Université de Bordeaux **2024-2025**
Semestre 7 **Modules, Algèbre commutative**

Corrigé du Devoir maison n°2

Soient $m, n \in \mathbf{N}_{>0}$. Le but du problème est de préciser les résultats du cours concernant $\mathsf{M}_{n\times m}(\mathbf{Z})$, en s'intéressant notamment aux aspects *effectifs* : pour chaque question, il faut justifier que les constructions sont calculables algorithmiquement à partir de la division euclidienne. Il n'est pas demandé de calculer la complexité des algorithmes [1].

Si $M_1, M_2 \in \mathsf{M}_{n\times m}(\mathbf{Z})$, on écrit $M_1 \equiv M_2$ (resp. $M_1 \sim M_2$) s'il existe $P \in \mathsf{GL}_n(\mathbf{Z})$ (resp. $(P, Q) \in \mathsf{GL}_n(\mathbf{Z}) \times \mathsf{GL}_m(\mathbf{Z})$) tel que $M_2 = PM_1$ (resp. $M_2 = PM_1Q^{-1}$). Cela définit deux relations d'équivalence [2] sur $\mathsf{M}_{n\times m}(\mathbf{Z})$.

(1) Soient $a, b \in \mathbf{Z}$ non tous les deux nuls et d leur pgcd. Rappeler l'algorithme d'Euclide étendu, qui fournit des éléments $u, v \in \mathbf{Z}$ tels que $au + bv = d$. En déduire un élément $P \in \mathsf{SL}_2(\mathbf{Z})$ tel que $P\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} d \\ 0 \end{smallmatrix}\right)$.

(2) Plus généralement, si $a_1, \dots, a_n \in \mathbf{Z}$ sont non tous nuls et $d = \mathsf{pgcd}(a_1, \dots, a_n)$, construire algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ telle que $P \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Appliquer cet algorithme pour construire $P \in \mathsf{GL}_3(\mathbf{Z})$ telle que $P \begin{pmatrix} 6 \\ 10 \\ 15 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Soit $M = (a_{i,j})_{\substack{1\le i\le n \\ 1\le j\le m}} \in \mathsf{M}_{n\times m}(\mathbf{Z})$. Pour $i \in \{1, \dots, n\}$, notons $p_M(i)$ le plus petit indice $j \in \{1, \dots, m\}$ tel que $a_{i,j} \neq 0$ (avec la convention $p_M(i) = \infty$ si la i-ème ligne de M est nulle). On dit que M est *échelonnée* suivant les lignes lorsque $p_M(i) = \infty$ ou $p_M(i-1) < p_M(i)$ pour tout $i \in \{2, \dots, n\}$. Elle est dite *échelonnée réduite* si en outre pour tout $i \in \{1, \dots, r\}$, on a $a_{i,p_M(i)} > 0$ et $k \in \{1, \dots, i-1\}) \Rightarrow 0 \le a_{k,p_M(i)} < a_{i,p_M(i)}$, où r est le nombre de lignes non nulles de M.

(3) (a) Montrer qu'on peut construire algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ telle que PM soit échelonnée.

(b) Montrer qu'on peut construire algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ telle que PM soit échelonnée réduite. Appliquer l'algorithme à la matrice $M = \left(\begin{smallmatrix} 4 & 6 & 11 & 22 \\ 8 & 12 & 10 & 31 \\ 18 & 27 & 27 & 74 \end{smallmatrix}\right)$.

(4) (Plus difficile) Soient $M_1, M_2 \in \mathsf{M}_{n\times m}(\mathbf{Z})$ échelonnées réduites telles que $M_2 \equiv M_1$. Montrer que $M_1 = M_2$ (procéder par récurrence sur n).

Ce qui précède montre que si $M \in \mathsf{M}_{n\times m}(\mathbf{Z})$, il existe $\widetilde{M} \in \mathsf{M}_{n\times m}(\mathbf{Z})$ échelonnée réduite *unique* telle que $\widetilde{M} \equiv M$. Cette dernière s'appelle la *forme normale de Hermite* de M. On s'en doute, ce qui précède est utile pour résoudre les systèmes linéaires à coefficients entiers (du type $MX = Y$ avec $X \in \mathbf{Z}^m$ et $Y \in \mathbf{Z}^n$), en particulier pour déterminer le noyeau et l'image d'un morphisme de groupes $\mathbf{Z}^m \to \mathbf{Z}^n$, chercher une base adaptées à des sous-modules dans un $\mathbf{Z}$-module libre de rang fini, *etc.*

1. Encore moins que ces derniers soient performants
2. Associées aux actions de $\mathsf{GL}_n(\mathbf{Z})$ (resp. $\mathsf{GL}_n(\mathbf{Z}) \times \mathsf{GL}_m(\mathbf{Z})$) sur $\mathsf{M}_{n\times m}(\mathbf{Z})$ données par $(P, M) \mapsto PM$ (resp. $((P, Q), M) \mapsto PMQ^{-1}$) pour $P \in \mathsf{GL}_n(\mathbf{Z})$, $Q \in \mathsf{GL}_m(\mathbf{Z})$ et $M \in \mathsf{M}_{n\times m}(\mathbf{Z})$.

