Forme normal de Smith

ref: 131 dvpt, Combenchon, Algèbre le grand combat.
Objectif Agrégation.

Théorème: Soit A un anneau euclidien. Soit $M \in \mathcal{M}_{m\times n}(A)$ alors il existe existe une famille $(f_1,..,f_r) \in A\setminus\{0\}$ vérifiant $f_1 | ... | f_r$ et telle que M soit équivalente à la matrice D:

$$D = \begin{bmatrix} f_1 & & & \\ & \ddots & & \\ & & f_r & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}$$

i.e Il existe $(P,Q) \in GL_m(A) \times GL_n(A)$ telles que: $M = PDQ$.
De plus le nombre de $(f_1,..,f_r)$ est unique et les $f_1,..,f_r$ sont uniques à un inversible près.

Preuve: Existence: ref: 131 dvpt.

1) Si M est nulle, le résultat est ok.

Supposons M non nulle et on considère f_1 le coefficient non nul de stathme minimal parmi toutes les matrice U tel que $M \sim U$. $\exists \varphi$ existe car $\varphi: A\setminus\{0\} \longrightarrow \mathbb{N}$

Soit U une matrice qui a pour coefficient f_1, quitte à permuter deux colonnes et deux lignes on a:

$$M \sim \begin{pmatrix} f_1 & u_{12} & \cdots & u_{1n} \\ u_{21} & & & \\ \vdots & & M_1 & \\ u_{m1} & & & \end{pmatrix}$$

On écrit pour tout $i \in [\![2, m]\!]$, $u_{i1} = q_i f_1 + r_i$ avec $\delta(r_i) < \delta(f_1)$.
Puis on fait $L_i \leftarrow L_i - q_i L_1$ alors

$$M \sim \begin{pmatrix} f_1 & u_{12} & \cdots & u_{1m} \\ r_2 & & & \\ \vdots & & M_2 & \\ r_m & & & \end{pmatrix}$$

Or $\delta(r_i) < \delta(f_1)$ donc par minimalité de f_1 on a $r_i = 0$ i.e:

$$M \sim \begin{pmatrix} f_1 & u_{12} & \cdots & u_{1m} \\ 0 & & & \\ \vdots & & M_2 & \\ 0 & & & \end{pmatrix}$$

De la même manière on écrit $u_{1i} = q_i' f_1 + r_i'$ et en faisant $C_i \leftarrow C_i - q C_1$ on a :

$$M \sim \begin{pmatrix} f_1 & r_1' & \cdots & r_m' \\ 0 & & & \\ \vdots & & M_2 & \\ 0 & & & \end{pmatrix}$$

De plus $\delta(r_i') < \delta(f_1)$ donc $r_i' = 0$ ainsi

$$M \sim \begin{pmatrix} f_1 & \circ & \cdots & \circ \\ 0 & & & \\ \vdots & & M_2 & \\ 0 & & & \end{pmatrix}$$

Il reste à voir que f_1 divise tous les coeffs de M_2. On note $M_2 = (m_{ij})_{\substack{1 \le i \le m-1 \\ 1 \le j \le n-1}}$ alors si on fait $L_1 \leftarrow L_1 + L_i$ on a :

$$M \sim \begin{pmatrix} f_1 & m_{i1} & \cdots & m_{i\,n-1} \\ 0 & & & \\ \vdots & & M_3 & \\ 0 & & & \end{pmatrix}$$

On écrit $m_{ij} = q_{ij} f_1 + r_{ij}$ et avec $C_j \leftarrow C_j - q_j C_1$ on obtient.

$$M \sim \begin{pmatrix} f_1 & r_1'' & \cdots & r_{n-1}'' \\ 0 & & & \\ \vdots & & M_3 & \\ 0 & & & \end{pmatrix}$$

Or $\delta(r_j'') < \delta(f_1)$ donc $r_{ij} = 0$ i.e $f_1 \mid m_{ij}$ ainsi

$$M \sim \begin{pmatrix} f_1 & \circ & \cdots & \circ \\ 0 & & & \\ \vdots & & f_1 M_2' & \\ 0 & & & \end{pmatrix} \quad \text{où } M_2 \in \mathcal{M}_{m-1,n-1}(A).$$

Par conclure on fait une récurrence sur $m+n$.

Si $m+n=2$: Alors $M \in \mathcal{M}_{1,1}(A)$ alors le résultat est vrai.

