Chapitre 2

Matrices euclidiennes et formes canoniques

Ce chapitre ainsi que les deux suivants est constitué de rappels d'algèbre, d'un intérêt par ailleurs général.

On commencera par rappeler quelques notions d'algèbre commutative: anneau principal et euclidien; on montrera en particulier que les anneaux euclidiens sont principaux, et comment l'algorithme d'Euclide permet un calcul effectif des PGCD.

Puis on commencera l'étude des *matrices à éléments dans un anneau euclidien*. On caractérisera les matrices inversibles au sens de l'anneau (ou unimodulaires), ce qui permettra de généraliser au cas matriciel la notion d'équivalence, c'est-à-dire l'égalité à un inversible près. L'algèbre matricielle étant non commutative, il conviendra de différencier équivalence à gauche, équivalence à droite, et équivalence bilatérale.

Puis on s'intéressera à deux problèmes classiques du calcul matriciel: la triangulation et la diagonalisation. On montrera qu'une matrice est

- équivalente (à gauche ou à droite) à une matrice triangulaire
- équivalente à une matrice diagonale

On montrera, dans le cas euclidien, que le calcul d'une forme triangulaire (forme d'Hermite) sur une matrice unimodulaire revient à un calcul d'inverse.

2.1 Corps des fractions. Anneau principal. Anneau euclidien

2.1.1 Anneau. Corps des fractions

On supposera connue la définition d'un anneau.

On rappelle qu'un anneau est *commutatif* lorsque sa seconde loi (multiplicative) est commutative. Un anneau est dit *intègre* lorsqu'on a:

$$a.b = 0 \Rightarrow (a = 0 \; ou \; b = 0) \tag{2.1}$$

Enfin, un anneau est dit unitaire si sa loi multiplicative possède un élément neutre. **On supposera ces trois propriétés toujours vérifiées.** Dans tout ce qui suivra "anneau" signifiera "anneau commutatif unitaire intègre". On a alors le théorème suivant:

Théorème 2.1 (Corps des fractions) *A tout anneau on peut associer son* corps des fractions*, corps dont il est un sous-anneau.*

Preuve: la construction est la même que celle des fractions ordinaires à partir des entiers relatifs. Le fait que l'anneau de départ soit un sous-anneau du corps résulte de l'existence d'un élément neutre pour la multiplication.

2.1.2 Anneau principal

Définition 2.1 (Idéal) *Un idéal d'un anneau est un sous-groupe additif tel que le produit d'un élément quelconque de cet idéal par un élément quelconque de l'anneau est encore un élément de l'idéal.*

Définition 2.2 (Idéal principal) *Un idéal d'un anneau est dit principal s'il est engendré par un seul élément a, i.e. tous ses éléments peuvent se mettre sous la forme xa, où x est un élément de l'anneau.*

Remarque: $\{0\}$ est un idéal principal, engendré par 0 et 0 seulement.

Définition 2.3 (Anneau principal) *Un anneau est dit principal si tous ses idéaux sont principaux.*

On rappelle qu'un anneau est dit *factoriel* si tous ses éléments non inversibles peuvent être décomposés de manière unique (à des éléments inversibles près) en produit de facteurs premiers non inversibles. On montre que tout anneau principal est factoriel.

Définition 2.4 (PGCD) *Soit $\mathcal{A}$ un anneau principal, et $(a_1, \ldots, a_n)$ n éléments de $\mathcal{A}$. d est un PGCD de $(a_1, \ldots, a_n)$ si d est un générateur de l'idéal engendré par $(a_1, \ldots, a_n)$.*

Remarques:

- on peut définir la notion de PGCD sans supposer que $\mathcal{A}$ soit principal. Cette dernière propriété nous garantit simplement l'existence d'un PGCD.
- $\mathrm{PGCD}(0, \ldots, 0) = 0$.

Théorème 2.2 (Identité de Bezout) *Les trois propriétés suivantes sont équivalentes:*

- *d est un PGCD des $(a_1, \ldots, a_n)$*

- *d est un plus grand commun diviseur des $(a_1, \ldots, a_n)$, i.e. d est un diviseur*[1] *commun des $(a_1, \ldots, a_n)$ et d est multiple de tout diviseur commun des $(a_1, \ldots, a_n)$*
- *d est un diviseur commun des $(a_1, \ldots, a_n)$ et il existe n éléments $(x_1, \ldots, x_n)$ de $\mathcal{A}$ tels que*

$$\sum_{i=1}^{i=n} x_i a_i = d \tag{2.2}$$

Cette dernière identité est dite identité de Bezout.

