Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Matrices sur un anneau euclidien

1 Matrices sur un anneau euclidien

On considère un anneau *euclidien* A *ie* un anneau intègre muni d'une application :

$$\phi : A \setminus \{0\} \longrightarrow \mathbb{N}$$

telle que :

1. soient $a, b \in A \setminus \{0\}$; si $b|a$ on a $\phi(b) \leq \phi(a)$
2. pour $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\phi(r) < \phi(b)$.

Alors l'anneau A est principal.
La *formule de Cramer* $M.\widetilde{M} = \det(M)I$, dans laquelle $\widetilde{M}$ désigne la *transposée de la comatrice* de M, montre qu'une matrice $M \in \mathbf{M}_n(A)$ est *inversible* si et seulement si $\det(M)$ est inversible dans A. On notera $\mathbf{GL}_n(A)$ le groupe des matrices carrées d'ordre n *inversibles*.
Soit $\mathbf{M}_{m,n}(A)$ le A-module des matrices à coefficients dans A avec m lignes et n colonnes ; on considère l'action du groupe $\mathbf{GL}_m(A) \times \mathbf{GL}_n(A)$ agit sur $\mathbf{M}_{m,n}(A)$ définie par :

$$\begin{array}{rcl} (\mathbf{GL}_m(A) \times \mathbf{GL}_n(A)) \times \mathbf{M}_{m,n}(A) & \longrightarrow & \mathbf{M}_{m,n}(A) \\ ((U,V),M) & \longrightarrow & U\,M\,V^{-1} \end{array}$$

L'orbite d'une matrice $M \in \mathbf{M}_{m,n}(A)$ est :

$$\{M' \in \mathbf{M}_{m,n}(A) \,/\, \text{il existe } U \in \mathbf{GL}_m(A) \text{ et } V \in \mathbf{GL}_n(A) \text{ tels que } M' = U\,M\,V\}$$

Deux matrices $M, M' \in \mathbf{M}_{m,n}(A)$ sont *équivalentes* si et seulement si elles sont dans une même orbite.

1.1 Invariants déterminantiels

Considérons une matrice $M \in \mathbf{M}_{m,n}(A)$ à m lignes et n colonnes. Pour tout entier k avec $1 \leq k \leq \min(m,n)$, on désigne par $d_k(M)$ [1] le *pgcd* des mineurs d'ordre k de M. Notons $\mathrm{rg}(M)$ [2] le plus grand entier k pour lequel on a $d_k(M) \neq 0$ (*ie.* pour lequel il existe un mineur d'ordre k de M qui est non nul).

Proposition 1
On a $d_k(M) \neq 0$ *pour* $1 \leq k \leq \mathrm{rg}(M)$. *De plus* $d_{k-1}(M)$ *divise* $d_k(M)$ *pour* $2 \leq k \leq \mathrm{rg}(M)$.

1. $d_k(M)$ n'est défini qu'à un élément inversible de A près puisqu'il en est ainsi du *pgcd*. Lorsque $A = \mathbb{Z}$ on pourra supposer que $d_k(M) \in \mathbb{N}$ et lorsque $A = K[X]$ que $d_k(M)$ est nul ou unitaire. Ainsi *normalisés*, les éléments $d_k(A)$ sont uniques.

2. $\mathrm{rg}(M)$ n'est autre que le *rang* de la matrice M considérée comme matrice à coefficients dans $K = \mathrm{Frac}(A)$, le corps des fractions de A

$\triangledown$ Supposons que $d_k(M) \neq 0$ ce qui est vrai pour $k = \mathrm{rg}(M)$; la matrice M possède donc un mineur d'ordre k qui est non nul. Mais chaque mineur d'ordre k de M est combinaison linéaire à coefficients dans A de mineurs d'ordre $k-1$ de sorte que l'on a $d_{k-1}(M) \neq 0$.
De plus $d_{k-1}(M)$ divise chaque mineur d'ordre $k-1$ de M, donc divise chaque mineur d'ordre k, donc leur pgcd $d_k(M)$. $\triangle$

Pour $m, n \in \mathbb{N}$ et R anneau commutatif, soit $\mathbf{M}_{m,n}(R)$ le R-module des matrices à coefficients dans R à m lignes et n colonnes. Pour $m, n, q \in \mathbb{N}$ le produit des matrices définit une application bilinéaire :

$$\mathbf{M}_{m,n}(R) \times \mathbf{M}_{n,q}(R) \longrightarrow \mathbf{M}_{m,q}(R)$$

Considérons un produit de matrices $C = AB$ avec $A = (a_{i,k})_{1\leq i\leq m, 1\leq k\leq n}$, $B = (b_{k,j})_{1\leq k\leq n, 1\leq j\leq q}$ et $C = (c_{i,j})_{1\leq i\leq m, 1\leq j\leq q}$. Pour $1 \leq i_1 < \cdots < i_p \leq m$ et $1 \leq j_1 < \cdots < j_p \leq q$ où $p \leq \min(m, q)$ on désigne par $C\begin{vmatrix} i_1, \cdots, i_p \\ j_1, \cdots, j_p \end{vmatrix}$ le mineur correspondant.[3].

Lemme 1 (formule de Binet-Cauchy)
Soit $C = A.B$ avec $A \in \boldsymbol{M}_{m,n}(R)$, $B \in \boldsymbol{M}_{n,q}(R)$ et $C \in \boldsymbol{M}_{m,q}(R)$; on a :

$$C\begin{vmatrix} i_1, \cdots, i_p \\ j_1, \cdots, j_p \end{vmatrix} = \sum_{1\leq k_1<\cdots<k_p\leq n} A\begin{vmatrix} i_1, \cdots, i_p \\ k_1, \cdots, k_p \end{vmatrix} B\begin{vmatrix} k_1, \cdots, k_p \\ j_1, \cdots, j_p \end{vmatrix}$$

$\triangledown$ Remarquons que l'on a

$$\begin{pmatrix} c_{i_1,j_1} & \cdots & c_{i_1,j_p} \\ \vdots & & \vdots \\ c_{i_p,j_1} & \cdots & c_{i_p,j_p} \end{pmatrix} = \begin{pmatrix} a_{i_1,1} & \cdots & a_{i_1,n} \\ \vdots & & \vdots \\ a_{i_p,1} & \cdots & a_{i_p,n} \end{pmatrix} \begin{pmatrix} b_{1,j_1} & \cdots & b_{1,j_p} \\ \vdots & & \vdots \\ b_{n,j_1} & \cdots & b_{n,j_p} \end{pmatrix}$$

de sorte que l'on ait ramené à calculer le déterminant d'une matrice carrée C d'ordre p produit de deux matrices rectangulaires A et B :

$$C = \begin{pmatrix} c_{1,1} & \cdots & c_{1,p} \\ \vdots & & \vdots \\ c_{p,1} & \cdots & c_{p,p} \end{pmatrix} = \underbrace{\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{p,1} & \cdots & a_{p,n} \end{pmatrix}}_{=A} \underbrace{\begin{pmatrix} b_{1,1} & \cdots & b_{1,p} \\ \vdots & & \vdots \\ b_{n,1} & \cdots & b_{n,p} \end{pmatrix}}_{=B}$$

On a alors :

$$\begin{aligned} \det(C) &= |c_{i,j}|_{1\leq i,j\leq p} \\ &= |\sum_{k=1}^{n} a_{i,k} b_{k,j}|_{1\leq i,j\leq p} \\ &= \sum_{k_1,\cdots,k_p=1}^{n} b_{k_j,j} |a_{i,k_j}|_{1\leq i,j\leq p} \\ &= \sum_{k_1,\cdots,k_p=1}^{n} b_{k_1,1}\cdots b_{k_p,p} A\begin{vmatrix} 1, \cdots, p \\ k_1, \cdots, k_p \end{vmatrix} \end{aligned}$$

Si $p > n$ on a $\det(C) = 0$.
Dans le cas $p \leq n$, seuls restent dans la somme les termes pour lesquels on a :

$$1 \leq k_1 < \cdots < k_p \leq n$$

3. *ie.* le déterminant de la sous-matrice de C formée des ligne d'indices $i_1, \cdots, i_p$ et des colonnes $j_1, \cdots, j_p$.

