q \in \mathbb{Z}$ tel que $z_1^{2^p} = 1$ et $z_2^{2^q} = 1$ d'où, comme $2^{p+q} = 2^p 2^q$:

$$\left(z_1 z_2^{-1}\right)^{2^{p+q}} = \frac{\left(z_1^{2^p}\right)^{2^q}}{\left(z_2^{2^q}\right)^{2^p}} = \frac{1^{2^q}}{1^{2^p}} = 1.$$

Donc $z_1 z_2^{-1}$ appartient à G.

Ainsi, par la caractérisation des sous-groupes, G est un sous-groupe de $\mathbb{U}$.

3. a. Soit $p \in \mathbb{N}$. Pour tout $z \in \mathbb{U}_{2^p}$, on a $z^{2^p} = 1$ donc $z \in G$. Ainsi, $\mathbb{U}_{2^p} \subset G$.
Par suite, pour tout $p \in \mathbb{N}$, $2^p \in \{n \in \mathbb{N}^* \mid \mathbb{U}_n \subset G\}$ et donc $\{n \in \mathbb{N}^* \mid \mathbb{U}_n \subset G\}$ est infini.

b. On note $A = \{n \in \mathbb{N}^* \mid \mathbb{U}_n \subset G\}$. D'après la question précédente, A est un sous-ensemble infini de $\mathbb{N}$ donc la suite $(u_n)_{n\in\mathbb{N}}$ telle que :

$$\begin{cases} u_0 = \min(A) \\ u_{n+1} = \min(A \setminus \{u_0, ..., u_n\}) \quad \text{pour tout } n \in \mathbb{N} \end{cases}$$

est bien définie et $u_n \geq n$ pour tout $n \in \mathbb{N}$ (récurrence immédiate).
Ainsi, pour tout $n \in \mathbb{N}$, on a $\mathbb{U}_{u_n} \subset G$ et :

$$n \leq u_n = \#\mathbb{U}_{u_n} \leq \#G$$

Donc, en faisant tendre n vers $+\infty$, d'après le théorème des gendarmes, $\#G = +\infty$.

On aurait pu également exhiber un sous-ensemble inifini de G :
On considère l'ensemble $E = \{e^{i\frac{2\pi}{2^p}} \mid p \in \mathbb{N}\}$. Alors pour tout $p, q \in \mathbb{N}$, $p \neq q$, on a :

$$e^{i\frac{2\pi}{2^p}} - e^{i\frac{2\pi}{2^q}} = e^{i\frac{2\pi}{2^p}}\left(1 - e^{2\pi i\frac{2^q-2^p}{2^{p+q}}}\right)$$

comme $p \neq q$, on a $2^q - 2^p \neq 0$ et on a $|2^q - 2^p| \leq \max(2^p, 2^q) \leq 2^{p+q}$ d'où $2\pi\frac{2^q-2^p}{2^{p+q}} \in]-2\pi, 2\pi[$.
Or, pour $\theta \in]-2\pi, 2\pi[$, $e^{i\theta} = 1$ si, et seulement si, $\theta = 0$ donc $e^{2\pi i\frac{2^q-2^p}{2^{p+q}}} \neq 1$ et ainsi :

$$e^{i\frac{2\pi}{2^p}} \neq e^{i\frac{2\pi}{2^q}}$$

Par suite, E est infini. Et d'après la question précédente, pour tout $p \in \mathbb{N}$, $e^{i\frac{2\pi}{2^p}} \in \mathbb{U}_{2^p} \subset G$; d'où $E \subset G$ et ainsi G est infini.

4. On suppose par l'absurde que G est monogène.

   a. Comme G est monogène, il existe $z \in G$ tel que $G = \langle z \rangle$. Comme $z \in G$, il existe $p \in \mathbb{N}$ tel que, pour $n = 2^p$, $z^n = 1$ donc $z \in \mathbb{U}_n$. Or, comme $\mathbb{U}_n$ est un groupe, $G = \langle z \rangle \subset \mathbb{U}_n$.

   b. Avec les notations de la question précédente, on a $G \subset \mathbb{U}_n$ et $\mathbb{U}_n$ est un ensemble fini, donc G est fini, contradiction car G est infini d'après la question 3b.

