DM 05 : *simple as* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ [corrigé]

Exercice 1. Crochets de Lie.

Étant donné $A, B \in M_2(\mathbb{R})$, on définit leur *crochet de Lie* $[A, B] = AB - BA$.

Le but de l'exercice est de déterminer l'ensemble $\mathcal{S} = \left\{ [A, B] \,\middle|\, A, B \in M_2(\mathbb{R}) \right\}$ des crochets de Lie.

1. Montrer que $\forall M \in \mathcal{S}, \operatorname{tr}(M) = 0$.

   Soit $M \in \mathcal{S}$. *On peut donc trouver* $A, B \in M_2(\mathbb{R})$ *tel que* $M = [A, B]$. *On a alors*

   $$\begin{aligned} \operatorname{tr}(M) = \operatorname{tr}([A, B]) &= \operatorname{tr}(AB - BA) \\ &= \operatorname{tr}(AB) - \operatorname{tr}(BA) && \textit{(linéarité de la trace)} \\ &= 0. && \textit{(cyclicité de la trace)} \end{aligned}$$

2. Montrer que $\mathcal{S}$ est *stable par multiplication par un scalaire*, c'est-à-dire $\forall M \in \mathcal{S}, \forall \lambda \in \mathbb{R}, \lambda M \in \mathcal{S}$.

   Soit $M \in \mathcal{S}$ *(on peut donc trouver* $A, B \in M_2(\mathbb{R})$ *tels que* $M = [A, B]$*) et* $\lambda \in \mathbb{R}$. *On a alors*

   $$\lambda M = \lambda(AB - BA) = (\lambda A)B - B(\lambda A) = [\lambda A, B],$$

   ce qui montre $\lambda M \in \mathcal{S}$, *et conclut.*

3. Montrer que $\mathcal{S}$ est *stable par similitude*, c'est-à-dire $\forall M \in \mathcal{S}, \forall N \in M_2(\mathbb{R}), M \sim N \Rightarrow N \in \mathcal{S}$.

   Soit $M \in \mathcal{S}$ *(on peut donc trouver* $A, B \in M_2(\mathbb{R})$ *tels que* $M = [A, B]$*) et* $N \in M_2(\mathbb{R})$ *tels que* $M \sim N$. *On peut donc trouver* $P \in \mathrm{GL}_2(\mathbb{R})$ *tel que* $N = P^{-1}MP$. *On a alors*

   $$\begin{aligned} [P^{-1}AP, P^{-1}BP] &= (P^{-1}AP)(P^{-1}BP) - (P^{-1}BP)(P^{-1}AP) \\ &= P^{-1}(AB - BA)P \\ &= P^{-1}MP = N, \end{aligned}$$

   ce qui montre que $N \in \mathcal{S}$, *et conclut.*

4. Montrer que $\operatorname{diag}(1, -1)$, $E_{1,2}$ et $E_{2,1} - E_{1,2}$ appartiennent à $\mathcal{S}$.

   En bidouillant avec les matrices élémentaires, on obtient

   $$\begin{aligned} \operatorname{diag}(1, -1) = E_{1,1} - E_{2,2} &= E_{1,2}E_{2,1} - E_{2,1}E_{1,2} = [E_{1,2}, E_{2,1}] \\ E_{1,2} = E_{1,2}E_{2,2} - \underbrace{E_{2,2}E_{1,2}}_{=0_2} &= [E_{1,2}, E_{2,2}] \end{aligned}$$

   $$\textit{et} \quad E_{2,1} - E_{1,2} = (E_{1,2} + E_{2,1})\,E_{1,1} - E_{1,1}\,(E_{1,2} + E_{2,1}) = [E_{1,2} + E_{2,1}, E_{1,1}].$$

5. Déduire de tout ce qui précède que $\mathcal{S} = \left\{ M \in M_2(\mathbb{R}) \,\middle|\, \operatorname{tr}(M) = 0 \right\}$.

   La première question de l'exercice montre l'inclusion directe. Soit maintenant $M \in M_2(\mathbb{R})$ *tel que* $\operatorname{tr}(M) = 0$. *On va montrer* $M \in \mathcal{S}$ *en utilisant la classification des matrices de* $M_2(\mathbb{R})$ *à similitude près.*

Cas 1. *Supposons que* M *possède deux valeurs propres* $\lambda \neq \lambda'$ *dans* $\mathbb{R}$. *On a alors* $M \sim \operatorname{diag}(\lambda, \lambda')$.
Par invariance de la trace, on a donc $\lambda + \lambda' = \operatorname{tr}\big(\operatorname{diag}(\lambda, \lambda')\big) = \operatorname{tr} M = 0$, *ce qui montre* $\lambda' = -\lambda$.
On a donc $M \sim \lambda \operatorname{diag}(1, -1)$.

- *D'après la question 4, on a* $\operatorname{diag}(1, -1) \in \mathcal{S}$.
- *D'après la question 2, on en déduit* $\lambda \operatorname{diag}(1, -1) \in \mathcal{S}$.
- *D'après la question 3, on en déduit* $M \in \mathcal{S}$.

Cas 2. *Supposons que* M *possède une unique valeur propre* $\lambda \in \mathbb{R}$.

On a alors $M = \lambda I_2$ *ou* $M \sim \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ *et le même argument d'invariance de la trace que dans le premier cas montre* $\lambda = 0$, *donc* $M = 0_2$ *ou* $M \sim E_{1,2}$.
L'égalité $0_2 = [0_2, 0_2]$ *et la question 4 montrent que les deux matrices* 0_2 *et* $E_{1,2}$ *appartiennent à* $\mathcal{S}$.
La question 3 conclut alors.

Cas 3. *Supposons que* M *ne possède pas de valeur propre réelle. On en déduit l'existence de* $a \in \mathbb{R}$ *et* $b \in \mathbb{R}^*$ *tels que* $M \sim \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Encore une fois, par invariance de la trace, on a $0 = \operatorname{tr} M = 2a$, *donc* $a = 0$ *et* $M \sim b(E_{2,1} - E_{1,2})$.
On obtient $M \in \mathcal{S}$ *comme dans le premier cas : on a successivement* $E_{2,1} - E_{1,2}$, $b(E_{2,1} - E_{1,2})$ *et* M *qui appartiennent à* $\mathcal{S}$.

