X 2016-MP
épreuve A

Durée : 4 heures

Soit $n \geqslant 1$ un entier. On appelle *point entier* de $\mathbb{R}^n$ un point dont toutes les coordonnées sont entières, c'est-à-dire un point de $\mathbb{Z}^n$. Si $\mathcal{K}$ est une partie de $\mathbb{R}^n$, on note $\overset{\circ}{\mathcal{K}}$ son intérieur. On appelle points entiers de $\mathcal{K}$ (resp. points entiers intérieurs) les points de $\mathcal{K} \cap \mathbb{Z}^n$ (resp. les points de $\overset{\circ}{\mathcal{K}} \cap \mathbb{Z}^n$). On note $\mathrm{Card}(\mathcal{K} \cap \mathbb{Z}^n)$ et $\mathrm{Card}(\overset{\circ}{\mathcal{K}} \cap \mathbb{Z}^n)$ le nombre (éventuellement infini) de points entiers de $\mathcal{K}$ et de son intérieur $\overset{\circ}{\mathcal{K}}$.

Soit h_β l'homothétie de rapport $\beta \in \mathbb{R}$ (centrée en 0), on note $\beta\mathcal{K} = h_\beta(\mathcal{K})$ l'image de $\mathcal{K}$ par h_β. Si τ_x est la translation de vecteur $x \in \mathbb{R}^n$, on note $\mathcal{K} - x = \tau_{-x}(\mathcal{K})$ l'image de $\mathcal{K}$ par τ_{-x}.

Si $M = (m_{i,j})$ est une matrice de $\mathcal{M}_n(\mathbb{R})$, $m_{i,j}$ est le coefficient de la i-ème ligne et de la j-ième colonne.

On note $(x_1 \mid \ldots \mid x_n)$ la matrice de $\mathcal{M}_n(\mathbb{R})$ dont les colonnes sont les vecteurs $x_1, \ldots, x_n$ de $\mathbb{R}^n$.

On note I_n la matrice identité de $\mathcal{M}_n(\mathbb{R})$ et $E_{i,j}$ la matrice de $\mathcal{M}_n(\mathbb{R})$ dont tous les coefficients sont nuls sauf celui de la i-ième ligne et j-ième colonne qui vaut 1.

On note $\mathcal{M}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ dont tous les coefficients sont entiers.

On note $\lfloor a \rfloor$ la partie entière d'un réel a : c'est le plus grand entier inférieur ou égal à a ; et $\{a\} = a - \lfloor a \rfloor \in [0, 1[$ la partie fractionnaire de a. On note $\rfloor a \lfloor$ le plus grand entier strictement inférieur à a.

Pour des entiers $a_1, \ldots, a_k$ non tous nuls, on note $\mathrm{pgcd}(a_1, \ldots, a_k)$ le plus grand entier (strictement positif) qui divise tous les a_i.

Première partie

1°) Soit $M \in \mathcal{M}_n(\mathbb{R})$ une matrice inversible et à coefficients entiers.

a) Montrer que M^{-1} est à coefficients rationnels.

b) Montrer l'équivalence des propositions suivantes :

i) M^{-1} est à coefficients entiers.

ii) $\det M$ vaut -1 ou 1.

Dans la suite on note $GL_n(\mathbb{Z})$ l'ensemble des matrices carrées de taille n à coefficients entiers et de déterminant ± 1. C'est un sous-groupe de $GL_n(\mathbb{R})$. On remarque que pour $i \neq j$ et $c \in \mathbb{Z}$, la matrice $I_n + cE_{i,j}$ appartient à $GL_n(\mathbb{Z})$.