5. Soit H un sous-groupe fini de G. Notons $n \in \mathbb{N}^*$ le cardinal de H et $h_1, ...h_n$ ses éléments.
Si $n = 1$, alors $H = \{1\}$ qui est cyclique.
Supposons $n \geq 2$. Quitte à renuméroter les éléments de H qui est un sous-groupe et donc contient 1, on peut supposer que $h_1 = 1$.
Pour tout $i \in [\![1, n]\!]$, comme $H \subset G$, il existe $q_i \in \mathbb{N}$ tel que $h_i^{2^{q_i}} = 1$; de plus, comme l'ensemble $P_i = \{r_i \in \mathbb{N} \mid h_i^{2^{r_i}} = 1\}$ est un sous-ensemble de $\mathbb{N}$ non vide (car q_i y appartient), il possède un plus petit élément p_i - qui vérifie donc $h_i^{2^{p_i}} = 1$.
Ainsi, pour tout $j \in [\![2, n]\!]$, comme on a $h_j^{2^{p_j}} = 1$, h_j est une racine 2^{p_j}-ième de l'unité donc il existe $k_j \in [\![0, 2^{p_j} - 1[\![$ tel que :

$$h_j = e^{i\frac{2k_j\pi}{2^{p_j}}};$$

or par minimalité de p_j dans P_j, $k_j \wedge 2^{p_j} = 1$.
L'ensemble $\{p_2, ..., p_n\}$ est un ensemble fini, donc il possède un plus grand élément $p = p_{i_0}$ avec un certain $i_0 \in [\![2, n]\!]$.
Comme $k_{i_0} \wedge 2^p = 1$, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $uk_{i_0} + v2^p = 1$ donc :

$$h_{i_0}^u = e^{i\frac{2ku\pi}{2^p}} = e^{i\frac{2(1-v2^p)\pi}{2^p}} = e^{i\frac{2\pi}{2^p}}$$

(en fait, on peut en déduire que h_{i_0} est un générateur de $\mathbb{U}_{2^p}$).
Maintenant, pour tout $j \in [\![2, n]\!]$, on a :

$$\frac{2k_j\pi}{2^{p_j}} = \frac{2k_j 2^{p-p_j}\pi}{2^p}$$

et comme $p_j \leq p$, $k_j 2^{p-p_j}$ est un entier.
Ainsi, on a, pour tout $j \in [\![2, n]\!]$,

$$h_j = e^{i\frac{2k_j\pi}{2^{p_j}}} = e^{i\frac{2k_j 2^{p-p_j}\pi}{2^p}} = \left(h_{i_0}^u\right)^{k_j 2^{p-p_j}} = h_{i_0}^{uk_j 2^{p-p_j}}$$

avec $uk_j 2^{p-p_j} \in \mathbb{Z}$.
Il en résulte que $\langle h_{i_0} \rangle = H$ et donc H est monogène.

De plus, on peut remarquer (mais ce n'est pas demandé) que puisque h_{i_0} est un générateur de $\mathbb{U}_{2^p}$, on a $H = \mathbb{U}_{2^p}$. Ainsi tout sous-groupe fini de G est non seulement monogène, mais de la forme $\mathbb{U}_{2^p}$.

Problème 1.

Problème : étude d'une famille de matrices carrées d'ordre 3

Dans l'algèbre $\mathscr{M}_3(\mathbb{C})$ des matrices carrées d'ordre 3 à coefficients complexes, on note E l'ensemble des matrices $M(a,b,c) = \begin{pmatrix} a+b+c & b+c & b+c \\ b & a+b & b \\ b-c & b-c & a+b-c \end{pmatrix}$, avec (a,b,c) dans $\mathbb{C}^3$.

On note $I = M(1,0,0)$, $J = M(0,1,0)$, et $K = M(0,0,1)$.

On note $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ et $e_3 = (0,0,1)$ les vecteurs de la base canonique de $\mathbb{C}^3$.

