Composition de Mathématiques

Le 9 novembre 2016 – De 13 heures à 17 heures

Si, au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons des initiatives qu'il est amené à prendre.

Les calculatrices et les téléphones portables sont interdits.
Les réponses non justifiées ne seront pas prises en compte.

❖ I – Problème ❖

Soient E, un espace vectoriel réel ; u, un endomorphisme de E et P, un polynôme non nul à coefficients réels.

1. On suppose que λ est une valeur propre de u. Démontrer que $P(\lambda)$ est une valeur propre de $P(u)$.

2. On suppose que $P(u)$ est l'endomorphisme nul.

2. a. Démontrer que toute valeur propre de u est racine de P.

2. b. Toute racine de P est-elle valeur propre de u ?

3. On suppose que

$$u^3 - u^2 + u - I_E = 0.$$

Que dire du spectre de u ?

❖ II – Problème ❖

On suppose connue une base $\mathscr{B} = (e_1, e_2, e_3)$ de $E = \mathbb{R}^3$ et on considère l'endomorphisme f de E dont la matrice relative à $\mathscr{B}$ est

$$A = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 1 & -3 \\ -1 & 1 & -2 \end{pmatrix}.$$

Partie A. Réduction de A

1. Quel est le rang de A ?

2. Expliciter une base de $\operatorname{Ker} A$ et une représentation cartésienne de $\operatorname{Im} A$.

3. Calculer A^n pour tout $n \in \mathbb{N}^*$.

4. En déduire deux réels a et b tels que

$$f^2(e_1 + a \cdot e_2 + b \cdot e_3) \neq 0.$$

5. Déterminer les valeurs propres et les sous-espaces propres de A.

6. On cherche à démontrer que la matrice A est semblable à la matrice

$$A' = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

6. a. On suppose qu'il existe une base $\mathscr{B}' = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$ de E dans laquelle f est représenté par la matrice A'.

Exprimer les vecteurs $f(\varepsilon_1)$, $f(\varepsilon_2)$ et $f(\varepsilon_3)$ en fonction de ε_1, ε_2 et ε_3. Exprimer ensuite ε_2 et ε_3 en fonction de ε_1.

6. b. On suppose en outre que la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ est de la forme

$$P = \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

Identifier la seule matrice P possible, vérifier qu'elle est inversible et expliciter son inverse P^{-1}.

6. c. Conclure.

Partie B. Application à la résolution d'un système différentiel

On cherche les solutions du système différentiel

$$\begin{cases} x'(t) = x(t) - y(t) + 2z(t) \\ y'(t) = -2x(t) + y(t) - 3z(t) \\ z'(t) = -x(t) + y(t) - 2z(t) \end{cases}$$

qui vérifient la condition initiale

$$\{x(0) = -2, \quad y(0) = 0, \quad z(0) = -2\}.$$

7. Pour tout $t \in \mathbb{R}$, on pose

$$X_t = \begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} \quad \text{et} \quad Y_t = P^{-1}X_t = \begin{pmatrix} u(t) \\ v(t) \\ w(t) \end{pmatrix}.$$

7. a. Exprimer la matrice colonne X_t' en fonction de X_t et de A.

7. b. Démontrer que $Y_t' = P^{-1}X_t'$, puis exprimer Y_t' en fonction de Y_t.

8. En déduire les expressions de $x(t)$, $y(t)$, $z(t)$.

9. On cherche si le support de l'arc paramétré

$$\big[\big(x(t), y(t), z(t)\big),\ t \in \mathbb{R}\big]$$

est contenu dans un plan affine.

9. a. On suppose qu'il existe quatre réels a, b, c et d tels que

$$\forall\, t \in \mathbb{R}, \quad ax(t) + by(t) + cz(t) = d.$$

Démontrer que

$$\forall\, t \in \mathbb{R}, \quad \begin{pmatrix} a & b & c \end{pmatrix} \cdot AX_t = 0.$$

9. b. Déterminer une base de $\operatorname{Ker} {}^tA$.

9. c. Conclure.