Preuve: il suffit essentiellement de remarquer que d est un PGCD des $(a_1, \ldots, a_n)$ si et seulement si on a

$$\sum_{i=1}^{i=n} a_i \mathcal{A} = d\mathcal{A} \tag{2.3}$$

Le reste de la preuve est laissée en exercice.

Définition 2.5 (Eléménts premiers entre eux) $(a_1, \ldots, a_n)$ *sont* premiers entre eux *s'ils ont un PGCD inversible (par exemple l'élément neutre de la multiplication).*

On appelle aussi *équation diophantine* l'identité de Bezout. De manière générale la division est inconnue dans un anneau; c'est l'équation diophantine qui tient lieu d'équation d'inversion lorsque l'ont dispose d'éléments premiers entre eux. C'est là que réside l'intérêt des idéaux principaux.

Exemples d'anneaux principaux: tous les corps sont des anneaux principaux; également l'anneau des entiers relatifs, celui des polynômes. Tous ces anneaux sont en fait des anneaux *euclidiens*; nous allons voir que tous les anneaux euclidiens sont des anneaux principaux.

2.1.3 Anneau euclidien

Définition. Propriété fondamentale

Définition 2.6 (Anneau euclidien) *Un anneau*[2] *$\mathcal{A}$ est dit* euclidien *s'il existe une application δ, dite application degré, de $\mathcal{A} - \{0\}$ dans l'ensemble des entiers naturels, telle que*

- *pour tout $x \in \mathcal{A}$, $y \in \mathcal{A} - \{0\}$, il existe q et r dans $\mathcal{A}$ tels que*
  - *$x = qy + r$*
  - *$r = 0$ ou $\delta(r) < \delta(y)$*
- *si x divise y, avec x et y non nuls, alors $\delta(x) \leq \delta(y)$*

La première condition exprime l'existence d'une *division euclidienne*; q est le quotient, r le reste. De la seconde condition on peut déduire que tous les éléments inversibles sont de même degré, et que ce degré est minimal. Quitte à opérer une translation sur la fonction degré, on supposera toujours que les éléments inversibles sont de degré nul.

Dans le cas d'un anneau principal on peut définir un pseudo-degré satisfaisant uniquement à la deuxième condition en prenant pour $\delta(x)$ le nombre de facteurs premiers de x, en posant par convention $\delta(x) = 0$ pour x inversible.

---

[1] par convention, 0 est le seul diviseur de 0

[2] non réduit à 0

Théorème 2.3 (condition suffisante d'unicité du reste) *On se donne un anneau euclidien, et on suppose de plus que pour tout a,b dans l'anneau on a*

$$\deg(a+b) \leq \max(\deg(a), \deg(b)) \tag{2.4}$$

Alors le quotient et le reste de division euclidienne sont uniques.

Preuve: posons deux divisions euclidiennes de a par b, soit

$$a = bq_1 + r_1 \tag{2.5}$$
$$a = bq_2 + r_2 \tag{2.6}$$

Alors on a $r_1 - r_2 = b(q_1 - q_2)$; si r_1 est différent de r_2, on a $q_1 \neq q_2$ et

$$\begin{aligned} \deg(r_1 - r_2) &\leq \max(\deg(r_1), \deg(r_2)) \\ &< \deg(b) \\ &\leq \deg b(q_1 - q_2) \\ &= \deg(r_1 - r_2) \end{aligned}$$

ce qui est contradictoire.

Remarques:

- il s'agit d'une unicité *véritable*, et non pas d'une unicité à un élément inversible près
- l'anneau euclidien des fractions rationnelles propres (c.f. exercice) est un exemple d'anneau où la division euclidienne n'est pas unique.

Théorème 2.4 (essentiel) *Un élément x d'un idéal non nul[3] $\mathcal{I}$ d'un anneau euclidien engendre $\mathcal{I}$ si et seulement si x est non nul et de degré minimal dans $\mathcal{I}$.*

En particulier tous les anneaux euclidiens sont principaux.