2°) Soit $M = (x_1 \mid \ldots \mid x_n) \in GL_n(\mathbb{R})$.

a) Montrer que $M \in GL_n(\mathbb{Z})$ si et seulement si $M(\mathbb{Z}^n) = \mathbb{Z}^n$.

b) Montrer l'équivalence des propositions suivantes :

i) $M \in GL_n(\mathbb{Z})$.

ii) Les points entiers du parallélépipède

$$\mathcal{P} = \{\sum_{i=1}^{n} t_i x_i \mid \forall\, i \in \{1, \ldots, n\}, t_i \in [0,1]\}$$

sont exactement les 2^n points $\sum_{i=1}^{n} \varepsilon_i x_i$, où $\varepsilon_i \in \{0,1\}$ pour tout $i \in \{1, \ldots, n\}$.

3°) Pour tout α dans $\mathbb{R}$ et pour tous entiers i et j distincts compris entre 1 et n, décrire l'effet sur une matrice carrée M de taille n de la multiplication à gauche par $I_n + \alpha E_{i,j}$. Même question pour la multiplication à droite.

4°) Soient $n \geqslant 2$ et $a_1, \ldots, a_n$ des entiers non tous nuls. Le but de cette question est de montrer qu'il existe une matrice M de $\mathcal{M}_n(\mathbb{Z})$ dont la première colonne est $(a_1, \ldots, a_n)$ et de déterminant le $\operatorname{pgcd}(a_1, \ldots, a_n)$. Pour cela on raisonne par récurrence sur n.
Soit $N \in \mathcal{M}_{n-1}(\mathbb{Z})$ une matrice dont la première colonne est $(a_2, \ldots, a_n)$. Etant donnés $u, v \in \mathbb{Q}$, on considère la matrice

$$M = \begin{pmatrix} a_1 & 0 & \ldots & 0 & u \\ & & & & va_2 \\ & & & & va_3 \\ & & N & & \\ & & & & \vdots \\ & & & & va_n \end{pmatrix}$$

a) Exprimer $\det M$ en fonction de $\det N$, u et v.

b) On suppose que les nombres $a_2, \ldots, a_n$ sont non tous nuls et que $\det N = \operatorname{pgcd}(a_2, \ldots, a_n)$. Montrer que l'on peut choisir u et v de sorte que M réponde à la question.

c) Conclure la récurrence.

5°) Soit $M \in \mathcal{M}_n(\mathbb{Z})$, de déterminant non nul. On souhaite montrer qu'il existe une matrice A dans $GL_n(\mathbb{Z})$ telle que MA soit triangulaire supérieure et en notant $MA = (c_{i,j})$, on ait les inégalités $0 < c_{1,1}$ et $0 \leqslant c_{i,j} < c_{i,i}$ pour tous $i, j \in \{1, \ldots, n\}$ tels que $i < j$.

a) On note $M = (x_1 \mid \ldots \mid x_n)$. Soient $x'_1, \ldots, x'_n$ les éléments de $\mathbb{Z}^{n-1}$ obtenus en prenant les $(n-1)$ dernières coordonnées de $x_1, \ldots, x_n$.
Montrer qu'il existe $a_1, \ldots, a_n$ dans $\mathbb{Q}$, non tous nuls, tels que $\sum_{i=1}^{n} a_i x'_i = 0$.
Montrer que l'on peut choisir les a_i entiers et premiers entre eux dans leur ensemble.

b) Montrer qu'il existe une matrice A dans $GL_n(\mathbb{Z})$ telle que la première colonne de $\widetilde{C} = MA_1$ ait tous ses coefficients $\widetilde{c}_{i,1}$ nuls sauf le premier $\widetilde{c}_{1,1}$ que l'on peut prendre strictement positif.

c) En considérant pour tout $j = 2, \dots, n$ la division euclidienne

$$\widetilde{c}_{1,j} = q_j \widetilde{c}_{1,1} = r_j,\, 0 \leqslant r_j < \widetilde{c}_{1,1}$$

montrer que l'on peut supposer $\widetilde{c}_{1,1} > \widetilde{c}_{1,j}$, quiite à changer A_1.

d) Conclure par récurrence.

