Matrices & arithmétique : Facteurs invariants (Hermite-Smith)

L'objet de ce problème est l'étude des matrices à coefficients dans l'anneau $\mathbb{Z}$.

Pour tout $n \in \mathbb{N}^*$, on note $\mathcal{M}_n(\mathbb{Z})$, l'ensemble des matrices d'ordre n à coefficients entiers.
On note également, $\mathcal{GL}_n(\mathbb{Z})$, le sous-ensemble de $\mathcal{M}_n(\mathbb{Z})$ des matrices inversibles et dont l'inverse est également une matrice à coefficients entiers.
Ainsi, $A := \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$, mais $A \notin \mathcal{GL}_2(\mathbb{Z})$, car $A \in \mathcal{GL}_2(\mathbb{Q})$, mais $A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \notin \mathcal{M}_2(\mathbb{Z})$.

1 Etude de $\mathcal{SL}_2(\mathbb{Z})$

Dans cette partie, nous considérons uniquement des matrices d'ordre 2 à coefficients dans $\mathbb{Z}$ (si nécessaire dans $\mathbb{Q}$).
On note

$$\det : \mathcal{M}_2(\mathbb{Z}) \longrightarrow \mathbb{Z}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto ad - bc.$$

▷ **1.1.**
Soit $M, M' \in \mathcal{M}_2(\mathbb{Z})$. Montrer que

$$\det(M \times M') = \det(M) \times \det(M')$$

▷ **1.2.**

Considérons une matrice $M \in \mathcal{M}_2(\mathbb{Z})$, non nulle. Supposons que M s'écrive $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c et $d \in \mathbb{Z}$.

Notons $N = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, une autre matrice de $\mathcal{M}_2(\mathbb{Z})$.

1. Evaluer $M \times N$ et $N \times M$.
   On donnera la réponse en fonction de $\det M$.
2. En déduire que si $\det(M) \in \{-1, 1\}$, alors $M \in \mathcal{GL}_2(\mathbb{Z})$ et donner M^{-1} (pour chacun des deux cas).
3. Montrer que si $ad - bc \in \mathbb{Z} \setminus \{-1, 0, 1\}$, alors M est inversible dans $\mathcal{GL}_2(\mathbb{Q})$ mais que $M^{-1} \notin \mathcal{M}_2(\mathbb{Z})$.
4. Enfin, montrer que si $ad - bc = 0$, alors M est diviseur de 0. Conclure que M n'est pas inversible.

On a donc démontré que

$$\mathcal{GL}_2(\mathbb{Z}) = \{M \in \mathcal{M}_2(\mathbb{Z}) \mid \det M \in \{1, -1\}\}$$

On note

$$\mathcal{SL}_2(\mathbb{Z}) = \{M \in \mathcal{M}_2(\mathbb{Z}) \mid \det M = 1\}$$

▷ **1.3.**
Strucure.

1. Montrer que $\mathcal{GL}_2(\mathbb{Z})$ est un groupe.
2. Montrer que $\mathcal{SL}_2(\mathbb{Z})$ est un sous-groupe de $(\mathcal{GL}_2(\mathbb{Z}), \times)$.

Par la suite, on s'intéresse tout particulièrement aux matrices

$$H := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

▷ **1.4.**
Exemples de matrices de $SL_2(\mathbb{Z})$

1. Montrer que H et $B \in SL_2(\mathbb{Z})$.

2. Compléter les matrices suivantes pour obtenir des matrices de $\mathcal{SL}_2(\mathbb{Z})$

$$C_1 := \begin{pmatrix} 1 & 7 \\ \cdot & \cdot \end{pmatrix} \quad C_2 := \begin{pmatrix} 3 & \cdot \\ \cdot & 3 \end{pmatrix} \quad C_3 := \begin{pmatrix} 13 & \cdot \\ 17 & \cdot \end{pmatrix}$$

3. Pourquoi la matrice C_4 suivante ne peut pas être complétée en une matrice de $\mathcal{SL}_2(\mathbb{Z})$?

$$C_4 := \begin{pmatrix} 4 & \cdot \\ 8 & \cdot \end{pmatrix}$$

4. Montrer que pour tout $m \in \mathbb{N}$, on peut trouver une matrice M de $\mathcal{SL}_2(\mathbb{Z})$ tel que $\mathrm{tr}(M) = m$.

▷ **1.5.**
Groupe engendré par H et B.
On note $\mathcal{G} =< H, B >$, le groupe engendré par H et B, i.e. le plus petit sous-groupe de $\mathcal{GL}_2(\mathbb{Z})$ contenant H et B.

1. Montrer que $\mathcal{G} < \mathcal{SL}_2(\mathbb{Z})$.

Nous allons maintenant montrer l'inclusion réciproque (question (d) et (e)), après avoir fait quelques calculs.

2. Calculer $H^{-1}BH^{-1}$ et $HB^{-1}H$. Calculer $\left(H^{-1}BH^{-1}\right)^4$.
3. Ecrire simplement la valeur de H^n et B^n, pour tout entier $\underline{n \in \mathbb{Z}}$. (On attend une démonstration).

▷ **1.6.**
Considérons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{SL}_2(\mathbb{Z})$.

1. Montrer que nécessairement $a \wedge c = 1$
2. L'algorithme d'Euclide pour a et c permet de créer deux suites finies d'entiers $(q_k)_{1 \leqslant k \leqslant N}$ et $(r_k)_{0 \leqslant k \leqslant N+1}$ telles que $r_0 = a$, $r_1 = c$, $r_N = a \wedge c$, $r_{N+1} = 0$ et pour tout $k \in [\![1, N]\!]$, $r_{k-1} = q_k \times r_k + r_{k+1}$.

   Calculer $B^{-q_N} \cdots \times B^{-q_2} H^{-q_1} M$ si N est pair et $H^{-q_N} B^{-q_N - 1} \cdots \times B^{-q_2} H^{-q_1} M$ si N est impair.
3. En déduire qu'il existe deux matrices G_1 et $G_2 \in \mathcal{G}$, deux entiers $\beta, \delta \in \mathbb{Z}$ tels que

$$G_1 \times M \times G_2 = \begin{pmatrix} a \wedge c & \beta \\ 0 & \delta \end{pmatrix}$$

4. Quelle est la valeur de δ ?
   Pour le calcul de δ, on pourra exploiter la question 1.
5. En déduire qu'il existe $G_3 \in \mathcal{G}$ tel que $G_1 \times M \times G_3 = I_2$.
6. Conclure

2 Matrices élémentairement équivalentes

Dans cette partie, n est un entier fixé quelconque supérieur ou égal à 2.