(5) Soit $M = (a_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \in \mathsf{M}_{n\times m}(\mathbf{Z})$. On pose $\delta(M) = \max\left\{ \max_{1\leq i\leq n} |a_{i,1}|\,,\, \max_{1\leq j\leq m} |a_{1,j}| \right\}$ (la plus grande valeur absolue des coefficients de la première ligne et de la première colonne de M.
(a) Montrer qu'on peut calculer algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ et $Q \in \mathsf{GL}_m(\mathbf{Z})$ telles que $PMQ^{-1} = (b_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ vérifie $i > 1 \Rightarrow b_{i,1} = 0$ et $j > 1 \Rightarrow b_{1,j} = 0$ [indication : effectuer des opérations sur les lignes et les colonnes de M de façon à réduire la quantité $\delta(M)$ au maximum].

(b) Montrer qu'on peut calculer algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ et $Q \in \mathsf{GL}_m(\mathbf{Z})$ telles que PMQ^{-1} soit diagonale.

(6) Soient $a, b \in \mathbf{Z}$ non tous les deux nuls. Posons $d = \mathsf{pgcd}(a, b)$ et $m = \mathsf{ppcm}(a, b)$. Soient $u, v \in \mathbf{Z}$ tel que $au + bv = d$. Écrivons $a = d\alpha$ et $b = d\beta$. Calculer le produit $\left(\begin{smallmatrix} u & v \\ -\beta & \alpha \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -\beta v \\ 1 & \alpha u \end{smallmatrix}\right)$.

(7) En déduire que si $M \in \mathsf{M}_{n\times m}(\mathbf{Z})$, on peut construire algorithmiquement $P \in \mathsf{GL}_n(\mathbf{Z})$ et $Q \in \mathsf{GL}_m(\mathbf{Z})$ telles que $\widehat{M} = PMQ^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ où $d_1, \ldots, d_r \in \mathbf{N}_{>0}$ et $d_k \mid d_{k+1}$ pour tout $k \in \{1, \ldots, r-1\}$. Appliquer l'algorithme à la matrice $M = \left(\begin{smallmatrix} 4 & 6 & 11 & 22 \\ 8 & 12 & 10 & 31 \\ 18 & 27 & 27 & 74 \end{smallmatrix}\right)$.

On a vu en cours que les entiers $d_1, \ldots, d_r$ sont uniques. La matrice $\widehat{M}$ s'appelle la *forme normale de Smith* de M : elle est unique d'après ce qui précède [3].

On s'en doute, hormis celui de la question (3) (b), les algorithmes qui précèdent s'étendent en remplaçant $\mathbf{Z}$ par un anneau euclidien [4]. C'est aussi le cas de celui de la question (3) (b), sous réserve qu'on sache définir convenablement la notion de matrice échelonnée *réduite*.

(8) Définir la notion de matrice échelonnée réduite dans le cas où $A = K[X]$ (où K est un corps).

Solution : (1) • L'algorithme d'Euclide étendu est la construction de trois suites $(r_k)_{0\leq k\leq N}$, $(u_k)_{0\leq k<N}$ et $(v_k)_{0\leq k<N}$ définies de la façon suivante. On initialise les suites en posant $r_0 = a$, $r_1 = b$, $(u_0, v_0) = (1, 0)$ et $(u_1, v_1) = (0, 1)$. Ces suites étant connues au rang k avec $r_k \neq 0$, soit $r_{k-1} = q_k r_k + r_{k+1}$ la division euclidienne de r_{k-1} par r_k : on a $r_{k+1} = 0$ ou $\varphi(r_{k+1}) < \varphi(r_k)$. On pose alors $(u_{k+1}, v_{k+1}) = (u_{k-1}, v_{k-1}) - q_k(u_k, v_k)$. Si on n'avait jamais $r_k = 0$, ce qui précède fournirait une suite $(\varphi(r_k))_{k\in\mathbf{N}}$ strictement décroissante d'éléments de $\mathbf{N}$, ce qui est absurde. Il existe donc $N \in \mathbf{N}_{>0}$ tel que $r_{N-1} \neq 0$ et $r_N = 0$. Observons que $\mathsf{pgcd}(r_{k-1}, r_k) = \mathsf{pgcd}(r_k, r_{k+1})$: un récurrence triviale montre donc que $\mathsf{pgcd}(r_k, r_{k+1}) = d$ pour tout $k \in \{0, \ldots, N-1\}$. En particulier, on a $r_{N-1} = \mathsf{pgcd}(r_{N-1}, r_N) = d$. De même, une récurrence immédiate montre que pour tout $k \in \{1, \ldots, N-1\}$, on a $r_n = au_n + bv_n$. Finalement, l'égalité $r_{N-1} = au_{N-1} + bv_{N-1}$ fournit une égalité de Bézout.
Dans la pratique, il est commode de présenter l'algorithme sous forme d'un tableau de la façon suivante :