Exercice 2. Autour du théorème de Cayley-Hamilton.

0. Démontrer le cas particulier ($n = 2$) du *théorème de Cayley-Hamilton* :

$$\forall A \in M_2(\mathbb{R}),\ A^2 - \operatorname{tr}(A)\, A + \det(A)\, I_2 = 0_2.$$

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. *On a alors*

$$A^2 - \operatorname{tr}(A)\, A + \det(A)\, I_2 = \begin{pmatrix} a^2 + bc - a^2 - ad + ad - bc & ab + bd - ab - bd \\ ac + cd - ac - cd & bc + d^2 - ad - d^2 + ad - bc \end{pmatrix} = 0_2.$$

1. **Polynômes en** A. Étant donné $M \in M_n(\mathbb{R})$, on appelle *polynôme en* M toute matrice de la forme $\sum_{k=0}^{d} \lambda_k M^k$, où $d \in \mathbb{N}$ et $\lambda_0, \ldots, \lambda_d \in \mathbb{R}$. On note $\mathbb{R}[M] \subseteq M_n(\mathbb{R})$ l'ensemble des polynômes en M.
Soit $A \in M_2(\mathbb{R})$. Montrer l'égalité

$$\mathbb{R}[A] = \left\{ \lambda_0 I_2 + \lambda_1 A \,\middle|\, \lambda_0, \lambda_1 \in \mathbb{R} \right\}.$$

- *L'inclusion réciproque est claire.*
- *Avant de nous lancer dans la démonstration de l'inclusion directe à proprement parler, nous allons commencer par un résultat préliminaire.*

  - *Pour tout* $n \in \mathbb{N}$, *on note* $P(n)$ *l'assertion «* $\exists \alpha, \beta \in \mathbb{R} : A^n = \alpha I_2 + \beta A$. *»*
    Montrons $\forall n \in \mathbb{N}, P(n)$ *par récurrence.*

    Initialisation. *L'initialisation est claire :* $\alpha = 1$ *et* $\beta = 0$ *conviennent.*

Hérédité. *Soit* $n \in \mathbb{N}$ *tel que* $P(n)$ *: on peut donc trouver* $\alpha, \beta \in \mathbb{R}$ *tels que* $A^n = \alpha I_2 + \beta A$.
On a alors

$$\begin{aligned} A^{n+1} &= A A^n \\ &= A(\alpha I_2 + \beta A) \\ &= \alpha A + \beta A^2 \\ &= \alpha A + \beta (\mathrm{tr}(A) A - \mathrm{dét}(A) I_2) \\ &= -\beta \, \mathrm{dét}(A) I_2 + (\alpha + \beta \, \mathrm{tr}(A)) A, \end{aligned}$$

ce qui conclut, en posant $\alpha' = -\beta \, \mathrm{dét}(A)$ *et* $\beta' = \alpha + \beta \, \mathrm{tr}(A)$.
Cela montre $P(n+1)$*, et clôt la récurrence.*

- *Passons à la démonstration proprement dite : soit* $M \in \mathbb{R}[A]$.
On peut donc trouver $\lambda_0, \dots, \lambda_d \in \mathbb{R}$ *tels que* $M = \sum_{k=0}^{d} \lambda_k A^k$. *D'après le point précédent, pour tout* $k \in [\![0, d]\!]$*, on peut trouver* α_k *et* $\beta_k \in \mathbb{R}$ *tels que* $A^k = \alpha_k I_2 + \beta_k A$. *On en déduit*

$$M = \left(\sum_{k=0}^{d} \lambda_k \alpha_k \right) I_2 + \left(\sum_{k=0}^{d} \lambda_k \beta_k \right) A,$$

ce qui conclut.

2. **Carré d'un crochet de Lie.** On réutilise la notation $[\cdot, \cdot]$, vue à l'exercice précédent.
   (a) Montrer l'*identité de Hall* : $\forall A, B, C \in M_2(\mathbb{R}), \left[[A, B]^2, C \right] = 0_2$.

   Soit $A, B, C \in M_2(\mathbb{R})$.
   Notons $M = [A, B]$.
   D'après la question 1 de l'exercice 1, on a $\mathrm{tr}(M) = 0$.
   D'après la question 0, on en déduit $M^2 + \mathrm{dét}(M) I_2 = 0_2$*, c'est-à-dire que* $M^2 = -\mathrm{dét}(M) I_2$.
   Ainsi, M^2 *est une matrice scalaire, et commute donc à tout élément de* $M_2(\mathbb{R})$.
   En particulier, $[M^2, C] = \left[[A, B]^2, C \right] = 0_2$.

   (b) Soit $A, B \in M_2(\mathbb{R})$ et $n \in \mathbb{N}^*$ tels que $[A, B]^n = I_2$. Montrer que n est pair et que $[A, B]^4 = I_2$.

   Comme dans la question précédente, notons $M = [A, B]$.
   On a vu à la question précédente que M^2 *était scalaire. On peut donc trouver* $\mu \in \mathbb{R}$ *tel que* $M^2 = \mu I_2$.
   On en déduit, par une récurrence immédiate, que $\forall k \in \mathbb{N}, M^{2k} = \mu^k I_2$.
   On en déduit alors $\forall k \in \mathbb{N}, M^{2k+1} = \mu^k M$. *La matrice* M *étant de trace nulle, aucune matrice de la forme* λM *ne saurait valoir* I_2.
   Cela démontre déjà que n *est nécessairement pair. En outre, l'égalité* $M^n = I_2$ *donne* $\mu^{n/2} I_2 = I_2$*, d'où l'on tire* $\mu^{n/2} = 1$ *(par exemple en considérant le coefficient* $(1, 1)$*).*
   Le nombre réel μ *est donc une racine de l'unité : on en déduit* $\mu = \pm 1$ *et, dans tous les cas,* $[A, B]^4 = M^4 = \mu^2 I_2 = I_2$.