❖ III – Problème ❖

On note E_1, l'ensemble des matrices de la forme

$$M(a,b,c) = \begin{pmatrix} b+c & b-a \\ a-b & a+c \end{pmatrix}$$

où (a,b,c) parcourt $\mathbb{R}^3$. On note en particulier

$$U = M(1,0,0), \quad V = M(0,1,0) \quad \text{et} \quad I = M(0,0,1).$$

On considère aussi

$$E_1' = \{M(a,0,0),\ a \in \mathbb{R}^*\}$$
$$E_2' = \{M(0,b,0),\ b \in \mathbb{R}^*\}$$
$$E_3' = \{M(0,0,c),\ c \in \mathbb{R}^*\}$$

et $E' = E_1' \cup E_2' \cup E_3'$.

1. Calculer UV et VU.
2. Calculer U^2 et V^2.
3. Démontrer que $(E', \times)$ est un groupe commutatif.
4. Démontrer que l'ensemble E_1 est un sous-espace vectoriel de $\mathfrak{M}_2(\mathbb{R})$. Quelle est sa dimension ? Donner une base de E_1.
5. *Dans cette question,* on considère U et V comme des matrices à coefficients *complexes*.
5.a. Calculer le polynôme minimal de U.
5.b. En déduire les valeurs propres de U, ainsi que ses sous-espaces propres.
5.c. Expliquer comment définir une matrice

$$P \in GL_2(\mathbb{C})$$

telle que $P^{-1}UP$ soit diagonale.
5.d. En déduire, sans autre calcul, que $P^{-1}VP$ est aussi diagonale.
5.e. En déduire que toute matrice $M \in E_1$ est semblable à une matrice diagonale.
6.a. Démontrer que E_1 est un sous-anneau de $\mathfrak{M}_2(\mathbb{R})$.
6.b. Quels sont les éléments inversibles de E_1 ?

❖ IV – Problème ❖

Les deux parties sont indépendantes.

Partie A.

1. Déterminer l'ensemble des entiers relatifs x qui vérifient le système (S) suivant.

$$\begin{cases} x = 2 \pmod 3 \\ x = 2 \pmod 5 \\ x = 2 \pmod 7 \\ x = 2 \pmod 9 \end{cases} \qquad (S)$$

2. Quelles sont les solutions de ce système comprises (au sens large) entre $-1\,000$ et -500 ?
3. En appliquant l'algorithme d'Euclide, démontrer que le pgcd de deux solutions consécutives de ce système est égal à 1.

Partie B.

On travaille ici dans l'anneau $\mathbb{Z}/7\mathbb{Z}$ en identifiant chaque entier relatif $x \in \mathbb{Z}$ à sa classe $\mathscr{C}(x)$ modulo 7.

On rappelle que $(\mathbb{Z}/7\mathbb{Z})^\times$ désigne l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/7\mathbb{Z}$ et que cet ensemble est muni d'une structure de groupe pour la multiplication.
4. Quel est l'ordre du groupe $(\mathbb{Z}/7\mathbb{Z})$?
5. Quel est l'ordre du groupe $(\mathbb{Z}/7\mathbb{Z})^\times$?
6. Calculer 5^n modulo 7 en fonction de n.
7. Que peut-on en déduire sur le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$?
8.a. Calculer $1\,916^{57}$ modulo 7.
8.b. Pour quels entiers $n \in \mathbb{N}$ l'entier $1\,916^n$ est-il congru à 4 modulo 7 ?

Solution I ❁ Polynôme annulateur d'un endomorphisme

1. Par hypothèse, il existe un vecteur $x_0 \neq 0_E$ tel que $u(x_0) = \lambda x_0$. Par récurrence, on en déduit que

$$\forall\, n \in \mathbb{N}, \quad u^n(x_0) = \lambda^n x_0$$

et, par combinaison linéaire, que :

$$\forall\, P \in \mathbb{R}[X], \quad P(u)(x_0) = P(\lambda)\, x_0.$$

Comme le vecteur x_0 n'est pas nul, cela montre que $P(\lambda)$ est une valeur propre de l'endomorphisme $P(u)$.
2. a. Si $P(u)$ est l'endomorphisme nul, alors sa seule valeur propre est 0. D'après la première question, $P(\lambda) = 0$ pour tout $\lambda \in \mathrm{Sp}(u)$.
2. b. Le polynôme minimal de l'application nulle ω est égal à X. Tout multiple de X est un polynôme annulateur de ω mais peut admettre des racines non nulles : c'est le cas de $X(X-1)(X+1)$ par exemple...
3. Le polynôme

$$X^3 - X^2 + X - 1 = (X-1)(X^2+1)$$

est un polynôme annulateur de u, qui admet 1 pour seule racine réelle, donc $\mathrm{Sp}(u) \subset \{1\}$.