6°) Soit $M \in \mathcal{M}_n(\mathbb{Z})$ de déterminant non nul. Montrer qu'il existe une matrice A dans $GL_n(\mathbb{Z})$ telle que AM soit triangulaire inférieure et en notant $AM = (c_{i,j})$, on ait l'inégalité $0 \leqslant c_{i,j} < c_{j,j}$ pour tous $i, j \in \{1, \dots, n\}$ tels que $j < i$.

Deuxième partie

Soient $s_0, s_1, \dots, s_n$ des points de $\mathbb{R}^n$ tels que les vecteurs $s_1 - s_0$, $s_2 - s_0$, $\dots, s_n - s_0$ soient linéairement indépendants. On appelle *simplexe de sommets* $s_0, \dots, s_n$ l'ensemble :

$$\begin{aligned}\mathcal{S} &= \{\sum_{i=0}^{n} t_i s_i \mid \forall\, i = 0, \dots, n, t_i \geqslant 0, \sum_{i=0}^{n} t_i = 1\} \\ &= \{s_0 + \sum_{i=1}^{n} t_i(s_i - s_0) \mid \forall\, i = 1, \dots, n, t_i \geqslant 0, \sum_{i=1}^{n} t_i \leqslant 1\}\end{aligned}$$

Si de plus les s_i sont tous des points entiers, on dit que $\mathcal{S}$ est un simplexe entier. On définit le volume du simplexe $\mathcal{S}$ de sommets $s_0, \dots, s_n$ par

$$\text{Vol}(S) := \frac{1}{n!} |\det(s_1 - s_0, s_2 - s_0, \dots, s_n - s_0)|$$

7°) Soit $\mathcal{S}$ le simplexe de sommets $s_0, s_1, \dots, s_n$.

a) Montrer que $\mathcal{S}$ est un compact convexe de $\mathbb{R}^n$.

b) Montrer que $\overset{\circ}{\mathcal{S}} = \{\sum_{i=0}^{n} t_i s_i \mid \forall\, i = 0, \dots, n, t_i > 0, \sum_{i=0}^{n} t_i = 1\}$. En déduire que si $0 \in \overset{\circ}{\mathcal{S}}$, alors pour tout $\lambda \in [0, 1[$, $\lambda S \subset \overset{\circ}{\mathcal{S}}$.

c) Pour $i = 0, \dots, n$, on note $\widehat{s}_i = (1, s_i)$ le point de $\mathbb{R}^{n+1}$ dont les coordonnées sont 1, suivi des coordonnées de s_i.
Exprimer $|\det(\widehat{s}_0, \widehat{s}_1, \dots, \widehat{s}_n)|$ en fonction de Vol($\mathcal{S}$). En déduire que le volume d'un simplexe ne dépend pas de l'ordre des sommets.

8°) Soit $V \geqslant 0$ un réel.

a) Donner un exemple de simplexe entier de $\mathbb{R}^2$, de volume supérieur ou égal à V et n'ayant aucun point intérieur entier.

b) Donner un exemple de simplexe entier de $\mathbb{R}^3$, de volume supérieur ou égal à V, et dont les seuls points entiers sont les sommets.

9°) Soit $\mathcal{K}$ un compact convexe de $\mathbb{R}^n$ tel que $0 \in \overset{\circ}{\mathcal{K}}$.

a) Montrer que l'ensemble des $\lambda \geqslant 0$ tels que $-\lambda\mathcal{K} \subset \mathcal{K}$ est un intervalle.

On noter $a(\mathcal{K}) = \sup\{\lambda \geqslant 0 \mid -\lambda\mathcal{K} \subset \mathcal{K}\}$.

b) Montrer que $a(\mathcal{K}) < \infty$ et que $a(\mathcal{K}) = \max\{\lambda \geqslant 0 \mid -\lambda\mathcal{K} \subset \mathcal{K}\}$.

c) Montrer que $0 < a(\mathcal{K}) \leqslant 1$. En déduire que $a(\mathcal{K}) = 1$ si et seulement si $\mathcal{K}$ est symétrique par rapport à 0.