3. **Critère de nilpotence.** Rappelons qu'une matrice $M \in M_n(\mathbb{R})$ est *nilpotente* si $\exists p \in \mathbb{N} : M^p = 0_n$.
   (a) Soit $A \in M_2(\mathbb{R})$. Montrer que les assertions suivantes sont équivalentes :
      i. A nilpotente ;
      ii. $\mathrm{Sp}_{\mathbb{C}}(A) = \{0\}$;
      iii. $\mathrm{tr}(A) = \mathrm{dét}(A) = 0$;
      iv. $A^2 = 0_2$.

- *Supposons* A *nilpotente. On peut donc trouver* $p \in \mathbb{N}$ *tel que* $M^p = 0_2$.
  Soit $\lambda \in \mathrm{Sp}_{\mathbb{C}}(A)$. *On peut donc trouver un vecteur propre* X *associé à la valeur propre* λ, *c'est-à-dire* $X \in \mathbb{C}^2$ *non nul tel que* $AX = \lambda X$.
  Par une récurrence immédiate, on a $\forall k \in \mathbb{N}, A^k X = \lambda^k X$. *En particulier,* $A^p X = \lambda^p X$, *ce qui donne* $\lambda^p X = 0_{\mathbb{C}^2}$.
  Comme $X \neq 0_{\mathbb{C}^2}$, *on en déduit* $\lambda^p = 0$, *puis* $\lambda = 0$.
  Cela montre l'inclusion $\mathrm{Sp}_{\mathbb{C}}(A) \subseteq \{0\}$.
  Par ailleurs, comme $\mathrm{Sp}_{\mathbb{C}}(A)$ *est l'ensemble des racines complexes d'un polynôme* χ_A *de degré* 2, *on a* $\mathrm{Sp}_{\mathbb{C}}(A) \neq \varnothing$, *et il s'ensuit l'égalité* $\mathrm{Sp}_{\mathbb{C}}(A) = \{0\}$.
- *Supposons* $\mathrm{Sp}_{\mathbb{C}}(A) = \{0\}$.
  Le polynôme $\chi_A = X^2 - \mathrm{tr}(A)X + \mathrm{dét}(A)$ *a donc* 0 *pour unique racine complexe. D'après les relations de Viète, on en déduit* $\mathrm{tr}(A) = 0 + 0 = 0$ *et* $\mathrm{dét}(A) = 0 \times 0 = 0$.
- *Supposons* $\mathrm{tr}(A) = \mathrm{dét}(A) = 0$.
  D'après la question 0, on a immédiatement $A^2 = 0$.
- *Il est clair que toute matrice de carré nul est nilpotente.*

Cela montre l'équivalence entre les quatre assertions.

(b) Existe-t-il deux matrices $A, B \in \mathrm{M}_2(\mathbb{R})$ telles que $ABAB = 0_2$ mais $BABA \neq 0_2$?

Non ! En effet, si l'on a $ABAB = 0_2$, *on en déduit* $BABABA = 0_2$ *en multipliant à gauche par* B *et à droite par* A, *donc* $(BA)^3 = 0_2$.
D'après l'équivalence précédente, cette nilpotence de BA *entraîne à son tour* $(BA)^2 = 0_2$, *c'est-à-dire* $BABA^2 = 0_2$.

(c)$^+$ Existe-t-il deux matrices $A, B \in \mathrm{M}_3(\mathbb{R})$ telles que $ABAB = 0_3$ mais $BABA \neq 0_3$?

On peut par exemple prendre $A = E_{2,2} + E_{3,3}$ *et* $B = E_{1,2} + E_{2,3}$. *On a donc*

- $AB = \cancel{E_{2,2}E_{1,2}} + E_{2,2}E_{2,3} + \cancel{E_{3,3}E_{1,2}} + \cancel{E_{3,3}E_{2,3}} = E_{2,3}$, *donc* $ABAB = E_{2,3}^2 = 0_3$;
- $BA = E_{1,2}E_{2,2} + \cancel{E_{1,2}E_{3,3}} + \cancel{E_{2,3}E_{2,2}} + E_{2,3}E_{3,3} = E_{1,2} + E_{2,3}$, *donc*

$$BABA = (E_{1,2} + E_{2,3})^2 = \cancel{E_{1,2}E_{1,2}} + E_{1,2}E_{2,3} + \cancel{E_{2,3}E_{1,2}} + \cancel{E_{2,3}E_{2,3}} = E_{1,3} \neq 0_3.$$

4.$^+$ (a) Montrer $\forall A, B \in \mathrm{M}_2(\mathbb{R}), \mathrm{dét}(A+B) + \mathrm{dét}(A-B) = 2\,\mathrm{dét}\,A + 2\,\mathrm{dét}\,B$.

Soit $A, B \in \mathrm{M}_2(\mathbb{R})$. *On a*

$$\begin{aligned}(A+B)^2 + (A-B)^2 &= A^2 + AB + BA + B^2 + A^2 - AB - BA + B^2 \\ &= 2A^2 + 2B^2.\end{aligned}$$

En utilisant le théorème de Cayley-Hamilton $\forall M \in \mathrm{M}_2(\mathbb{R}), M^2 = \mathrm{tr}(M)\,M - \mathrm{dét}(M)\,I_2$, *il s'ensuit*

$$\begin{aligned}\mathrm{tr}(A+B)\,(A+B) - \mathrm{dét}(A+B)\,I_2 + \mathrm{tr}(A-B)\,(A-B) - \mathrm{dét}(A-B)\,I_2 \\ = 2\left[\mathrm{tr}(A)\,A - \mathrm{dét}(A)\,I_2 + \mathrm{tr}(B)\,B - \mathrm{dét}(B)\,I_2\right].\end{aligned}$$

Or, on a $\mathrm{tr}(A+B)\,(A+B) + \mathrm{tr}(A-B)\,(A-B) = 2\ \mathrm{tr}(A)\,A + 2\ \mathrm{tr}(B)\,B$, *notamment par linéarité de la trace, donc on peut simplifier les termes faisant intervenir la trace de part et d'autre pour obtenir*

$$-\left(\mathrm{dét}(A+B) + \mathrm{dét}(A-B)\right)\,I_2 = -2\left(\mathrm{dét}(A) + \mathrm{dét}(B)\right)\,I_2.$$

Par exemple en considérant les coefficients $(1,1)$ *de part et d'autre, on en déduit l'égalité demandée.*

(b) Montrer que pour tout $n \geqslant 1$ et tous $A_1, \dots, A_n \in M_2(\mathbb{R})$, on a

$$\sum_{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n} \det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n) = 2^n \sum_{k=1}^{n} \det(A_k).$$

Pour tout $n \in \mathbb{N}^*$, on note $P(n)$ l'assertion

$$\forall A_1, \dots, A_n \in M_2(\mathbb{R}), \quad \sum_{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n} \det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n) = 2^n \sum_{k=1}^{n} \det(A_k).$$

Montrons $\forall n \in \mathbb{N}^*, P(n)$ par récurrence.

