Forme normale de Smith

↳ **Refs** : 131 dev p 201-206, OA p 287 (algo), Grand Combat p 579 et 1034 (exemples) et PGCD (+ Gr Ab pour ex)

Soit A un anneau euclidien et S un stathme euclidien de A.

Lemme : Soit $M \in M_{m,n}(A)$ et $P \in Gl_n(A)$. Les mineurs de taille k de MP sont combinaisons linéaires des mineurs de taille k de M à coefficients dans A.

Théorème : (Forme normale de Smith) Soit $M \in M_{m,n}(A)$ $(m, n \in \mathbb{N}^*)$. Il existe une unique (à facteurs inversibles près) suite $f_1, \dots f_r$ dans $A \setminus \{0\}$ telle que $f_1 | \dots | f_r$ et telle que M est équivalente à $\begin{pmatrix} f_1 & & & (0) \\ & \ddots & & \\ & & f_r & \\ (0) & & & 0 \end{pmatrix}$.
Les $f_1, \dots f_r$ sont appelés invariants de M.

Preuve du lemme : Soit $M_{I,J}$ la matrice extraite de M de taille $k \times k$ correspondant aux indices $I = \{i_1, \dots, i_k\}$ pour les lignes et $J = \{j_1, \dots, j_k\}$ pour les colonnes.
Notons C_j les colonnes de M, et $C_{I,j}$ la j-ième colonne en ne gardant que les lignes d'indice dans I, alors $M = (C_1 | \dots | C_n)$ et $M_{I,J} = (C_{I,j_1} | \dots | C_{I,j_k})$.
On note $P = (p_{i,j})_{i,j \in [\![1,n]\!]}$, alors $MP = \left(\sum_{l=1}^{n} p_{l,1} C_l \,|\, \dots \,|\, \sum_{l=1}^{n} p_{l,n} C_l \right)$
et donc la matrice extraite de MP de taille $k \times k$ correspondant aux indices I et J est : $(MP)_{I,J} = \left(\sum_{l=1}^{n} p_{l,j_1} C_{I,l} \,|\, \dots \,|\, \sum_{l=1}^{n} p_{l,j_k} C_{I,l} \right)$ ⚠ Faux dans le livre

Donc par multilinéarité du déterminant :
$$\det((MP)_{I,J}) = \sum_{l_1=1}^{n} p_{l_1,j_1} \sum_{l_2=1}^{n} p_{l_2,j_2} \dots \sum_{l_k=1}^{n} p_{l_k,j_k} \underbrace{\det(C_{I,l_1} | \dots | C_{I,l_k})}_{=0 \text{ si } \exists i,j \text{ tq } l_i = l_j}$$
et donc par caractère alterné du déterminant
$$\det((MP)_{I,J}) = \sum_{1 \le l_1 \ne \dots \ne l_k \le n} p_{l_1,j_1} p_{l_2,j_2} \dots p_{l_k,j_k} \underbrace{\det(C_{I,l_1} | \dots | C_{I,l_k})}_{\text{mineur de taille } k \times k}$$

On a bien obtenu une combinaison linéaire de mineurs de taille k de M à coefficients dans A.

Preuve du théorème : Etape 1 : On suppose $m, n \ge 2$. Montrons qu'il existe $f_1 \in A$ tel que M soit équivalente à la matrice $\left(\begin{array}{c|c} f_1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & V \\ 0 & \end{array}\right)$ où pour tout $(i,j) \in [\![1, m-1]\!] \times [\![1, n-1]\!]$, $f_1 | v_{i,j}$
Si $M = 0$ alors $f_1 = 0$ et $V = 0$ conviennent et c'est terminé.
Supposons maintenant M non nulle, on note X l'ensemble des matrices équivalentes à M (orbite par l'act° par congruence). On considère alors un $f_1 \in A \setminus \{0\}$ tel que $S(f_1) = \min(\{S(v_{i,j}) \mid V \in X, (i,j) \in [\![1,m]\!] \times [\![1,n]\!]\})$, qui existe car S est à valeurs dans $\mathbb{N}$. On regarde alors U une matrice équivalente à M qui contient le coefficient f_1. (Dans l'idée, f_1 c'est un pgcd des coef de M)