On admet le résultat suivant que l'on pourra utiliser sans démonstration pour la suite de cette partie.

Théorème 1.
Soit $\mathcal{S}$ un simplexe de $\mathbb{R}^n$ et k un entier. Si Vol$(\mathcal{S}) \geqslant k$, il existe $k+1$ points distincts $v_0, \dots, v_k$ de $\mathcal{S}$ tels que $v_i - v_j \in \mathbb{Z}^n$ quels que soient i et j entre 0 et k.

10°) Dans toute cette question, $\mathcal{S}$ est un simplexe de $\mathbb{R}^n$ tel que $0 \in \overset{\circ}{\mathcal{S}}$. On veut montrer que

$$\mathrm{Card}(\overset{\circ}{\mathcal{S}} \cap \mathbb{Z}^n) \geqslant 2\rfloor \mathrm{Vol}(\mathcal{S})\Big(\frac{a(\mathcal{S})}{a(\mathcal{S})+1}\Big)^n \lfloor + 1$$

On pose alors $a = a(\mathcal{S})$ et $k = \rfloor \mathrm{Vol}(\mathcal{S})\Big(\frac{a(\mathcal{S})}{a(\mathcal{S})+1}\Big)^n \lfloor$.

a) Exprimer, pour $\beta \in \mathbb{R}^*$ et $x \in \mathbb{R}^n$, Vol$(\beta\mathcal{S})$ et Vol$(\mathcal{S} - x)$.

Montrer que pour $\lambda \in [0, 1[$ suffisamment proche de 1, Vol$(\frac{\lambda a}{a+1}\,\mathcal{S}) > k$.

b) Pour λ comme dans la question précédente, soient $v_0, \dots, v_k$ les $k+1$ points distincts dans $\frac{\lambda a}{a+1}\,\mathcal{S}$ vérifiant $v_i - v_j \in \mathbb{Z}^n$ pour tout i, j dont l'existence est assurée par le Théorème 1.
Montrer que les points $v_i - v_j$ sont dans $\lambda\mathcal{S}$. En déduire que les $v_i - v_j$ sont dans l'intérieur de $\mathcal{S}$.

c) Montrer qu'il existe un indice $j \in \{0, \dots, k\}$ tel que les $(2k+1)$ points $0, \pm(v_i - v_j)$ pour $i \in \{0, \dots, k\} \setminus \{j\}$ soient distincts. En déduire l'énoncé de la question **10°)**, puis que

$$\mathrm{Card}(\overset{\circ}{\mathcal{S}} \cap \mathbb{Z}^n) \geqslant \mathrm{Vol}(\mathcal{S})\Big(\frac{a(\mathcal{S})}{2}\Big)^n$$

Troisième partie

On dit que deux simplexes $\mathcal{S}$ et $\mathcal{S}'$ de $\mathbb{R}^n$ sont *équivalents* s'il existe un ordre d'énumération des sommets $s_0, \dots, s_n$ de $\mathcal{S}$ et $s'_0, \dots, s'_n$ de $\mathcal{S}'$ et une matrice A de $GL_n(\mathbb{Z})$ tels que $A(s_i - s_0) = s'_i - s'_0$ pour tout $i = 1, \dots, n$.

11°) Montrer que deux simplexes entiers $\mathcal{S}$ et $\mathcal{S}'$ sont équivalents si et seulement s'il existe une matrice $A \in GL_n(\mathbb{Z})$ et un vecteur $b \in \mathbb{Z}^n$ tels que $\mathcal{S}' = A(\mathcal{S}) - b$.

12°) Montrer que le volume, le nombre de points entiers et le nombre de points intérieurs entiers sont les mêmes pour deux simplexes entiers équivalents.

13°) Montrer qu'un simplexe entier $\mathcal{S}$ est équivalent à un simplexe entier contenu dans le cube $[0, \mathrm{Vol}(\mathcal{S})]^n$.