Preuve:

Condition suffisante: soit y dans $\mathcal{I}$; opérons la division euclidienne de y par x, et soit r le reste. $\mathcal{I}$ étant un idéal, r est donc dans $\mathcal{I}$. Or si r est non nul, c'est un élément de $\mathcal{I}$ de degré inférieur strict à celui de x. Cela est inpossible; on en déduit que x divise y. Ceci étant vrai pour tout y, x engendre $\mathcal{I}$.

Condition nécessaire: soit y un élément de $\mathcal{I}$ de degré minimal (il en existe). Alors (voir plus haut) y engendre $\mathcal{I}$ comme x. On en déduit qu'ils se divisent mutuellement et que leurs degrés sont égaux; x est donc de degré minimal.

Remarque: la condition nécessaire reste vrai dans un anneau principal en prenant le pseudo-degré. En effet, deux éléments générateurs de $\mathcal{I}$ se divisent mutuellement, et ils divisent tous les éléments de $\mathcal{I}$.

Corollaire 2.1 on en déduit que tout élément de degré nul est inversible (la reciproque étant établie par convention).

[3] i.e., non réduit à 0

Algorithme d'Euclide

Soit $(a_1, \ldots, a_n)$ n éléments de $\mathcal{A}$, non tous nuls. On définit l'algorithme suivant:

- initialisation
  1. pour $j = 1$ à n faire
     (a) $r_j = a_j$
     (b) $\alpha_{j,k} = \delta_{j,k}$, où $\delta_{j,k}$ est l'indice de Kronecker associé à (j, k)
     (c) $\beta_{j,k} = \delta_{j,k}$
- boucle
  - si tous les r_j, ou tous sauf un, sont nuls, STOP, sinon:
  - soit r_{j_0} un élément de degré minimal parmi les r_j non nuls.
    1. Poser la division des r_j par r_{j_0}, soit $r_j = q_j r_{j_0} + s_j$
    2. faire $r_j = s_j$ pour $j \neq j_0$
    3. faire $\alpha_{i,j_0} = \alpha_{i,j_0} + \sum_{j \neq j_0} \alpha_{i,j} q_j$
    4. pour $j \neq j_0$ faire $\beta_{j,i} = \beta_{j,i} - q_j \beta_{j_0,i}$
  - recommencer la boucle

Théorème 2.5 (Algorithme d'Euclide) *L'algorithme précedent s'arrête au bout d'un nombre fini de coups. Tous les r_j sont alors nuls sauf r_{j_0}, et r_{j_0} est un PGCD des $(a_1, \ldots, a_n)$, avec:*

1. $\sum_{j=1}^{j=n} \beta_{j_0,i} a_i = r_{j_0}$
2. $a_i = \alpha_{i,j_0} r_{j_0}$, i = 1 à n

Preuve: On vérifie sans peine qu'à chaque étape de l'algorithme on a:

$$a_i = \sum_{j=0}^{j=n} \alpha_{i,j} r_j \tag{2.7}$$

$$r_j = \sum_{i=0}^{i=n} \beta_{j,i} a_i \tag{2.8}$$

On en déduit en particulier que les r_j ne peuvent tous être nuls, car les a_i ne le sont pas. D'autre part, le degré de r_{j_0} diminue à chaque itération tant que tous les restes s_j ne sont pas nuls. L'algorithme s'arrête donc au bout d'un nombre fini d'itérations. Les deux identités précédentes, appliquées au dernier terme de la suite des r_{j_0}, permettent de conclure.

2.2 Matrices à éléments dans un anneau euclidien

2.2.1 Définition. Matrices unimodulaires

Définition 2.7 (matrice entière, euclidienne) *Une matrice entière est une matrice dont les éléments sont dans un anneau $\mathcal{A}$. Elle est dite euclidienne si l'anneau est euclidien.*

Suivant la convention établie précédemment, on supposera *toujours* l'anneau commutatif unitaire intègre. Le rang d'une matrice entière est alors défini comme étant le rang de cette matrice lorsqu'on considère ses éléments comme faisant partie du corps des fractions associé. On peut aussi procéder directement en calculant les mineurs de la matrice.