I. Généralités sur l'ensemble (E), et étude de certains éléments de (E)

1. Montrer que E est un sous-espace vectoriel de $\mathscr{M}_3(\mathbb{C})$.
   En donner la dimension et une base.
2. Montrer que E est un sous-anneau de $(\mathscr{M}_3(\mathbb{C}), +, \times)$.
   L'anneau E est-il commutatif ?
3. Déterminer les matrices M de E qui vérifient l'égalité $M^2 = I$.
4. Dans cette question, on pose $S = M\left(1, -\dfrac{2}{3}, c\right)$.
   Soit f l'endomorphisme de $\mathbb{C}^3$ dont la matrice est S dans la base canonique.
   Préciser la nature de f, et ses éléments caractéristiques. Indication : $w = (2-3c, 2, 2+3c)$.

II. Calcul de la puissance n-ième d'une matrice de E

On fixe a, b, c. Pour simplifier on note M plutôt que $M(a,b,c)$. On pose $L = bJ + cK$.

1. Pour tout n de $\mathbb{N}^*$, calculer L^n en fonction de b, n, L.
2. En déduire, si $b \neq 0$, une expression de M^n (avec $n \geqslant 0$) en fonction de n, a, b, I, L.
3. Dans cette question, on suppose $ab(a+3b) \neq 0$. Montrer que M est inversible et que l'expression de M^n obtenue en (II.2) est encore valable pour les exposants n de $\mathbb{Z}^{-*}$.
4. Dans cette question, on suppose $b = 0$. Calculer M^n pour tout n de $\mathbb{N}$.
   Montrer en quoi le résultat obtenu est cohérent avec celui de la question (II.2).

III. Changements de base ; inversibilité des éléments de E

On fixe la valeur des scalaires a, b, c, et pour simplifier on note M plutôt que $M(a, b, c)$.

Soit f l'endomorphisme de $\mathbb{C}^3$ dont la matrice est M dans la base canonique.

On définit les vecteurs $u_1 = (1, -1, 0)$, $u_2 = (1, 0, -1)$ et $u_3 = (b + c, b, b - c)$.

1. Montrer que u_1, u_2, u_3 forment une base de $\mathbb{C}^3$ si et seulement si $b \neq 0$.
2. On suppose $b \neq 0$. Déterminer la matrice D de f dans la base u_1, u_2, u_3.
3. On suppose $b = 0$. Montrer que les vecteurs u_1, u_2, e_1 forment une base de $\mathbb{C}^3$, et calculer la matrice T de f dans cette base.
4. Déduire de (III.2) et (III.3) que $M(a, b, c)$ est inversible si et seulement si $a(a + 3b) \neq 0$.

Correction.

I. 1. On remarque que $E = \mathrm{Vect}(I, J, K)$ car pour tout $M(a, b, c) \in E$, on a $M = aI + bJ + cK$, donc E est un sous-espace vectoriel de $M_3(\mathbb{C})$.
De plus, la famille (I, J, K) est libre : en effet, si, pour $a, b, c \in \mathbb{C}$, $M = aI + bJ + cK = 0_3$, alors $b = 0$ (coefficient de ligne 2, colonne 3), puis $a = a + b = 0$ (coefficient de ligne 2, colonne 2) puis $c = b + c = 0$ (coefficient de ligne 1, colonne 3). Par suite, E est de dimension 3 et (I, J, K) en est une base car $E = \mathrm{Vect}(I, J, K)$.

2. E est un sous-groupe de $(M_3(\mathbb{C}), +)$ car c'est un sous-espace vectoriel de celui-ci d'après la question précédente. Il reste à montrer que E est stable par produit et que $I_3 \in E$.
Remarquons tout d'abord que :
   - $I^2 = I \in E$,
   - $IJ = JI = J \in E$,
   - $IK = KI = K \in E$,
   - $J^2 = 3J \in E$,
   - $JK = 0_3 \in E$,
   - $KJ = 3K \in E$ et
   - $K^2 = 0_3 \in E$.