On pourra utiliser la question **6°)** *pour une matrice M bien choisie.*

On admet le résultat suivant que l'on pourra utiliser sans démonstration.

Théorème 2.
Pour tout entier strictement positif k, il existe une constante strictement positive $C(n, k)$ telle que pour tout simplexe entier $\mathcal{S}$ de $\mathbb{R}^n$ possédant exactement k points intérieurs entiers, Vol($\mathcal{S}$) $\leqslant C(n, k)$.

14°) Déduire du Théorème 2. que pour tout entier strictement positif k, il n'existe à équivalence près qu'un nombre fini de simplexes entiers de $\mathbb{R}^n$ ayant exactement k points intérieurs.

Solution

Nous noterons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$ et il est important de remarquer (c'est banal mais fondamental pour ce problème) que ces vecteurs sont dans $\mathbb{Z}^n$.

Dans tout le problème, on confond matrice carrée réelle d'ordre n et endomorphisme de $\mathbb{R}^n$ canoniquement associé, ainsi que vecteur de $\mathbb{R}^n$ et matrice colonne canoniquement associée.
Cela peut conduire à des rencontres inattendues dans l'énoncé de cette épreuve, du genre $\widehat{s_i} = (1, s_i)$, où s_i est une colonne de hauteur n et $\widehat{s_i}$ une colonne de hauteur $n + 1$. De même on pourra écrire : soit $t = (t_1, \ldots, t_n)$ et $y = Mt$ où M est une matrice carrée et y un nouveau vecteur. De même l'énoncé dit : la première colonne de M est $(a_1, \ldots, a_n)$, ce qui peut surprendre, mais c'est juste une habitude à prendre. Nous n'aurons jamais à considérer des matrices lignes, donc le risque de confusion est quasi-nul ...

Première partie

Question 1.

a) On a $\mathcal{M}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Q})$. Donc si M est inversible elle est inversible en tant que matrice à coefficients dans le **corps** $\mathbb{Q}$. Son inverse M^{-1} est donc encore à coefficients rationnels.
Variante : On sait que $M^{-1} = \dfrac{1}{\det M} M^\dagger$ où $M^\dagger = (\text{com } M)^T$ est la transposée de la matrice des cofacteurs de M.
Comme le déterminant de M est entier et ses cofacteurs aussi (ce sont tous des déterminants de matrices à coefficients entiers), M^{-1} est bien à coefficients rationnels.

$$\boxed{M \in \mathcal{M}_n(\mathbb{Z}) \cap GL_n(\mathbb{R}) \implies M^{-1} \in \mathcal{M}_n(\mathbb{Q})}$$

b) $\star$ Si $M \in \mathcal{M}_n(\mathbb{Z})$ est inversible telle que M et M^{-1} sont à coefficients entiers, alors $\det M$ et $\det(M^{-1})$ sont dans $\mathbb{Z}$ tels que :

$$1 = \det I_n = \det(M)\det(M^{-1})$$

Donc $\det(M)$ est un diviseur de 1, *i.e.* vaut 1 ou -1.
$\star$ Si $M \in \mathcal{M}_n(\mathbb{Z})$ est telle que $\det(M) \in \{-1, 1\}$, comme on a déjà dit que si M est à coefficients entiers , alors il en est de même de $M^\dagger$ et en divisant par 1 ou par -1, $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

Bref :

$$\boxed{\text{Pour } M \in \mathcal{M}_n(\mathbb{Z}),\, M^{-1} \in \mathcal{M}_n(\mathbb{Z}) \iff \det(M) \in \{-1, 1\}}$$

Faut-il justifier les remarques de l'énoncé ?

A cet instant cela ne coûte pas très cher, donc on ne s'en prive pas :

[Comme I_n commute avec tout le monde et puisque $i \neq j \implies E_{i,j}E_{i,j} = 0$:

$$(I_n + cE_{i,j})(I_n - cE_{i,j}) = I_n - c^2(E_{i,j})^2 = I_n - 0 = I_n$$

donc $I_n + cE_{i,j} \in GL_n(\mathbb{Z})$. On peut aussi dire que le déterminant d'une telle matrice de transvection vaut 1.]