Quitte à permuter les lignes L_1 et L_i et les colonnes C_1 et C_j si f_1 est en position (i,j), on peut supposer que f_1 se situe en position $(1,1)$ ie

$U = \left(\begin{array}{c|ccc} f_1 & u_{1,2} & \cdots & u_{1,n} \\ \hline u_{2,1} & & & \\ \vdots & & * & \\ u_{m,1} & & & \end{array}\right)$. On écrit maintenant la division euclidienne des éléments de la première colonne par f_1 : $\forall i \in [\![2,m]\!], \exists (q_i, r_i) \in A^2, u_{i,1} = q_i f_1 + r_i$ et $\delta(r_i) < \delta(f_1)$.

On effectue alors les opérations $L_i \leftarrow L_i - q_i L_1$ pour $i \in [\![2,m]\!]$, et on obtient une nouvelle matrice équivalente à U (donc à M) de la forme $\left(\begin{array}{c|ccc} f_1 & u_{1,2} & \cdots & u_{1,n} \\ \hline r_2 & & & \\ \vdots & & * & \\ r_n & & & \end{array}\right)$

Par minimalité de f_1, puisque $\forall i$, $\delta(r_i) < \delta(f_1)$, on en déduit que $\forall i$, $r_i = 0$.

On recommence le processus en effectuant la division euclidienne des éléments de la première ligne par f_1 : $\forall j \in [\![2,n]\!], \exists (q_j', r_j') \in A^2$, $u_{1,j} = q_j' f_1 + r_j'$ et $\delta(r_j') < \delta(f_1)$. Donc en effectuant les opérations $C_j \leftarrow C_j - q_j' C_1$ pour $j \in [\![2,n]\!]$ on obtient une nouvelle matrice équivalente à M de la forme $\left(\begin{array}{c|ccc} f_1 & r_2' & \cdots & r_n' \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$.

De nouveau par minimalité de f_1, puisque $\forall j$, $\delta(r_j') < \delta(f_1)$, on en déduit que $\forall j$, $r_j' = 0$.

Ainsi, M est équivalente à une matrice de la forme $\left(\begin{array}{c|ccc} f_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & V & \\ 0 & & & \end{array}\right)$.

où $V \in M_{m-1,n-1}(A)$. Il reste à montrer que pour tout $(i,j) \in [\![m-1, n-1]\!]$, $f_1 \mid v_{i,j}$.

Soit $i \in [\![2,m]\!]$. L'opération $L_1 \leftarrow L_1 + L_i$ nous fournit la matrice équivalente suivante : $\left(\begin{array}{c|ccc} f_1 & v_{i,2} & \cdots & v_{i,n} \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$. Comme précédemment, on effectue la division euclidienne de la première ligne par f_1 :

$\forall j \in [\![2,n]\!], \exists (q_j'', r_j'') \in A^2$, $v_{i,j} = q_j'' f_1 + r_j''$ où $\delta(r_j'') < \delta(f_1)$.

Encore une fois, on effectue les opérations $C_j \leftarrow C_j - q_j'' C_1$ pour $j \in [\![2,n]\!]$, et on obtient une matrice équivalente à M de la forme $\left(\begin{array}{c|ccc} f_1 & r_2'' & \cdots & r_n'' \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$, et encore une fois par minimalité de f_1, $\forall j$, $r_j'' = 0$.

Cela signifie donc que $\forall j \in [\![2,n]\!]$, $v_{i,j} = q_j'' f_1$ ie $f_1 \mid v_{i,j}$.

Cela est vrai pour tout $i \in [\![2,m]\!]$, donc les coefficients de V sont bien divisibles par f_1.

Étape 2 : Montrons le théorème par récurrence forte sur $m+n \geq 2$.