On regroupe ces termes par *paquets* de $p!$ termes chacun qui ne diffèrent que par l'ordre des indices. La somme des termes d'un même paquet est alors égale à

$$\sum \epsilon(k_1,\cdots,k_p) A\begin{vmatrix}1,\cdots,p\\k_1,\cdots,k_p\end{vmatrix} b_{k_1,1}\cdots b_{k_p,p} = A\begin{vmatrix}1,\cdots,p\\k_1,\cdots,k_p\end{vmatrix} B\begin{vmatrix}k_1,\cdots,k_p\\1,\cdots,p\end{vmatrix}$$

où $\epsilon(k_1,\cdots,k_p)$ est la signature de la permutation $\begin{pmatrix}1 & 2 & \cdots & p\\ k_1 & k_2 & \cdots & k_p\end{pmatrix}$ et finalement on a :

$$\det(C) = \sum_{1\le k_1<\cdots<k_p\le n} A\begin{vmatrix}1,\cdots,p\\k_1,\cdots,k_p\end{vmatrix} B\begin{vmatrix}k_1,\cdots,k_p\\1,\cdots,p\end{vmatrix}$$

$\triangle$
Remarque : On peut exprimer la formule de Binet-Cauchy de manière plus synthétique.
Pour $1 \le p \le n$, on désignera par $\Lambda(p,n)$ l'ensemble des suites $\underline{i} = (i_1,\cdots,i_p)$ d'entiers telles que :

$$1 \le i_1 < \cdots < i_p \le n$$

Pour toute matrice $A \in \mathbf{M}_{m,n}(R)$ et tout entier $p \le \min(m,n)$, on considère la matrice des p-mineurs de A :

$$\Lambda^p(A) = (A\begin{vmatrix}\underline{i}\\\underline{j}\end{vmatrix})_{\underline{i}\in\Lambda(p,m),\underline{j}\in\Lambda(p,n)} \in \mathbf{M}_{C_m^p,C_n^p}(K)$$

La formule de Binet-Cauchy s'écrit alors :

$$\Lambda^p(C) = \Lambda^p(A)\ \Lambda^p(B)$$

Proposition 2
Soient $M, M' \in \boldsymbol{M}_{m,n}(A)$ des matrices équivalentes ; alors $d_k(M)$ et $d_k(M')$ sont associés[4] *pour $k \ge 1$. En particulier on a* $\mathrm{rg}(M) = \mathrm{rg}(M')$.

$\triangledown$ Considérons d'abord le cas où $M' = M\,V$ avec $V \in \mathbf{GL}_n(A)$. Pour *tout* mineur Δ' d'ordre k de M' la formule de *Binet-Cauchy* montrer que $\Delta' = \sum_i \Delta_i \Xi_i$ où Δ_i (*resp.* Ξ_i) est un mineur d'ordre k de M (*resp.* de V). Alors si $d_k(M) = 0$ on a $\Delta_i = 0$ pour tout i de sorte que $\Delta' = 0$ et par suite $d_k(M') = 0$. Si $d_k(M) \neq 0$, on a $d_k(M)|\Delta_i$ pour tout i de sorte que $d_k(M)||\Delta' = 0$ et par suite $d_k(M)|d_k(M')$.
Comme on a $M = M'\,V^{-1}$, on a aussi $d_k(M) = 0$ si $d_k(M') = 0$ et $d_k(M')Id_k(M)$ si $d_k(M') \neq 0$. Ainsi on a $d_k(M) \neq 0$ si et seulement $d_k(M') \neq 0$, $d_k(M)$ et $d_k(M')$ sont associés et $\mathrm{rg}(M) = \mathrm{rg}(M')$.
On en déduit par *transposition* la propriété lorsque $M' = U\,M$ avec $U \in \mathbf{GL}_m(A)$. $\triangle$

1.2 Forme réduite de Smith

Une matrice $S \in \mathbf{M}_{m,n}(A)$ est *de (la forme réduite de) Smith* si l'on a[5] :

$$\begin{array}{rcl} S_{i,j} & = & 0 \text{ pour } i \neq j \\ S_{i,i} & \neq & 0 \text{ pour } 1 \le i \le r \\ S_{i,i} & | & S_{i+1,i+1} \text{ pour } 1 \le i \le r-1 \\ S_{i,i} & = & 0 \text{ pour } r < i \le \min(m,n) \end{array}$$

4. *ie.* on a $d_k(M') = u\,d_k(M)$ avec u inversible dans A. Si les *pgcd* sont *normalisés* on a $d_k(M') = d_k(M)$.
5. Lorsque $A = \mathbb{Z}$ on *normalise* S par la condition $S_{i,i} \ge 0$ et si ou $A = K[X]$ par la condition $S_{i,i}$ est nul ou unitaire

Lemme 2
Soit $S \in \boldsymbol{M}_{m,n}(A)$ une matrice de la forme réduite de Smith ; pour tout $k \geq 1$ on a

$$d_k(S) = S_{1,1} \cdots S_{k,k}$$

En particulier on a $\mathrm{rg}(S) = r$ où $0 \leq r \leq \min(m,n)$ est le plus grand indice tel que $S_{r,r} \neq 0$.

$\triangledown$ Soit $\Delta = S\begin{vmatrix} i_1, \cdots, i_k \\ j_1, \cdots, j_k \end{vmatrix}$ un mineur d'ordre k de S ; si Δ n'est pas *centré sur la diagonale* (*ie.* si $(i_1, \cdots, i_k) \neq (j_1, \cdots, j_k)$), une ligne ou une colonne de Δ est nulle de sorte que $\Delta = 0$.
Supposons que $\Delta = S\begin{vmatrix} i_1, \cdots, i_k \\ i_1, \cdots, i_k \end{vmatrix}$. S'il existe l'un des indices $i_j > r$ on a encore $\Delta = 0$. C'est en particulier le cas lorsque $k > r$ de sorte que l'on a $d_k(S) = 0$. Supposons alors que $k \leq r$ et que $1 \leq i_1 < \cdots < i_k \leq r$; on a alors $S_{1,1} | S_{i_1,i_1}, \cdots, S_{k,k} | S_{i_k,i_k}$ de sorte que $S_{1,1} \cdots S_{k,k} | \Delta = S_{i_1,i_1} \cdots S_{i_k,i_k}$ et l'on a $d_k(S) = S_{1,1} \cdots S_{k,k} \neq 0$. $\triangle$

Théorème 1 (forme réduite de Smith)
Toute matrice $M \in \boldsymbol{M}_{m,n}(A)$ est équivalente à une matrice de la forme réduite de Smith S unique à la multiplication de ses coefficients par des éléments inversibles de A près[6].

$\triangledown$ Pour établir l'unicité il suffit de remarquer que si S est une matrice de la forme réduite de Smith équivalente à M, on a $\mathrm{rg}(M) = \mathrm{rg}(S) = r$ et $d_k(M) = d_k(S)$ pour $1 \leq k \leq r$ de sorte que $S_{1,1} = d_1(M)$ et $S_{k,k} = \dfrac{d_k(M)}{d_{k-1}(M)}$ pour $2 \leq k \leq r$.
L'existence est fournie par l'algorithme décrit ci-dessous. $\triangle$.
Soit $M \in \mathbf{M}_{m,n}(A)$; les coefficients *non nuls* $S_{1,1}, \cdots, S_{r,r}$ d'une forme réduite de Smith S de M sont appelés les *facteurs invariants*[7] de M.

Corollaire 1
Soient $M, M' \in \boldsymbol{M}_{m,n}(A)$ alors M et M' sont équivalentes si et seulement si leurs facteurs invariants $d_k(M)$ et $d_k(M')$ sont associés[8] *pour tout $k \geq 1$.*

$\triangledown$ Si $\mathrm{rg}(M) = \mathrm{rg}(M') = r$ et $d_k(M) = d_k(M')$ pour $1 \leq k \leq r$ (à un élément inversible de A près), M et M' sont équivalentes à une même matrice de Smith donc sont équivalentes. La réciproque a déjà été établie. $\triangle$

1.3 Réduction à la forme de Smith

1.3.1 Matrices élémentaires

Pour des indices $1 \leq i < j \leq n$ et des coefficients $a, b, c, d \in A$ on considère la matrice carrée d'ordre n :

$$X_{i,j}^{(n)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & & a & \cdots & b & \cdots & \ddots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & & c & \cdots & d & \cdots & \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

6. S est unique si l'on impose que ses coefficients sont *normalisés*.
7. Ils sont donc définis à la multiplication par des éléments inversibles de A près. Ils sont uniques dans le cas *normalisé*.
8. égaux dans le cas *normalisé*.

(a, b sont sur la ligne i ; c, d sur la ligne j ; a, c sur la colonne i et b, d sur la colonne j ; les coefficients de la diagonale autres que a, d sont égaux à 1).

Remarquons que la matrice $X_{i,j}^{(n)} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a pour déterminant $ad - bc$.