On rappelle que $\mathcal{GL}_n(\mathbb{Z})$, est l'ensemble des matrices d'ordre n, à coefficients entiers, inversibles et dont les inverses sont également à coefficients entiers. On admet qu'il s'agit d'un groupe.
Pour tout $(i, j) \in \mathbb{N}^2$, on note $E_{i,j}$, la matrice ayant un 1 en ligne i et colonne j et des 0 ailleurs.
On note également pour tout $i \neq j \in \mathbb{N}$ et tout $\lambda \in \mathbb{Q}$, $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$.
On notera plus rapidement $T_{i,j}$ au lieu de $T_{i,j}(1)$ lorsque $\lambda = 1$.

On note $\mathcal{SL}_n(\mathbb{Z})$, le groupe engendré par les matrices $(T_{i,j})_{i, \neq j}$.
Rappelons qu'il s'agit du plus petit groupe contenant les matrices $(T_{i,j})_{i \neq j}$.

Soient A et B de $\mathcal{M}_n(\mathbb{Z})$. On dit que A est élémentairement équivalente à B si (et seulement si) :

$$\exists\ P, Q \in \mathcal{SL}_n(\mathbb{Z}) \text{ telles que } A = PBQ^{-1}$$

On note alors $A \equiv_e B$.

▷ **2.1.**
Montrer que $\mathcal{SL}_n(\mathbb{Z}) < \mathcal{GL}_n(\mathbb{Z})$

▷ **2.2.**
En déduire que $\equiv_e$ est une relation d'équivalence.

▷ **2.3.**
Lorsque $M' = T_{i,j}(\lambda) \times M$, comment se déduit (les lignes de) M' de (celles de) M ?
On attend un résultat et une démonstration.

▷ **2.4.**
Donner l'expression de la matrice $S_{i,j} = T_{i,j}(1) \times T_{j,i}(-1) \times T_{i,j}(1)$ avec $(i \neq j)$.
Pourquoi est-ce bien une matrice de $\mathcal{SL}_n(\mathbb{Z})$.

▷ **2.5.**
De même quelle est la forme de la matrice $T_{i,j}(-1) \times T_{j,i}(1) \times T_{i,j}(-1)$, peut-on la décrire en termes de $S_{k,h}$?

3 Théorème des facteurs invariants

Dans cette partie, nous démontrons le théorème des facteurs invariants, ou des formes normales de Smith-Hermite

Toute matrice $A \in \mathcal{M}_n(\mathbb{Z})$ est élémentairement semblables à une matrice de la forme

$$D_r(d_1, \dots d_r) = \left(\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots 0 & \\ 0 & d_2 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & d_r & 0 & \cdots & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{array}\right)$$

avec $d_1 | d_2 | d_3 \cdots | d_r$ (relation de divisibilité).

Une version pour les matrices rectangulaires, et à coefficients dans un anneau principal quelconque existe

Nous commencerons par l'étude du cas $n = 2$. La démonstration générale se fera par récurrence.

▷ **3.1.**
Cas $n = 2$ et M matrice diagonale.
Considérons $M = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$.
On note $\delta = a \wedge b$.

1. Montrer qu'il existe $u, v \in \mathbb{Z}$ tels que
$$B^u \times M \times B^v = \begin{pmatrix} a & 0 \\ \delta & b \end{pmatrix} (:= A')$$
(Les matrices H et B ont été définies en première partie)
2. Montrer qu'il existe $a', b' \in \mathbb{Z}$ et $\epsilon \in \{-1, 1\}$ tels que
$$H^{-a'} \times M' \times H^{-b'} = \begin{pmatrix} 0 & \epsilon \times (a \vee b) \\ \delta & 0 \end{pmatrix}$$
3. En exploitant I.5.(b), montrer que M est élémentairement équivalente à $D_2(a \wedge b, -\epsilon \times a \vee b)$.

▷ **3.2.**
Pourquoi le théorème des facteurs invariants est vraie si M est une matrice d'ordre 1 ?

▷ **3.3.**
Soit $n \in \mathbb{N}^*$ et $n \geqslant 2$. Supposons que le théorème des facteurs invariants est vraie pour toute matrice de taille $n - 1$.
Considérons une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ d'ordre n, non nulle.

1. Notons $\nu = \min\{|[M]_{i,j}| \mid i, j \in \mathbb{N}_n \text{ et } [M]_{i,j} \neq 0\}$. On suppose que $\nu = |[M]_{i_0,j_0}|$.
Donner deux matrices S_1 et $S_2 \in \mathcal{SL}_n(\mathbb{Z})$ tels que $M' = S_1 \times M \times S_2$ avec $[M']_{1,1} = \nu$, $[M']_{i_0,j_0} = [M]_{1,1}$, et pour $i \neq i_0$, $j \neq j_0$, $[M']_{i,j_0} = \pm[M]_{i,1}$, $[M']_{i_0,j} = \pm[M]_{1,j}$ et $[M']_{i,j} = [M]_{i,j}$.
On fera attention au cas : $[M]_{i_0,j_0} > 0$ ou $[M]_{i_0,j_0} < 0$ et aux situations $i_0 = 1$, $i_0 \neq 1$, $j_0 = 1$, $j_0 \neq 1$.

2. Montrer qu'il existe deux matrices $Q_1, Q_2 \in \mathcal{SL}_n(\mathbb{Z})$ tels que $M'' = Q_1 \times M' \times Q_2$ avec pour tout $i, j \in \mathbb{N}_n$, $[M'']_{1,j} = ([M']_{1,j})\%\nu$ (reste de la division euclidienne) et $[M'']_{i,1} = ([M']_{i,1})\%\nu$ et $[M'']_{i,j} = [M]_{i,j}$
3. En déduire que M est élémentairement équivalente à une matrice $\left(\begin{array}{c|ccc} a & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{array}\right)$ avec $M_1 \in \mathcal{M}_{n-1}(\mathbb{Z})$, puis à une matrice de la forme $D_r(a, d_2 \ldots, d_r)$ avec $d_2 | d_3 \cdots | d_r$.
4. En exploitant la question III.1., montrer que $M \equiv_e D_r(a \wedge d_2, a \vee d_2, d_3 \ldots d_r)$. Conclure.