Solution II ❁ Réduction d'une matrice

Partie A. Réduction de A

1. Les deux premières colonnes de A ne sont pas proportionnelles, donc le rang de A est supérieur à 2. Par ailleurs, on peut remarquer que

$$C_3 = C_1 - C_2 \tag{1}$$

donc le rang de A est inférieur à 2. Le rang de A est donc égal à 2.
2. D'après le théorème du rang, la dimension de $\mathrm{Ker}\, A$ est égale à 1 et la relation de liaison (1) signifie que le vecteur $e_1 - e_2 - e_3$ appartient au noyau de f. Donc

$$\mathrm{Ker}\, A = \mathbb{R} \cdot \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

❧ L'image de A est le sous-espace engendré par les colonnes de A. Comme le rang de A est égal à 2 et que les deux premières colonnes de A ne sont pas proportionnelles,

$$\mathrm{Im}\, A = \mathrm{Vect}\left(\begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \right).$$

Le vecteur $x \cdot e_1 + y \cdot e_2 + z \cdot e_3$ appartient donc à $\mathrm{Im}\, f$ si, et seulement si,

$$\begin{vmatrix} 1 & -1 & x \\ -2 & 1 & y \\ -1 & 1 & z \end{vmatrix} = 0.$$

En développant ce déterminant par la troisième colonne, on en déduit que

$$\mathrm{Im}\, A = [x + z = 0].$$

3. On vérifie que

$$A^2 = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & -1 \\ -1 & 0 & -1 \end{pmatrix},$$

ce qui montre, d'après la question précédente, que $\mathrm{Im}(A^2) = \mathrm{Ker}(A)$. Par conséquent, A^3 est la matrice nulle et donc :

$$\forall\, n \geqslant 3, \quad A^n = 0.$$

4. Comme la première colonne de A^2 n'est pas nulle, on en déduit que $f^2(e_1) \neq 0$: il suffit de choisir $(a, b) = (0, 0)$.
5. La matrice A est nilpotente, donc son spectre est réduit à $\{0\}$ et le sous-espace propre associé à 0 est simplement $\mathrm{Ker}\, A$.
6. a. S'il existe une base $\mathscr{B}' = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$ de E dans laquelle la matrice de f est égale à A', alors (en lisant les *colonnes* de A') il faut que

$$f(\varepsilon_1) = \varepsilon_2, \quad f(\varepsilon_2) = \varepsilon_3, \quad f(\varepsilon_3) = 0.$$

On en déduit que $\varepsilon_2 = f(\varepsilon_1)$ et $\varepsilon_3 = f^2(\varepsilon_1)$.
6. b. Par hypothèse sur la première colonne de P, il faut que $\varepsilon_1 = e_1$. D'après l'analyse précédente, il faut donc que

$$\varepsilon_2 = f(e_1) \quad \text{et} \quad \varepsilon_3 = f^2(e_1).$$

On déduit des matrices A et A^2 que la seule matrice possible est la suivante.

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & -1 \\ 0 & -1 & -1 \end{pmatrix}$$

❧ On voit facilement que le rang de cette matrice est égal à 3. Cette famille $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ est donc une base de E et cette matrice P est bien inversible.
❧ On vérifie ensuite que

$$P^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & -2 \end{pmatrix}.$$

(On peut par exemple remarquer que $e_1 = \varepsilon_1$, puis que $e_3 = \varepsilon_1 + \varepsilon_2 - 2\varepsilon_3$ et en déduire que $e_2 = -\varepsilon_2 + \varepsilon_3$: la matrice P^{-1} est aussi la matrice de passage de $\mathscr{B}'$ à $\mathscr{B}$.)
6. c. La matrice P qu'on vient de trouver est inversible : c'est donc la matrice de passage de la base $\mathscr{B}$ à une base $\mathscr{B}' = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$. Par construction,

$$f(\varepsilon_1) = \varepsilon_2 \quad \text{et} \quad f(\varepsilon_2) = \varepsilon_3.$$

Enfin, $f(\varepsilon_3) = 0$ (puisque f^3 est l'endomorphisme nul).