Question 2.

Commençons par remarquer que si $M \in \mathcal{M}_n(\mathbb{Z})$, alors pour toute colonne (ou vecteur) x à coefficients entiers Mx est encore à coefficients entiers. Ainsi $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$ et c'est l'inclusion contraire qui pose problème . . .

a) $\star$ Si $M(\mathbb{Z}^n) = \mathbb{Z}^n$.
$e_1, \ldots, e_n \in \mathbb{Z}^n = M(\mathbb{Z}^n)$, donc l'image de M (en tant qu'endomorphisme de $\mathbb{R}^n$ ou $\mathbb{Q}^n$) contient une base de $\mathbb{R}^n$ (ou de $\mathbb{Q}^n$) et M est surjectif, donc bijectif. Cela prouve que $M \in GL_n(\mathbb{R})$.

Par hypothèse, pour tout $j \in [\![1, n]\!]$, il existe $y_j \in \mathbb{Z}^n$ tel que $My_j = e_j$. Comme $M \in GL_n(\mathbb{R})$, on a en fait $y_j = M^{-1}e_j$ et on vient donc de montrer que pour tout j, la $j^{\text{ème}}$ colonne de M^{-1} est à coefficients entiers. Ainsi $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Donc M et M^{-1} sont à coefficients entiers et $M \in GL_n(\mathbb{Z})$.

$\star$ Si $M \in GL_n(\mathbb{Z})$.
M et M^{-1} sont à coefficients entiers. Alors pour tout vecteur $y \in \mathbb{Z}^n$, le vecteur $x = M^{-1}y$ est à coefficients entiers et $Mx = y$. Cela prouve que $M(\mathbb{Z}^n)$ contient $\mathbb{Z}^n$ et comme on a dit que $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$ est banal, on a $M(\mathbb{Z}^n) = \mathbb{Z}^n$.

$$\boxed{M \in GL_n(\mathbb{Z}) \iff M(\mathbb{Z}^n) = \mathbb{Z}^n}$$

Ce que l'on peut aussi écrire : $M \in GL_n(\mathbb{Z}) \iff [x \in \mathbb{Z}^n \iff Mx \in \mathbb{Z}^n]$, car si $M \in GL_n(\mathbb{Z})$ on a banalement $x \in \mathbb{Z}^n \implies Mx \in \mathbb{Z}^n$ et on a aussi $Mx \in \mathbb{Z}^n \implies x = M^{-1}(Mx) \in \mathbb{Z}^n$.

b) $i) \implies ii)$. On suppose donc que l'on a $M \in GL_n(\mathbb{Z})$.

Pour $t = (t_1, \ldots, t_n)$, on a : $\sum\limits_{j=1}^{n} t_j x_j = \sum\limits_{j=1}^{n} t_j M e_j = M(\sum\limits_{j=1}^{n} t_j e_j) = Mt$.

Donc, par le résultat **2°) a)** : $t \in \mathbb{Z}^n \iff M(t) = \sum\limits_{j=1}^{n} t_j x_j \in \mathbb{Z}^n$.

Si pour tout $j \in [\![1, n]\!]$ on a $t_j \in [0, 1]$ alors $\sum\limits_{j=1}^{n} t_j x_j \in \mathbb{Z}^n$ si et seulement si chaque t_j est entier donc vaut 0 ou 1, ce qui fait donc 2^n listes possibles et 2^n points, car la famille $(x_1, \ldots, x_n)$ est une base de $\mathbb{R}^n$ (image de la base canonique par M inversible) et donc des listes de coordonnées différentes donnent des points différents.

$ii) \implies i)$. En prenant tous les t_i nuls sauf l'un qui vaut 1, l'hypothèse entraîne que les vecteurs $x_1, \ldots, x_n$ sont tous des points entiers et $M \in \mathcal{M}_n(\mathbb{Z})$.