En particulier on a un homomorphisme *injectif* de groupes :

$$\begin{array}{ccc} \mathbf{SL}_2(A) & \longrightarrow & \mathbf{SL}_n(A) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longrightarrow & X_{i,j}^{(n)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{array}$$

Considérons une matrice $M \in \mathbf{M}_{m,n}(A)$. Pour $1 \leq i \leq m$, on désigne par $L_i(M)$ la ligne i de M et pour $1 \leq j \leq n$, on désigne par $C_j(M)$ la colonne j de M.
On a alors, pour $1 \leq i < r \leq m$ et $k \neq i, r$:

$$\left\{ \begin{array}{rcl} L_i(X_{i,r}^{(m)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} M) & = & aL_i(M) + bL_r(M) \\ L_r(X_{i,r}^{(m)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} M) & = & cL_i(M) + dL_r(M) \\ L_k(X_{i,r}^{(m)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} M) & = & L_k(M) \end{array} \right.$$

et pour $1 \leq j < s \leq n$ et $k \neq j, s$:

$$\left\{ \begin{array}{rcl} C_j(M\, X_{j,s}^{(n)} \begin{pmatrix} a & c \\ b & d \end{pmatrix}) & = & aC_j(M) + bC_s(M) \\ C_s(M\, X_{j,s}^{(n)} \begin{pmatrix} a & c \\ b & d \end{pmatrix}) & = & cC_j(M) + dC_s(M) \\ C_k(M\, X_{j,s}^{(n)} \begin{pmatrix} a & c \\ b & d \end{pmatrix}) & = & C_k(M) \end{array} \right.$$

1.3.2 Elimination de Gauss *sans dénominateurs*

Ainsi certaines combinaisons linéaires à coefficients dans A de lignes (de colonnes) de M s'expriment matriciellement par une multiplication à gauche (à droite) de M par une matrice élémentaire de déterminant égal à 1. Ceci va nous permettre d'annuler des coefficients de M sans changer de classe d'équivalence.

Lemme 3 (élimination d'une fin de ligne)
Soit $M \in \boldsymbol{M}_{m,n}(A)$ telle que $M_{i,j} \neq 0$, alors il existe une matrice $V \in \boldsymbol{GL}_n(A)$, produit de matrices élémentaires de déterminant égal à 1, telle que la matrice $M' = MV$ vérifie :

$$M'_{i,j} \mid M_{i,j} \quad (1)$$
$$M'_{i,s} = 0 \text{ pour tout } s > j \quad (2)$$

Lorsque $M_{i,j} | M_{i,s}$ pour tout $s \geq j$, on a $C_j(M') = C_j(M)$ (en particulier $M'_{i,j} = M_{i,j}$) sinon $M'_{i,j}$ est un diviseur strict de $M_{i,j}$.

$\triangledown$ Pour tout s, $j < s \leq n$, tel que $M_{i,s} \neq 0$ on pose $x = M_{i,j}$ et $y = M_{i,s}$. Si z est le pgcd de x et y, il existe $a, b \in A$ tels que $ax + by = z$ (formule de Bezout).

On prend $c = -y/z$ et $d = x/z$ et $V = X_{j,s}^{(n)} \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. On a $\det(V) = ad - bc = 1$.

De plus $C_j(M') = aC_j(M) + bC_s(M)$. En particulier $M'_{i,j} = ax + by = z | M_{i,j}$. On a encore $C_s(M') = cC_j(M) + dC_s(M)$ de sorte que $M'_{i,s} = cx + dy = 0$.
Si $x = M_{i,j} | y = M_{i,s}$ on a $z = x$ de sorte que $a = 1$ et $b = 0$ d'où $C_j(M') = C_j(M)$ sinon $M'_{i,j} = z$ est un diviseur strict de $M_{i,j} = x$. $\triangle$.

Lemme 4 (élimination d'une fin de colonne)
Soit $M \in \boldsymbol{M}_{m,n}(A)$ telle que $M_{i,j} \neq 0$, alors il existe une matrice $U \in \boldsymbol{GL}_m(A)$, produit de matrices élémentaires de déterminant égal à 1, telle que la matrice $M' = U\,M$ vérifie :

$$M'_{i,j} \quad | \quad M_{i,j} \tag{3}$$
$$M'_{r,j} \quad = \quad 0 \text{ pour tout } r > i \tag{4}$$

Lorsque $M_{i,j}|M_{r,j}$ pour tout $r \geq i$, on a $L_i(M') = L_i(M)$ (en particulier $M'_{i,j} = M_{i,j}$) sinon $M'_{i,j}$ est un diviseur strict de $M_{i,j}$.

$\triangledown$ Pour tout r, $i < r \leq m$, tel que $M_{r,j} \neq 0$ on pose $x = M_{i,j}$ et $y = M_{r,j}$. Si z est le pgcd de x et y, il existe $a, b \in A$ tels que $ax + by = z$ (formule de Bezout). On prend $c = -y/z$ et $d = x/z$ et on a $U = X_{i,r}^{(m)} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a $\det(U) = ad - bc = 1$.
De plus $L_i(M') = aL_i(M) + bL_r(M)$. En particulier $M'_{i,j} = ax + by = z|M_{i,j}$. On a encore $L_r(M') = cL_i(M) + dL_r(M)$ de sorte que $M'_{r,j} = cx + dy = 0$.
Si $x = M_{i,j}|y = M_{r,j}$ on a $z = x$ de sorte que $a = 1$ et $b = 0$ d'où $L_i(M') = L_i(M)$ sinon $M'_{i,j} = z$ est un diviseur strict de $M_{i,j} = x$. $\triangle$

Corollaire 2 (élimination d'une fin de ligne et de colonne)
Soient $M \in \boldsymbol{M}_{m,n}(A)$ telle que $M_{i,j} \neq 0$; alors il existe $U \in \boldsymbol{GL}_m(A)$ et $V \in \boldsymbol{GL}_n(A)$, produits de matrices élémentaires de déterminant égal à 1, telles que la matrice $M' = U\,M\,V$ vérifie :

$$M'_{i,j} \quad | \quad M_{i,j} \tag{5}$$
$$M'_{i,s} \quad = \quad 0 \textit{ pour } s > j \tag{6}$$
$$M'_{r,j} \quad = \quad 0 \textit{ pour } r > i \tag{7}$$

$\triangledown$ On *répète* la boucle d'opérations suivante :

1. On élimine la fin de la ligne i à partir de la position (i, j)
2. On élimine la fin de la colonne j à partir de la position (i, j)

jusqu'à ce que la fin de la ligne i et la fin de la colonne j soient simultanément nulles (l'une de ces opérations pouvant partiellement annuler l'autre).
Supposons qu'après une étape $M_{i,j}$ n'a pas changé ; cela signifie que $M_{i,j}$ divisait la fin de la ligne i et la fin de la colonne j ; mais alors on a pu annuler la fin de la ligne i *sans changer* la colonne j puis annuler la fin de la colonne j *sans changer* la ligne i et on sort donc de la boucle. Ainsi tant que l'on reste dans la boucle on remplace le coefficient $M_{i,j}$ par un diviseur *strict* et comme A est *noethérien* on sort de la boucle après un nombre fini d'étapes. $\triangle$

Cependant pour appliquer ce résultat on doit avoir $M_{i,j} \neq 0$; un *pivotage* permet de se ramener à ce cas.

Lemme 5 (pivot)
Soient $M \in \boldsymbol{M}_{m,n}(A)$ telle que $M_{i,j} = 0$; on suppose qu'il existe $r > i$ tel que $M_{r,j} \neq 0$ ou qu'il existe $s > j$ tel que $M_{i,s} \neq 0$ alors il existe une matrice élémentaire $U \in \boldsymbol{GL}_m(A)$ ou $V \in \boldsymbol{GL}_n(A)$ de déterminant 1, telle que $M' = U\,M$ ou $M' = M\,V$ vérifie $M'_{i,j} \neq 0$.

$\triangledown$ Il suffit de prendre l'une des matrices $U = X_{i,r}^{(m)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ou $V = X_{j,s}^{(n)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. $\triangle$

1.3.3 Calcul de la forme réduite de Smith.

En combinant les méthodes d'élimination linéaire et du pivot, on construit à partir d'une matrice $M \in \mathbf{M}_{m,n}(A)$ des matrices $U \in \mathbf{GL}_m(A)$ et $V \in \mathbf{GL}_n(A)$, produits de matrices élémentaires de déterminant égal à 1, telles que $M' = U\,M\,V$ soit *diagonale*. Pour obtenir une forme réduite de Smith, il faut de plus assurer la *condition de divisibilité* des coefficients successifs.

Lemme 6
Soit $M \in \boldsymbol{M}_{m,n}(A)$ une matrice diagonale pour laquelle existent des indices i, j tels que $x = M_{i,i} \neq 0$ ne divise pas $y = M_{j,j} \neq 0$; il existe des matrices $U \in \boldsymbol{GL}_m(A)$ et $V \in \boldsymbol{GL}_n(A)$, produits de matrices élémentaires de déterminant égal à 1, telles si $M' = U\,M\,V$ on a $M'_{i,i} = z$ et $M'_{j,j} = z'$ avec $z = \mathrm{pgcd}(x, y)$ et $z' = \mathrm{ppcm}(x, y)$.