Correction des exercices

▷ Corrigé de l'exercice 1.1

Pour simplifier les notations, considérons que $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$.

On a alors

$$\begin{aligned} \det(M \times M') &= \det \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} = (aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc') \\ &= aa'cb' + aa'dd' + bc'cb' + bc'dd' - ab'ca' - ab'dc' - bd'ca' - bd'dc' \\ &= ada'd' - adb'c' - bca'd' + bcb'c' \\ &= (ad-bc)(a'd'-b'c) = \det M \times \det M' \end{aligned}$$

Pour toute matrices $M, M' \in \mathcal{M}_2(\mathbb{Z})$, $\det(M \times M') = \det(M) \times \det(M')$.

▷ Corrigé de l'exercice 1.2

1. Le calcul est direct :

$$M \times N = N \times M = \det M I_2.$$

2. Ainsi, si $ad - bc = \det M = 1$, on a $M \times N = N \times M = I_2$, donc M est inversible dans $\mathcal{M}_n(\mathbb{Z})$ car son inverse est $N \in \mathcal{M}_n(\mathbb{Z})$.
   Ainsi, si $ad - bc = \det M = -1$, on a $M \times (-N) = (-N) \times M = I_2$, donc M est inversible dans $\mathcal{M}_n(\mathbb{Z})$ car son inverse est $-N \in \mathcal{M}_n(\mathbb{Z})$.

Bilan : si $\det(M) \in \{-1, 1\}$, alors $M \in \mathcal{GL}_2(\mathbb{Z})$
et $M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ (cas $\det M = 1$) et $M^{-1} = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix}$ (cas $\det M = -1$).

3. Supposons que $ad - bc \in \mathbb{Z} \setminus \{-1, 0, 1\}$, alors M est également inversible (comme précédemment) dans $\mathcal{M}_n(\mathbb{Q})$ avec $M^{-1} = \dfrac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
   Pour que cette matrice soit à coefficients entiers, il faut que $ad - bc$ divise a, b, c et d.
   Il existe donc, $a', b', c', d' \in \mathbb{Z}$ tel que $a = (ad-bc)a'$, $b = (ad-bc)b'$, $c = (ad-bc)c'$ et $d = (ad-bc)d'$.
   Cela donne donc, en remplaçant chaque facteur : $ad - bc = (ad-bc)^2(a'd' - b'c')$.
   Et donc $(ad-bc)(a'd'-b'c') = 1$.
   Or ces deux nombres sont entiers donc $(ad-bc) \in \mathbb{Z}^\times = \{-1, 1\}$ (les inversibles de $\mathbb{Z}$). Contradiction.

Nécessairement, $M^{-1} \notin \mathcal{M}_2(\mathbb{Z})$.

4. Si $ad - bc = 0$, alors $M \times N = 0$, donc M est un diviseur de 0 (M est non nulle et N, nécessairement également).
   Alors si M était inversible, on aurait $N = I_2 \times N = M^{-1} \times M \times N = M^{-1} \times 0 = 0$ (matrice nulle).
   Contradiction, car N est non nulle (comme M).

M n'est pas inversible.

▷ Corrigé de l'exercice 1.3

1. L'ensemble $\mathcal{M}_n(\mathbb{Z})$ est un anneau (non commutatif). Puisque les règles opératoires sont celles des anneaux classiques) et que $I_n \in \mathcal{M}_n(\mathbb{Z})$, et pour tout $A, B \in \mathcal{M}_n(\mathbb{Z})$, $A - B$ et $A \times B \in \mathcal{M}_n(\mathbb{Z})$.
   En fait $\mathcal{M}_n(\mathbb{Z})$ est donc un sous-anneau de $\mathcal{M}_n(\mathbb{R})$.
   Et donc l'ensemble de ces éléments inversibles forme un groupe.
   Donc $\mathcal{GL}_2(\mathbb{Z})$ est un groupe.

   On peut aussi montrer que $\mathcal{GL}_2(\mathbb{Z})$ est un sous-groupe de $\mathcal{GL}_2(\mathbb{Q})$. On applique la caractérisation 2 vue en cours.
   — $I_2 \in \mathcal{GL}_2(\mathbb{Z})$, donc $\mathcal{GL}_2(\mathbb{Z})$ est non vide.

— Soient $A, B \in \mathcal{GL}_2(\mathbb{Z})$, alors $B^{-1} \in \mathcal{M}_2(\mathbb{Z})$,
donc $A \times B^{-1} \in \mathcal{M}_2(\mathbb{Z})$:
pour tout $i, j \in \mathbb{N}_2$, $[AB^{-1}]_{i,j} = [A]_{i,1}[B^{-1}]_{1,j} + [A]_{i,2}[B^{-1}]_{2,j} \in \mathbb{Z}$.
Puis l'inverse de $A \times B^{-1}$ est $B \times A^{-1}$, produit de deux matrices entières,
donc $(AB^{-1})^{-1} \in \mathcal{M}_2(\mathbb{Z})$.
Ainsi, si $A, B \in \mathcal{GL}_2(\mathbb{Z})$, alors $A \times B^{-1} \in \mathcal{GL}_2(\mathbb{Z})$.

$\boxed{\mathcal{GL}_2(\mathbb{Z}) \text{ est un groupe.}}$

2. — $I_2 \in \mathcal{SL}_2(\mathbb{Z})$, car $\det I_2 = 1$. Donc $\mathcal{SL}_2(\mathbb{Z})$ est non vide.
— Soient $A, B \in \mathcal{SL}_2(\mathbb{Z})$, alors $A, B^{-1} \in \mathcal{GL}_2(\mathbb{Z})$,
avec $\det A = 1$ et $1 = \det I_2 = \det(BB^{-1}) = \det B \times \det B^{-1} = \det B^{-1}$ ($\det B = 1$).
donc $\det(AB^{-1}) = \det A \times \det(B^{-1}) = 1 \times 1 = 1$.
Ainsi, si $A, B \in \mathcal{SL}_2(\mathbb{Z})$, alors $A \times B^{-1} \in \mathcal{SL}_2(\mathbb{Z})$.