3. Cela redémontre de façon effective le fait, vu en cours, que les matrices sous forme normale de Smith constituent un système complet de représentants de $\mathsf{M}_{n\times m}(\mathbf{Z})$ pour la relation d'équivalence $\sim$.

4. Rappelons qu'il s'agit d'un anneau A intègre pour lequel il existe une application $\varphi\colon A \setminus \{0\} \to \mathbf{N}$ telle que pour tout $(a, b) \in A \times A \setminus \{0\})$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$ (une telle (on ne requiert pas l'unicité du couple (q, r)). Les exemples à garder à l'esprit sont $A = \mathbf{Z}$ avec $\varphi(a) = |a|$ pour tout $a \in \mathbf{Z}\setminus\{0\}$ et $A = K[X]$ (où K est un corps) avec $\varphi(P) = \deg(P)$ pour tout $P \in K[X] \setminus \{0\}$.

a	1	0	
b	0	1	q_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_n	u_n	v_n	q_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$

La $n+1$-ième ligne n'est alors que la $n-1$-ième moins q_n fois la n-ième ($L_{n+1} \leftarrow L_{n-1} - q_n L_n$).

Remarque. Rappelons que la suite de Fibonacci $(F_n)_{n\in\mathbf{N}}$ est définie par $F_0 = F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$ pour tout $n > 1$. On a $F_n = \frac{1}{\sqrt{5}}\left(\phi^{n+1} - (-\phi)^{-n-1}\right)$ où $\phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or (F_n est donc l'entier le plus proche de $\frac{\phi^{n+1}}{\sqrt{5}}$).

Proposition. (Lamé). *Soient $0 < b < a$ des entiers et d leur pgcd. Si l'algorithme d'Euclide appliqué à (a, b) termine en N étapes, alors $dF_{N+1} \leq a$ et $dF_N \leq b$. En particulier, le nombre d'étapes dans l'algorithme d'Euclide est un $\mathsf{O}(\ln(b))$.*

Démonstration. On raisonne par récurrence. Si $N = 1$, alors a est un multiple de b : on a $b = d = dF_1$ et $a \geq 2d = dF_2$. Supposons $N > 1$: la première étape transforme (a, b) en $(b, a - qb)$ où $r = a - qb \leq a - b$. Par hypothèse de récurrence, on a donc $dF_N \leq b$ et $dF_{N-1} \leq r \leq a - b$, de sorte que $a \geq dF_{N-1} + b \geq d(F_{N-1} + F_N) = dF_{N+1}$. On a $\ln(F_N) \sim (N + 1)\ln(\phi)$ d'après ce qui précède : la majoration $F_N \leq dF_N \leq b$ implique que $N = \mathsf{O}(\ln(b))$. □

À chaque étape de l'algorithme, on fait une division euclidienne, deux multiplications et deux soustractions : finalement, l'algorithme d'Euclide étendu requiert $\mathsf{O}(\ln(\max\{a, b\}))$ opérations.

• Écrivons $a = da'$ et $b = db'$: on a $a'u + b'v = 1$ (l'anneau A est intègre), donc $M = \left(\begin{smallmatrix} u & v \\ -b' & a' \end{smallmatrix}\right)$ appartient à $\mathsf{SL}_2(A)$, et $P\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} d \\ 0 \end{smallmatrix}\right)$.

(2) • On construit P récursivement. Si $n = 1$, il n'y a rien à faire : supposons $n > 1$.

► Si $a_{n-1} = a_n = 0$, on applique l'algorithme au vecteur $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-2} \end{pmatrix} \in \mathbf{Z}^{n-2}$: il existe $P_0 \in \mathsf{SL}_{n-2}(\mathbf{Z})$ telle que $P_0 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-2} \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$: on pose alors $P = \left(\begin{smallmatrix} P_0 & 0 \\ 0 & \mathrm{I}_2 \end{smallmatrix}\right) \in \mathsf{SL}_n(\mathbf{Z})$.