$\triangledown$ On a la formule de Bezout $ax + by = z$ et l'on remarque que :

$$\begin{pmatrix} 1 & 0 \\ -\dfrac{by}{z} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} a & -\dfrac{y}{z} \\ b & \dfrac{x}{z} \end{pmatrix} = \begin{pmatrix} z & 0 \\ 0 & z' \end{pmatrix}$$

On prend alors [9]

$$U = X_{i,j}^{(m)} \begin{pmatrix} 1 & 0 \\ -\dfrac{by}{z} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } V = X_{i,j}^{(n)} \begin{pmatrix} a & -\dfrac{y}{z} \\ b & \dfrac{x}{z} \end{pmatrix}$$

$\triangle$

On en déduit l'existence d'une forme réduite de Smith d'une matrice M. on ramène d'abord M à la forme diagonale. Ensuite, en multipliant M à gauche ou à droite par une matrice de

9. plus en détail : on commence par ajouter à la ligne i de M la ligne j ; pour cela on multiplie M à gauche par la matrice $U = X_{i,j}^{(m)} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Appelons encore M la matrice ainsi obtenue. On annule la fin de la ligne i de M au delà de la position (i, i) : on pose donc $x = M_{i,i}$ et $y = M_{j,j}$. Si z est le pgcd de x et y, il existe $a, b \in A$ tels que $ax + by = z$ (formule de Bezout). On prend $c = -y/z$ et $d = x/z$ et on multiplie à droite par la matrice

$$X_{i,j}^{(n)} \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

pour obtenir une matrice M'.
On a alors $L_k(M') = L_k(M)$ pour $k \neq i, j$ et l'on a :

$$\begin{aligned} M'_{i,i} &= z \\ M'_{i,j} &= 0 \\ M'_{j,i} &= by \\ M'_{j,j} &= z' \end{aligned}$$

où z' est le ppcm de x et y.
Puisque $M'_{i,i} = z$ divise $M'_{j,i} = by$ on peut annuler la fin de la colonne i au delà de la position (i, i) *sans changer* la ligne i. Il suffit pour cela de multiplier M' à gauche par la matrice $X_{i,j}^{(m)} \begin{pmatrix} 1 & 0 \\ bc & 1 \end{pmatrix}$ On obtient alors la matrice diagonale M'' avec

$$\begin{aligned} M''_{k,k} &= M_{k,k} \text{ pour } k \neq i, j \\ M''_{i,i} &= z \\ M''_{j,j} &= z' \end{aligned}$$

la forme $U = X_{i,r}^{(m)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (ou $V = X_{j,s}^{(n)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) on peut de plus supposer que les termes diagonaux nuls sont regroupés à la fin de la diagonale de M. Soit $r = \mathrm{rg}(M)$. On applique alors le lemme précédent, pour tout i, $1 \leq i \leq r-1$, à tous les couples non nuls $M_{i,i}$, $M_{j,j}$ avec $i+1 \leq j \leq r$.

2 Modules sur un anneau euclidien

Soit A un anneau *euclidien* de corps des fractions $K = \mathrm{Frac}(A)$; un A-module E est un groupe abélien E, noté additivement, muni d'une loi de composition :

$$\begin{array}{rcl} A \times E & \longrightarrow & E \\ (a, x) & \longrightarrow & a.x \end{array}$$

vérifiant les propriétés :

1. $a.(x+y) = a.x + a.y$ pour $a \in A$ et $x, y \in E$
2. $1.x = x$ pour $x \in E$
3. $(a.(b.x) = (ab).x$ pour $a, b \in A$ et $x \in E$.

Un *sous-A-module* de E est un sous-groupe E' tel que pour tout $a \in A$ et tout $x \in E'$ on a $ax \in E'$; le groupe quotient E/E' est alors un A-module pour la loi de composition $(a, \overline{x}) \longrightarrow \overline{ax}$.
Les sous-A-modules de A sont les idéaux de A.
Etant donnés des A-modules E et F un *A-homomorphisme* est un homomorphisme de groupes $u : E \longrightarrow F$ tel que $u(a.x) = a.u(x)$ pour $a \in A$ et $x \in E$.
Un *A-isomorphisme* est un A-homomorphisme bijectif.
Si $u : E \longrightarrow F$ est un A-homomorphisme, le *noyau* $\mathrm{Ker}(u) = \{x \in E / u(x) = 0\}$ est un sous-A-module de E, l'*image* $\mathrm{Im}(u) = u(E)$ est un sous-A-module de F et f induit un A-isomorphisme $\overline{u} : E/\mathrm{Ker}(u) \longrightarrow \mathrm{Im}(u)$.
Une *suite exacte courte* est la donnée de deux A-homomorphismes $u : E \longrightarrow F$ et $u : F \longrightarrow G$:

$$0 \longrightarrow E \xrightarrow{u} F \xrightarrow{v} G \longrightarrow 0$$

tels que u est injectif, $\mathrm{Im}(u) = \mathrm{Ker}(v)$ et v est surjectif.

Exemples :
1) $A = \mathbb{Z}$: un $\mathbb{Z}$-module est un groupe abélien.
2) Un $K[X]$-module E est caractérisé par le K-espace vectoriel sous-jacent (noté encore) E et le K-endomorphisme :

$$\begin{array}{rcl} \varphi = m_X : E & \longrightarrow & E \\ x & \longrightarrow & X.x \end{array}$$

de sorte que les $K[X]$-modules s'identifient aux couples (E, φ) où E est un K-espace vectoriel et $\varphi \in \mathrm{End}_K(E)$. Un $K[X]$-homomorphisme $u : E \longrightarrow F$ est une application K-linéaire $u : E \longrightarrow F$ telle que $u \circ \varphi = \psi \circ u$ où φ (*resp.* ψ) est l'homothétie de rapport X sur E (*resp.* F). On a donc le *diagramme commutatif* :

$$\begin{array}{ccc} E & \xrightarrow{u} & F \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ E & \xrightarrow{u} & F \end{array}$$

Soit E un A-module ; une famille $(e_i)_{1\leq i\leq m}$ d'éléments de E est un *système générateur* (*resp. une base*) si, pour tout $x \in E$ il existe des éléments (*resp.* il existe des éléments *uniques*) $(a_i)_{1\leq i\leq m}$ de A tels que $\sum_{i=1}^{m} a_i x_i = x$. On dit alors que le A-module E est de *type fini* (*resp. libre de rang fini*).

Lemme 7
Soient A un anneau euclidien et L un A-module libre de rang fini ; toutes les bases de L possèdent le même nombre d'éléments m (appelé de rang de E) ; m est égal à la dimension du K-espace vectoriel $E_{(K)} = E \otimes_A K$.

$\triangledown$ Soit $(e_i)_{1\leq i\leq m}$ une base de L ; on a :

$$E_{(K)} = \{\frac{a}{b}x \,/\, \frac{a}{b} \in K \ , x \in E \text{ et } \frac{a}{b}x = \frac{a'}{b'}x' \Leftrightarrow \text{ il existe } c \in A \setminus \{0\} \text{ tel que } caxb' = ca'x'b\}$$

$(e_i)_{1\leq i\leq m}$ est alors une famille génératrice du K-espace vectoriel $E_{(K)}$; supposons alors que l'on ait une combinaison linéaire nulle des $(e_i)_{1\leq i\leq m}$ à coefficients dans F ; quitte à réduire les coefficients au même dénominateur on a $\sum_{i=1}^{m} \frac{a_i}{b} e_i = 0$ donc $\sum_{i=1}^{m} a_i e_i = 0$ dans K de sorte qu'il existe $c \in A \setminus \{0\}$ tel que $\sum_{i=1}^{m} c a_i e_i = 0$ dans A ; on a donc $ca_i = 0$ et comme A est intègre, on a $a_i = 0$ pour $1 \leq i \leq m$. $\triangle$

Lemme 8
Soit L un A-module ; alors L est libre de rang fini m si et seulement s'il existe une suite finie de longueur m :

$$L_0 = \{0\} \subset \cdots \subset L_i \subset L_{i+1} \subset L_m = L$$

avec $L_{i+1}/L_i \simeq A$ pour $0 \leq i \leq m-1$.

$\triangledown$ Supposons L libre de rang m, il existe donc une base $(e_i)_{1\leq i\leq m}$ de L. On prend $L_i = \bigoplus_{j=1}^{i} A\, e_j$ pour $1 \leq i \leq m$.
Réciproquement supposons que L possède une suite vérifiant les conditions de l'énoncé. Pour tout i, $0 \leq i \leq m-1$, L_{i+1}/L_i est un A-module libre de rang 1 ; prenons $e_{i+1} \in L_{i+1}$ tel que $L_{i+1}/L_i = A\,\overline{e_{i+1}}$. On a alors :

$$L_{i+1} = L_i \oplus A\, e_{i+1}$$

En effet si $x \in L_{i+1}$, on a $\overline{x} = \lambda \overline{e_{i+1}}$ de sorte que $x = \lambda e_{i+1} + y$ avec $y \in L_i$. on a donc $L_{i+1} = L_i + A\, e_{i+1}$. D'autre part si $x \in L_i \cap A\, e_{i+1}$ on a $x = \lambda e_{i+1} \in L_i$ de sorte que $\overline{x} = \lambda \overline{e_{i+1}} = \overline{0}$ d'où $\lambda = 0$ et $x = 0$.
Par récurrence sur i, on obtient donc que $(e_j)_{1\leq j\leq i}$ est une base de L_i. $\triangle$

Proposition 3
Soit L un A-module libre de rang fini m sur un anneau euclidien A ; tout sous-module L' de L est libre de rang fini $n \leq m$.