Réciproquement, soit $j \in [\![1, n]\!]$ et $z = M^{-1}e_j \in \mathbb{R}^n$. On a donc $Mz = e_j$.

On peut écrire : $z = (z_1, \ldots, z_n) = (\lfloor z_1 \rfloor, \ldots, \lfloor z_n \rfloor) + (\{z_1\}, \ldots, \{z_n\})$ et chaque $\{z_i\}$ appartient à $[0, 1[$.

En notant $\lfloor z \rfloor = (\lfloor z_1 \rfloor, \ldots, \lfloor z_n \rfloor)$ et $\{z\} = (\{z_1\}, \ldots, \{z_n\})$, on a donc :

$$M\{z\} = Mz - M\lfloor z \rfloor = e_j - M\lfloor z \rfloor$$

Comme $\lfloor z \rfloor$ est à coefficients entiers, il en est de même de $M\lfloor z \rfloor$ et donc $M\{z\} = \sum \{z_j\} x_j$ est à coefficients entiers, les $\{z_j\}$ appartenant à $[0, 1[$.

Par l'hypothèse faite sur $\mathcal{P}$, il n'y a plus de marge de manoeuvre et les $\{z_j\}$ valent tous 0, ce qui prouve z est à coefficients entiers.

On vient donc de montrer que les colonnes de M^{-1} sont à coefficients entiers et $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

Ainsi M et M^{-1} sont à coefficients entiers et $M \in GL_n(\mathbb{Z})$.

$$\boxed{(i) \iff (ii)}$$

Question 3.

Cette question est très banale, elle doit donc être placée ici car son résultat devrait servir sous peu ...

On résout donc, mais surtout on place le résultat dans un coin de sa mémoire.

$\star$ Pour $M = (m_{k,\ell}) \in \mathcal{M}_n(\mathbb{R})$, on a :

$$(I_n + \alpha E_{i,j})M = M + \alpha E_{i,j}(\sum_{k,\ell} m_{k,\ell} E_{k,\ell}) = M + \alpha \sum_{k,\ell} m_{k,\ell} E_{i,j} E_{k,\ell}$$

On a : $j \neq k \implies E_{i,j}E_{k,\ell} = 0$; et $E_{i,j}E_{j,\ell} = E_{i,\ell}$, donc il reste :

$$(I_n + \alpha E_{i,j})M = M + \sum_{\ell} \alpha m_{j,\ell} E_{i,\ell}$$

On a donc ajouté à la matrice M une matrice dont toutes les lignes sont nulles sauf la $i^{\text{ème}}$ (présence des matrices $E_{i,\ell}$) qui est égale à α fois la $j^{\text{ème}}$ ligne de M (présence des coefficients $m_{j,\ell}$). Ceci doit être dans votre cours sous l'appellation « manipulation élémentaire » et codé :

$$L_i \leftarrow L_i + \alpha L_j$$

$\star$ En procédant de la même manière, ou mieux en transposant (ce qui échange les rôles de i et j), on voit que matrice $M(I_n + \alpha E_{i,j})$ se déduit de M en ajoutant à la $j^{\text{ème}}$ colonne de M, α fois sa $i^{\text{ème}}$, ce qui se code sous la forme : $C_j \leftarrow C_j + \alpha C_i$.

Question 4.

Il semble que la condition $n \geqslant 2$ n'ait pas fait partie de l'énoncé originel donné aux candidats ...