$\boxed{\mathcal{SL}_2(\mathbb{Z}) \text{ est un sous-groupe de } (\mathcal{GL}_2(\mathbb{Z}), \times).}$

▷ Corrigé de l'exercice 1.4

1. H est inversible d'inverse $H^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$, donc $H \in \mathcal{GL}_2(\mathbb{Z})$.
Puis $\det H = 1 \times 1 - 0 \times 1 = 1$.
B est inversible d'inverse $B^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$, donc $B \in \mathcal{GL}_2(\mathbb{Z})$.
Puis $\det B = 1 \times 1 - 0 \times 1 = 1$.
(On peut exploiter la réponse à I.2.(b)).

$\boxed{H \text{ et } B \in SL_2(\mathbb{Z}).}$

2. Il n'a pas uncité de réponse, on peut prendre par exemple $C_1 = \begin{pmatrix} 1 & 7 \\ 1 & 8 \end{pmatrix}$ ou $C_1 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$.
Pour, une réponse s'impose (mais elle n'est pas unique) $C_2 := \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$ (ou sa transposé).
Enfin pour la dernière matrice, on travaille un peu plus : on cherche $b, d \in \mathbb{Z}$ tel que $13d - 17b = 1$.
C'est la recherche d'un couple de Bézout ; on peut appliquer l'algorithme d'Euclide :

$$17 = 13 \times 1 + 4 \quad \text{puis} \quad 13 = 4 \times 3 + 1$$

Donc $1 = 13 - 3 \times (17 - 13) = 4 \times 13 - 3 \times 17$ On peut prendre $C_3 = \begin{pmatrix} 13 & 3 \\ 17 & 4 \end{pmatrix}$.

$\boxed{\text{Bilan (sans unicité) : } C_1 = \begin{pmatrix} 1 & 7 \\ 1 & 8 \end{pmatrix}, C_2 := \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}, C_3 = \begin{pmatrix} 13 & 3 \\ 17 & 4 \end{pmatrix}.}$

3. Pour que $C_4 \in \mathcal{SL}_2(\mathbb{Z})$, il faut qu'il existe $b, d \in \mathbb{Z}$ tels que $4d + 8b = 1$ ce qui impose (Bézout) $4 \wedge 8 = 1$.
Or $4 \wedge 8 = 4$, il est donc

$\boxed{\text{impossible de trouver } b, d \in \mathbb{Z} \text{ tels que } C_4 := \begin{pmatrix} 4 & b \\ 8 & d \end{pmatrix} \in \mathcal{SL}_2(\mathbb{Z}).}$

4. Pour tout entier $m \in \mathbb{N}$, la matrice $\begin{pmatrix} 1 & m-2 \\ 1 & m-1 \end{pmatrix}$ a une trace égale à $1 + (m-1) = 1$ et un déterminant égal à $1 \times (m-1) - 1 \times (m-2) = m - 1 - m + 2 = 1$.
Etant à coefficients entiers, de déterminant égal à 1, cette matrice appartient à $\mathcal{SL}_2(\mathbb{Z})$.

$\boxed{M := \begin{pmatrix} 1 & m-2 \\ 1 & m-1 \end{pmatrix} \in \mathcal{SL}_2(\mathbb{Z}) \text{ et vérifie } \operatorname{tr}(M) = m.}$

▷ Corrigé de l'exercice 1.5

1. $H \in \mathcal{SL}_2(\mathbb{Z})$ et $B \in \mathcal{SL}_2(\mathbb{Z})$. Donc $\mathcal{SL}_2(\mathbb{Z})$ est un groupe contenant H et B.
Or le groupe $\mathcal{G}$ est le plus petit groupe (au sens de l'inclusion) contenant H et B,
il contient donc tout sous-groupe contenant H et B, donc

$$\boxed{\mathcal{G} < \mathcal{SL}_2(\mathbb{Z}).}$$

2. D'après la formule trouvée en I.2.(b), $H^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ alors que $H^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ Le calcul donne (en raisonnant sur les opérations élémentaires sur les lignes ou appliquant directement le calcul) :

$$\boxed{H^{-1}BH^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad - \quad HB^{-1}H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}$$

On trouve alors

$$\boxed{\left(H^{-1}BH^{-1}\right)^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2}$$

3. Montrons par récurrence, pour $n \in \mathbb{N}$,
$\mathcal{Q}_n$: « $H^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ et $B^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ »
— $\mathcal{Q}_0$ est vraie car $H^0 = I_2 = B^0$.
Notons que $\mathcal{Q}_1$ est également vraie.
— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{Q}_n$ est vraie.

$$H^{n+1} = H^n \times H = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$
$$B^{n+1} = B^n \times B = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ n+1 & 1 \end{pmatrix}$$

Donc $\mathcal{Q}_n$ est vraie.

Soit $n \in \mathbb{Z}^-$, alors $-n \in \mathbb{N}$, et $H^n = \left(H^{-n}\right)^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ d'après la question I.2.(b).

Et $B^n = \left(B^{-n}\right)^{-1} = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ d'après la question I.2.(b).

Donc

$$\boxed{\text{pour tout entier relatif, } n \in \mathbb{Z},\ H^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ et } B^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.}$$

▷ Corrigé de l'exercice 1.6

1. Puisque $M \in \mathcal{SL}_2(\mathbb{Z})$, $\det M = 1$ et donc $ad - bc = 1$.
Donc d'après la relation de Bézout, $a \wedge c | 1$ et donc

$$\boxed{a \wedge c = 1.}$$

2. Un premier calcul donne

$$H^{-q_1}M = \begin{pmatrix} 1 & -q_1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r_0 - q_1 r_1 & b - q_1 d \\ r_1 & d \end{pmatrix} = \begin{pmatrix} r_2 & b - q_1 d \\ r_1 & d \end{pmatrix}$$

Définissons alors également par récurrence une suite β_n par :

$$\beta_0 = b, \beta_1 = d \quad \forall\, 1 \leqslant k \leqslant N, \beta_{n+1} = \beta_{n-1} - q_n \beta_n$$