Définition 2.8 (matrice unimodulaire) *Une matrice carrée entière est dite unimodulaire si elle admet un inverse qui soit une matrice entière.*

Interprétation différentielle: on prend R[s] comme anneau euclidien, et à l'indéterminée s on substitue l'opérateur $\frac{d}{dt}$. Le produit par une unimodulaire à gauche (resp. à droite) correspond alors à un changement de variable *différentiellement réversible* dans l'espace d'arrivée (resp. sur les inconnues de l'équation différentielle). Cette interprétation présente l'intérêt d'être extensible en dehors du cas linéaire stationnaire. On voit également que c'est essentiellement l'opération de *composition d'opérateurs différentiels* qui est importante, l'addition étant plutôt un artefact résultant de la linéarité.

Théorème 2.6 (caractérisation des matrices unimodulaires) *Une matrice entière carrée est unimodulaire si et seulement si sont déterminant est inversible dans l'anneau.*

Preuve: La partie nécessaire résulte du fait que le déterminant du produit de deux matrices est le produit de leurs déterminants.

Partie suffisante: la matrice est alors de rang plein, et donc inversible dans le corps des fractions associé. Les formules classiques d'inversion de Cramer nous montrent que l'inverse est encore dans l'anneau.

2.2.2 Opérations élémentaires

On définit les *opérations élémentaires de lignes* sur les matrices entières de la manière suivante:

Définition 2.9 (opérations élémentaires de lignes) *Ce sont les opérations suivantes:*

- *permutation de deux lignes*
- *multiplication d'une ligne par un élément* inversible *de l'anneau*
- *ajout à une ligne du produit d'une* autre *ligne par un élément* quelconque *de l'anneau*

On définit de même les opérations élémentaires de colonnes.

Théorème 2.7 *Les opérations élémentaires de lignes (resp. de colonnes) sont équivalentes au produit à gauche (resp. à droite) par les matrices suivantes:*

- *permutation de deux lignes:*
$$\begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & 1 & & & \\ & & & \vdots & & \vdots & & & \\ & & & 1 & \cdots & 0 & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{bmatrix}$$
- *multiplication de la i^{eme} ligne par un élément λ inversible de l'anneau: $Id + (1-\lambda)M_i$, où M_i a tous ses éléments nuls sauf le i^{eme} élément de la diagonale, égal à 1.*
- *ajout à la i^{eme} ligne du produit de la j^{eme} ligne par un élément λ quelconque de l'anneau: $Id + \lambda N_{i,j}$, où $N_{i,j}$ a tous ses éléments nuls sauf celui de la i^{eme} ligne et de la j^{eme} colonne, égal à 1.*

Toutes ces matrices sont unimodulaires.

Preuve: Un simple calcul montre que les matrices représentent bien les opérations correspondantes. L'inverse d'une opération élémentaire étant une opération élémentaire de même type, on en déduit que ces matrices sont unimodulaires.

Définition 2.10 (Equivalence de matrices) *On dira que deux matrices euclidiennes sont ligne (resp. colonne) équivalentes si on peut passer de l'une à l'autre par des opérations élémentaires de lignes (resp. de colonnes). On dira qu'elles sont équivalentes si on peut passer de l'une à l'autre par des opérations élémentaires de lignes* ou *de colonnes.*

Remarque: on vérifie qu'il s'agit bien de relations d'équivalence.

Equivalence à gauche et à droite: on dira que deux matrices entières sont équivalentes à gauche (resp.à droite) si l'une est égale au produit à gauche (resp. à droite) de l'autre par une unimodulaire. De manière analogue on définit l'équivalence bilatérale; on parlera de matrices bi-équivalentes. Deux matrices ligne-équivalentes sont donc équivalentes à gauche. Nous verrons que la réciproque est vraie dans le cas des matrices euclidiennes; elle ne l'est pas dans un anneau principal quelconque.

2.2.3 Forme triangulaire (Hermite)

Lemme 2.1 Soit $(a_1, \ldots, a_n)$ un vecteur [4] ligne de n éléments de l'anneau euclidien, et r un PGCD des a_i. Alors le vecteur $(a_1, \ldots, a_n)$ est colonne équivalent à $(r, 0, \ldots, 0)$[5]. On a un résultat analogue sur la ligne équivalence en transposant tout.

Preuve: Il suffit de vérifier que l'algorithme d'Euclide, décrit précédemment, s'implémente au moyen d'opérations élémentaires.

Cas d'un anneau principal: le résultat demeure en remplaçant la ligne (resp. colonne) équivalence par l'équivalence à gauche (resp. à droite). On commence par montrer qu'il existe une matrice de déterminant r ayant $(a_1, \ldots, a_n)$ comme première ligne.