► Si a_{n-1} et a_n ne sont pas tous les deux nuls, on dispose de $\delta = \mathsf{pgcd}(a_{n-1}, a_n)$. D'après la question (1), il existe $P_1 \in \mathsf{SL}_2(\mathbf{Z})$ effectivement calculable telle que $P_1\left(\begin{smallmatrix} a_{n-1} \\ a_n \end{smallmatrix}\right) = \left(\begin{smallmatrix} \delta \\ 0 \end{smallmatrix}\right)$: si $\widetilde{P}_1 = \left(\begin{smallmatrix} \mathrm{I}_{n-2} & 0 \\ 0 & P_1 \end{smallmatrix}\right) \in \mathsf{SL}_n(\mathbf{Z})$, on a $v := \widetilde{P}_1 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_{n-2} \\ \delta \\ 0 \end{pmatrix}$. On applique l'algorithme au vecteur $v \in \mathbf{Z}^{n-1}$: il existe $P_2 \in \mathsf{GL}_{n-1}(\mathbf{Z})$ telle que $P_2 v = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ (on a bien entendu $\mathsf{pgcd}(a_1, \ldots, a_{n-2}, \delta) = d$). On pose $\widetilde{P}_2 = \left(\begin{smallmatrix} P_2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathsf{GL}_n(\mathbf{Z})$ et $P = \widetilde{P}_2 \widetilde{P}_1 \in \mathsf{SL}_n(\mathbf{Z})$.

Remarque. Lorsque $n > 1$, on peut en fait avoir $P \in \mathsf{SL}_n(\mathbf{Z})$, quitte à la multiplier à gauche par $\mathrm{diag}(1, \ldots, 1, -1)$.

• Appliquons l'algorithme au vecteur $\begin{pmatrix} 6 \\ 10 \\ 15 \end{pmatrix}$. On a $\mathsf{pgcd}(10, 15) = 5$, et $P_1 = \left(\begin{smallmatrix} -1 & 1 \\ -3 & 2 \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$ est telle que $P_1\left(\begin{smallmatrix} 10 \\ 15 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 5 \\ 0 \end{smallmatrix}\right)$. Ensuite, on a $\mathsf{pgcd}(6, 5) = 1$, et $P_2 = \left(\begin{smallmatrix} 1 & -1 \\ -5 & 6 \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$ est telle que $P_2\left(\begin{smallmatrix} 6 \\ 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. On pose alors $P = \left(\begin{smallmatrix} P_1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & P_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 & -1 \\ -5 & -6 & 6 \\ 0 & -3 & 2 \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$.

(3) (a) Là encore, on procède récursivement. Si $m = 1$, il n'y a rien à faire : supposons $m > 1$. Notons v la première colonne de M.

Si $\mathrm{la}v = 0$, on a $M = \left(\begin{smallmatrix} 0 & M' \end{smallmatrix}\right)$ avec $M' \in \mathsf{M}_{n\times(m-1)}(\mathbf{Z})$. On applique l'algorithme à M' : il existe $P \in \mathsf{GL}_n(\mathbf{Z})$ telle que PM' soit échelonnée, il en est de même de PM.

Supposons $v \neq 0$: notons d le pgcd des coefficients de v. D'après la question précédente, il existe $P_1 \in \mathsf{SL}_n(\mathbf{Z})$ telle que $P_1 v = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, et donc $L \in \mathsf{M}_{1,m-1}(\mathbf{Z})$ et $M' = \mathsf{M}_{n\times(m-1)}(\mathbf{Z})$ telles que $P_1 M = \left(\begin{smallmatrix} d & L \\ 0 & M' \end{smallmatrix}\right)$. On applique l'algorithme à M' : il existe $P_2 \in \mathsf{GL}_n(\mathbf{Z})$ telle que $P_2 M'$ soit échelonnée. Si $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & P_2 \end{smallmatrix}\right) P_1 \in \mathsf{SL}_n(\mathbf{Z})$, la matrice PM et échelonnée réduite.