La formule de changement de base nous dit que $P^{-1}AP$ est la matrice de f relative à la base $\mathscr{B}'$. Les relations précédentes prouvent que $P^{-1}AP = A'$. On a ainsi démontré que les matrices A et A' sont semblables.

Partie B. Application à la résolution d'un système différentiel

7. a. Pour tout $t \in \mathbb{R}$,

$$X_t' = \begin{pmatrix} x'(t) \\ y'(t) \\ z'(t) \end{pmatrix} = AX_t.$$

7. b. Comme la matrice P est indépendante de t, les fonctions u, v et w sont des combinaisons linéaires *à coefficients constants* des fonctions x, y et z. Donc

$$Y_t' = P^{-1}X_t' = P^{-1}(AX_t) = (P^{-1}AP)P^{-1}X_t = (P^{-1}AP)Y_t$$

pour tout $t \in \mathbb{R}$.

8. Cette équation différentielle matricielle peut s'écrire sous la forme d'un système différentiel triangulaire (et donc simple à résoudre) :

$$\begin{cases} u'(t) = 0 \\ v'(t) = u(t) \\ w'(t) = v(t) \end{cases}$$

dont les solutions sont :

$$\begin{cases} u(t) = u(0) \\ v(t) = u(0)t + v(0) \\ w(t) = \dfrac{u(0)}{2}t^2 + v(0)t + w(0). \end{cases} \tag{2}$$

On sait comment choisir les constantes d'intégration : comme $Y_0 = P^{-1}X_0$, alors

$$u(0) = -4, \quad v(0) = -2 \quad \text{et} \quad w(0) = 4$$

et comme $X_t = PY_t$, on en déduit l'expression des solutions :

$$\forall\, t \in \mathbb{R}, \quad \begin{cases} x(t) = -2t^2 - 6t - 2 \\ y(t) = 2t^2 + 10t \\ z(t) = 2t^2 + 6t - 2. \end{cases}$$

9. a. Si une fonction est constante, alors sa dérivée est nulle. Par conséquent,

$$ax'(t) + by'(t) + cz'(t) = 0$$

c'est-à-dire

$$\begin{pmatrix} a & b & c \end{pmatrix} X_t' = \begin{pmatrix} a & b & c \end{pmatrix} AX_t = 0.$$

9. b. On sait que les matrices A et ${}^tA$ ont même rang, donc le noyau de ${}^tA$ est une droite vectorielle. En inspectant les colonnes de ${}^tA$, on constate que $C_1 + C_3 = 0$ et donc que la colonne

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

appartient au noyau de ${}^tA$: c'est donc une base de $\operatorname{Ker} {}^tA$.

9. c. En tranposant le résultat de la question précédente,

$$\forall\, t \in \mathbb{R}, \quad \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} AX_t = 0$$

donc

$$\forall\, t \in \mathbb{R}, \quad x'(t) + z'(t) = 0.$$

On en déduit que la fonction $x+z$ est constante et en tenant compte de la condition initiale que

$$\forall\, t \in \mathbb{R}, \quad x(t) + z(t) = -4.$$

La courbe paramétrée par $\big[x(t), y(t), z(t)\big]_{t\in\mathbb{R}}$ est donc contenue dans le plan affine $[x + z = -4]$.

Solution III ❀ Sous-algèbre de $\mathfrak{M}_2(\mathbb{R})$

1. Avec

$$U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

on trouve $UV = VU = I$.

2. On trouve : $U^2 = -V$ et $V^2 = -U$.

3. Tout élément de E' est proportionnel à I, U ou V. Comme

$$\begin{array}{ccc} I^2 = I & U^2 = -V & V^2 = -U \\ IU = UI = U & IV = VI = V & UV = VU = I \end{array}$$

le produit de deux éléments quelconques de E' est encore un élément de E'. La multiplication matricielle est donc une *loi de composition interne* sur E'.