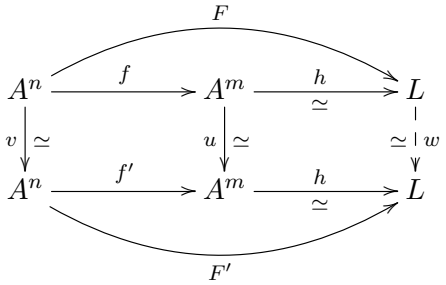
$\triangledown$ Considérons une suite $L_0 = \{0\} \subset \cdots \subset L_i \subset L_{i+1} \subset L_m = L$ de sous-modules de L avec $L_{i+1}/L_i \simeq A$ pour $0 \leq i \leq m-1$. Posons $L'_i = L_i \cap L'$ et soit $n \leq m$ le plus petit entier tel que $L'_n = L'$. On a donc $L'_0 = \{0\} \subset \cdots \subset L'_i \subset L'_{i+1} \subset L'_n = L'$. De plus l'homomorphisme *canonique* $L'_{i+1}/L'_i \longrightarrow L_{i+1}/L_i \simeq A$ est injectif ; son image est donc un idéal Aa de A, mais on a $a = 0$ ou $Aa \simeq A$ de sorte que L' est libre de rang $\leq n$. $\triangle$

Proposition 4 (théorème de la base adaptée)
Soient L un A-module libre de rang fini m sur un anneau euclidien A et L' un sous-module de L, $r \leq m$ le rang de L' ; alors il existe une base $(\epsilon_i)_{1\leq i\leq m}$ de L et des éléments $d_1, \cdots, d_r$ non nuls tels que $d_1|\cdots|d_r$ et $(d_i\,\epsilon_i)_{1\leq i\leq r}$ soit une base de L'. De plus les facteurs invariants d_i, $1 \leq i \leq r$, sont uniques à la multiplication par des éléments inversibles de A près.

$\triangledown$ Soit $(x_i)_{1\leq i\leq m}$ une *base* de L, on a le A-isomorphisme associé :

$$\begin{array}{rccc} h: & A^m & \longrightarrow & L \\ & (a_i)_{1\leq i\leq m} & \longrightarrow & \displaystyle\sum_{i=1}^{n} a_i x_i \end{array}$$

Munissons A^m de la base canonique $(e_i^{(m)})_{1\leq i\leq m}$ [10] ainsi que A^n de la base canonique $(e_j^{(n)})_{1\leq j\leq n}$.
Soit $(y_j)_{1\leq i\leq n}$ un *système générateur* de L' ; on désigne par $M \in \mathbf{M}_{m,n}(A)$ la matrice dont la colonne $C_j(M)$ [11] $(1 \leq j \leq n)$ est constituée des composantes de y_j dans la base $(x_i)_{1\leq i\leq m}$.
Il existe des matrices $U \in \mathrm{GL}_m(A)$ et $V \in \mathrm{GL}_n(A)$ telles que $S = U\,M\,V$ soit de la *forme réduite de Smith*.
On considère, $f : A^n \longrightarrow A^m$(*resp.* $u : A^m \longrightarrow A^m$, *resp.* $v : A^n \longrightarrow A^n$, *resp.* $f' : A^n \longrightarrow A^m$) l'homomorphisme dont la matrice dans les bases canoniques de A^m et A^n est M (*resp.* U,*resp.* V^{-1}, *resp.* S) ; on a $f' \circ v = u \circ f$ et u et v sont des isomorphismes. Ainsi le diagramme suivant est *commutatif* :



On a

$$\mathrm{Im}(F) = L'$$

et :

$$f'(e_j^{(n)}) = \begin{cases} d_j e_j^{(m)} & \text{pour } 1 \leq j \leq r \\ 0 & \text{pour } r+1 \leq j \leq n \end{cases}$$

avec $d_1, \cdots, d_r \in A \setminus \{0\}$ et $d_1|\cdots|d_r$, de sorte que :

$$F'(e_j^{(n)}) = (h \circ f')(e_j^{(n)})(= \begin{cases} d_j x_j & \text{pour } 1 \leq j \leq r \\ 0 & \text{pour } r+1 \leq j \leq n \end{cases}$$

d'où :

$$(w \circ F)(v^{-1}(e_j^{(n)})) = (F' \circ v)(v^{-1}(e_j^{(n)})) = \begin{cases} d_j x_j & \text{pour } 1 \leq j \leq r \\ 0 & \text{pour } r+1 \leq j \leq n \end{cases}$$

Pour $1 \leq i \leq m$ on pose $\epsilon_i = w^{-1}(xi)$ [12] de sorte que $(\epsilon_i)_{1\leq i\leq m}$ est une base de L et l'on a finalement :

$$F(v^{-1}(e_j^{(n)})) = \begin{cases} d_j \epsilon_j & \text{pour } 1 \leq j \leq r \\ 0 & \text{pour } r+1 \leq j \leq n \end{cases}$$

10. on a donc $h(e_i^{(m)}) = x_i$ pour $1 \leq i \leq m$.
11. on a donc $h(C_j(M)) = y_j$
12. on a donc $\epsilon_i = w^{-1}(h(e_i^m)) = h(u^{-1}e_i^m) = h(C_i(U^{-1}))$ *ie.* ϵ_i est l'élément de L dont les composantes dans la base $(x_i)_{1\leq i\leq m}$ forment la colonne $C_i(U^{-1})$

Puisque $\mathrm{Im}(F) = L'$, la famille $(d_j\epsilon_j)_{1\leq j\leq r}$ *engendre* L' et comme elle est *libre*, il s'agit d'une *base* de L'.
Considérons alors $(\epsilon'_i)_{1\leq i\leq m}$ une base de L et des éléments $d'_1, \cdots, d'_r$ non nuls tels que $d'_1|\cdots|d'_r$ et $(d'_i\,\epsilon'_i)_{1\leq i\leq r}$ soit une base de L'. Soit $U \in \mathbf{GL}_m(A)$ (*resp.* $V \in \mathbf{GL}_r(A)$) la matrice dont les colonnes sont les composantes des vecteurs ϵ_j, $1 \leq j \leq m$, (*resp.* $d_j\epsilon_j$, $1 \leq j \leq r$) dans la base $(\epsilon'_i)_{1\leq i\leq m}$ (*resp.* $(d'_i\,\epsilon'_i)_{1\leq i\leq r}$). On a $S' = U\,S\,V^{-1}$ où $S' \in \mathrm{M}_{m,r}(A)$ est la matrice de forme réduite de Smith dont les termes diagonaux sont les d'_i pour $1 \leq i \leq r$. Ainsi les matrices S et S' sont équivalentes donc d_i et d'_i sont associés pour $1 \leq i \leq r$. $\triangle$

Lemme 9
Tout A-module de type fini E est de présentation finie ie. on a une suite exacte[13]

$$A^n \xrightarrow{f} A^m \xrightarrow{\varphi} E \longrightarrow 0$$

$\triangledown$ Soit E de type fini ; il possède un système générateur fini $(x_1, \cdots, x_m)$ d'où un unique homomorphisme $\varphi : A^m \longrightarrow E$ défini par $\varphi(e_i^{(m)}) = x_i$ $(1 \leq i \leq m)$ où $(e_i^{(m)})_{1\leq i\leq m}$ est la base canonique de A^m.
Mais $\mathrm{Ker}(\varphi)$ est un sous-module de A^m donc est de type fini : soit $(y_1, \cdots, y_n)$ un système générateur de $\mathrm{Ker}(\varphi)$; on a donc un unique homomorphisme $f : A^n \longrightarrow A^m$ défini par $f(e_j^{(n)}) = y_j$ $(1 \leq j \leq n)$ où $(e_j^{(n)})_{1\leq j\leq n}$ est la base canonique de A^n et E est le conoyau de f. $\triangle$

Proposition 5 (structure des A-modules de type fini)
Soit A un anneau euclidien ; tout A-module de type fini E est de la forme :

$$E \simeq A^r \oplus A/Ad_1 \oplus \cdots \oplus A/Ad_s$$

avec $d_1, \cdots, d_s$ non nuls et non inversibles tels que $d_1|\cdots|d_s$. De plus l'entier r est indépendant de la décomposition et les facteurs invariants d_i, $1 \leq i \leq s$, sont uniques à la multiplication par des éléments inversibles de A près.