On a alors $\beta_2 = \beta_0 - q1\beta_1 = b - q_1 d$, terme en haut à droite de la matrice.
Finalement, on pose, pour tout $h \in \mathbb{N}$ tel que $h \leqslant N$

$$\mathcal{Q}_n : \text{´ si } h = 2k, B^{-q_h} \cdots \times B^{-q_2} H^{-q_1} M = \begin{pmatrix} r_h & \beta_h \\ r_{h+1} & \beta_{h+1} \end{pmatrix}$$
$$\text{et si } h = 2k+1, H^{-q_h} \cdots \times B^{-q_2} H^{-q_1} M = \begin{pmatrix} r_{h+1} & \beta_{h+1} \\ r_h & \beta_h \end{pmatrix} \text{ ˇ}$$

— Pour $h=0$, pair, on regarde donc $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} r_0 & \beta_0 \\ r_1 & \beta_1 \end{pmatrix}$.
Donc $\mathcal{Q}_0$ est vraie.
De même le calcul précédent prouve que $\mathcal{Q}_1$ est vraie.
— Soit $h \leqslant N-1$, supposons que $\mathcal{Q}_h$ est vraie.
Si $h+1$ est pair, alors h est impair, on a d'après $\mathcal{Q}_h$:

$$\begin{aligned} B^{-q_{h+1}} \times H^{-q_h} \cdots \times B^{-q_2} H^{-q_1} M &= \begin{pmatrix} 1 & 0 \\ -q_{h+1} & 1 \end{pmatrix} \times \begin{pmatrix} r_{h+1} & \beta_{h+1} \\ r_h & \beta_h \end{pmatrix} \\ &= \begin{pmatrix} r_{h+1} & \beta_{h+1} \\ r_h - q_{h+1} r_{h+1} & \beta_h - q_{h+1} r_{h+1} \end{pmatrix} = \begin{pmatrix} r_{h+1} & \beta_{h+1} \\ r_{h+2} & \beta_{h+2} \end{pmatrix} \end{aligned}$$

Si $h+1$ est impair, alors h est pair, on a d'après $\mathcal{Q}_h$:

$$\begin{aligned} H^{-q_{h+1}} \times B^{-q_h} \cdots \times B^{-q_2} H^{-q_1} M &= \begin{pmatrix} 1 & -q_{h+1} \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} r_h & \beta_h \\ r_{h+1} & \beta_{h+1} \end{pmatrix} \\ &= \begin{pmatrix} r_h - q_{h+1} r_{h+1} & \beta_h - q_{h+1} r_{h+1} \\ r_{h+1} & \beta_{h+1} \end{pmatrix} = \begin{pmatrix} r_{h+2} & \beta_{h+2} \\ r_{h+1} & \beta_{h+1} \end{pmatrix} \end{aligned}$$

Donc, tous les cas sont vérifiés et $\mathcal{Q}_{h+1}$ est correct.
On trouve donc pour $h=N$

$$\boxed{\underbrace{B^{-q_N} \cdots \times B^{-q_2} H^{-q_1} M}_{N \equiv 0[2]} = \begin{pmatrix} r_N & \beta_N \\ r_{N+1} & \beta_{N+1} \end{pmatrix} \text{ et } \underbrace{H^{-q_N} \cdots \times B^{-q_2} H^{-q_1} M}_{N \equiv 1[2]} = \begin{pmatrix} r_{N+1} & \beta_{N+1} \\ r_N & \beta_N \end{pmatrix}}$$

3. Notons que $r_{N+1}=0$ et $r_N = a \wedge c = 1$.
D'après la question précédente,
• si N est pair, alors en notant $G_1 = B^{-q_N} \cdots \times B^{-q_2} H^{-q_1} \in \mathcal{SL}_2(\mathbb{Z})$ (car produit d'éléments de $\mathcal{SL}_2(\mathbb{Z})$ qui est un groupe) et $G_2 = I_2 \in \mathcal{SL}_2(\mathbb{Z})$.
On a alors $G_1 \times M \times G_2 = \begin{pmatrix} 1 & \beta_N \\ 0 & \beta_{N+1} \end{pmatrix}$.
• si N est impair, alors en notant $G_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} H^{-q_N} \cdots \times B^{-q_2} H^{-q_1} \in \mathcal{SL}_2(\mathbb{Z})$ (car produit d'éléments de $\mathcal{SL}_2(\mathbb{Z})$ qui est un groupe) et $G_2 = I_2 \in \mathcal{SL}_2(\mathbb{Z})$.
On a alors $G_1 \times M \times G_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \beta_{N+1} \\ 1 & \beta_N \end{pmatrix} = \begin{pmatrix} 1 & \beta_N \\ 0 & -\beta_{N+1} \end{pmatrix}$.
Dans tous les cas (indépendamment de la parité de N) :

$$\boxed{\text{Il existe deux matrices } G_1 \text{ et } G_2 \in \mathcal{G}, \text{ deux entiers } \beta, \delta \in \mathbb{Z} \text{ tels que } G_1 \times M \times G_2 = \begin{pmatrix} 1 & \beta \\ 0 & \delta \end{pmatrix}.}$$

4. On a vu que $a \wedge c = 1$, et puis $M \in \mathcal{SL}_2(\mathbb{Z})$ donc $\det M = 1$.
Par ailleurs, $G_1, G_2 \in \mathcal{G} \subset \mathcal{SL}_2(\mathbb{Z})$, donc on a également $\det G_1 = \det G_2 = 1$.
Et, avec la première réponse ($\det AB = \det A \det B$), on trouve que $\det \begin{pmatrix} 1 & \beta \\ 0 & \delta \end{pmatrix} = 1 \times \delta = 1$

$$\boxed{\delta = 1}$$

On fait simplement l'opération sur les colonnes $C_2 \leftarrow C_2 - \beta C_1$, soit le calcul matriciel par la droite par $H^{-\beta}$.
On trouve alors

$$G_1 \times M \times G_2 \times H^{-\beta} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} = I_2$$

$$\boxed{G_1 \times M \times G_3 = I_2}$$

5. $\mathcal{G}$ est un groupe, donc G_1'' et G_3'' sont inversible dans $\mathcal{G}$, on a donc

$$M = (G_1'')^{-1} \times (G_3'')^{-1} \in \mathcal{G}$$

Ainsi tous les éléments de $\mathcal{SL}_2(\mathbb{Z})$ sont dans $\mathcal{G}$, i.e $\mathcal{SL}_2(\mathbb{Z}) \subset \mathcal{G}$.
Nous avons vu en I.5.(a) l'inclusion réciproque.