Initialisation. *Soit $A_1 \in M_2(\mathbb{R})$. On a $\det(-A_1) = \det(A_1)$, car la formule explicite du déterminant rend clair que $\forall \lambda \in \mathbb{R}, \forall A \in M_2(\mathbb{R}), \det(\lambda A) = \lambda^2 \det(A)$. Ainsi,*

$$\det(A_1) + \det(-A_1) = 2\det(A_1),$$

d'où $P(1)$.

Hérédité. *Soit $n \in \mathbb{N}^*$ tel que $P(n)$.*

Soit $A_1, \dots, A_n, A_{n+1} \in M_2(\mathbb{R})$. On a

$$\begin{aligned}
&\sum_{(\varepsilon_1,\dots,\varepsilon_n,\varepsilon_{n+1})\in\{-1,1\}^{n+1}} \det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n + \varepsilon_{n+1} A_{n+1}) \\
&= \sum_{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n} \big[\det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n + A_{n+1}) \\
&\qquad\qquad + \det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n - A_{n+1})\big] \\
&= \sum_{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n} \big[2\det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n) + 2\det(A_{n+1})\big] \qquad \textit{(ques. préc.)} \\
&= 2 \sum_{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n} \det(\varepsilon_1 A_1 + \cdots + \varepsilon_n A_n) + 2^{n+1}\det(A_{n+1}) \qquad \textit{(linéarité)} \\
&= 2 \times 2^n \sum_{k=1}^{n} \det(A_k) + 2^{n+1}\det(A_{n+1}) \qquad \textit{(d'après } P(n)\textit{)} \\
&= 2^{n+1} \sum_{k=1}^{n+1} \det(A_k),
\end{aligned}$$

ce qui montre $P(n+1)$ et clôt la récurrence.

Exercice 3. Densité des matrices inversibles.

Soit $A \in M_2(\mathbb{R})$. Montrer qu'il existe $\delta > 0$ tel que

$$\forall t \in \mathbb{R}, 0 < |t| < \delta \Rightarrow A - tI_2 \in GL_2(\mathbb{R}).$$

Soit $A \in M_2(\mathbb{R})$. On rappelle que t est valeur propre de A si et seulement si la matrice $A - tI_2$ n'est pas inversible.

Il suffit donc de trouver $\delta > 0$ tel que l'ensemble $]-\delta, 0[\cup]0, \delta[$ ne contienne aucune valeur propre de A.

Cela est très facile car l'ensemble $Sp_{\mathbb{R}}(A)$ des valeurs propres réelles de A est fini (il possède 0, 1 ou 2 éléments suivant le signe du discriminant du polynôme caractéristique χ_A).

Plus précisément :

- *si* $\mathrm{Sp}_{\mathbb{R}}(A) \subseteq \{0\}$, A *ne possède aucune valeur propre non nulle et* $\delta = 1$ *convient ;*
- *si* $\mathrm{Sp}_{\mathbb{R}}(A) \cap \mathbb{R}^* \neq \varnothing$, *cette intersection est finie, et l'on peut choisir* $\lambda \in \mathrm{Sp}_{\mathbb{R}}(A) \cap \mathbb{R}^*$ *de valeur absolue minimale* $\delta = |\delta|$.
  Cette minimalité montre qu'aucune valeur propre de A *n'appartient à* $]-\delta, 0[\cup]0, \delta[$, *et conclut.*

Exercice 4. Le groupe $\mathrm{GL}_2(\mathbb{Z})$.

Dans cet exercice, on note $M_2(\mathbb{Z})$ l'ensemble des matrices $A \in M_2(\mathbb{R})$ dont tous les coefficients sont des entiers relatifs. On note également

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ A \in M_2(\mathbb{Z}) \;\middle|\; \det A \in \{-1, 1\} \right\}.$$

1. Soit $A \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{R})$. Montrer que $A^{-1} \in M_2(\mathbb{Z})$ si et seulement si $A \in \mathrm{GL}_2(\mathbb{Z})$.

   - *Supposons* $A^{-1} \in M_2(\mathbb{Z})$. *On a donc* $\det(A^{-1}) \in \mathbb{Z}$ *vu la définition du déterminant, puis, par multiplicativité du déterminant,* $1 = \det(I_2) = \det(A)\det(A^{-1})$.
     Comme les seules décompositions de 1 *en produit de deux entiers sont* $1 = 1 \times 1 = (-1) \times (-1)$, *on en déduit que* $\det(A) = \det(A^{-1}) = \pm 1$, *et donc que* $A \in \mathrm{GL}_2(\mathbb{Z})$.
   - *Réciproquement, supposons* $A \in \mathrm{GL}_2(\mathbb{Z})$, *et notons* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *On a alors*

   $$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbb{Z}),$$

   ce qui conclut.

2. Soit $A \in M_2(\mathbb{R})$.
   (a) On suppose $\forall X \in \mathbb{Z}^2, AX \in \mathbb{Z}^2$. Montrer que $A \in M_2(\mathbb{Z})$.

   L'hypothèse entraîne $C_1(A) = A \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{Z}^2$ *et* $C_2(A) = A \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{Z}^2$, *donc* $A \in M_2(\mathbb{Z})$.

   (b) On suppose $\forall X \in \mathbb{R}^2, X \in \mathbb{Z}^2 \Leftrightarrow AX \in \mathbb{Z}^2$. Montrer que $A \in \mathrm{GL}_2(\mathbb{Z})$.

   - *Commençons par montrer que* A *est inversible. Supposons par l'absurde que* $\ker(A) \neq \{0\}$ *: on peut donc trouver* $x, y \in \mathbb{R}$ *non tous les deux nuls tels que* $A \begin{pmatrix} x \\ y \end{pmatrix} = 0_{\mathbb{R}^2}$.