[4] "vecteur" est à prendre au sens de "matrice à une ligne ou une colonne", puisqu'il n'y a pas d'espace vectoriel sous-jacent (en fait, un module).

[5] si tous les a_i sont nuls, $r = 0$.

Le résultat est en effet vrai pour $n = 2$. Supposons le vrai pour n, et notons D_n la matrice correspondante. Soit r_n un PGCD des $(a_1, \ldots, a_n)$, et r_{n+1} un PGCD des $(a_1, \ldots, a_{n+1})$. Alors r_{n+1} est un PGCD de r_n et de a_{n+1}. Il existe donc p et q tels que $pr_n - qa_{n+1} = r_{n+1}$. Il suffit maintenant de prendre

$$D_{n+1} = \left[\begin{array}{ccc|c} & D_n & & \begin{matrix} a_{n+1} \\ 0 \\ 0 \end{matrix} \\ \hline \frac{a_1 q}{r_n} & \cdots & \frac{a_n q}{r_n} & p \end{array}\right] \tag{2.9}$$

ce qui prouve la récurrence.

Soit maintenant l'identité de Bezout pour $(a_1, \ldots, a_n)$:

$$\sum_{i=1}^{i=n} \alpha_i a_i = r \tag{2.10}$$

et U une matrice unimodulaire ayant $\alpha_1, \ldots, \alpha_n$ pour première ligne (les $\alpha_1, \ldots, \alpha_n$ sont premiers entre eux). Alors le produit à gauche du vecteur $(a_1, \ldots, a_n)$ par U est un vecteur de la forme $(r, b_2, \ldots, b_n)$, où les b_i sont des multiples du PGCD r. Il est alors facile, par des opérations de lignes (donc par le produit à gauche par une unimodulaire) de se ramener à $(r, 0, \ldots, 0)$.

Théorème 2.8 (Forme d'Hermite) *Toute matrice euclidienne de taille $p \times q$ est ligne équivalente (resp. colonne équivalente) à une matrice euclidienne H de la forme suivante:*

- $H = \left[\begin{array}{ccccc} h_{1,1} & \cdots & h_{1,p} & \cdots & h_{1,q} \\ & \ddots & & & \vdots \\ 0 & & h_{p,p} & \cdots & h_{p,q} \end{array}\right]$ *pour* $p \leq q$
- $H = \left[\begin{array}{ccc} h_{1,1} & \cdots & h_{1,q} \\ & \ddots & \vdots \\ 0 & & h_{q,q} \\ \hline & 0 & \end{array}\right]$ *pour* $p \geq q$

(respectivement:

- $H = \left[\begin{array}{ccc|c} h_{1,1} & & 0 & \\ \vdots & \ddots & & 0 \\ h_{p,1} & \cdots & h_{p,p} & \end{array}\right]$ *pour* $p \leq q$
- $H = \left[\begin{array}{ccc} h_{1,1} & & 0 \\ \vdots & \ddots & \\ h_{q,1} & \cdots & h_{q,q} \\ \vdots & & \vdots \\ h_{p,1} & \cdots & h_{p,q} \end{array}\right]$ *pour* $p \geq q$*)*

avec $d^o h_{i,j} < d^o h_{j,j}$[6] (resp. $d^o h_{j,i} < d^o h_{j,j}$) pour $i < j$ lorsque $h_{j,j}$ est non inversible et non nul, et $h_{i,j}$ (resp. $h_{j,i}$) = 0 lorsque $h_{j,j}$ est inversible. Une telle matrice ligne (resp. colonne) équivalente à une matrice M est dite forme d'Hermite supérieure (resp. inférieure) de M.

Remarque: par définition, toutes les formes d'Hermite supérieures (resp. inférieures) d'une matrice sont donc ligne (resp. colonne) équivalentes.

Preuve: on s'intéressera à la forme supérieure; le lecteur transposera pour la forme inférieure.

[6] à condition bien sûr que l'élément diagonal $h_{j,j}$ soit défini

On procède par récurrence sur le nombre q de colonnes de la matrice M de départ.

Le résultat est vrai pour $q = 1$, d'après le lemme 2.1. Supposons maintenant le résultat vrai pour q et considérons M à $q + 1$ colonnes.