- Initialisation : Si $m+n=2$, $M \in M_{1,1}(A)$ et le résultat est immédiat.
- Hérédité : Soit $m+n \geq 3$ et supposons le résultat vrai pour tout couple $(p,q) \in \mathbb{N}^*$ tel que $p+q \leq m+n-1$. Si $m=1$ ou $n=1$, alors il est possible de faire le même raisonnement qu'à l'étape précédente pour obtenir $\begin{pmatrix} f_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

On peut donc supposer $m, n \geq 2$. D'après l'étape précédente, M est équivalente à une matrice de la forme $\left(\begin{array}{c|c} f_1 & 0 - 0 \\ 0 & \\ \vdots & f_1 M' \\ 0 & \end{array}\right)$ où f_1 est un élément non nul de stathme minimal (non nul car on peut supposer $M \neq 0$ sinon le résultat est clair), et $M' \in M_{m-1,n-1}(A)$. Par hypothèse de récurrence, M' est équivalente à une matrice de la forme $\begin{pmatrix} f_2' & & & & (0) \\ & \ddots & & & \\ & & f_r' & & \\ & & & 0 & \\ (0) & & & & \ddots \; 0 \end{pmatrix}$ où $f_2' \mid \dots \mid f_r'$. Alors posons pour $j \in [\![2, r]\!]$, $f_j = f_1 f_j'$, de sorte que $f_1 \mid f_2 \mid \dots \mid f_r$, et ainsi M est équivalente à la matrice $\begin{pmatrix} f_1 & & & & (0) \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ (0) & & & & \ddots \; 0 \end{pmatrix}$ et c'est gagné !

Étape 3 : Montrons l'unicité (aux inversibles près).

Soit $k \in [\![1, \min(m,n)]\!]$. On note $I_k(M)$ l'idéal de A engendré par les mineurs de taille k de M. Nous allons montrer que $I_k(M)$ ne dépend que de la classe d'équivalence de M ie que $\forall (P,Q) \in GL_m(A) \times GL_n(A)$, $I_k(M) = I_k(PMQ^{-1})$.
Soit $(P,Q) \in GL_m(A) \times GL_n(A)$. D'après le lemme, les mineurs de taille k de MQ^{-1} sont des combinaisons linéaires à coefficients dans A des mineurs de taille k de M, ainsi $I_k(MQ^{-1}) \subseteq I_k(M)$. Or cette propriété reste vraie en considérant la multiplication à gauche : les mineurs de taille k de PM' sont des combinaisons linéaires à coefficients dans A des mineurs de taille k de M' (on fait la même chose en considérant les lignes : $(PM')_{I,J} = \begin{pmatrix} \sum_{\ell=1} p_{i_1,\ell} L_{\ell,J} \\ \vdots \\ \sum_{\ell=1} p_{i_k,\ell} L_{\ell,J} \end{pmatrix}$ et ensuite on refait pareil en utilisant les propriétés du déterminant).

Donc pour toute matrice M', $I_k(PM') \subseteq I_k(M')$. Ainsi
$I_k(PMQ^{-1}) \subset I_k(MQ^{-1}) \subset I_k(M)$.

Or on a aussi $M = P^{-1}(PMQ^{-1})Q$ donc le même argument montre que $I_k(M) \subset I_k(PMQ^{-1})$, ce qui nous donne bien $I_k(M) = I_k(PMQ^{-1})$.
Ainsi, si l'on considère $S = \begin{pmatrix} f_1 & & & & (0) \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ (0) & & & & \ddots \; 0 \end{pmatrix}$ une forme normale de Smith de M, alors on a pour tout $k \in [\![1, \min(m,n)]\!]$, $I_k(M) = I_k(S) = \begin{cases} \langle f_1 \times \dots \times f_k \rangle & \text{si } k \in [\![1, r]\!] \\ \{0\} & \text{sinon} \end{cases}$
(un seul mineur non nul à chaque fois : le mineur principal)