   Ainsi, pour tous $M = M(a, b, c), N = N(d, e, f) \in E$, on a, d'après la remarque précédente et le fait que E est un sous-espace vectoriel :

$$\begin{aligned} MN = \; & ad\underbrace{I^2}_{\in E} + ae\underbrace{IJ}_{\in E} + af\underbrace{IK}_{\in E} + bd\underbrace{JI}_{\in E} + be\underbrace{J^2}_{\in E} \\ & + bf\underbrace{JK}_{\in E} + cd\underbrace{KI}_{\in E} + ce\underbrace{KJ}_{\in E} + cf\underbrace{K^2}_{\in E} \in E \end{aligned}$$

   et $I_3 = I \in E$.
   Par suite, E est un sous-anneau de $M_3(\mathbb{C})$. Celui-ci n'est pas commutatif car J et K sont dans E mais ne commutent pas comme le montrent les calculs précédents.

3. Soit $M = aI + bJ + cK \in E$ avec $a, b, c \in \mathbb{C}$. On a, en utilisant les calculs précédents :

$$M^2 = a^2 I + b(2a + 3b)J + c(2a + 3b)K.$$

Donc, (I, J, K) étant une base de E, on a $M^2 = I$ si, et seulement si,

$$\begin{cases} a^2 = 1 \\ b(2a+3b) = 0 \\ c(2a+3b) = 0 \end{cases} \Leftrightarrow \begin{cases} a = \pm 1 \\ (b = 0 \text{ et } c = 0) \text{ ou } (b = \mp\frac{2}{3} \text{ et } c \in \mathbb{C}) \end{cases}$$

Ce qui correspond aux matrices :

$$\pm I,\ \pm M(1, -\frac{2}{3}, c) \text{ pour } c \in \mathbb{C}.$$

4. D'après la question précédente, $S^2 = I$ donc f est une symétrie de $\mathbb{C}^3$.
Les éléments caractéristiques d'une symétrie sont donnés par les sous-espaces $F = \mathrm{Ker}(f - \mathrm{Id})$ et $G = \mathrm{Ker}(f + \mathrm{Id})$ (en effet, la symétrie f est entièrement déterminée par F et G car f est la symétrie par rapport à F parallèlement à G).
On a :
$$S - I = -\frac{2}{3}J + cK \text{ et } S + I = 2I - \frac{2}{3}J + cK$$
De plus, $S - I$ est de rang 1 et doncKer$(S - I)$ est de dimension 2 (théorème du rang) ; et on remarque que $\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ sont dans le noyau de $S - I$ (en remarquant que la première colonne moins la deuxième est nulle et de même pour la première moins la troisième) et forment une famille libre. Ainsi :
$$F = \mathrm{Vect}\left((1, -1, 0), (1, 0, -1)\right).$$
Comme f est une symétrie, F et G sont supplémentaire dans $\mathbb{C}^3$ et F est de dimension 2 donc G est de dimension 1. En utilisant l'indication, on remarque que $f(w) = -w$ d'où $w \in G \setminus \{(0, 0, 0)\}$ et ainsi :
$$G = \mathrm{Vect}(w).$$

II. 1. On a :
$$L^2 = b^2J^2 + bc(JK + KJ) + c^2K^2 = 3b^2J + 3bcK = 3bL$$
et
$$L^3 = L^2 \times L = 3bL^2 = 3^2b^2L$$
On conjecture donc que, pour $n \in \mathbb{N}^*$, $L^n = (3b)^{n-1}L$. Ce qui se montre aisément par récurrence sur $\mathbb{N}^*$:

— <u>Initialisation :</u> on a
$$L^1 = L = 1.L = (3b)^0L$$
donc la conjecture est vraie au rang $n = 1$.

— <u>Hérédité :</u> soit $n \in \mathbb{N}^*$. On suppose $L^n = (3b)^{n-1}L$. Alors :
$$L^{n+1} = L^n \times L \underbrace{=}_{\text{H.R.}} (3b)^{n-1}L^2 = (3b)^{n-1} \times 3b \times L = (3b)^nL.$$

On a donc montré, par récurrence sur $\mathbb{N}^*$, que pour tout $n \in \mathbb{N}^*$,
$$L^n = (3b)^{n-1}L.$$