$\triangledown$ On a une suite exacte :

$$A^n \xrightarrow{f} A^m \xrightarrow{\varphi} E \longrightarrow 0$$

Munissons A^m de la base canonique $(e_i^{(m)})_{1\leq i\leq m}$ ainsi que A^n de la base canonique $(e_j^{(n)})_{1\leq j\leq n}$; les A-homomorphismes $f : A^n \longrightarrow A^m$ *s'identifient* alors aux matrices $M \in \mathbf{M}_{m,n}(A)$: la colonne $C_j(M) \in A^m$ de M $(1 \leq j \leq n)$ est formée des composantes de $f(e_j^{(n)})$ dans la base $(e_i^{(m)})_{1\leq i\leq m}$.
Il existe des matrices $U \in \mathrm{GL}_m(A)$ et $V \in \mathrm{GL}_n(A)$ telles que $S = U\,M\,V$ soit de la *forme réduite de Smith*. On considère, $u : A^m \longrightarrow A^m$ (*resp.* $v : A^n \longrightarrow A^n$, *resp.* $f' : A^n \longrightarrow A^m$) l'homomorphisme dont la matrice dans les bases canoniques de A^m et A^n est U (*resp.* V^{-1}, *resp.* S) ; on a $f' \circ v = u \circ f$ et u et v sont des isomorphismes. Ainsi le diagramme suivant est *commutatif* :

$$\begin{array}{ccccccc} A^n & \xrightarrow{f} & A^m & \xrightarrow{\varphi} & E & \longrightarrow & 0 \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle w} & & \\ A^n & \xrightarrow{f'} & A^m & \xrightarrow{\varphi'} & E' & \longrightarrow & 0 \end{array}$$

13. on a même une suite exacte $0 \longrightarrow A^n \xrightarrow{f} A^m \xrightarrow{\varphi} E \longrightarrow 0$; dans la démonstration il suffit de prendre pour $(y_1, \cdots, y_n)$ une *base* de $\mathrm{Ker}(\varphi)$. De plus, on verra que pour $A = K[X]$ et E un $K[X]$-module de type fini de torsion, la *suite exacte caractéristique* sera un choix *canonique* d'une telle suite exacte.

d'où l'existence d'un A-isomorphisme w entre E et le conoyau E' de f'. Or on a :

$$f'(e_j^{(n)})(= \begin{cases} d_j e_j^{(m)} & \text{pour } 1 \leq j \leq s \\ 0 & \text{pour } s+1 \leq j \leq n \end{cases}$$

avec $d_1, \cdots, d_s \in A \setminus \{0\}$ et $d_1 | \cdots | d_s$. On a ainsi [14] :

$$E \simeq A^r \oplus A/Ad_1 \oplus \cdots \oplus A/Ad_s$$

de sorte que $E_{(K)} \simeq K^r$. En particulier $r = \dim_K(E_{(K)})$ et r *ne dépend pas de la décomposition de* E.
L'unicité des facteurs invariants est étudiée ci-dessous. $\triangle$

Soient A un anneau euclidien et E un A-module de *type fini* ; alors

$$T(E) = \{x \in E \,/\, \text{il existe } a \in A \setminus \{0\} \text{ tel que } ax = 0\}$$

est un sous-A-module de E.

Corollaire 3
Le sous-A-module de $T(E)$ possède un supplémentaire L qui est libre [15] *; on a $E = T(E) \oplus L$.*

$\triangledown$ Il existe un A-isomorphisme :

$$f : E \longrightarrow A^r \oplus A/Ad_1 \oplus \cdots \oplus A/Ad_s$$

on a $f(T(E)) = A/Ad_1 \oplus \cdots \oplus A/Ad_s$ et on prend $L = f^{-1}(A^r)$. $\triangle$

On dit qu'un A-module L est *sans torsion* si $T(L) = \{0\}$. On a donc le résultat suivant :

Corollaire 4
Soient A un anneau euclidien et L un A-module de type fini ; alors L est libre si et seulement si L est sans torsion.

$\triangledown$ Si L est libre, L possède une base $(e_i)_{1 \leq i \leq m}$; si $x = \sum_{i=1}^{m} a_i e_i$ vérifie $ax = 0$ avec $a \neq 0$ on a $aa_i = 0$ et $a_i = 0$ pour $1 \leq i \leq m$ d'où $x = 0$.
Réciproquement supposons L sans torsion ; on a $L \simeq A/Ad_1 \oplus \cdots \oplus A/Ad_s \oplus A^r$; si $s \geq 1$, l'élément $\overline{1} \in A/Ad_1$ vérifierait $d_1\overline{1} = \overline{0}$ ce qui n'est pas possible ; on a donc $s = 0$ et $L \simeq A^r$. $\triangle$

On dit qu'un A-module E est *de torsion* si $T(E) = E$.

Corollaire 5
Soient A un anneau euclidien et E un A-module de type fini de torsion ;

$$E \simeq A/Ad_1 \oplus \cdots \oplus A/Ad_s$$

avec $d_1, \cdots, d_s$ non nuls et non inversibles tels que $d_1 | \cdots | d_s$.
Les facteurs invariants d_i, $1 \leq i \leq s$, sont uniques à la multiplication par un élément inversible de A près.

---

14. Lorsque d_i est inversible dans A, on a $A/\langle d_i \rangle = \{\overline{0}\}$; il faut donc supprimer les éléments d_i inversibles de la liste $(d_1, \cdots, d_s)$
15. $T(E)$ et L sont de type fini puisque A est *noethérien*.

$\triangledown$ On a $E \simeq A^r \oplus A/Ad_1 \oplus \cdots \oplus A/Ad_s$; si on avait $r \geq 1$, E contiendrait un élément non nul $x \in E$ libre donc non de torsion.
L'unicité des facteurs invariants est étudiée ci-dessous. $\triangle$

Corollaire 6
Un $\mathbb{Z}$-module E est de type fini et de torsion si et seulement si E est un groupe abélien fini.

$\triangledown$ Tout groupe abélien fini est de torsion. Réciproquement soit E un $\mathbb{Z}$-module E est de type fini et de torsion ; on a : $E \simeq \mathbb{Z}/\langle d_1\rangle \oplus \cdots \oplus \mathbb{Z}/\langle d_s\rangle$; avec les $d_i \neq 0$; alors E est fini. $\triangle$

Etude de l'unicité des facteurs invariants :
Soit E un A-module ; l'*annulateur* de $x \in E$ est l'idéal $\mathrm{ann}(x) = \{a \in A \,/\, ax = 0\}$ de A.
Un A-module E est *cyclique* s'il est engendré par un élément x avec $\mathrm{ann}(x)$ *non trivial*[16] de sorte que $E \simeq A/\mathrm{ann}(x)$.

Lemme 10
Soient A un anneau euclidien, $E = A/\langle d\rangle$ un A-module cyclique, π est un élément irréductible de A, $k = A/\langle\pi\rangle$ le corps résiduel ; alors $\pi|d$ si et seulement si le k-espace vectoriel $E/\pi E$ est de dimension 1[17].

$\triangledown$ Supposons que $\pi|d$. Les sous-modules de E correspondent aux idéaux de A *contenant* $\langle d\rangle$; on a $\langle d\rangle \subset \langle\pi\rangle$ de sorte que le sous-module πE de E correspond à l'idéal $\langle\pi\rangle$ de A et l'on a $E/\pi E \simeq A/\langle\pi\rangle = k$.
Par ailleurs si π ne divise pas d, π et d sont premiers entre eux et la formule de Bezout montre que $E = \pi E$. $\triangle$

Pour un A-module de type fini E, on désigne par $\rho(E)$ *le minimum du nombre d'éléments des systèmes générateurs* de E[18].

Lemme 11
Si E est de type fini et de torsion avec $E \simeq A/\langle d_1\rangle \oplus \cdots \oplus A/\langle Ad_s\rangle$, somme directe de modules cycliques tels que $d_1|\cdots|d_s$; on a $\rho(E) = s$.

$\triangledown$ Remarquons que la famille $(\overline{e_i})_{1\leq i\leq s}$ avec $e_i = (\delta_{i,j})_{1\leq j\leq s}$ est un système générateur de E de sorte que $\rho(E) \leq s$.
Réciproquement soit π un élément irréductible de A *divisant* d_1 ; on a l'isomorphisme de k-espaces vectoriels :

$$E/\pi E \simeq k^s$$

Si l'on avait $\rho(E) < s$ il existerait un système générateur $(x_i)_{1\leq i\leq t}$ de E avec $t < s$; mais $(\overline{x_i})_{1\leq i\leq t}$ serait un système générateur de $E/\pi E \simeq k^s$ ce qui n'est pas possible. $\triangle$.
Ainsi *s ne dépend pas de la décomposition de E.*

Lemme 12
Soient $E = A/\langle d\rangle$ un A-module cyclique et $a \in A$, on a :

$$a\,E = \begin{cases} \{\overline{0}\} & \text{si } a \in \langle d\rangle \\ \langle\overline{\Delta}\rangle & \text{si } a \notin \langle d\rangle \end{cases}$$

16. On a donc $\mathrm{ann}(x) = \langle d\rangle$ avec d non nul et non inversible.
17. On a $\dim_k(E/\pi E) \leq 1$.
18. lorsque L est libre de rang r, on a $\rho(L) = r$, lorsque E est cyclique on a $\rho(E) = 1$.

où $\Delta = \text{pgcd}(a,d)$ *et* $\langle\overline{\Delta}\rangle$ *désigne le sous-A-module cyclique de* E *engendré par* $\overline{\Delta}$. *De plus, lorsque* $a \notin \langle d\rangle$, *on a :*

$$\text{ann}(\overline{\Delta}) = \{x \in A \,/\, ax \in \langle d\rangle\}$$

$\triangledown$ Pour tout $\overline{x} \in E$, comme $a = \Delta\, b$ on a $a\overline{x} = \Delta\, b\overline{x}$ et comme on a la formule de Bezout $a\,a' + d\,d' = \Delta$, il en résulte que $\Delta\overline{x} = (a\,a' + d\,d')\overline{x} = a\,a'\overline{x}$. Ainsi aE est engendré par $\overline{\Delta}$.
D'autre part $a \in \text{ann}(\overline{\Delta})$ si et seulement si $d|a\Delta$. Comme on a $a\,x\,a' + d\,d'\,x = \Delta\,x$, on a $d|a\,\Delta$ si et seulement si $d|a\,x$. $\triangle$.