- La multiplication matricielle est une opération notoirement *associative*.
- La matrice $I = M(0, 0, 1)$ est *neutre* pour la multiplication matricielle et appartient à E'.
- Pour toute matrice $A \in E'$, trois cas se présentent :
  - Si $A \in E_1'$, alors il existe $a \neq 0$ tel que $A = aU$, donc A est inversible et
  $$A^{-1} = a^{-1}U^{-1} = a^{-1}V = M(0, a^{-1}, 0) \in E_2' \subset E'.$$
  - Si $A \in E_2'$, alors il existe $b \neq 0$ tel que $A = bV$, donc A est inversible et
  $$A^{-1} = b^{-1}V^{-1} = b^{-1}U = M(b^{-1}, 0, 0) \in E_1' \subset E'.$$
  - Si $A \in E_3'$, alors il existe $c \neq 0$ tel que $A = cI$, donc A est inversible et
  $$A^{-1} = c^{-1}I = M(0, 0, c^{-1}).$$

On a ainsi prouvé que, dans tous les cas, une matrice de E' admet un *inverse* qui appartient bien à E'.

- Toute matrice de E' est proportionnelle à I ou à U ou à $V = -U^{-1}$. Comme U, U^{-1} et I commutent, on en déduit que deux matrices quelconques de E' *commutent*.

Ainsi $(E', \times)$ est un groupe commutatif.

4. Par définition,

$$M(a, b, c) = aU + bV + cI$$

donc E_1 est le sous-espace de $\mathfrak{M}_2(\mathbb{R})$ engendré par les matrices U, V et I.

- Il est clair que $M(a, a, -a) = 0$ pour tout $a \in \mathbb{R}$ et en particulier $U + V - I = 0$, donc la famille (U, V, I) est liée.

En revanche, si $aU + bV = M(a, b, 0) = 0$, alors $a = b = 0$, donc la famille (U, V) est libre.

On en déduit que la famille (U, V) est une base de E_1, qui est donc un sous-espace de dimension 2.

REMARQUE.— De même, les couples (U, I) et (V, I) sont des bases de E_1.

5. a. Comme U n'est pas une homothétie, le couple $(I, U) = (U^0, U^1)$ est libre, donc U n'a pas de polynôme annulateur unitaire de degré 1.

Le calcul de U^2 montre que $-U^2 + U = I$, donc que $X^2 - X + 1$ est un polynôme annulateur unitaire de degré 2.

Le polynôme annulateur unitaire de plus bas degré, *alias* le polynôme minimal de U, est donc $X^2 - X + 1$.

5. b. Les racines du polynôme minimal de U sont $e^{i\pi/3}$ et $e^{-i\pi/3}$.

☙ On profite de ce que ces racines soient conjuguées pour calculer les deux sous-espaces propres *en même temps*.

Soit $\alpha \in \mathbb{C}$, une racine du polynôme minimal de U :

$$\alpha^2 - \alpha + 1 = 0.$$

On cherche le noyau de $U - \alpha I$:

$$\begin{pmatrix} -\alpha & -1 \\ 1 & 1-\alpha \end{pmatrix} \begin{pmatrix} 1 \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \iff \beta = -\alpha = \frac{1}{\alpha - 1}.$$

Comme $\alpha^2 - \alpha + 1 = 0$, alors $-\alpha = \frac{1}{\alpha-1}$, ce qui prouve que le noyau de $(U - \alpha I)$ contient le vecteur

$$\begin{pmatrix} 1 \\ -\alpha \end{pmatrix}.$$

Comme $(U - \alpha I)$ n'est pas la matrice nulle, son rang est donc égal à 1 et son noyau est une droite vectorielle.

Ainsi, les deux racines α et $\overline{\alpha}$ du polynôme minimal de U sont les valeurs propres de U. Les sous-espaces propres associés à ces deux valeurs propres sont respectivement

$$\mathbb{R} \cdot \begin{pmatrix} 1 \\ -\alpha \end{pmatrix} \quad \text{et} \quad \mathbb{R} \cdot \begin{pmatrix} 1 \\ -\overline{\alpha} \end{pmatrix}.$$

REMARQUE.— D'après le cours, les valeurs propres de U sont *des* racines de tout polynôme annulateur de U et sont *les* racines du polynôme minimal de U.

5. c. Une matrice $P \in GL_2(\mathbb{C})$ est la matrice de passage de la base canonique $\mathscr{B} = (e_1, e_2)$ de $\mathbb{C}^2$ à une base $\mathscr{B}' = (\varepsilon_1, \varepsilon_2)$ de $\mathbb{C}^2$. Dans ces conditions, le produit $P^{-1}UP$ est la matrice relative à la base $\mathscr{B}'$ de l'endomorphisme u de $\mathbb{C}^2$ représenté par U dans la base canonique $\mathscr{B}$.