On commence par supposer que q est inférieur strict à p le nombre de lignes. Soit M_1 la matrice extraite de M en rayant la dernière colonne, et M_2 la matrice constituée de la dernière colonne. Par récurrence, on peut, par opérations de ligne, mettre M_1 sous forme d'Hermite $\tilde{H}$. On peut donc, par les mêmes opérations de lignes, mettre M sous la forme $[\tilde{H}, N]$, soit:

$$M \sim \left[\begin{array}{ccc|c} \tilde{h}_{1,1} & \cdots & \tilde{h}_{1,q} & n_1 \\ & \ddots & \vdots & \vdots \\ 0 & & \tilde{h}_{q,q} & n_q \\ \hline & & & n_{q+1} \\ & 0 & & \vdots \\ & & & n_p \end{array}\right] \tag{2.11}$$

D'après le lemme précédent, on peut alors, par des opérations sur les $p - q$ dernières lignes de cette matrice, la mettre sous la forme:

$$M \sim \left[\begin{array}{ccc|c} \tilde{h}_{1,1} & \cdots & \tilde{h}_{1,q} & n_1 \\ & \ddots & \vdots & \vdots \\ 0 & & \tilde{h}_{q,q} & n_q \\ \hline & & & \tilde{n}_{q+1} \\ & & & 0 \\ & 0 & & \vdots \\ & & & 0 \end{array}\right] \tag{2.12}$$

Cela ne change, bien sûr, rien à la composition des q premières lignes. Pour conclure la récurrence, il nous suffit de remplacer les n_i, pour $i = 1$ à q, par le reste de leur division par $\tilde{n}_{q+1}$[7]. Pour cela, on retranche à la i^{eme} ligne le produit de la $(q+1)^{eme}$ par le quotient. Cela ne change pas la valeur des $\tilde{h}$.

Le résultat est donc montré pour $q \leq p$. Il est alors vrai pour $q > p$. En effet, il suffit de procéder comme dans le cas où $q = p$, puisqu'on n'exige rien sur les colonnes de numéro supérieur strict à p.

Remarques:

- à partir du moment où l'on dispose d'un algorithme de division euclidienne, la preuve précédente est parfaitement constructive, *via* l'algorithme d'Euclide. L'algorithme correspondant est un algorithme de pivot de Gauss.
- dans le cas où l'anneau est un corps, on voit facilement que la forme d'Hermite, dans le cas d'une matrice carrée de rang plein, est une matrice diagonale inversible; au prix de quelques opérations suppléméntaires, on peut se ramener à l'identité. On peut donc dire que, dans le cas général, le calcul d'une forme d'Hermite d'une matrice est ce qui se rapproche le plus d'un inversion (à gauche ou à droite) au sens du calcul dans l'anneau. Si de plus on se rappelle que c'est l'identité de Bezout qui tient lieu d'inversion dans un anneau, on ne sera pas surpris de constater (chapître suivant) que la forme d'Hermite permette de calculer l'identité de Bezout dans le cas matriciel.

[7] si $\tilde{n}_{q+1}$ n'est pas nul

Cas d'un anneau principal: le résultat demeure à condition de choisir la bonne notion d'équivalence et d'abandonner les spécifications sur les degrés. La preuve est alors identique au cas euclidien en utilisant le même lemme. On obtient simplement une forme triangulaire. On parlera encore de forme d'Hermite.

Exemple: on considère l'anneau des polynômes R[s], et la matrice:

$$M = \begin{bmatrix} 1 & s^3+s & s^2+s & 2s \\ 0 & s & s+1 & s^2+s \\ 0 & s & 1 & s^2+1 \end{bmatrix} \tag{2.13}$$

dont on cherche une forme d'Hermite inférieure. Il nous faut donc procéder par opérations de colonnes en regardant les lignes de haut en bas.