     - *Si* $x \neq 0$, *le vecteur* $X = \dfrac{1}{2x} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1/2 \\ * \end{pmatrix}$ *vérifie encore* $AX = 0_{\mathbb{R}^2}$.
       On a donc trouvé un vecteur $X \in \mathbb{R}^2$ *vérifiant* $X \notin \mathbb{Z}^2$ *mais* $AX \in \mathbb{Z}^2$, *ce qui contredit l'hypothèse.*
     - *Si* $y \neq 0$, *on obtient à nouveau une contradiction en considérant* $X = \dfrac{1}{2y} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} * \\ 1/2 \end{pmatrix}$.
   - *L'hypothèse donne clairement* $\forall X \in \mathbb{Z}^2, AX \in \mathbb{Z}^2$, *donc* $A \in M_2(\mathbb{Z})$ *d'après la question précédente.*
   - *Soit* $X \in \mathbb{Z}^2$. *En appliquant l'hypothèse à* $A^{-1}X$, *on a équivalence entre* $A^{-1}X \in \mathbb{Z}^2$ *et* $X \in \mathbb{Z}^2$ *(assertion que l'on a supposée vraie), donc* $A^{-1}X \in \mathbb{Z}^2$.
     On a ainsi montré $\forall X \in \mathbb{Z}^2, A^{-1}X \in \mathbb{Z}^2$, *et la question précédente montre que* $A^{-1} \in M_2(\mathbb{Z})$.

   On a donc $A \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{R})$ *et* $A^{-1} \in M_2(\mathbb{Z})$ *: la première question de l'exercice entraîne alors* $A \in \mathrm{GL}_2(\mathbb{Z})$.

3. **Éléments d'ordre fini.**

(a) Donner un exemple de matrice $A \in GL_2(\mathbb{Z})$ telle que $\forall p \in \mathbb{N}^*, A^p \neq I_2$.

Une récurrence immédiate montre que $\forall p \in \mathbb{N}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$, *donc* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *convient.*

(b) Déterminer les $\lambda \in \mathbb{U}$ tels que $2\,\mathrm{Ré}(\lambda) \in \mathbb{Z}$.

Analyse. *Soit* $\lambda \in \mathbb{U}$ *tel que* $2\,\mathrm{Ré}(\lambda) \in \mathbb{Z}$.

Comme $\lambda \in \mathbb{U}$, *on a* $\mathrm{Ré}(\lambda)^2 \leqslant \mathrm{Ré}(\lambda)^2 + \mathrm{Im}(\lambda)^2 = 1$, *donc* $\mathrm{Ré}(\lambda) \in [-1, 1]$.

Comme en outre $2\,\mathrm{Ré}(\lambda) \in \mathbb{Z}$, *on en déduit* $\mathrm{Ré}(\lambda) \in \left\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\right\}$.

Comme $\lambda \in \mathbb{U}$, *on peut trouver* $\theta \in \mathbb{R}$ *tel que* $\lambda = e^{i\theta}$ *(et donc* $\mathrm{Ré}(\lambda) = \cos\theta$*). On distingue alors les cinq cas précédents :*

- *si* $\cos\theta = -1$, *on a* $\theta \equiv \pi \pmod{2\pi}$, *donc* $\lambda = -1$;
- *si* $\cos\theta = -\frac{1}{2}$, *on a* $\theta \equiv \pm\frac{2\pi}{3} \pmod{2\pi}$, *donc* $\lambda = j$ *ou* $\lambda = \bar{j}$;
- *si* $\cos\theta = 0$, *on a* $\theta \equiv \pm\frac{\pi}{2} \pmod{2\pi}$, *donc* $\lambda = i$ *ou* $\lambda = -i$;
- *si* $\cos\theta = \frac{1}{2}$, *on a* $\theta \equiv \pm\frac{\pi}{3} \pmod{2\pi}$, *donc* $\lambda = \zeta_6$ *ou* $\lambda = \overline{\zeta_6}$;
- *si* $\cos\theta = 1$, *on a* $\theta \equiv 0 \pmod{2\pi}$, *donc* $\lambda = 1$.

Ainsi $\lambda \in \{\pm 1, \pm i, j, \bar{j}, \zeta_6, \overline{\zeta_6}\} = \{\pm 1, \pm i\} \cup \{1, \zeta_6, j, -1, \bar{j}, \overline{\zeta_6}\} = \mathbb{U}_4 \cup \mathbb{U}_6$.

Synthèse. *Réciproquement, il est clair que les éléments de* $\mathbb{U}_4 \cup \mathbb{U}_6$ *conviennent.*

On remarque que tous les λ *ainsi obtenus vérifient* $\lambda^{12} = 1$.

(c) Soit $A \in GL_2(\mathbb{Z})$ tel que $\exists p \in \mathbb{N}^* : A^p = I_2$. Montrer que $A^{12} = I_2$.

On peut trouver $p \in \mathbb{N}^*$ *tel que* $A^p = I_2$. *On va considérer* A *comme une matrice réelle et lui appliquer le théorème de classification à similitude près. Il y a trois cas.*

Cas 1. A *possède deux valeurs propres réelles distinctes* $\lambda \neq \mu$.

On a alors $A \sim \mathrm{diag}(\lambda, \mu)$, *donc on peut trouver* $P \in GL_2(\mathbb{C})$ *tel que* $P^{-1}AP = \mathrm{diag}(\lambda, \mu)$. *En élevant à la puissance* p, *on obtient* $I_2 = P^{-1}I_2P = (P^{-1}AP)^p = \mathrm{diag}(\lambda^p, \mu^p)$, *donc* $\lambda^p = \mu^p = 1$. *Cela entraîne en particulier* $\lambda, \mu \in \{-1, 1\}$. *Quitte à les échanger, on peut supposer* $\lambda = 1$ *et* $\mu = -1$.

On a donc $A = P\,\mathrm{diag}(1, -1)P^{-1}$, *d'où* $A^2 = I_2$.

A fortiori, $A^{12} = I_2$.

Cas 2. A *possède une unique valeur propre réelle* λ.