Les colonnes de $P^{-1}UP$ représentent donc les vecteurs $u(\varepsilon_1)$ et $u(\varepsilon_2)$ dans la base $\mathscr{B}'$ et par suite $P^{-1}UP = \mathrm{Diag}(\lambda, \mu)$ si, et seulement si,

$$u(\varepsilon_1) = \lambda \cdot \varepsilon_1 \quad \text{et} \quad u(\varepsilon_2) = \mu \cdot \varepsilon_2.$$

En notant $\alpha = e^{i\pi/3}$ et en posant

$$P = \begin{pmatrix} 1 & 1 \\ -\alpha & -\overline{\alpha} \end{pmatrix},$$

on définit une matrice inversible telle que

$$P^{-1}UP = \mathrm{Diag}(\alpha, \overline{\alpha}).$$

En effet, les colonnes de cette matrice correspondent à deux vecteurs propres de U associés à deux valeurs propres *distinctes* : ce sont donc deux vecteurs linéairement indépendants de $\mathbb{C}^2$, qui constituent donc une base de $\mathbb{C}^2$.

5. d. Comme $V = U^{-1}$,

$$\begin{aligned} P^{-1}VP = (P^{-1}UP)^{-1} &= \mathrm{Diag}(\alpha^{-1}, \overline{\alpha}^{-1}) \\ &= \mathrm{Diag}(\overline{\alpha}, \alpha) \end{aligned}$$

puisque α et $\overline{\alpha}$ sont des complexes de module 1.

5. e. D'après **4.**, toute matrice $M \in E_1$ est de la forme

$$M(a, b, 0) = aU + bV.$$

Par conséquent, avec la matrice P définie au **5.c.**,

$$\begin{aligned} P^{-1}M(a, b, 0)P &= aP^{-1}UP + bP^{-1}VP \\ &= \mathrm{Diag}(a\alpha - b\overline{\alpha},\ a\overline{\alpha} - b\alpha). \end{aligned}$$

Toute matrice de E_1 est donc diagonalisable.

REMARQUE.— Une même matrice de passage convient pour *toutes* les matrices de E_1.

6. a. La structure de sous-espace montre que $(E_1, +)$ est un *sous-groupe* de $\mathfrak{M}_2(\mathbb{R})$.

D'après **4.**, tout élément de E_1 peut s'écrire $M(a, b, 0)$ et comme

$$\begin{aligned} &M(a_1, b_1, 0)M(a_2, b_2, 0) \\ &\qquad = (a_1U + b_1V)(a_2U + b_2V) \\ &\qquad = -b_1b_2U - a_1a_2V + (a_1b_2 + b_1a_2)I \\ &\qquad = (a_1a_2 - b_1b_2)U + (a_1b_2 + b_1a_2 - a_1a_2)I \end{aligned}$$

la multiplication matricielle est une *loi de composition interne* sur E_1.

L'*élément unité* I de $\mathfrak{M}_2(\mathbb{R})$ appartient bien à E_1.

Donc E_1 est bien un sous-anneau de $\mathfrak{M}_2(\mathbb{R})$.

6. b. La matrice $M(a_1, b_1, 0)$ est inversible dans E_1 si, et seulement si, il existe une matrice $M(a_2, b_2, 0)$ telle que

$$M(a_1, b_1, 0)M(a_2, b_2, 0) = I = 0 \cdot U + 1 \cdot I.$$

Comme (U, I) est une *base* de E_1 d'après **4.**, on déduit de la formule du produit calculée à la question précédente que : $M(a_1, b_1, 0)$ est inversible dans E_1 si, et seulement si, le système

$$\begin{cases} (b_1 - a_1)a_2 + a_1b_2 = 1 \\ a_1a_2 - b_1b_2 = 0 \end{cases}$$

d'inconnue $(a_2, b_2) \in \mathbb{R}^3$ admet une unique solution.

Le déterminant de ce système est égal à

$$a_1b_1 - a_1^2 - b_1^2 = -\Big(a_1 - \frac{b_1}{2}\Big)^2 - \frac{3}{4}b_1^2$$

où a_1 et b_1 sont *réels* (et non pas complexes). Il est donc nul si, et seulement si, $(a_1, b_1) = (0, 0)$. Par conséquent, toute matrice non nulle de E_1 est inversible dans E_1.