(b) • D'après la question précédente, on peut suppoer que $M = (a_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq m}}$ est échelonnée. Posons $r = \mathsf{rg}(M)$: les r premières lignes de M sont non nulles, et les $n-r$ dernières sont nulles. Pour $i \in \{1,\dots,r\}$, soit $\varepsilon_i \in \{\pm 1\}$ tel que $\varepsilon_i a_{i,p(i)} > 0$: quitte à multiplier M à gauche par $\mathrm{diag}(\varepsilon_1,\dots,\varepsilon_r,1,\dots,1)$, on se ramène au cas où $a_{i,p(i)} > 0$ pour tout $i \in \{1,\dots,r\}$.
Si $r = 1$, la matrice M est réduite. Supposons que $r > 1$ et soit $\ell \in \{2,\dots,r\}$ tel que pour tout $i \in \{1,\dots,\ell-1\}$, on ait $1 \leq k < i \Rightarrow 0 \leq a_{k,p_M(i)} < a_{i,p_M(i)}$. Pour $1 \leq k < \ell$, soit $a_{k,p_M(\ell)} = a_{\ell,p_M(\ell)} q_{k,\ell} + r_{k,\ell}$ avec $q_{k,\ell}, r_{k,\ell} \in \mathbf{Z}$ tels que $0 \leq r_{k,\ell} < a_{\ell,p_M(\ell)}$ la division euclidienne de $a_{k,p_M(\ell)}$ par $a_{\ell,p_M(\ell)}$. Posons alors $Q = \mathrm{I}_n - \sum_{k=1}^{\ell-1} q_{k,\ell} E_{k,p_M(\ell)}$ (où $(E_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq m}}$ désigne la base canonique que $\mathsf{M}_{n\times m}(\mathbf{Z})$). La matrice Q est unipotente : on a $Q \in \mathsf{SL}_n(\mathbf{Z})$. Notons $L_1,\dots,L_n$ les lignes de la matrice M : la matrice QM s'obtient à partir de la matrice M en remplaçant L_k par $L_k - q_{k,\ell}L_\ell$ pour tout $k \in \{1,\dots,\ell-1\}$. Comme les coefficients $a_{\ell,j}$ sont nuls pour $1 \leq j < p_M(\ell)$, cela ne modifie pas les $p_M(\ell)-1$ premières colonnes de M, et ça remplace la $p_M(\ell)$-ème colonne par $\begin{pmatrix} r_{1,\ell}\\ \vdots\\ r_{\ell-1,\ell}\\ a_{\ell,p_M(\ell)}\\ 0\\ \vdots\\ 0\end{pmatrix}$. En outre, cela ne modifie pas les lignes d'indice $> \ell$, ce qui implique que $p_{QM} = p_M$. En répétant cette construction, on construit inductivement une suite $(Q_2,\dots,Q_r)$ d'éléments de $\mathsf{SL}_n(\mathbf{Z})$ telle que $P_r P_{r-1}\cdots P_2 M$ soit échelonnée réduite.
• Supposons $M = \left(\begin{smallmatrix} 4 & 6 & 11 & 22\\ 8 & 12 & 10 & 31\\ 18 & 27 & 27 & 74\end{smallmatrix}\right)$. On a $\mathsf{pgcd}(4,8,18) = 2$: l'algorithme de la question (2) fournit la matrice $P_1 = \left(\begin{smallmatrix} 0 & -2 & 1\\ -1 & -4 & 2\\ 0 & -9 & 4\end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$ vérifiant $P_1\left(\begin{smallmatrix}4\\8\\18\end{smallmatrix}\right) = \left(\begin{smallmatrix}2\\0\\0\end{smallmatrix}\right)$. On a alors $P_1 M = \left(\begin{smallmatrix} 2 & 3 & 7 & 12\\ 0 & 0 & 3 & 2\\ 0 & 0 & 18 & 17\end{smallmatrix}\right)$. Ensuite, on a $\mathsf{pgcd}(3,18) = 3$, et $P_2 = \left(\begin{smallmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -6 & -1\end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$ vérifie $P_2\left(\begin{smallmatrix}7\\3\\18\end{smallmatrix}\right) = \left(\begin{smallmatrix}7\\3\\0\end{smallmatrix}\right)$. On a alors $P_2P_1M = \left(\begin{smallmatrix} 2 & 3 & 7 & 12\\ 0 & 0 & 3 & 2\\ 0 & 0 & 0 & 5\end{smallmatrix}\right)$: c'est une matrice échelonnée. Elle n'est pas réduite : si $P_3 = \left(\begin{smallmatrix} 1 & -2 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{smallmatrix}\right) \in \mathsf{SL}_3(\mathbf{Z})$, on a $P_3P_2P_1M = \left(\begin{smallmatrix} 2 & 3 & 1 & 8\\ 0 & 0 & 3 & 2\\ 0 & 0 & 0 & 5\end{smallmatrix}\right)$, enfin si on prend $P_4 = \left(\begin{smallmatrix} 1 & 0 & -1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$, la matrice $P_4P_3P_2P_1M = \left(\begin{smallmatrix} 2 & 3 & 1 & 3\\ 0 & 0 & 3 & 2\\ 0 & 0 & 0 & 5\end{smallmatrix}\right)$ est échelonnée réduite.