- *Si* $A = \lambda I_2$, *on a* $\lambda^p = 1$, *donc* $\lambda = \pm 1$ *et* $A^2 = I_2$.
- *Sinon, on a* $A \sim \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. *On en déduit* $\pm 1 = \det A = \lambda^2$, *donc* $\lambda = \pm 1$.
  - *Si* $\lambda = 1$, *on a* $A^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$, *ce qui contredit l'hypothèse* $A^p = I_2$.
  - *Si* $\lambda = -1$, *on a* $A^p = (-1)^p \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix}$ *(par une récurrence immédiate ou grâce au binôme de Newton), ce qui contredit également l'hypothèse.*

Ce sous-cas ne se produit donc pas.

Cas 3. A *possède deux valeurs propres complexes non réelles conjuguées : on peut donc trouver* $\lambda \in \mathbb{C} \setminus \mathbb{R}$ *tel que* $A \underset{\mathbb{C}}{\sim} \operatorname{diag}(\lambda, \overline{\lambda})$.

On a alors $\pm 1 = \det A = \lambda \times \overline{\lambda} = |\lambda|^2$, *donc* $\lambda \in \mathbb{U}$ *et* $\operatorname{tr} A = \lambda + \overline{\lambda} = 2\,\mathrm{Ré}(\lambda)$.
On en déduit $\lambda \in \mathbb{U}$ *et* $2\,\mathrm{Ré}(\lambda) \in \mathbb{Z}$. *D'après la question précédente, on a* $\lambda^{12} = 1$.
Ainsi, $A^{12} = P \operatorname{diag}(\lambda^{12}, \overline{\lambda}^{12}) P^{-1} = P I_2 P^{-1} = I_2$.

4. **Couples de matrices engendrant un groupe libre.** Soit $A, B \in \mathrm{GL}_2(\mathbb{Z})$.

► On appelle *mot réduit en* A *et* B tout produit de l'une des deux formes suivantes :

$$\begin{cases} A^{i_1} B^{i_2} A^{i_3} \cdots A^{i_r} & \text{si } r \text{ impair} \\ A^{i_1} B^{i_2} A^{i_3} \cdots B^{i_r} & \text{si } r \text{ pair} \end{cases} \quad \text{ou} \quad \begin{cases} B^{i_1} A^{i_2} B^{i_3} \cdots B^{i_r} & \text{si } r \text{ impair} \\ B^{i_1} A^{i_2} B^{i_3} \cdots A^{i_r} & \text{si } r \text{ pair,} \end{cases}$$

où $r > 0$ et où les exposants $i_1, i_2, i_3, \ldots, i_r$ sont des entiers relatifs **non nuls**. Pour des raisons évidentes, les mots du premier (resp. deuxième) type seront dits *commençant par* A (resp. B).
Par exemple, $A^2 B^{-1} A B A B^{-12}$ est un mot réduit (commençant par A).

► On dit que (A, B) *engendre un groupe libre* si tout mot réduit en A et B est différent de I_2.

(a) Montrer que dans les cas suivants, (A, B) n'engendre pas un groupe libre :

♠ A et B sont deux éléments de $\mathrm{GL}_2(\mathbb{Z})$ qui commutent.

On a $ABA^{-1}B^{-1} = I_2$.

♡ $A = C^7$ et $B = C^{17}$, pour une certaine matrice $C \in \mathrm{GL}_2(\mathbb{Z})$.

On a $A^{17} B^{-7} = I_2$.

♢ $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et B est un élément quelconque de $\mathrm{GL}_2(\mathbb{Z})$.

On a (après calcul) $A^6 = I_2$.

♣⁺ $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

On a $AB^{-1}A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, *dont on vérifie facilement* [1] *que la puissance quatrième vaut* I_2.
On a donc $AB^{-1}A^2B^{-1}A^2B^{-1}A^2B^{-1}A = I_2$.

(b) Dans les deux questions suivantes, on fixe $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

Soit $(n_k)_{k \in \mathbb{N}}$ et $(m_k)_{k \in \mathbb{N}}$ deux suites d'entiers relatifs non nuls. On définit une suite de matrices $(M_k)_{k \in \mathbb{N}}$ par $M_0 = I_2$ et $\forall k \in \mathbb{N}$, $\left(M_{2k+1} = M_{2k} A^{n_k} \text{ et } M_{2k+2} = M_{2k+1} B^{m_k}\right)$.
Enfin, on définit la suite $(c_k)_{k \in \mathbb{N}}$ par

$$\forall k \in \mathbb{N}, c_k = \begin{cases} [M_k]_{1,1} & \text{si } k \text{ pair} \\ [M_k]_{1,2} & \text{si } k \text{ impair.} \end{cases}$$

Montrer que la suite $(|c_{n+1}| - |c_n|)_{n \in \mathbb{N}}$ est croissante.

Soit $n \in \mathbb{N}$.

► *Supposons* n *pair : on peut donc trouver* $k \in \mathbb{N}$ *tel que* $n = 2k$. *On a alors successivement*

- $M_n = M_{2k} = \begin{pmatrix} c_{2k} & * \\ * & * \end{pmatrix}$;

1. C'est le nombre complexe $-i$, après tout.

- $M_{n+1} = M_{2k+1} = \begin{pmatrix} c_{2k} & * \\ * & * \end{pmatrix}\begin{pmatrix} 1 & 2n_k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} c_{2k} & c_{2k+1} \\ * & * \end{pmatrix}$;
- $M_{n+2} = M_{2k+1} = \begin{pmatrix} c_{2k} & c_{2k+1} \\ * & * \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2m_k & 1 \end{pmatrix} = \begin{pmatrix} c_{2k+2} & * \\ * & * \end{pmatrix}$,

donc $c_{2k+2} = c_{2k} + 2m_k\, c_{2k+1}$.
D'après l'inégalité triangulaire, $|c_{2k+2}| \geqslant 2\,|m_k|\;|c_{2k+1}| - |c_{2k}|$.
Comme $m_k \neq 0$, *on en déduit* $|c_{2k+2}| \geqslant 2\,|c_{2k+1}| - |c_{2k}|$.