REMARQUE.— L'anneau E_1 est donc en fait un *corps*.

Solution IV ❁ Questions d'arithmétique

Partie A.

1. L'entier x est solution du système (S) si, et seulement si, $(x-2)$ est divisible par 3, par 5, par 7 et par 9.

Tout entier divisible par 9 est aussi divisible par 3, donc x est solution de (S) si, et seulement si, $(x-2)$ est divisible par 5, par 7 et par 9.

Comme 5, 7 et 9 sont deux à deux premiers entre eux, l'entier x est solution de (S) si, et seulement si, $(x-2)$ est divisible par $5\times 7\times 9 = 315$.

Ainsi, l'entier x est solution de (S) si, et seulement si,

$$\exists\, k\in\mathbb{Z},\qquad x = 2+315k.$$

2. Tout d'abord,

$$-1\,000 \leqslant 2+315k \leqslant -500 \iff -1\,002 \leqslant 315k \leqslant -502.$$

Les quotients de la division euclidienne de 502 et de 1 002 par 315 sont respectivement égaux à 2 et à 3, donc le système (S) possède exactement deux solutions comprises entre -500 et -1000 : il s'agit de -628 (pour $k=-2$) et de -943 (pour $k=-3$).

3. Il s'agit de calculer le pgcd de $b = 315k+2$ et de

$$a = 315(k+1)+2 = 315k+317.$$

Soient q et r, deux entiers tels que $a = bq+r$ (on ne suppose pas que $0\leqslant r<|b|$, de telle sorte qu'il ne s'agit pas forcément de la division euclidienne de a par b). On a

$$a = bq+r \in b\mathbb{Z}+r\mathbb{Z} \quad\text{et}\quad r = a-bq \in a\mathbb{Z}+b\mathbb{Z}$$

de telle sorte que

$$a\mathbb{Z}+b\mathbb{Z} \subset b\mathbb{Z}+r\mathbb{Z} \quad\text{et}\quad b\mathbb{Z}+r\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}.$$

Autrement dit, $a\wedge b = b\wedge r$.

On remarque alors que

$$a = 1\times b+315 \quad\text{et que}\quad b = k\times 315+2$$

donc

$$a\wedge b = b\wedge 315 = 315\wedge 2 = 1.$$

On a prouvé que deux solutions consécutives de (S) sont deux entiers premiers entre eux.

Partie B.

4. L'ensemble $\mathbb{Z}/7\mathbb{Z}$ est un groupe *additif* qui compte 7 éléments : c'est un groupe d'ordre 7.

5. Comme 7 est premier, l'anneau $\mathbb{Z}/7\mathbb{Z}$ est en fait un corps, donc tout élément non nul de $\mathbb{Z}/7\mathbb{Z}$ est inversible. Par conséquent, $(\mathbb{Z}/7\mathbb{Z})^\times$ est un groupe *multiplicatif* d'ordre 6.

6. Il est clair que $5^0 = 1$ et que $5^1 = 5$. On calcule ensuite de proche en proche :

$$5^2 = 4,\quad 5^3 = 6,\quad 5^4 = 2,\quad 5^5 = 3,\quad 5^6 = 1.$$

Pour tout entier $n\in\mathbb{N}$, on note $0\leqslant r_n<6$, le reste de la division euclidienne de n par 6 :

$$n = 6q_n+r_n.$$

Comme $5^6 = 1$, alors

$$5^n = 5^{6q_n+r_n} = (5^6)^{q_n}\times(5^{r_n}) = 5^{r_n}.$$

7. Les calculs précédents prouvent que tout élément de $(\mathbb{Z}/7\mathbb{Z})^\times$ est une puissance de 5, c'est-à-dire que le groupe *multiplicatif* $(\mathbb{Z}/7\mathbb{Z})^\times$ est cyclique d'ordre 6 et engendré par 5.

8. a. On vérifie rapidement que $1916 = 5$ modulo 7 et que $57 = 3$ modulo 6. D'après la question précédente,

$$1916^{57} = 5^3 = 6 \pmod 7.$$

8. b. D'après ce qui précède, $1916^n = 5^n$ modulo 7 et

$$5^n = 4 \pmod 7 \iff n = 2 \pmod 6.$$

Donc 1916^n est congru à 4 modulo 7 si, et seulement si, n est congru à 2 modulo 6.