Corollaire 7 (*unicité* des facteurs invariants)
Soit A *un anneau ; considérons un* A*-module* E *somme directe de modules cycliques*

$$E \simeq A/Ad_1 \oplus \cdots \oplus A/Ad_s$$

tels que $d_1|\cdots|d_s$ *; on a* $\langle d_k\rangle = \{a \in A/\rho(aE) \leq s-k\}$ pour $1 \leq k \leq s$.

$\triangledown$ Soit $a \in A$; on a :

$$aE \simeq A/\text{ann}(\Delta_1) \times \cdots \times A/\text{ann}(\Delta_s) \text{ avec } \text{ann}(\Delta_1) \supset \cdots \supset \text{ann}(\Delta_s)$$

et $\Delta_i = \text{pgcd}(a, d_i)$ pour $1 \leq i \leq r$. Considérons $a \notin \langle d_k\rangle$, donc $\text{ann}(\Delta_k) \neq A$ de sorte que $\text{ann}(\Delta_t) \neq A$ pour $k \leq t \leq s$ et l'on a $\rho(aE) \geq s-k+1 > s-k$ [19].
Réciproquement si $a \in \langle d_k\rangle$ on a $\text{ann}(\Delta_k) = A$, donc $\text{ann}(\Delta_1) = \cdots = \text{ann}(\Delta_{k-1}) = A$ d'où $\rho(aE) \leq s-k$. $\triangle$

3 Réduction des endomorphismes

3.1 $K[X]$-modules

Rappelons qu'un $K[X]$-module E est caractérisé par le K-espace vectoriel sous-jacent (noté encore) E et le K-endomorphisme :

$$\begin{array}{rcl} \varphi = m_X : E & \longrightarrow & E \\ x & \longrightarrow & X.x \end{array}$$

de sorte que les $K[X]$-modules s'identifient aux couples (E,φ) où E est un K-espace vectoriel et $\varphi \in \text{End}_K(E)$. Un $K[X]$-homomorphisme $u : E \longrightarrow F$ est une application K-linéaire $u : E \longrightarrow F$ telle que $u \circ \varphi = \psi \circ u$ où φ (*resp.* ψ) est l'homothétie de rapport X sur E (*resp.* F). On a donc le *diagramme commutatif* :

$$\begin{array}{ccc} E & \xrightarrow{\;u\;} & F \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ E & \xrightarrow{\;u\;} & F \end{array}$$

Lemme 13
Soit E *un* $K[X]$*-module ;* E *est de type fini et de torsion si et seulement si* E *est un* K*-espace vectoriel de dimension finie.*

19. de sorte que $\rho(aE) \leq s-k \Rightarrow a \in \text{ann}(\Delta_k)$

$\triangledown$ Soit E un $K[X]$-module avec E ; on pose $\varphi = m_X$; si E est un K-espace vectoriel de dimension finie, le $K[X]$-module E est de dimension finie. De plus pour tout $x \in E$, $\text{ann}(x) \neq \{0\}$ sinon l'homomorphisme $f \longrightarrow f.x$ de $K[X]$ dans E serait injectif de sorte que E est de torsion.
Réciproquement supposons que E est de type fini et de torsion ; on a donc :

$$E \simeq K[X]/\langle f_1\rangle \times \cdots \times K[X]/\langle f_s\rangle$$

avec les polynômes f_i, $1 \leq i \leq s$ *non nuls*, de sorte que E est un K-espace vectoriel de dimension finie. $\triangle$

Soit E un K-espace vectoriel de dimension finie m ; considérons l'espace vectoriel $L_E = E^{(\mathbb{N})}$ des *suites à support fini* $(x_k)_{k\in\mathbb{N}}$ d'éléments de E muni du K-endomorphisme $\mathcal{D}$ de *décalage* :

$$\mathcal{D}(x_0, x_1, x_2, \cdots\cdots) = (0, x_0, x_1, x_2, \cdots\cdots)$$

de sorte que L_E est un $K[X]$-module [20] caractérisé par $m_X = \mathcal{D}$.
On a l'application K-linéaire injective :

$$\begin{array}{ccc} E & \longrightarrow & L_E \\ x & \longrightarrow & \widetilde{x} = (x, 0, 0, \cdots) \end{array}$$

Tout $\xi = (x_k)_{k\geq 0} \in L_E$ s'écrit donc de manière unique $\xi = \sum_{k=0}^{d} X^k \widetilde{x_k}$ [21] avec $a_d \neq 0$ et $a_k = 0$ pour tout $k \geq d+1$ (de sorte que L_E est le $K[X]$-module des *polynômes vectoriels* à coefficients dans E).

Lemme 14
L_E est un $K[X]$-module libre de rang fini m.

$\triangledown$ Soient $(e_i)_{1\leq i\leq m}$ une base du K-espace vectoriel E et $\xi = (x_k)_{k\in\mathbb{N}} \in L_E$; pour tout $k \geq 0$, on a $x_k = \sum_{i=1}^{m} \lambda_{i,k} e_k$ avec les coefficients $\lambda_{i,k} \in K$ uniques et $x_k = 0$ pour $k \geq d+1$. Formons alors les polynômes $P_i = \sum_{k=0}^{d} \lambda_{i,k} X^k \in K[X]$ pour $1 \leq k \leq m$. On a alors, de manière unique, $\xi = \sum_{i=1}^{m} P_i.\widetilde{e_i}$. Ainsi $(\widetilde{e_i})_{1\leq i\leq m}$ est une base du $K[X]$-module L_E. $\triangle$
Pour toute base $(e_i)_{1\leq i\leq m}$ de E, on obtient donc un isomorphisme de $K[X]$-module

$$\begin{array}{ccc} K[X]^m & \longrightarrow & L_E \\ (P_i)_{1\leq i\leq m} & \longrightarrow & \sum_{i=1}^{m} P_i.\widetilde{e_i} \end{array}$$

permettant d'identifier les *polynômes vectoriels* à coefficients dans E aux *vecteurs polynômiaux* de $K[X]^m$.

Soit φ un K-endomorphisme de E ; l'application :

$$\begin{array}{rccc} L_\varphi : & L_E & \longrightarrow & L_E \\ & (x_k)_{k\geq 0} & \longrightarrow & (\varphi(x_k))_{k\geq 0} \end{array}$$

20. On a $L_E \simeq E \otimes_K K[X]$
21. pour tout $x \in E$ on a $\widetilde{x} = x \otimes 1$.

est un $K[X]$-endomorphisme de L_E [22].
Remarquons que la matrice M de L_φ dans la base $(\widetilde{e_i})_{1\leq i\leq m}$ de L_E est la matrice M de φ dans la base $(e_i)_{1\leq i\leq m}$ de E de sorte que la matrice du $K[X]$-homomorphisme :

$$C_\varphi = Xid_{L_X} - L_\varphi : L_E \longrightarrow L_E$$

est la matrice *caractéristique* $C_M \in \mathrm{M}_n(K[X])$ de M.
De plus, désignons par E_φ le $K[X]$-module dont l'espace vectoriel sous-jacent est E et dont la multiplication par X est $m_X = \varphi$. On considère alors le $K[X]$-homomorphisme [23] :

$$\begin{array}{rccc} T_\varphi : & L_E & \longrightarrow & E_\varphi \\ & (x_k)_{k\geq 0} & \longrightarrow & \displaystyle\sum_{k=0}^{+\infty} \varphi^k(x_k) \end{array}$$

Proposition 6 (suite exacte caractéristique)
La suite de $K[X]$-homomorphismes :

$$0 \to L_E \xrightarrow{C_\varphi = Xid_{L_X} - L_\varphi} L_E \xrightarrow{T_\varphi} E_\varphi \to 0$$

est exacte.