(4) Par hypothèse, il existe $P \in \mathsf{GL}_n(\mathbf{Z})$ telle que $M_2 = PM_1$. Montrons par récurrence sur n que $M_1 = M_2$. Si $n = 1$, on a $P \in \mathbf{Z}^\times = \{\pm 1\}$, donc $M_2 = \pm M_1$. Cela implique que $p_{M_1} = p_{M_2}$. Si $M_1 = 0$, on a fini : supposons $M_1 \neq 0$. Comme M_1 et M_2 sont réduites, leurs coefficients d'indice $(1, p_{M_1}(1))$ dont tous les deux dans $\mathbf{N}_{>0}$, ce qui montre que $P = 1$, et donc $M_1 = M_2$.
Supposons $n > 1$. Si $M_1 = 0$, alors $M_2 = 0$ et on a fini : supposons $M_1 \neq 0$. Les $p_{M_1}(1)-1$ premières colonnes de M_1 sont nulles : il en est de même des $p_{M_1}(1)-1$ premières colonnes de M_2. Cela implique que $p_{M_1}(1) - 1 \leq p_{M_2}(1) - 1$, *i.e.* $p_{M_1}(1) \leq p_{M_2}(1)$. Par symétrie, on a bien sûr $p_{M_2}(1) \leq p_{M_1}(1)$, ce qui montre que $p_{M_1}(1) = p_{M_2}(1)$. Notons $(e_1,\dots,e_n)$ la base canonique de $\mathbf{Z}^n$: les $p_{M_1}(1)$-èmes colonnes de M_1 et M_2 sont de la forme ae_1 et be_1 respectivement, avec $a, b \in \mathbf{N}_{>0}$ parce que M_1 et M_2 sont réduites. On a alors $be_1 = aPe_1$, ce qui implique que $a = b$ (prendre le pgcd des coefficients de Pe_1). Il en résulte que $Pe_1 = e_1$, et donc qu'il existe $L \in \mathsf{M}_{1\times(n-1)}(\mathbf{Z})$ et $Q \in \mathsf{GL}_{n-1}(\mathbf{Z})$ tels que $P = \left(\begin{smallmatrix} 1 & L\\ 0 & Q\end{smallmatrix}\right)$. Écrivons de même $M_1 = \left(\begin{smallmatrix} L_1\\ M_1'\end{smallmatrix}\right)$ et $M_2 = \left(\begin{smallmatrix} L_2\\ M_2'\end{smallmatrix}\right)$ avec $L_1, L_2 \in \mathsf{M}_{1\times m}(\mathbf{Z})$ et $M_1', M_2' \in \mathsf{M}_{(n-1)\times m}(\mathbf{Z})$. Ces dernières ont échelonnées réduites. La multiplication par blocs

implique que $M_2' = QM_1'$: l'hypothèse de récurrence montre que $M_1' = M_2'$. Par ailleurs, on a $L_2 = L_1 + LM_1'$. Écrivons $L = (\alpha_2, \dots, \alpha_n)$ et $M_1 = (a_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$: si $i \in \{2, \dots, r\}$ la $p_{M_1}(i)$-ème composante du vecteur ligne LM_1' est $\sum_{k=2}^{i} \alpha_k a_{k,p_{M_1}(i)}$. Comme elle est égale à celle de $L_2 - L_1$ qui est strictement inférieure à $a_{i,p_{M_1}(i)}$ vu que M_1 est échelonnée réduite, on a $\left|\sum_{k=2}^{i} \alpha_k a_{k,p_{M_1}(i)}\right| < a_{i,p_{M_1}(i)}$. On a en particulier $|\alpha_2| < 1$, et donc $\alpha_2 = 0$ vu que $\alpha_2 \in \mathbf{Z}$. De proche en proche, on en déduit de même que $\alpha_i = 0$ pour tout $i \in \{2, \dots, r\}$. Comme les $n - r$ dernières lignes de M_1' sont nulles, on a donc $LM_1' = 0$, d'où $L_2 = L_1$, ce qui montre finalement que $M_1 = M_2$.

(5) (a) Là encore, on procède inductivement. Si la première ligne et la première colonne de M sont nulles, il n'y a rien à faire (on prend $P = \mathrm{I}_n$ et $Q = \mathrm{I}_m$). Sinon, quitte à multiplier M à gauche et à droite par des matrices de permutation (et, au besoin, multiplier le première ligne par -1), on peut supposer que $\delta(M) = a_{1,1} > 0$. Pour $k \in \{2, \dots, n\}$, soit $a_{k,1} = q_k a_{1,1} + a'_{k,1}$ avec $0 \leq a'_{k,1} < a_{1,1}$ la division euclidienne de $a_{k,1}$ par $a_{1,1}$. Posons alors $P = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ -q_2 & 1 & \ddots & & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ -q_n & 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathsf{GL}_n(\mathbf{Z})$: on a $PM = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a'_{2,1} & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ a'_{n,1} & * & \cdots & * \end{pmatrix}$. De même, on peut construire explicitement une matrice $Q \in \mathsf{GL}_m(\mathbf{Z})$ telle que $PMQ^{-1} = \begin{pmatrix} a_{1,1} & a'_{1,2} & \cdots & a'_{1,m} \\ a'_{2,1} & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ a'_{n,1} & * & \cdots & * \end{pmatrix}$ où pour tout $k \in \{2, \dots, m\}$, $0 \leq a'_{1,k} < a_{1,1}$ est le reste de la division euclidienne de $a_{1,k}$ par $a_{1,1}$. Si $a'_{k,1} = 0$ pour tout $k \in \{2, \dots, n\}$ et $a'_{1,k} = 0$ pour tout $k \in \{2, \dots, m\}$, on a fini. Sinon, on a $\delta(PMQ^{-1}) < \delta(M)$: on applique ce qui précède à la matrice PMQ^{-1}. On construit ainsi inductivement une suite $M_0 = M, M_1, \dots, M_s$ d'éléments de $\mathsf{M}_{n\times m}(\mathbf{Z})$ telle que $(\delta(M_k))_{0\leq k\leq s}$ soit strictement décroissante et $M_k \sim M_{k-1}$ pour tout $k \in \{1, \dots, s\}$. Comme il n'existe pas de suite infinie strictement décroissante dans $\mathbf{N}$, l'algorithme s'arrête au bout d'un nombre fini d'étapes, ce qui signifie qu'il existe un indice s tel que M_s ait la forme requise.