► *Supposons* n *impair : on peut donc trouver* $k \in \mathbb{N}$ *tel que* $n = 2k+1$. *On a alors successivement*

- $M_n = M_{2k+1} = \begin{pmatrix} * & c_{2k+1} \\ * & * \end{pmatrix}$;
- $M_{n+1} = M_{2k+2} = \begin{pmatrix} * & c_{2k+1} \\ * & * \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2m_k & 1 \end{pmatrix} = \begin{pmatrix} c_{2k+2} & c_{2k+1} \\ * & * \end{pmatrix}$;
- $M_{n+2} = M_{2k+3} = \begin{pmatrix} c_{2k+2} & c_{2k+1} \\ * & * \end{pmatrix}\begin{pmatrix} 1 & 2n_{k+1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & c_{2k+3} \\ * & * \end{pmatrix}$,

donc $c_{2k+3} = 2n_{k+1}\, c_{2k+2} + c_{2k+1}$.
D'après l'inégalité triangulaire, $|c_{2k+3}| \geqslant 2\,|n_{k+1}|\;|c_{2k+2}| - |c_{2k+1}|$.
Comme $n_{k+1} \neq 0$, *on en déduit* $|c_{2k+3}| \geqslant 2\,|c_{2k+2}| - |c_{2k+1}|$.

Dans tous les cas, on a montré $|c_{n+2}| \geqslant 2\,|c_{n+1}| - |c_n|$, *d'où* $|c_{n+2}| - |c_{n+1}| \geqslant |c_{n+1}| - |c_n|$, *ce qui conclut.*

(c)$^+$ En déduire que (A, B) engendre un groupe libre.

► *On reprend les notations de la question précédente.*
Comme $c_0 = 1$ *et* $c_1 = 2$, *la question précédente entraîne* $\forall n \in \mathbb{N}, |c_{n+1}| - |c_n| \geqslant 1$, *c'est-à-dire que la suite* $(|c_n|)_{n\in\mathbb{N}}$ *est strictement croissante.*
On en déduit $\forall n \in \mathbb{N}^*, |c_n| > 1$. *En particulier, pour tout* $n \in \mathbb{N}^*$, *la matrice* M_n *possède un coefficient de valeur absolue* > 1 *et n'est donc pas la matrice identité.*
Vu la définition de la suite de matrices $(M_n)_{n\in\mathbb{N}}$ *cela montre qu'aucun mot réduit en* A *et* B *commençant par* A *ne vaut* I_2.

► *On pourrait refaire le travail pour les mots commençant par* B, *mais il y a une manière intelligente de se ramener au cas précédent.*
Posons $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. *Il s'agit d'une matrice d'échange, qui est donc égale à son propre inverse, et on vérifie que*

$$PAP = P^{-1}AP = B \qquad \textit{et} \qquad PBP = P^{-1}BP = A.$$

Soit alors $r \in \mathbb{N}^*$ *et* $i_1, \dots, i_r$ *des entiers relatifs non nuls.*

- *Si* r *est impair, on a*

$$\begin{aligned} B^{i_1}A^{i_2}B^{i_3}\cdots B^{i_r} &= (P^{-1}AP)^{i_1}(P^{-1}BP)^{i_2}(P^{-1}AP)^{i_3}\cdots(P^{-1}AP)^{i_r} \\ &= P^{-1}A^{i_1}PP^{-1}B^{i_2}PP^{-1}A^{i_3}P\cdots P^{-1}A^{i_r}P \\ &= P^{-1}\underbrace{\left(A^{i_1}B^{i_2}A^{i_3}\cdots A^{i_r}\right)}_{\neq I_2}P. \end{aligned}$$

  Or, ce produit n'est pas I_2 *: étant donné une matrice* $M \in M_2(\mathbb{R})$, *si* $P^{-1}MP = I_2$, *on en déduit* $M = PI_2P^{-1} = I_2$ *; par contraposée, si* $M \neq I_2$, *on a* $P^{-1}MP \neq I_2$.

- *Exactement de la même façon, si* r *est pair, on a*

$$B^{i_1}A^{i_2}B^{i_3}\cdots A^{i_r} = P^{-1}\underbrace{\left(A^{i_1}B^{i_2}A^{i_3}\cdots B^{i_r}\right)}_{\neq I_2}P \neq I_2.$$

Cela montre que les mots réduits en A *et* B *commençant par* B *sont également* $\neq I_2$*, et conclut la démonstration.*

5.$^+$ En s'inspirant du cours, montrer que les matrices $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *engendrent* $GL_2(\mathbb{Z})$, c'est-à-dire que toute matrice de $GL_2(\mathbb{Z})$ peut s'écrire sous la forme d'un produit $A_1^{i_1} A_2^{i_2} \cdots A_r^{i_r}$, où $r \in \mathbb{N}$ et, pour tout $k \in [\![1, r]\!]$, on a $A_k \in \{P, D, T\}$ et $i_k \in \mathbb{Z}$.

Discussion informelle.

L'idée est qu'on va pouvoir faire tourner un algorithme de Gauss : les opérations permises sont des échanges $L_1 \leftrightarrow L_2$ *(par multiplication à gauche par* P*), des « dilatations »* $L_2 \leftarrow -L_2$ *(par multiplication à gauche par* D*) et des transvections* $L_1 \leftarrow L_1 + nL_2$ *(par multiplication à gauche par* T^n*), et l'objectif est de ramener une matrice* $A \in GL_2(\mathbb{Z})$ *quelconque à* I_2*. On pourrait aussi disposer des mêmes opérations sur les colonnes données par les multiplications à droite par les mêmes matrices, mais ce n'est pas nécessaire.*

Que nous manque-t-il par rapport au pivot « normal » qui nous a permis dans le cours de trouver les générateurs de $GL_n(K)$ *? Deux choses.*

- *On ne peut faire que des transvections avec des coefficients entiers, et uniquement celles qui modifient la première ligne ; à vrai dire, comme on a le droit d'échanger les deux lignes, ce deuxième point n'est pas vraiment un problème. Le premier n'en est pas un non plus* ***si on arrive****, comme dans le pivot usuel,* ***à travailler avec un pivot égal à*** 1 *: les coefficients de nos matrices étant entiers, on arrivera ainsi à « déblayer » la colonne.*
- *Plus sérieux, on n'a pas de dilatation, à part avec un coefficient* -1*. Il est donc plus difficile d'arriver à des pivots égaux à* 1*.*