Si $m+n>2$: Si $m=1$ ou $n=1$ le cas précédent donne le résultat

On peut donc supposer que $m, n \geq 2$ et par le cas précédent montre que :

$$M \sim \begin{pmatrix} f_1 & \circ & \cdots & \circ \\ 0 & & & \\ \vdots & & f_1 M' & \\ 0 & & & \end{pmatrix}$$

Par hypothèses de récurrence, il existe $P', Q' \in GL_n(A)$ et $f_2', \ldots, f_r'$ tq $f_2 \mid \ldots \mid f_r$ et :

$$M' = P' \operatorname{diag}(f_2', \ldots, f_r', 0, \ldots, 0) Q'$$

Ainsi avec $P = \begin{pmatrix} 1 & 0 \\ 0 & P' \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 0 \\ 0 & Q' \end{pmatrix}$ on a :

$$M \sim \begin{pmatrix} f_1 & & & & \\ & f_1 f_2 & & & \\ & & \ddots & & \\ & & & f_1 f_r & \\ & & & & 0 \\ & & & & & \ddots \end{pmatrix}$$

Ainsi avec $f_1 = g_1$, $f_i = g_1 f_i'$ on a : $f_1 | f_2 | \dots | f_r$ d'où le résultat.

si $i \geq 2$

$f_{i+1} | f_i$ car $f_{i+1}' | f_i'$

Unicité : Soit $k \leq \min(m,n)$, notons $I_k(M)$ l'idéal engendré par les mineurs de tailles k de M.

Montrons que pour $P, Q \in GL_n(A)$ alors $I_k(M) = I_k(PMQ)$.

Pour cela on remarque que par multilinéarité du det, si $P \in \mathcal{M}_n(A)$, les mineurs de taille k de PM sont des combinaisons linéaires de mineurs de taille k de M.

Ainsi $I_k(PM) \subseteq I_k(M)$ et on a de même pour la multiplication à gauche $I_k(MP) \subseteq I_k(M)$.

Donc pour $P, Q \in GL_n(A)$ on a :

$$I_k(M) = I_k(P^{-1}PMQQ^{-1}) \subseteq I_k(P^{-1}PMQ) \subseteq I_k(PMQ) \subseteq I_k(MQ) \subseteq I_k(M).$$

Ainsi $I_k(M) = I_k(PMQ)$.

En particulier ici si on note S la forme de Smith de M :

$$I_k(M) = I_k(S) = \begin{cases} \langle f_1 \dots f_k \rangle & \text{si } 1 \leq k \leq r \\ 0 & \text{sinon} \end{cases}$$

Ainsi si on a S' une autre forme de Smith, on a :

$$\forall k, \quad \langle f_1' \dots f_k' \rangle = I_k(M) = I_k(S) = \langle f_1 \dots f_k \rangle$$

donc $r = r'$ et par unicité du pgcd à un inversible près on a $u_1, \dots, u_r \in A^\times$ tel que :

$$f_1' = u_1 f_1$$

$$\vdots$$

$$f_1' \dots f_r' = u_r f_1 \dots f_r$$

Ainsi $f_1(u_1 f_2' - u_2 f_2) = 0$ donc par intégrité $f_2' = u_1^{-1} u_2 f_2$.

Donc $\forall j$, $f_j' = u_j f_j$ d'où le résultat. ∎

Rmq: On détaille le faite que les mineurs de taille k de MP sont des combinaisons linéaires de ceux de taille k de M.

On fixe k et on note $\{i_1, .., i_k\}$ les lignes et $\{j_1, .., j_k\}$ colonnes et on note $M_{I \times J}$ la matrice extraite de M.

De plus on note $M = (C_1 | \dots | C_m)$

donc $(M)_{I \times J} = (C_{I,j_1} | \dots | C_{I,j_s})$ où $C_{I,i} = C_i$ où on ne garde que les lignes de I.

Si on note $P = (p_{ij})_{i,j \in [\![1,n]\!]} \in \mathcal{M}_n(A)$ alors:

$$MP = \left(\sum_{i=1}^{n} p_{i1} C_i \,|\, \dots \,|\, \sum_{i=1}^{n} p_{im} C_i \right)$$

donc $$(MP)_{I \times J} = \left(\sum_{i=1}^{n} p_{i j_1} C_{I,i} \,|\, \dots \,|\, \sum_{i=1}^{n} p_{i j_k} C_{I,i} \right).$$

Ainsi $$\det((MP)_{I \times J}) = \sum_{i=1}^{n} p_{i j_1} \det\left(C_{I,i} \,|\, \dots \,|\, \sum_{i=1}^{n} p_{i j_k} C_{I,i} \right)$$

$$= \sum_{\ell_1, .., \ell_k = 1}^{n} p_{\ell_1 j_1} p_{\ell_2 i_2} \cdots p_{\ell_k i_k} \det\left(C_{I,\ell_1} | \dots | C_{I,\ell_k} \right).$$

mineur de taille k de M.