$$\boxed{\text{Ainsi } \mathcal{SL}_2(\mathbb{Z}) = \mathcal{G} =< H, B > \text{ (groupe engendré par } H \text{ et } B).}$$

▷ Corrigé de l'exercice 2.1

$I_n \in \mathcal{SL}_n(\mathbb{Z})$, donc $\mathcal{SL}_n(\mathbb{Z})$ est non vide.
$\mathcal{SL}_n(\mathbb{Z})$ est un groupe : c'est un groupe engendré, le plus petit au sens de l'inclusion contenant les matrices $T_{i,j}$.
Or celle-ci sont toutes inversibles, donc dans $\mathcal{GL}_n(\mathbb{Z})$.
Par conséquent, $\mathcal{GL}_n(\mathbb{Z})$ est un groupe contenant toutes les matrice $T_{i,j}$,
il contient donc nécessairement $\mathcal{SL}_n(\mathbb{Z})$, le plus petit (au sens de l'inclusion).

$$\boxed{(\mathcal{SL}_n(\mathbb{Z}), +) < (\mathcal{GL}_n(\mathbb{Z}), +).}$$

▷ Corrigé de l'exercice 2.2

— Pour tout $A \in \mathcal{M}_n(\mathbb{Z})$, comme $I_n \in \mathcal{SL}_n(\mathbb{Z})$ et que $A = I_n \times A \times I_n^{-1}$,
on a $A \equiv_e A$, donc $\equiv_e$ est réflexive.
— Soient $A, B \in \mathcal{M}_n(\mathbb{Z})$, telles que $A \equiv_e B$.
Donc il existe $P, Q \in \mathcal{SL}_n(\mathbb{Z})$ telles que $A = PBQ^{-1}$.
Donc $P, Q \in \mathcal{GL}_n(\mathbb{Z})$ et on a $B = P^{-1}AQ$, comme $P^{-1}, Q^{-1} \in \mathcal{SL}_n(\mathbb{Z})$,
on affirme que $B \equiv_e A$, donc $\equiv_e$ est symétrique.
— Soient $A, B, C \in \mathcal{M}_n(\mathbb{Z})$, telles que $A \equiv_e B$ et $B \equiv_e C$.
Donc il existe $P, Q \in \mathcal{SL}_n(\mathbb{Z})$ telles que $A = PBQ^{-1}$.
Donc il existe $R, S \in \mathcal{SL}_n(\mathbb{Z})$ telles que $B = RCS^{-1}$.
Donc $A = (PR)C(QS)^{-1}$, et $PR \in \mathcal{SL}_n(\mathbb{Z})$ et $QS \in \mathcal{SL}_n(\mathbb{Z})$ car $\mathcal{SL}_n(\mathbb{Z})$ est un groupe.
Ainsi $A \equiv_e C$, donc $\equiv_e$ est transitive.

$$\boxed{\equiv_e \text{ est une relation d'équivalence sur } \mathcal{M}_n(\mathbb{Z}).}$$

▷ Corrigé de l'exercice 2.3

On a vu en cours que

$$\boxed{\forall\, k \neq i,\ L_k(M') = L_k(M) \text{ et } L_i(M') = L_i(M) + \lambda L_j(M).}$$

Montrons le :

$$T_{i,j}(\lambda) \times M = (I_n + \lambda E_{i,j}) \times M = M + \lambda E_{i,j} M$$

Or $M = \sum_{k,h} [M]_{k,h} E_{k,h}$ et $E_{i,j}E_{k,h} = \delta_{j,k}E_{i,h}$, donc

$$E_{i,j}M = \sum_{k,h} [M]_{k,h} E_{i,j}E_{k,h} = \sum_{h=1}^{n} [M]_{j,h} E_{i,h}$$

Donc pour $k \neq i$, $L_k(E_{i,j}M) = \sum_{h=1}^{n} [M]_{j,h} L_k(E_{i,h}) = 0$ et $L_i(E_{i,j}M) = \sum_{h=1}^{n} [M]_{j,h} L_i(E_i, h) = L_j(M)$.

Ainsi

$$\boxed{L_k(M') = L_k(M) + 0 \qquad L_i(M') = L_i(M) + \lambda L_i(E_{i,j}M) = L_i(M) + \lambda L_j(M).}$$

▷ Corrigé de l'exercice 2.4

On fait le calcul directement

$$\begin{aligned} S_{i,j} &= (I_n + E_{i,j})(I_n - E_{j,i})(I_n + E_{i,j}) = (I_n + E_{i,j} - E_{j,i} - E_{i,i})(I_n + E_{i,j}) \\ &= I_n + E_{i,j} - E_{j,i} - E_{i,i} + E_{i,j} + 0 - E_{j,j} - E_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} - E_{j,i} \end{aligned}$$

Autre méthode (en regardant le calcul sur les opérations élémentaires),

la multiplication à gauche par $T_{i,j}(1)$ conduit aux opérations élémentaires $\begin{cases} L_i^{(2)} \leftarrow L_i^{(1)} + L_j^{(1)} \\ L_j^{(2)} \leftarrow L_j^{(1)} \end{cases}$.

la multiplication à gauche par $T_{j,i}(-1)$ conduit aux opérations élémentaires $\begin{cases} L_i^{(3)} \leftarrow L_i^{(2)} = L_i^{(1)} + L_j^{(1)} \\ L_j^{(3)} \leftarrow L_j^{(2)} - L_i^{(2)} = -L_i^{(1)} \end{cases}$.

la multiplication à gauche par $T_{i,i}(1)$ conduit aux opérations élémentaires $\begin{cases} L_i^{(4)} \leftarrow L_i^{(3)} + L_j^{(3)} = L_j^{(1)} \\ L_j^{(4)} \leftarrow L_j^{(3)} = -L_i^{(1)} \end{cases}$.