2. On suppose $b \neq 0$. On a $M = aI + L$ et I commute avec L donc, par la formule du binôme de Newton, on obtient :

$$\begin{aligned}
M^n &= (aI+L)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} L^k \\
&= a^n I + \sum_{k=1}^{n} \binom{n}{k} a^{n-k} (3b)^{k-1} L \\
&= a^n I + \frac{1}{3b} \left(\sum_{k=1}^{n} \binom{n}{k} a^{n-k} (3b)^k \right) L \\
M^n &= a^n I + \frac{(a+3b)^n - a^n}{3b} L.
\end{aligned}$$

3. On suppose $ab(a+3b) \neq 0$. On pourrait calculer le déterminant de M, mais en lisant la fin de la question, on remarque qu'on peut trouver l'inverse potentielle de M en évaluant la formule précédente en $n = -1$ (si elle est bien définie !).
Comme $ab(a+3b) \neq 0$ et $\mathbb{C}$ est un anneau intégre, $a, b, (a+3b)$ sont non nuls et et on peut donc poser :

$$N = \frac{1}{a} I + \frac{\frac{1}{a+3b} - \frac{1}{a}}{3b} L = \frac{1}{a} I - \frac{1}{a(a+3b)} L.$$

On a alors :

$$\begin{aligned}
MN &= (aI+L)\left(\frac{1}{a} I - \frac{1}{a(a+3b)} L \right) \\
&= I - \frac{1}{a+3b} L + \frac{1}{a} L - \frac{1}{a(a+3b)} \underbrace{L^2}_{=3bL} \\
&= I + \frac{-a+a+3b-3b}{a(a+3b)} L \\
MN &= I
\end{aligned}$$

Ainsi, M est inversible d'inverse $M^{-1} = N$.
De plus, on a, pour $a' = -a - 3b$:

$$N = -\frac{1}{aa'} \left(a' I + L \right),$$

et d'après la question précédente, pour $n \in \mathbb{N}^*$,

$$\begin{aligned}
(a'I+L)^n &= a'^n I + \frac{(a'+3b)^n - a'^n}{3b} L \\
&= (-a-3b)^n I + \frac{(-a-3b+3b)^n - (-a-3b)^n}{3b} L \\
(a'I+L)^n &= (-1)^n \left((3a+b)^n I - \frac{(a+3b)^n - a^n}{3b} L \right).
\end{aligned}$$

Soit $m \in \mathbb{Z} \setminus \mathbb{N}$. Alors $n = -m \in \mathbb{N}^*$, et on a :

$$\begin{aligned}
M^m &= M^{-n} \\
&= N^n \\
&= \left(\frac{1}{aa'}\right)^n (a'I + L)^n \\
&= \frac{(-1)^n}{a^n(a+3b)^n}(-1)^n \left((3a+b)I - \frac{(a+3b)^n - a^n}{3b}L\right) \\
&= \frac{1}{a^n}I - \frac{\frac{1}{a^n} - \frac{1}{(a+3b)^n}}{3b}L \\
&= a^{-n}I + \frac{(a+3b)^{-n} - a^{-n}}{3b}L \\
M^m &= a^m I + \frac{(a+3b)^m - a^m}{3b}L.
\end{aligned}$$

Donc la formule obtenue en II.2. est valable pour tout entier n non nul.

4. Pour $b = 0$, on a $M = aI + cK$ et I, K commutent donc, pour $n \in \mathbb{N}$, en remarquant que $K^k = 0_3$ pour tout entier $k \geq 2$:

$$\begin{aligned}
M^n &= (aI + cK)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} c^k K^k \\
&= \sum_{k=0}^{1} \binom{n}{k} a^{n-k} c^k K^k \\
M^n &= a^n I + n a^{n-1} c K
\end{aligned}$$