Il est évident que les éléments de la première ligne sont premiers entre eux, puiqu'on a 1 en première position. On ramène les autres éléments de la première ligne à 0 en soustrayant à la colonne correspondante le produit de la première colonne par l'élément de la première ligne considéré. Comme la première colonne est nulle à partir du 2^{eme} élément, cela ne modifie pas les lignes 2 et 3. Autrement dit, on a

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & s & s+1 & s^2+s \\ 0 & s & 1 & s^2+1 \end{bmatrix} \tag{2.14}$$

Deuxième ligne: s est un élément de degré minimal. Les restes sont: 1 pour $s+1$, 0 pour s^2+s; les quotients sont: 1 pour $s+1$, $s+1$ pour s^2+s. A la troisième colonne on enlève le produit de la seconde par 1; à la quatrième, le produit de la seconde par $s+1$, soit:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & s & 1 & 0 \\ 0 & s & 1-s & 1-s \end{bmatrix} \tag{2.15}$$

On ramène maintenant à gauche le terme de degré minimal de la deuxième ligne en permutant les colonnes 2 et 3, soit:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & s & 0 \\ 0 & 1-s & s & 1-s \end{bmatrix} \tag{2.16}$$

puis on met à zéro l'élément (2,3) en enlevant à la troisième colonne le produit de la seconde par s, soit:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1-s & s^2 & 1-s \end{bmatrix} \tag{2.17}$$

On en a fini avec la deuxième ligne, puisque l'élément (2,1) est déjà à zéro.

Troisième ligne: on commence par permuter la troisième et la quatrième colonne:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1-s & 1-s & s^2 \end{bmatrix} \tag{2.18}$$

Puis on retranche à la dernière colonne le produit de la troisième par le quotient $-s-1$:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1-s & 1-s & 1 \end{bmatrix} \tag{2.19}$$

et par permutation des deux colonnes et division euclidienne on aboutit à:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1-s & 1 & 0 \end{bmatrix} \tag{2.20}$$

Il nous reste à faire baisser le degré des élément de la troisième ligne, ce qui est fait en enlevant à la deuxième ligne le produit de la troisième par $1-s$, soit:

$$M \underset{colonnes}{\sim} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.21}$$

ou, de manière condensée:

$$M \underset{colonnes}{\sim} \left[\begin{array}{c|c} Id_3 & 0 \end{array} \right] \tag{2.22}$$

Nous allons maintenant pouvoir caractériser les matrices unimodulaires dans un anneau euclidien.

Théorème 2.9 (Caractérisation des unimodulaires) *Soit M une matrice carrée euclidienne. Les trois propositions suivantes sont équivalentes:*

1. *M est unimodulaire*
2. *M est ligne-équivalente à l'identité*
3. *M est colonne-équivalente à l'identité*

Preuve: $2 \Rightarrow 1$ et $3 \Rightarrow 1$ sont des conséquences directes du résultat bien connu selon lequel $\det(AB) = \det A \det B$, et du fait que les matrices d'opérations élémentaires sont unimodulaires.

Les deux réciproques se montrent de la même manière, à savoir:

on considère une forme d'Hermite H de M (supérieure ou inférieure selon les cas). H est une matrice triangulaire. Puisque $\det M$ est inversible, $\det H$ l'est également; son degré vaut donc zéro. Or $\det H$ est égal au produit des éléments diagonaux de H, et on a donc:

$$0 \leq d^o h_{i,i} \leq d^o \det H = 0 \tag{2.23}$$

pour tout i. On en déduit que les $h_{i,i}$ sont inversibles et que H est diagonale (c.f. la propriété sur les degrés dans le théorème 2.8). H est donc (ligne *et* colonne) équivalente à l'identité.

Corollaire 2.2 Toute matrice unimodulaire dans un anneau euclidien peut se décomposer en produit de matrices d'opérations élémentaires.

Interprétation différentielle: cela signifie que tout opérateur différentiellement réversible peut alors se décomposer en opérateurs élémentaires où seule la i^{eme} variable x_i est transformée en $\tilde{x}_i = x_i + \sum_{j \neq i} \sum_{k=0}^{k=n_j} \lambda_{j,k} \frac{d^k x_j}{dt^k}$, les autres variables restant inchangées.

Corollaire 2.3 Deux matrices euclidiennes sont ligne (resp. colonne) équivalentes si et seulement si l'une est produit à gauche (resp. à droite) de l'autre par une matrice unimodulaire.

Remarque: ce résultat est *capital* en ce qu'il établit la correspondance entre la notion *opératoire* d'equivalence (transformation sur les lignes ou les colonnes) et la notion *algébrique* d'équivalence (produit par une unimodulaire). A noter qu'il existe des anneaux principaux où certaines matrices unimodulaires ne sont pas ligne équivalentes à l'identité; les deux notions d'équivalences ne sont alors pas identiques, et c'est la deuxième que l'on retient.