En particulier, si $S = \begin{pmatrix} f_1 & & & & (0) \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ (0) & & & & \ddots \; 0 \end{pmatrix}$ et $S' = \begin{pmatrix} f_1' & & & & (0) \\ & \ddots & & & \\ & & f_{r'}' & & \\ & & & 0 & \\ (0) & & & & \ddots \; 0 \end{pmatrix}$ sont deux formes normales de Smith de M, on voit déjà que $r = r'$ car les 2 matrices ont le même rang puisqu'elles sont équivalentes (pour être sûre que le rang est bien déf je les vois comme des matrices à coefficients dans le corps des fractions de A). Ensuite, on déduit de ce qu'il précède que pour tout $k \in [\![1, r]\!]$, $\langle f_1 \times \dots \times f_k \rangle = \langle f_1' \times \dots \times f_k' \rangle$.
Donc pour tout $k \in [\![1, r]\!]$, $f_1 \times \dots \times f_k$ et $f_1' \times \dots \times f_k'$ sont associés ie

il existe $u_1, \dots u_r \in A^\times$ tels que $f_1' = u_1 f_1$, $f_1 f_2' = u_2 f_1 f_2, \dots, f_1 \dots f_r' = u_r f_1 \dots f_r$
et ainsi de proche en proche, on obtient $\forall j \in [\![1, r]\!], \exists u_j' \in A^\times, f_j' = u_j' f_j$
D'où l'unicité à inversibles près.

<u>Remarques</u> : * Le lemme n'est qu'une version "faible" de la formule plus précise de Cauchy Binet : $\det((MN)_{I,J}) = \sum_{L = \{l_1 < \dots < l_k\} \subset [\![1,n]\!]} \det(M_{I,L}) \det(N_{L,J})$.

* Pour bien définir $GL_n(A)$* : on définit le déterminant d'une matrice en la voyant comme une matrice à coeff dans $\mathbb{K} = \mathrm{Frac}(A)$, et ensuite on a l'équivalence M inversible dans $M_n(A) \iff M \in GL_n(\mathbb{K})$ et $M^{-1} \in M_n(A) \iff \det(M) \in A^\times$, et alors les matrices vérifiant ces conditions sont les matrices de $GL_n(A)$.
*(et det de façon général).

* Le théorème reste vrai sur un anneau principal, mais c'est plus dur à montrer, il faut alors faire intervenir des "matrices de Bezout".

* Dans le cas d'un corps, on retrouve le résultat qui nous dit que toute matrice $M \in M_{n,m}(\mathbb{K})$ est équivalente à la matrice $\begin{pmatrix} \underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ (0) & & 1 \end{matrix}}_{\mathrm{rang}(M)} & (0) \\ & \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} \end{pmatrix}$.

* Ce théorème permet d'obtenir* le théorème de structure des modules de type fini sur un idéal principal (qui contient le théorème de structure des groupes abéliens de type fini) : "Soit V un module de type fini sur un anneau principal. Il existe $t \geq 0$ et des éléments $f_1, \dots f_r \in A$ tels que $f_1 | \dots | f_r$ et tels que $V \simeq A/\langle f_1 \rangle \oplus \dots \oplus A/\langle f_r \rangle \oplus A^t$". Mais on ne va pas s'attarder sur ces sorcelleries. *(en passant par le thm de la base adaptée)

* Trêve de bavardage, comment on fait en vrai ? Là le début de la preuve est bien sympa, mais ce n'est pas constructif ! En pratique, on fait l'algo suivant : ▶ Etape 0 : si la matrice est nulle, c'est fini

▶ Etape 1 : mettre en haut à gauche un élément de stathme minimal f_1.

▶ Etape 2 : pour tout $i \in [\![2, m]\!]$, on fait la DE de $u_{i,1}$ par f_1 : $u_{i,1} = q_i b_1 + r_i$ et $L_i \leftarrow L_i - q L_1$, alors $u_{i,1} \leftarrow r_i$, si $r_i \neq 0$, on échange L_1 et L_i et on revient au début de l'étape, si $r_i = 0$, passer à $i+1$, si $r_i = 0$ et $i = m$, fin de l'étape

▶ Etape 3 : on fait la même chose pour la première ligne

▶ Etape 4 : s'il existe $(i,j) \in [\![2,m]\!] \times [\![2,n]\!]$ tq $u_{1,1} \nmid u_{i,j}$, on fait $C_1 \leftarrow C_1 + C_j$ et on retourne en 3 (pfiouuu), sinon on repart du début avec la matrice $(u_{i,j})_{(i,j) \in [\![2,m]\!] \times [\![2,n]\!]}$.