(b) D'après ce qui précède, on sait calculer explicitement $P_1 \in \mathsf{GL}_n(\mathbf{Z})$ et $Q_1 \in \mathsf{GL}_m(\mathbf{Z})$ telles que $P_1 M Q_1^{-1} = \left(\begin{smallmatrix} a_1 & 0 \\ 0 & M' \end{smallmatrix}\right)$ avec $a_1 \in \mathbf{Z}$ et $M' \in \mathsf{M}_{(n-1)\times(m-1)}(\mathbf{Z})$. Lorsque $n = 1$ ou $m = 1$, on a fini. Sinon on applique l'algorithme à la matrice M' : il fournit $P' \in \mathsf{GL}_{n-1}(\mathbf{Z})$ et $Q' \in \mathsf{GL}_{m-1}(\mathbf{Z})$ telles que $P'M'Q'^{-1}$ soit diagonale : si $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & P' \end{smallmatrix}\right) P_1 \in \mathsf{GL}_n(\mathbf{Z})$ et $Q = \left(\begin{smallmatrix} 1 & 0 \\ 0 & Q' \end{smallmatrix}\right) Q_1 \in \mathsf{GL}_m(\mathbf{Z})$, la matrice PMQ^{-1} est diagonale.

(6) Comme $a\beta = b\alpha$ et $\alpha^2 bu + \beta^2 av = \frac{a^2}{d^2} bu + \frac{b^2}{d^2} av = ab\frac{au+bv}{d^2} = \frac{ab}{d} = m$, on a

$$\left(\begin{smallmatrix} u & v \\ -\beta & \alpha \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -\beta v \\ 1 & \alpha u \end{smallmatrix}\right) = \left(\begin{smallmatrix} d & 0 \\ 0 & m \end{smallmatrix}\right).$$

Observons au passage que $\left(\begin{smallmatrix} u & v \\ -\beta & \alpha \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -\beta v \\ 1 & \alpha u \end{smallmatrix}\right) \in \mathsf{SL}_2(\mathbf{Z})$.

(7) • D'après la question (5), on peut construire explicitement $P \in \mathsf{GL}_n(\mathbf{Z})$ et $Q \in \mathsf{GL}_m(\mathbf{Z})$ telles que PMQ^{-1} soit diagonale : quitte à remplacer M par PMQ^{-1}, on peut supposer que M est diagonale, et même de la forme $M = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_r \end{pmatrix}$ avec $a_1, \dots, a_r$ non nuls. Procédons récursivement. Si $r \leq 1$, il n'y a rien à faire : supposons $r > 1$. Posons $d_1 = \mathsf{pgcd}(a_1, \dots, a_r)$: quitte à factoriser d_1 dans M, on se ramène au cas où $d_1 = 1$. D'après la question précédente, on peut calculer des matrices $U_r, V_r \in \mathsf{SL}_2(\mathbf{Z})$