ref: Objectif Agreg

Corollaire: Soit $\mu_j(M) \in A$ tel que $\langle \mu_j(M) \rangle = I_j(M)$ en particulier $\mu_j(M)$ et le pgcd des mineurs de taille j de M alors on a:

$$a_j = \frac{\mu_j(M)}{\mu_{j-1}(M)} \text{ (à un inversible près). et } \mu_0(M) = 1$$

Preuve: On a vu dans l'unicité que

$$I_j(M) = \langle a_1 \cdots a_j \rangle$$

d'où $\mu_j(M) = u_1 a_1 \dots a_j$ et $\mu_{j-1}(M) = u_2 a_1 \dots a_{j-1}$, d'où le résultat.

Rmq: Supposons que A est seulement principal alors le théorème reste vrai mais pour cela on utilise des relations de Bezout entre coefficients.

II- Calcul des facteurs invariants d'une matrice:

Soit A un anneau euclidien, φ un stathme et $U \in \mathcal{M}_{m,n}(A)$.

Algorithme: On note $U = (u_{i,j})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ la matrice modifiée à chaque étape. La j-ème colonne C_j et la i-ème ligne L_i.

1 - Si $U = 0$, fin de l'algo

2 - Sinon, soit (i_0, j_0) tel que $\varphi(u_{i_0,j_0}) = \inf \{\varphi(u_{i,j}) \mid u_{i,j} \neq 0\}$. On permutte C_1 et C_{j_0} puis L_1 et L_{i_0} ainsi $u_{i_0 j_0}$ est en haut à gauche.

3 - On traite la première colonne, et on commence par $u_{2,1}$ ($i \leftarrow 2$).

3a - On effectue la division euclidienne de $u_{i,1}$ par $u_{1,1}$:

$$u_{i,1} = u_{11} q_i + r_i \quad \text{avec } r_i = 0 \text{ ou } \varphi(r_i) < \varphi(u_{11}).$$

On fait $L_i \leftarrow L_i - q_i L_1$ (i.e: $u_{i,1} = r_i$)

3b - Si $r_i \neq 0$, on fait $L_1 \leftrightarrow L_i$ et retourner en 3a.

3c - Si $r_i = 0$ et $i < m$, passer à la ligne suivante (ie $i \leftarrow i+1$) et aller en 3a.

3b - Si $r_i = 0$ et $i \geq m$ aller en 4.

4 - À ce stade on a: $U = \begin{pmatrix} u_{1,1} & * \\ 0 & \\ | & * \\ 0 & \end{pmatrix}$ on commence par $j \leftarrow 2$.

4a - On effectue la division euclidienne de $u_{1,j}$ par $u_{1,1}$:

$$u_{1j} = u_{11} q_j + s_j \quad \text{avec } s_j = 0 \text{ ou } \varphi(s_j) < \varphi(u_{11}).$$

On fait $C_j \leftarrow C_j - q C_1$.

4b - Si $s_j \neq 0$, alors $C_j \leftrightarrow C_1$ et retourner en 3.

4c - Si $s_j = 0$ et $j < n$, passer à la colonne suivante ($j \leftarrow j+1$) et aller en 4a

4d - Si $s_j = 0$ et $j = n$, aller au 5.

5. À ce stade on a: $U = \begin{pmatrix} u_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & * \\ 0 & \end{pmatrix}$

5a - S'il existe $i_1 \geq 2$ et $j_1 \geq 2$ tel que $u_{1,1}$ ne divise pas $u_{i_1 j_1}$ on fait: $C_1 \leftarrow C_1 + C_{j_1}$ et

aller en 3.

5b. On applique le même algo à la matrice extraite $(u_{i,j})_{\substack{1\le i\le m\\ 1\le j\le n}}$.

Rmq: C'est le même algo que pour calculer le rang de la matrice, mais ici on ne peut faire $L_1 \leftarrow L_1 - u_{i,i}^{-1} L_i$ donc on fait une division euclidienne.

Exemple:

Soit $C = \begin{pmatrix} X^3+X^2-4X+1 & X^3+2X^2-3X \\ 4X^3-X^2-6X+3 & 4X^3+3X^2-7X \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}[X])$.

Pour abaisser le degré on fait $C_2 \leftarrow C_2 - C_1$, on obtient alors:

$$C \sim \begin{pmatrix} X^3+X^2-4X+1 & X^2+X-2 \\ 4X^3-X^2-6X+3 & 4X^2-X-3 \end{pmatrix}$$

Or $u_{1,1}$ ne divise aucun élément

À continuer.