* L'algo représente la même idée que celle de la preuve, la seule différence, c'est qu'ici on travaille sur M, donc il risque d'y avoir des retours en arrière, mais la justification de la terminaison de l'algo, c'est exactement le même argument : $S(m_{1,1})$ décroît au fil des étapes et S est à valeurs dans $\mathbb{N}$.

* C'est parti sur un exemple : $M = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix}$ (C'est Euclide !)

$L_1 \leftrightarrow L_2$ $\begin{pmatrix} 6 & 7 \\ 10 & 14 \end{pmatrix}$

$10 = 6\times 1 + 4$, $L_2 \leftarrow L_2 - L_1$ $\begin{pmatrix} 6 & 7 \\ 4 & 7 \end{pmatrix}$

$L_2 \leftrightarrow L_1$ $\begin{pmatrix} 4 & 7 \\ 6 & 7 \end{pmatrix}$

$6 = 4\times 1 + 2$, $L_2 \leftarrow L_2 - L_1$ $\begin{pmatrix} 4 & 7 \\ 2 & 0 \end{pmatrix}$

$L_2 \leftrightarrow L_1$ $\begin{pmatrix} 2 & 0 \\ 4 & 7 \end{pmatrix}$

$4 = 2\times 2 + 0$, $L_2 \leftarrow L_2 - 2L_1$ $\begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}$

$2 \nmid 7$! $C_1 \leftarrow C_1 + C_2$ $\begin{pmatrix} 2 & 0 \\ 7 & 7 \end{pmatrix}$

$7 = 2\times 3 + 1$, $L_2 \leftarrow L_2 - 3L_1$ $\begin{pmatrix} 2 & 0 \\ 1 & 7 \end{pmatrix}$

$L_2 \leftrightarrow L_1$ $\begin{pmatrix} 1 & 7 \\ 2 & 0 \end{pmatrix}$

$2 = 2\times 1 + 0$, $L_2 \leftarrow L_2 - 2L_1$ $\begin{pmatrix} 1 & 7 \\ 0 & -14 \end{pmatrix}$

$7 = 7\times 1 + 0$, $C_2 \leftarrow C_2 - 7\times C_1$ $\begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix}$

$C_2 \leftarrow -C_2$ $\begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$

* Si A est une matrice de $M_n(\mathbb{K})$, alors ses polynômes invariants (Frobenius) sont les invariants non constants de $XI_n - A \in M_n(\mathbb{K}[X])$. Voici un exemple avec $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & -1 & -1 \end{pmatrix}$, alors $XI_n - M = \begin{pmatrix} X-1 & 0 & 0 \\ 0 & X-1 & 0 \\ 4 & 1 & X+1 \end{pmatrix}$

$L_1 \leftrightarrow L_3$ $\begin{pmatrix} 4 & 1 & X+1 \\ 0 & X-1 & 0 \\ X-1 & 0 & 0 \end{pmatrix}$

$C_2 \leftrightarrow C_2$ $\begin{pmatrix} 1 & 4 & X+1 \\ X-1 & 0 & 0 \\ 0 & X-1 & 0 \end{pmatrix}$

$X-1 = 1\times(X-1)+0$, $L_2 \leftarrow L_2 - (X-1)L_1$ $\begin{pmatrix} 1 & 4 & X+1 \\ 0 & -4(X-1) & -(X+1)(X-1) \\ 0 & X-1 & 0 \end{pmatrix}$

$4 = 4\times 1 + 0$, $X+1 = (X+1)\times 1 + 0$, $C_2 \leftarrow C_2 - 4C_1$, $C_3 \leftarrow C_3 - (X+1)C_1$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4(X-1) & -(X+1)(X-1) \\ 0 & X-1 & 0 \end{pmatrix}$

$L_2 \leftrightarrow L_3$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & -4(X-1) & -(X+1)(X-1) \end{pmatrix}$

$-4(X-1) = -4\times(X-1)+0$, $L_3 \leftarrow L_3 + 4L_2$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & -(X+1)(X-1) \end{pmatrix}$

$L_3 \leftarrow -L_3$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X^2-1 \end{pmatrix}$ $\to$ les invariants de M sont $X-1$ et X^2-1.