Or la propriété n'a pas vraiment de sens pour $n = 1$, et si on convient que le pgcd de $a_1 \in \mathbb{Z}^*$ est $|a_1|$ (il est dit qu'il est strictement positif), alors on donne un sens à la propriété au rang 1, mais elle est fausse car si $a_1 = -1$, le déterminant de la matrice (-1) vaut -1 et non pas $1 = \mathrm{pgcd}(-1)$.

a) Avant de calculer $\det M$ effectuons la manipulation $C_n \leftarrow C_n - vC_1$. Comme la première colonne de M est $(a_1, \dots, a_n)$, sa dernière colonne devient $(u - va_1, 0, \dots, 0)$ et les autres colonnes sont inchangées. Cette manipulation ne change pas la valeur du déterminant et en développant maintenant par rapport à la dernière colonne, il vient :

$$\boxed{\det(M) = (-1)^{n+1}(u - va_1)\det(N)}$$

b) Notons $d = \operatorname{pgcd}(a_1, \dots, a_n)$ et $\delta = \operatorname{pgcd}(a_2, \dots, a_n)$ (possible, car $a_2, \dots, a_n$ ne sont pas tous nuls).
On cherche des nombres rationnels u et v tels que $d = (-1)^{n+1}(u - va_1)\delta$ et on veut de plus que u et tous les nombres $va_2, \dots, va_n$ soient dans $\mathbb{Z}$.

Comme $d = \operatorname{pgcd}(a_1, \delta)$, les deux compères Bachet et Bézout nous disent qu'il existe des entiers relatifs U et V tels que $d = \delta U + a_1 V$.

Avec : $u = (-1)^{n+1}U$ et $v = (-1)^n \dfrac{V}{\delta} = (-1)^n \dfrac{V}{\det(N)}$, on a :
$\rightarrow u \in \mathbb{Z}$
$\rightarrow \forall\, i \geqslant 2, va_i = (-1)^n V \times \dfrac{a_i}{\det(N)} \in \mathbb{Z}$, puisque $a_2, \dots, a_n$ sont des multiples de δ.
$\rightarrow \det(M) = (-1)^{n+1}((-1)^{n+1}U - (-1)^n \dfrac{Va_1}{\delta})\delta = \delta U + a_1 V = d$.
La matrice M ainsi construite vérifie toutes les conditions exigées.

c) $\star$ le résultat étant faux au rang 1, on initialise au rang 2 :

Soient $a_1, a_2 \in \mathbb{Z}$, non tous deux nuls et d leur pgcd. Avec u et v dans $\mathbb{Z}$ tels que $a_1 u + a_2 v = d$, on construit la matrice $M = \begin{pmatrix} a_1 & -v \\ a_2 & u \end{pmatrix}$.
Elle est bien à coefficients dans $\mathbb{Z}$, de première colonne imposée et de déterminant adéquat. Bref elle convient.

$\star$ Supposons le résultat acquis à un certain rang $n - 1 \geqslant 2$ et passons au rang suivant.

$\rightarrow$ Si $a_2 = \dots = a_n = 0$.
Alors $M = \operatorname{diag}(a_1, 1, \dots, 1, \operatorname{sgn}(a_1))$ est à coefficients entiers, de première colonne $(a_1, 0, \dots, 0)$ et de déterminant $|a_1| = \operatorname{pgcd}(a_1, 0, \dots, 0)$, donc cette matrice convient.

$\rightarrow$ Sinon, l'hypothèse de récurrence nous dit que l'on peut trouver une matrice N dans $\mathcal{M}_{n-1}(\mathbb{Z})$ de première colonne $(a_2, \dots, a_n)$ et de déterminant $\operatorname{pgcd}(a_2, \dots, a_n)$. Alors en choisissant u et v comme expliqué en **b)** on construit une matrice M de $\mathcal{M}_n(\mathbb{Z})$ de première colonne $(a_1, \dots, a_n)$ et de déterminant $\operatorname{pgcd}(a_1, \dots, a_n)$.

Dans les deux cas l'hérédité est acquise et on conclut par le principe de récurrence.

Question 5.

On aurait dû nous dire que dans cette question on a encore $n \geqslant 2$, car en **a)** si on prend $n = 1$, l'expression « $x'_1 \in \mathbb{Z}^0$ » a un sens plutôt obscur pour les étudiants.