Ainsi $S_{i,j}$ est presque une matrice de transposition (permutation), c'est $I_n - E_{i,i} - E_{j,j} + E_{i,j} - E_{j,i}$, multiplier M par la gauche par cette matrice conduit à $L_i(M') = L_j(M)$ et $L_j(M') = -L_i(M)$

$S_{i,j}$ est le produit de trois éléments de $\mathcal{SL}_n(\mathbb{Z})$, puisque $T_{i,j}(1)$ est une matrice de transvection simple et $T_{j,i}(-1) = T_{j,i}^{-1}$ est l'inverse d'une matrice de transvection simple et que $\mathcal{SL}_n(\mathbb{Z})$ est un groupe -donc contient tous les inverses et les produits.

Ainsi $S_{i,j} \in \mathcal{SL}_n(\mathbb{Z})$.

▷ Corrigé de l'exercice 2.5

On trouve,

$$\begin{aligned} R_{i,j} &= (I_n - E_{i,j})(I_n + E_{j,i})(I_n - E_{i,j}) = (I_n - E_{i,j} + E_{j,i} - E_{i,i})(I_n - E_{i,j}) \\ &= I_n - E_{i,j} - E_{i,j} + 0 + E_{j,i} - E_{j,j} - E_{i,i} + E_{i,j} = I_n - E_{i,i} - E_{j,j} - E_{i,j} + E_{j,i} = S_{j,i} \end{aligned}$$

▷ Corrigé de l'exercice 3.1

1. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \delta$.
   On a donc (pour le calcul de B^u, voir I.5.(c)) :

$$B^u \times M \times B^v = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ ua & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ au+bv & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ \delta & b \end{pmatrix}$$

2. $\delta = a \wedge b$, donc $\delta | a$ et $\delta | b$, il existe $a', b' \in \mathbb{Z}$ tels que $a = \delta a'$ et $b = \delta b'$. On a alors (pour le calcul de $H^{a'}$, voir I.5.(c)) :

$$\begin{aligned} H^{-a'} \times M' \times H^{-b'} &= \begin{pmatrix} 1 & -a' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ \delta & b \end{pmatrix} \begin{pmatrix} 1 & -b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a - a'\delta & -a'b \\ \delta & b \end{pmatrix} \begin{pmatrix} 1 & -b' \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -a'b \\ \delta & b \end{pmatrix} \begin{pmatrix} 1 & -b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -a'b \\ \delta & -b'\delta + b \end{pmatrix} = \begin{pmatrix} 0 & -a'b \\ \delta & 0 \end{pmatrix} \end{aligned}$$

   Or $-a'b = -\dfrac{ab}{\delta} = -\dfrac{ab}{a \wedge b} = \epsilon \times a \vee b$ avec $\epsilon = 1$ si $ab < 0$ et $\epsilon = -1$ si $ab > 0$.

Il existe $a', b' \in \mathbb{Z}$ et $\epsilon = 1$ si $ab < 0$ et $\epsilon = -1$ si $ab > 0$ tels que $H^{-a'} \times M' \times H^{-b'} = \begin{pmatrix} 0 & \epsilon \times (a \vee b) \\ a \wedge b & 0 \end{pmatrix}$.

3. On considère alors $R = H^{-1}BH^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathcal{SL}_2(\mathbb{Z})$ d'après I.5.(b).
   On a (en notant M'', la matrice trouvée à la question précédente) :

$$R \times M'' = \begin{pmatrix} a \wedge b & 0 \\ 0 & -\epsilon(a \vee b) \end{pmatrix} (:= M''')$$

   Par transitivité, comme $M \equiv_e M' \equiv_e M'' \equiv_e M'''$, on trouve

M est élémentairement équivalente à $D_2(a \wedge b, -\epsilon \times a \vee b)$, avec $\epsilon = 1$ si $ab < 0$ et $\epsilon = -1$ si $ab > 0$.

   On note que $a \wedge b$ divise $\epsilon \times (a \vee b)$...

▷ Corrigé de l'exercice 3.2

Si M est d'ordre 1, alors $M = (d)$ est directement sous forme de la décomposition de Smith-Hermite.

> Donc le théorème des facteurs invariants est vraie si M est une matrice d'ordre 1.

▷ Corrigé de l'exercice 3.3

1. En fin de seconde partie, on a construit $S_{i,j} \in \mathcal{SL}_2(\mathbb{Z})$ (pour tout $i \neq j$)
   qui fait les opérations élémentaires (multiplication à gauche) : $\begin{cases} L_i \leftarrow L_j \\ L_j \leftarrow -L_i \end{cases}$,
   qui fait les opérations élémentaires (multiplication à droite) : $\begin{cases} C_i \leftarrow -C_j \\ C_j \leftarrow C_i \end{cases}$.

   Plusieurs cas possible selon les valeurs de i_0, j_0.
   — Si $i_0 = 1$ et $j_0 = 1$, et $[M]_{i_0,j_0} > 0$ on ne fait rien.
   et si $i_0 = 1$ et $j_0 = 1$, et $[M]_{i_0,j_0} < 0$, on multiplie par la matrice diagonale $\mathrm{D}(-1,-1,1\dots1) \in \mathcal{SL}_2(\mathbb{Z})$
   (se démontre comme $(HB^{-1}H)^2$ en I.5.(b)).
   On a donc bien l'équivalence élémentaire recherchée (avec I_n)
   — Si $i_0 \neq 1$ et $j_0 = 1$, (ν est situé sur la première colonne).
   on échange les lignes L_1 et L_{i_0}, selon que $[M]_{i_0,j_0}$ est positif ou négatif (respectivement),
   on fait $\begin{cases} L_1 \leftarrow L_{i_0} \\ L_{i_0} \leftarrow -L_1 \end{cases}$ ou $\begin{cases} L_1 \leftarrow -L_{i_0} \\ L_{i_0} \leftarrow L_1 \end{cases}$ (respectivement),
   autrement écrit, on multiplie à gauche par S_{1,i_0} ou $S_{i_0,1}$ respectivement (et I_n à droite).
   On a donc bien l'équivalence élémentaire recherchée.
   — Si $i_0 = 1$ et $j_0 \neq 1$, (ν est situé sur la première colonne) on échange les colonnes C_1 et C_{j_0}, selon que $[M]_{i_0,j_0}$ est positif ou négatif (respectivement),
   on fait $\begin{cases} C_1 \leftarrow C_{j_0} \\ C_{j_0} \leftarrow -C_1 \end{cases}$ ou $\begin{cases} C_1 \leftarrow -C_{j_0} \\ C_{j_0} \leftarrow C_1 \end{cases}$ (respectivement),
   autrement écrit, on multiplie à droite par $S_{j_0,1}$ ou S_{1,j_0} respectivement (et I_n à gauche).
   On a donc bien l'équivalence élémentaire recherchée.
   — Si $i_0 \neq 1$ et $j_0 \neq 1$, on fait successivement les deux opérations :
   $\begin{cases} L_1 \leftarrow L_{i_0} \\ L_{i_0} \leftarrow -L_1 \end{cases}$ puis $\begin{cases} C_1 \leftarrow C_{j_0} \\ C_{j_0} \leftarrow -C_1 \end{cases}$ (si $[M]_{i_0,j_0} > 0$) ou $\begin{cases} C_1 \leftarrow -C_{j_0} \\ C_{j_0} \leftarrow C_1 \end{cases}$ (si $[M]_{i_0,j_0} < 0$).
   On a donc bien l'équivalence élémentaire recherchée.