* Une autre utilité de cette forme de Smith, c'est de résoudre des systèmes à coeff dans A donc, par exemple, dans $\mathbb{Z}$: Si on veut résoudre $AX = B$, on écrit $PAQ = S$ et on se ramène à résoudre $SY = C$ où $C = PB$ et $Y = Q^{-1}X$ et $SY = C$ équivaut à $\begin{cases} f_1 y_1 = c_1 \\ \vdots \\ f_r y_r = c_r \\ c_{r+1} = \cdots = c_n = 0 \end{cases}$, ainsi on a une solution ssi $\forall i \in [\![1, r]\!]$ $f_i \mid c_i$ et $\forall i \in [\![r+1, m]\!]$, $c_i = 0$.

Et si cela est vérifié, $Y = \begin{pmatrix} c_1/f_1 \\ \vdots \\ c_r/f_r \\ y_{r+1} \\ \vdots \\ y_n \end{pmatrix}$ où les $y_{r+1}, \dots, y_n$ sont quelconques.

Exemple : on veut résoudre : $\begin{cases} 2x_1 + x_2 - 3x_3 - x_4 = 8 \\ x_1 - x_2 - 3x_3 + x_4 = 1 \\ 4x_1 - 4x_2 + 16x_4 = 16 \end{cases}$, $A = \begin{pmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{pmatrix}$, $B = \begin{pmatrix} 8 \\ 1 \\ 16 \end{pmatrix}$

On obtient $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$ et $P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 1 & 2 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (pour obtenir P et Q, on fait les opérat° faites sur les lignes de A sur I_3 et les opérations faites sur les colonnes de A sur I_4).

Alors $C = \begin{pmatrix} 1 \\ 6 \\ 12 \end{pmatrix}$ et $SY = C \iff \begin{cases} y_1 = 1 \\ 3y_2 = 6 \\ 12y_3 = 12 \end{cases} \iff Y = \begin{pmatrix} 1 \\ 2 \\ 1 \\ a \end{pmatrix}$ pour $a \in \mathbb{Z}$

Et donc $AX = B \iff X = QY = \begin{pmatrix} 5-2a \\ 1+2a \\ 1-2a \\ a \end{pmatrix}$ pour $a \in \mathbb{Z}$.

* Pour les leçons 122 et 162, faire toute la démo du théorème mais pas le lemme, pour la leçon 149, faire le lemme, l'unicité, (en insistant sur les points liés au dét, par exc $I_k(S) = \dots$), puis faire l'existence avec le temps restant, surtout l'étape 1, et étape 2 résumée en "par récurrence". Pour la leçon 142, rajouter (cf Grand Combat) au thm la propriété : "pour tout $j \in [\![0, r]\!]$, on a $f_j = \frac{\mu_j(M)}{\mu_{j-1}(M)}$ où $\mu_k(M)$ désigne un pgcd des mineurs de taille k de M."

et ensuite faire rapidement l'existence (comme pour la 149, juste l'étape 1 en speed, mais en insistant sur l'idée que f_1 est un pgcd), faire l'unicité mais à partir de *, on remplace par :

On en déduit que pour tout $k \in [\![1, r]\!]$, $I_k(M)$ l'idéal engendré par les k mineurs de M, est engendré par l'élément $f_1 \dots f_k$. Ainsi $f_1 \dots f_k = \mu_k(M)$ est un pgcd des k mineurs (unique à inversible près).

Et de proche en proche, on obtient $f_j = \frac{\mu_j(M)}{\mu_{j-1}(M)}$, d'où l'unicité à inversible près.

(cette formule permet de calculer directement les f_j mais parfois l'algo est pratique pour avoir P et Q, typiquement pour les équations diophantiennes par exemple), puis faire l'algo sur un exemple en insistant sur le fait que c'est juste l'algo d'Euclide puisqu'on veut mettre le pgcd des coef en haut à gauche (ne pas faire le lemme).