On remarque d'une part, que, comme $b = 0$, $cK = L$ et donc :

$$M^n = a^n I + n a^{n-1} L$$

et d'autre part, que, pour $b \neq 0$, on peut écrire, avec la formule du binôme de Newton :

$$\frac{(a+3b)^n - a^n}{3b} = \frac{a^n + na^{-1} \times 3b + (3b)^2 s - a^n}{3b} = na^{n-1} + 3bs.$$

où $s = \displaystyle\sum_{k=2}^{n} \binom{n}{k} a^{n-k}(3b)^{k-2}$, quantité est bien définie même si $b = 0$. Et dans ce cas ($b = 0$), on obtient bien, avec la formule obtenue en II.2. :

$$M^n = a^n I + (na^{n-1} + 3 \times 0 \times s)L = a^n I + na^{n-1} L.$$

On peut tout de même remarquer également, en reprenant le calcul du II.2. au niveau de $(*)$, qui, à cet endroit, ne faisait pas encore intervenir $b \neq 0$, que la formule $M^n = a^n I + (na^{n-1} + 3bs)L$ est bien valable pour tout $b \in \mathbb{C}$.

III. 1. Notons $\mathcal{B}$ la base canonique de $\mathbb{C}^3$ et $v = (1,1,1)$. La famille (u_1, u_2, u_3) est une base de $\mathbb{C}^3$ si, et seulement si, $\det_{\mathcal{B}}(u_1, u_2, u_3) \neq 0$. On a :

$$\begin{aligned}
\det_{\mathcal{B}}(u_1, u_2, u_3) &= \det_{\mathcal{B}}(u_1, u_2, bv + cu_2) \\
&= b \det_{\mathcal{B}}(u_1, u_2, v) + c \underbrace{\det_{\mathcal{B}}(u_1, u_2, u_2)}_{=0} \\
&= b \begin{vmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{vmatrix} \\
\det_{\mathcal{B}}(u_1, u_2, u_3) &= 3b.
\end{aligned}$$

La famille (u_1, u_2, u_3) est une base de $\mathbb{C}^3$ si, et seulement si, $3b \neq 0$ i.e. $b \neq 0$.

2. On a :

$$M \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = a \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad M \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \text{ et } M \begin{pmatrix} b+c \\ b \\ b-c \end{pmatrix} = (a+3b) \begin{pmatrix} b+c \\ b \\ b-c \end{pmatrix}$$

Ainsi,

$$f(u_1) = au_1, \quad f(u_2) = au_2 \text{ et } f(u_3) = (b+c)u_3.$$

On suppose $b \neq 0$. Alors $\mathcal{U} = (u_1, u_2, u_3)$ est une base de $\mathbb{C}^3$ et on a :

$$D = \mathrm{Mat}_{\mathcal{U}}(f) = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a+3b \end{pmatrix}$$

3. On a :

$$\det_{\mathcal{B}}(u_1, u_2, e_1) = \begin{vmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{vmatrix} = 1 \neq 0$$

donc $\mathcal{C} = (u_1, u_2, e_1)$ est une base de $\mathbb{C}^3$ et on a :

$$M \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a+b+c \\ b \\ b-c \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} b+c \\ b \\ b-c \end{pmatrix}$$

donc $f(e_1) = ae_1 + u_3$.
On suppose $b = 0$. Alors $u_3 = bv + cu_2 = cu_2$ et donc $f(e_1) = ae_1 + cu_2$. Par suite, on a :

$$T = \mathrm{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} a & 0 & 0 \\ 0 & a & c \\ 0 & 0 & a \end{pmatrix}$$

4.

— <u>1er cas :</u> si $b \neq 0$. Les matrices M et D (question III.2.) étant des matrices représentant un même endomorphisme (ici f), elle sont semblables et donc possèdent le même déterminant. Ainsi,

$$\det(M) = \det(D) = a^2(a+3b)$$

Par suite, M est inversible si, et seulement si, $a^2(a+3b) \neq 0$ ce qui équivaut à $a(a+3b) \neq 0$.

— <u>2ème cas :</u> si $b = 0$. Avec le même raisonnement que précédemment, M et T (question III.3.) possèdent le même déterminant, d'où :

$$\det(M) = \det(T) = a^3 = a^2(a + 3 \times 0) = a^2(a + 3b)$$

Par suite, M est inversible si, et seulement si, $a^2(a + 3b) \neq 0$ ce qui équivaut à $a(a + 3b) \neq 0$.

Dans tous les cas, M est inversible si, et seulement si, $a(a + 3b) \neq 0$.