   > Dans tous les cas, on peut placer, par opérations élémentaires, donc équivalences élémentaires, ν en position $(1,1)$ puis faire alors le reste des opérations envisagées...

2. Chaque terme de la première colonne de M' se divise par ν de la façon suivante : $[M']_{i,1} = \nu q_i + r_i$.
   Chaque terme de la première ligne de M' se divise par ν de la façon suivante : $[M']_{1,j} = \nu s_j + t_j$.
   Puis, on fait les opérations matricielles (pour $i \geqslant 1$) : $L_i \leftarrow L_i - q_i L_1$ et $C_j \leftarrow C_j - s_j C_1$.
   Cela se code matriciellement par la multiplication à gauche par $Q_1 = \prod_{i=2}^{n} T_{i,1}(-r_i) \in \mathcal{SL}_n(\mathbb{Z})$ (cela commute) et à droite par $Q_2 = \prod_{j=2}^{n} T_{1,j}(-s_j) \in \mathcal{SL}_n(\mathbb{Z})$

   > Il existe deux matrices $Q_1, Q_2 \in \mathcal{SL}_n(\mathbb{Z})$ tels que $M'' = Q_1 \times M' \times Q_2$
   > avec pour tout $i, j \in \mathbb{N}_n$, $[M'']_{1,j} = ([M']_{1,j})\%\nu = s_j$ et $[M'']_{i,1} = ([M']_{i,1})\%\nu = r_i$.

3. A la fin du processus algorithmique commencé lors des deux questions précédentes, nous n'avons pas trouvé une colonne et une ligne de 0, mais une colonne et une ligne de terme plus petit que ν.
   On recommence ainsi tout le processus :
   1. choix du minimum non nul sur la première colonne et première ligne (tant que cela est possible).
   2. déplacement en haut de la matrice, en conservant l'équivalence élémentaire
   3. division euclidienne des termes.

On obtient une suite des choix de minimum strictement décroissante et à valeurs entières donc nulle à partir d'un certain rang.
A l'étape juste précédente, on a eu impossibilité de choisir un minimum, i.e. tous les termes de la première ligne et première colonne (sauf celui en position $(1,1)$) sont nuls.

Ainsi M est élémentairement équivalente à une matrice $\left(\begin{array}{c|ccc} a & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{array}\right)$ avec $M_1 \in \mathcal{M}_{n-1}(\mathbb{Z})$.

Puis cette matrice M_1 est de taille $n-1$, on peut donc appliquer l'hypothèse de récurrence considérée comme vraie pour toute matrice de cette taille : M_1 est élémentairement équivalente à une matrice $D_{r-1}(d_2, \dots d_r)$ avec $d_2|d_3|\cdots|d_r$.
On note W_1 et $W_2 \in \mathcal{SL}_{n-1}(\mathbb{Z})$ telles que $W_1 \times M_1 \times W_2 = D_{r-1}(d_2, \dots d_r)$ avec $d_2|d_3|\cdots|d_r$, alors par blocs :

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & W_1 \end{array}\right) \times \left(\begin{array}{c|c} a & 0 \\ \hline 0 & M_1 \end{array}\right) \times \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & W_2 \end{array}\right) = \left(\begin{array}{c|c} a & 0 \\ \hline 0 & W_1M_1W_2 \end{array}\right) = D_r(a, d_1, \dots d_r)$$

Puis on décompose W_1 en produit de transposition de taille $n-1$, et on reporte dans un calcul par blocs, on trouve des transpositions de taille n.
Donc $\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & W_1 \end{array}\right)$ et $\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & W_2 \end{array}\right) \in \mathcal{SL}_n(\mathbb{Z})$, puis par transitivité,

Donc M est élémentairement équivalente à une matrice de la forme $D_r(a, d_2 \dots, d_r)$ avec $d_2|d_3 \cdots |d_r$.

4. D'après la question III.1, $D_2(a, d_2)$ est élémentairement équivalente à $D_2(a \wedge d_2, \epsilon \times a \vee d_2)$.
Là encore, en exploitant le produit par blocs avec des matrices du type $\left(\begin{array}{cc|c} \alpha & \beta & 0 \\ \gamma & \delta & \\ \hline 0 & & I_{n-2} \end{array}\right)$,
on trouve par transitivité, que

M est élémentairement équivalente à $D_r(a \wedge d_2, \epsilon \times a \vee d_2, d_3, \dots d_r)$ avec $d_2|d_3|\cdots|d_r$.

On alors $\delta_1 = a \wedge b | \delta_2 = a \vee b$, mais aussi $\delta_1|d_2|d_3 \dots$.
Puis on applique le même principe avec $(a \vee d_2)$ et d_3 (coefficient 2 et 3), on obtient $\delta_2 = (a \vee d_2) \wedge d_3$, donc $\delta_1|\delta_2|d_3| \dots d_r$ et ainsi de suite. Par blocs, on a des matrice élémentairement équivalentes.
En notant $\delta_k = (\vee_{i=1}^{k} d_k) \wedge d_{k+1}$, on trouve

$M \equiv_e D_r(\delta_1, \delta_2, \dots \delta_r)$ avec $\delta_1|\delta_2|\cdots|\delta_r$.

Et donc le théorème des facteurs invariants est vrai en taille n. La récurrence est démontrée.