Le point-clef est que la condition $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = \pm 1$ *peut être vue comme une relation de Bézout et montre que* a *et* c *(par exemple) sont premiers entre eux : l'algorithme d'Euclide permet donc de passer de* a *et* c *à* 1 *et* 0*, et les opérations permises vont refléter cet algorithme.*

Par exemple, 38 *et* 7 *sont premiers entre eux, et l'exécution de l'algorithme d'Euclide le montre rapidement :*

$$\begin{aligned} 38 &= 5 \times 7 + 3 \\ 7 &= 2 \times 3 + 1. \end{aligned}$$

Cela se traduit par une suite d'opérations

$$\begin{pmatrix} 38 & * \\ 7 & * \end{pmatrix} \xrightarrow{L_1 \leftarrow L_1 - 5L_2} \begin{pmatrix} 3 & * \\ 7 & * \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 7 & * \\ 3 & * \end{pmatrix} \xrightarrow{L_1 \leftarrow L_1 - 2L_2} \begin{pmatrix} 1 & * \\ 3 & * \end{pmatrix},$$

et le 1 *ainsi obtenu va déblayer la colonne, menant rapidement à* $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$*.*

Pour des raisons de déterminant, cette matrice sera même $\begin{pmatrix} 1 & * \\ 0 & \pm 1 \end{pmatrix}$*, et on arrive rapidement à* I_2*.*

Plutôt que de rédiger ce raisonnement de façon algorithmique, on va faire les matheux et raisonner plus abstraitement. Les idées restent néanmoins exactement les mêmes.

Démonstration.

Soit $M \in GL_2(\mathbb{Z})$*. On note*

$$\mathcal{O}_M = \left\{ A_1^{i_1} A_2^{i_2} \cdots A_r^{i_r} M \;\middle|\; r \in \mathbb{N}, A_1, \ldots, A_r \in \{P, D, T\}, i_1, \ldots, i_r \in \mathbb{Z} \right\}.$$

Par multiplicativité du déterminant, on a $\mathcal{O}_M \subseteq GL_2(\mathbb{Z})$*.*

Nous allons montrer (en trois étapes) que $I_2 \in \mathcal{O}_M$*.*

Première étape. *Montrons qu'il existe dans $\mathcal{O}_M$ une matrice de la forme* $\begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix}$.

Considérons, parmi toutes les matrices $B \in \mathcal{O}_M$, une dont le coefficient $(2,1)$ est le plus petit possible, en valeur absolue.
Plus formellement, $\left\{ \left| [B]_{2,1} \right| \,\middle|\, B \in \mathcal{O}_M \right\}$ est une partie de $\mathbb{N}$ qui n'est pas vide (elle contient $|[M]_{2,1}|$). Elle possède donc un minimum

$$m = \min \left\{ \left| [B]_{2,1} \right| \,\middle|\, B \in \mathcal{O}_M \right\},$$

et on peut trouver $B \in \mathcal{O}_M$ tel que $m = \left|[B]_{2,1}\right|$.

On va montrer que B a la forme voulue. Notons $B = \begin{pmatrix} a & * \\ c & * \end{pmatrix}$, si bien que $m = |c|$.

- *Commençons par montrer $c = 0$. Supposons par l'absurde $c \neq 0$. On a donc $m \in \mathbb{N}^*$.*
  On peut alors effectuer la division euclidienne de a par m : on peut trouver deux entiers $q \in \mathbb{Z}$ et $r \in [\![0, m-1]\!]$ tels que $a = qm + r$.

  - *Pour $k \in \{0,1\}$, on a $D^k M = \begin{pmatrix} a & * \\ (-1)^k c & * \end{pmatrix}$.*

    En choisissant bien k, on a donc $D^k M = \begin{pmatrix} a & * \\ |c| & * \end{pmatrix} = \begin{pmatrix} a & * \\ m & * \end{pmatrix} \in \mathcal{O}_M$.
  - *On a alors $T^{-q} D^k M = \begin{pmatrix} a - qm & * \\ m & * \end{pmatrix} = \begin{pmatrix} r & * \\ m & * \end{pmatrix} \in \mathcal{O}_M$.*
  - *On a enfin $PT^{-q} D^k M = \begin{pmatrix} m & * \\ r & * \end{pmatrix} \in \mathcal{O}_M$.*

  Or, par construction, $|r| = r < m$. Comme r est le coefficient $(2,1)$ d'un élément de $\mathcal{O}_M$, cela contredit la définition de m et conclut la démonstration de $c = 0$.
- *On peut donc écrire $M = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$. Comme $\alpha\delta = \det M = \pm 1$ et que α et δ dont des entiers, on en déduit $\alpha, \delta \in \{\pm 1\}$, ce qui conclut la première étape.*

Deuxième étape. *On a $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $PDP = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.*

Pour $k, \ell \in \{0,1\}$, on a donc $D^k (PDP)^\ell B = \begin{pmatrix} (-1)^\ell \alpha & (-1)^\ell \beta \\ 0 & (-1)^k \delta \end{pmatrix} \in \mathcal{O}_M$.

En choisissant bien k et ℓ, on a ainsi trouvé $C = D^k (PDP)^\ell B$ dans $\mathcal{O}_M$ telle que $C = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Troisième étape. *Notons $C = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. On a alors $T^{-\lambda} C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{O}_M$, ce qui conclut.*

La discussion précédente montre $\forall M \in GL_2(\mathbb{Z}), I_2 \in \mathcal{O}_M$. Montrons que cela conclut.
Soit $M \in GL_2(\mathbb{Z})$. En appliquant la $\forall$-assertion à M^{-1}, on obtient un entier $r \in \mathbb{N}$, des matrices $A_1, \ldots, A_r \in \{P, D, T\}$ et des entiers $i_1, \ldots, i_r \in \mathbb{Z}$ tels que

$$A_1^{i_1} A_2^{i_2} \cdots A_r^{i_r} M^{-1} = I_2.$$

On en déduit $M = A_1^{i_1} A_2^{i_2} \cdots A_r^{i_r}$ après multiplication à droite par M, ce qui conclut.