$\triangledown$ Pour tout $x \in E$ on a $T_\varphi(\widetilde{x}) = x$ de sorte que T_φ est surjectif.
Considérons ensuite (en sous-entendant le $\widetilde{\ }$) $\xi = \sum_{k=0}^{d} X^k x_k \in L_E$; on a alors :

$$C_\varphi(\xi) = X^{d+1}x_d + \sum_{k=1}^{d} X^k(x_{k-1} - \varphi(x_k)) - \varphi(x_0)$$

de sorte que $C_\varphi(\xi) \Longrightarrow \xi = 0$ et C_φ est injectif.
Puisque :

$$\begin{aligned} T_\varphi(C_\varphi(\xi)) &= T_\varphi(X^{d+1}x_d + \sum_{k=1}^{d} X^k(x_{k-1} - \varphi(x_k)) - \varphi(x_0)) \\ &= T_\varphi^{d+1}(x_d) + \sum_{k=1}^{d} T_\varphi^k(x_{k-1} - \varphi(x_k)) - \varphi(x_0)) \\ &= T_\varphi^{d+1}(x_d) + \sum_{k=1}^{d} T_\varphi^k(x_{k-1}) - \sum_{k=1}^{d} T_\varphi^{k+1}(x_k) - \varphi(x_0) \\ &= 0 \end{aligned}$$

on a $\mathrm{Im}(C_\varphi) \subset \mathrm{Ker}(T_\varphi)$.
Considérons enfin $\eta = \sum_{k=0}^{d+1} X^k y_k \in \mathrm{Ker}(T_\varphi)$ *i.e.* $\sum_{k=0}^{d+1} \varphi^k(y_k) = 0$.
On pose alors $\xi = \sum_{k=0}^{d} X^k x_k$ avec :

$$x_k = \begin{cases} y_{d+1} & \text{si } k = d \\ y_{k+1} + \varphi(x_{k+1}) & \text{si } 0 \leq k \leq d-1 \end{cases}$$

22. on a $L_\varphi = \varphi \otimes \mathrm{id}_{K[X]}$.
23. T_φ est l'unique $K[X]$-homomorphisme $T_\varphi : L_E \longrightarrow E_\varphi$ tel que $T_\varphi(x \otimes 1) = x$) d'après la *propriété universelle* des produits tensoriels de sorte que l'on a $T_\varphi(x \otimes X) = T_\varphi(X.(x \otimes 1)) = X.T_\varphi(x \otimes 1) = X.x = \varphi(x)$.

Mais $x_0 = y_1 + \varphi(x_1)$ de sorte que :

$$\begin{aligned}
\varphi(x_0) &= \varphi(y_1) + \varphi^2(x_1) \\
&= \varphi(y_1) + \varphi^2(y_2) + \varphi^3(x_2) \\
&\vdots \\
&= \varphi(y_1) + \varphi^2(y_2) + \cdots + \varphi^{d+1}(y_{d+1}) \\
&= -y_0
\end{aligned}$$

On a finalement $y_0 = -\varphi(x_0)$ de sorte que $\eta = C_\varphi(\xi)$ d'où $\mathrm{Im}(C_\varphi) = \mathrm{Ker}(T_\varphi)$. $\triangle$

3.2 Applications

3.2.1 Le théorème de Cayley-Hamilton

On a vu que la matrice M de L_φ dans la base $(\widetilde{e_i})_{1\leq i\leq m}$ de L_E est la matrice M de φ dans la base $(e_i)_{1\leq i\leq m}$ de E. La matrice C_M de C_φ dans la base $(\widetilde{e_i})_{1\leq i\leq m}$ de L_E est la matrice caractéristique de M, ainsi $\chi_\varphi = \det(C_\varphi) \in K[X]$ est le *polynôme caractéristique* de φ.

Proposition 7 (Cayley-Hamilton)
On a $\chi_\varphi(\varphi) = 0$.

$\triangledown$ La formule de Cramer s'écrit $\widetilde{C_\varphi}\, C_\varphi = \widetilde{C_\varphi}\, C_\varphi = \chi_\varphi \mathrm{Id}_{L_E}$.
Pour tout $x \in E_\varphi$, il existe $\xi \in L_E$ tel que $x = T_\varphi(\xi)$. On a donc $C_\varphi\, \widetilde{C_\varphi}\, \xi = \chi_\varphi\, \xi$. Comme $T_\varphi \circ C_\varphi = 0$ on a :

$$T_\varphi(\chi_\varphi\, \xi) = \chi_\varphi(\varphi)(x) = 0$$

Comme cette dernière égalité est vérifiée pour tout $x \in E_\varphi$ on a $\chi_\varphi = 0$. $\triangle$

3.2.2 Equivalence et similitude

Proposition 8
Deux endomorphismes φ, ψ *sont semblables si et seulement si les endomorphismes caractéristiques* C_φ, C_ψ *sont équivalents.*

$\triangledown$ Considérons un $K[X]$-isomorphisme $w : E_\varphi \longrightarrow V_\psi$; on a l'isomorphisme :

$$\begin{array}{rccc}
L_w : & L_E & \longrightarrow & L_V \\
& (x_k)_{k\geq 0} & \longrightarrow & (w(x_k))_{k\geq 0}
\end{array}$$

tel que

$$\begin{aligned}
L_w \circ C_\varphi &= L_w \circ (Xid_{L_X} - L_\varphi) \\
&= L_w - L_w \circ L_\varphi \\
&= L_w - L_\psi \circ L_w \\
&= (Xid_{L_X} - L_\psi) \circ L_w \\
&= C_\psi \circ L_w
\end{aligned}$$

de sorte que l'on a le diagramme commutatif :

$$\begin{array}{ccc}
L_E & \xrightarrow{C_\varphi = Xid_{L_X} - L_\varphi} & L_E \\
{\scriptstyle T_w}\downarrow & & \downarrow{\scriptstyle T_w} \\
L_V & \xrightarrow{C_\psi = Xid_{L_X} - L_\psi} & L_V
\end{array}$$

Supposons réciproquement que l'on ait le diagramme commutatif :

$$\begin{array}{ccc} L_E & \xrightarrow{C_\varphi = X id_{L_X} - L_\varphi} & L_E \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ L_V & \xrightarrow{C_\psi = X id_{L_X} - L_\psi} & L_V \end{array}$$

dans lequel u est v sont des isomorphismes de $K[X]$-modules ; on en déduit un $K[X]$-isomorphisme $w : E_\varphi \longrightarrow V_\psi$ rendant commutatif le diagramme :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_E & \xrightarrow{C_\varphi = X id_{L_X} - L_\varphi} & L_E & \xrightarrow{T_\varphi} & E_\varphi & \longrightarrow & 0 \\ & & {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} & & \vdots{\scriptstyle w} & & \\ 0 & \longrightarrow & L_V & \xrightarrow{C_\psi = X id_{L_X} - L_\psi} & L_V & \xrightarrow{T_\psi} & V_\psi & \longrightarrow & 0 \end{array}$$

comme u est v sont des isomorphismes, il en est de même [24] de w $\triangle$

3.2.3 Invariants de similitude

Considérons un endomorphisme φ d'un K-espace vectoriel E de dimension finie m ; reprenons la suite exacte caractéristique [25]

$$0 \to L_E \xrightarrow{C_\varphi = X id_{L_X} - L_\varphi} L_E \xrightarrow{T_\varphi} E_\varphi \to 0$$

Compte tenu du fait que L_E est un $K[X]$-module libre de rang fini m et que C_φ est injectif, on peut alors appliquer le théorème de la *base adaptée* à $L' = \mathrm{Im}(C_\varphi) = \mathrm{Ker}(T_\varphi) \subset L = L_E$: il existe une base $(\epsilon_1, \cdots, \epsilon_m)$ de L et des polynômes *unitaires* [26] $P_1, \cdots P_m \in K[X]$ uniques tels que $P_1 | \cdots | P_m$ et que $(P_1\epsilon_1, \cdots, P_m\epsilon_m)$ soit une base de L'.
On a $P_1 = \cdots = P_{m-r} = 1$ tandis que $I_1(\varphi) = P_{m-r+1}, \cdots I_r(\varphi) = P_m$ sont de degré ≥ 1 ; ces derniers sont les *invariants de similitude* de φ. Pour $1 \leq k \leq m$ le produit $P_1 \cdots P_k$ est égal au *pgcd des mineurs* d'ordre k de la matrice caractéristique de φ (dans une base quelconque de V). En particulier le *polynôme caractéristique* χ_φ de φ est égal au produit $I_1(\varphi) \cdots I_r(\varphi)$ des invariants de similitude de φ.
On a alors l'isomorphisme de $K[X]$-modules :

$$L/L' \simeq K[X]/\langle I_1(\varphi)\rangle \times \cdots \times K[X]/\langle I_r(\varphi)\rangle \xrightarrow{\overline{T_\varphi}} E_\varphi$$

Il en résulte en particulier que

- $\star$ p_m est le polynôme minimal $p_{\varphi,K}$ de φ. Ce résulte précise le théorème de Cayley-Hamilton en explicitant le quotient (exact) $\chi_\varphi / p_{\varphi,K}$.
- $\star$ Deux endomorphismes φ et ψ d'un K-espace vectoriel V de dimension finie sont semblables (i.e. les $K[X]$-modules V_φ et V_ψ sont isomorphes) si et seulement s'ils ont les mêmes invariants de similitude.

---

24. c'est le *lemme des cinq*
25. que l'on peut considérer aussi comme une *présentation* du $K[X]$-module E_φ ou encore une *résolution libre* de ce dernier
26. aucun des ces polynômes n'est nul car leur produit est égal au polynôme caractéristique χ_φ ; on peut donc supposer ces polynômes *unitaires*.