telles que $U_r \left(\begin{smallmatrix} a_{r-1} & 0 \\ 0 & a_r \end{smallmatrix}\right) V_r^{-1} = \begin{pmatrix} \mathsf{pgcd}(a_{r-1},a_r) & 0 \\ 0 & \mathsf{ppcm}(a_{r-1},a_r) \end{pmatrix}$. Quitte à multiplier la matrice M par $P_r := \begin{pmatrix} \mathrm{I}_{r-2} & 0 & 0 \\ 0 & U_r & 0 \\ 0 & 0 & \mathrm{I}_{n-r} \end{pmatrix} \in \mathsf{SL}_n(\mathbf{Z})$ à gauche et par Q_r^{-1} où $Q_r = \begin{pmatrix} \mathrm{I}_{r-2} & 0 & 0 \\ 0 & V_r & 0 \\ 0 & 0 & \mathrm{I}_{n-r} \end{pmatrix} \in \mathsf{SL}_m(\mathbf{Z})$ à droite, on se ramène au cas où $a_{r-1} \mid a_r$. On a alors $d_1 = \mathsf{pgcd}(a_1, \dots, a_{r-1})$. En itérant, on construit des suites $(P_k)_{2\leq k\leq r}$ déléments de $\mathsf{SL}_n(\mathbf{Z})$ et $(Q_k)_{2\leq k\leq r}$ d'éléments de $\mathsf{SL}_m(\mathbf{Z})$ telles que le coefficient d'indice $(1,1)$ du produit $(P_2 \cdots P_r)M(Q_2 \cdots Q_r)^{-1}$ soit 1. Cela montre qu'on peut se ramener en un nombre fini d'étapes à une matrice M de la forme $d_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & M' \end{smallmatrix}\right)$ avec $M' \in \mathsf{M}_{(n-1)\times(m-1)}(\mathbf{Z})$ diagonale. On peut appliquer l'algorithme à cette dernière : il existe $P' \in \mathsf{GL}_{n-1}(\mathbf{Z})$ et $Q' \in \mathsf{GL}_{m-1}(\mathbf{Z})$ telles que $P'M'Q'^{-1}$ soit de la forme $\begin{pmatrix} b_2 & & \\ & \ddots & \\ & & b_r \end{pmatrix}$ avec $b_k \mid b_{k+1}$ pour tout $k \in \{2, \dots, r-1\}$: si $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & P' \end{smallmatrix}\right) \in \mathsf{GL}_n(\mathbf{Z})$ et $PQ = \left(\begin{smallmatrix} 1 & 0 \\ 0 & Q' \end{smallmatrix}\right) \in \mathsf{GL}_m(\mathbf{Z})$, on a $PMQ^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ avec $d_k = d_1 a_k$ pour tout $k \in \{2, \dots, r\}$: on a $d_1, \dots, d_r \in \mathbf{N}_{>0}$ et $d_k \mid d_{k+1}$ pour tout $k \in \{1, \dots, r-1\}$.

• Appliquons l'algorithme à $M = \begin{pmatrix} 4 & 6 & 11 & 22 \\ 8 & 12 & 10 & 31 \\ 18 & 27 & 27 & 74 \end{pmatrix}$. Si $P_1 = \begin{pmatrix} 0 & -2 & 1 \\ -1 & -4 & 2 \\ 0 & -9 & 4 \end{pmatrix} \in \mathsf{GL}_3(\mathbf{Z})$, on a vu que $P_1 M = \begin{pmatrix} 2 & 3 & 7 & 12 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 18 & 17 \end{pmatrix}$. Ensuite, $Q_1 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 3 & -2 & 0 & 0 \\ 7 & -71 & 0 & \\ 12 & -12 & 0 & 1 \end{pmatrix} \in \mathsf{GL}_4(\mathbf{Z})$ vérifie $Q_1 \begin{pmatrix} 2 \\ 3 \\ 7 \\ 12 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$: on a $P_1 M^{\mathrm{t}} Q_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 18 & 17 \end{pmatrix}$. Si $Q_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \end{pmatrix} \in \mathsf{GL}_4(\mathbf{Z})$, on donc $P_1 M^{\mathrm{t}} Q_1 Q_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & 17 & 0 \end{pmatrix}$. Si $P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \in \mathsf{GL}_3(\mathbf{Z})$, on a alors $P_2 P_1 M^{\mathrm{t}} Q_1 Q_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 15 & 0 \end{pmatrix}$: finalement, en posant $Q_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathsf{GL}_4(\mathbf{Z})$, on a $P_2 P_1 M^{\mathrm{t}} Q_1 Q_2 Q_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 15 & 0 \end{pmatrix}$. Cela montre que la forme normale de Smith de M est $PMQ^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 15 & 0 \end{pmatrix}$ avec $P = P_2 P_1 = \begin{pmatrix} 0 & -2 & 1 \\ -1 & -4 & 2 \\ 1 & -5 & 2 \end{pmatrix} \in \mathsf{GL}_3(\mathbf{Z})$ et $Q = Q_3^{-1} Q_2^{-1\mathrm{t}} Q_1^{-1} = \begin{pmatrix} 2 & 3 & 7 & 12 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \in \mathsf{GL}_4(\mathbf{Z})$.

(8) Une matrice $M = (a_{i,j})_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} \in \mathsf{M}_{n\times m}(K[X])$ est échelonnée réduite lorsqu'elle est échelonnée, et si en outre :

- $a_{i,p_M(i)}$ est unitaire pour tout $i \in \{1, \dots, r\}$;
- $k \in \{1, \dots, i-1\}) \Rightarrow \deg(a_{k,p_M(i)}) < \deg(a_{i,p_M(i)})$.

(où r est le nombre de lignes non nulles de M, *i.e.* $r = \mathsf{rg}(M)$).