Enfin, dans le cas où l'anneau est un corps, le calcul d'une forme d'Hermite est en fait un calcul d'inversion. En effet, toutes les matrices de rang plein sont unimodulaires dans un corps. L'inverse est alors donné par le produit des matrices d'opérations élémentaires qui amènent la matrice de départ à l'identité.

2.2.4 Forme diagonale (Smith)

Lemme 2.2 Soit M une matrice euclidienne. Alors il existe deux matrices unimodulaires U et V telles que UMV soit de la forme

$$UMV = N = \begin{bmatrix} n_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \tilde{N} & \\ 0 & & & \end{bmatrix} \tag{2.24}$$

Preuve: on utilise l'algorithme suivant:

a) si M est de la forme souhaitée, STOP. Si tous les éléments de la première colonne sont nuls, amener une colonne non nulle en première position (il en existe). Si la matrice obtenue est de la forme souhaitée, STOP. Sinon poser $i = 0$ et $N_0 = M$ (éventuellement la matrice précédente).

b) par des opérations de lignes [8] mettre (lemme 2.1) N_i sous la forme

$$N_{i+\frac{1}{2}} = \begin{bmatrix} r_i & \cdots \\ 0 & \\ \vdots & \tilde{N}_{i+\frac{1}{2}} \\ 0 & \end{bmatrix} \tag{2.25}$$

où r_i est un PGCD des éléments de la première colonne de N_i. Si r_i divise tous les éléments de la première ligne de $N_{i+\frac{1}{2}}$, on se ramène alors par des opérations de colonnes à la forme demandée et l'algorithme s'arrête. Sinon on va en c).

c) par des opérations de colonnes [9] mettre $N_{i+\frac{1}{2}}$ sous la forme

$$N_{i+1} = \begin{bmatrix} r_{i+\frac{1}{2}} & 0 & \cdots & 0 \\ & & & \\ \vdots & & \tilde{N}_{i+1} & \\ & & & \end{bmatrix} \tag{2.26}$$

où $r_{i+\frac{1}{2}}$ est un PGCD des éléments de la première ligne de $\tilde{N}_{i+\frac{1}{2}}$. Si $r_{i+\frac{1}{2}}$ divise tous les éléments de la première colonne de N_{i+1}, on se ramène alors par des opérations de colonnes à la forme demandée et l'algorithme s'arrête. Sinon on incrémente i et on va en b).

Cet algorithme s'arrête au bout d'un nombre fini d'itérations. En effet, r_i et $r_{i+\frac{1}{2}}$ ne sont pas nuls pour $i > 0$, et le degré de r_{i+1} est inférieur strict à celui de r_i, puisque r_{i+1} divise strictement $r_{i+\frac{1}{2}}$, et ce dernier divise strictement r_i.

Remarque: en s'autorisant éventuellement une permutation de ligne et de colonne pour le cas où la première ligne et la première colonne seraient nulles, on voit que le $n_{1,1}$ final est un diviseur commun aux éléments de la première ligne *et* de la première colonne de M.

Le lemme reste vrai dans un anneau principal; il suffit de remplacer le degré par le pseudo-degré dans la preuve.

---

[8] ou par une unimodulaire à gauche dans un anneau principal

[9] ou par une unimodulaire à droite dans un anneau principal

Lemme 2.3 obtention d'une forme diagonale: toute matrice euclidienne M est équivalente à une matrice euclidienne diagonale$D$; autrement dit, il existe deux matrices unimodulaires U et V telles que:

$$M = UDV \tag{2.27}$$

avec

$$D = \begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_r & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.28}$$

où r est le rang de M.

Preuve: Il suffit d'appliquer le lemme précédent à M, puis à la matrice extraite $\tilde{N}$, etc... jusqu'à l'élément r de la diagonale. Les élément "en bas à droite" sont alors tous nuls, sans quoi on pourrait réappliquer l'algorithme précédent et ajouter un élément *diagonal* non nul, ce qui contredirait la conservation du rang lors de produit par des unimodulaires.

---

le résultat est évidemment valable dans un anneau principal.

Lemme 2.4 Toute matrice euclidienne diagonale[10] est équivalente à une matrice diagonale $\tilde{S}$ où le premier élément de la diagonal divise tous les autres.

Preuve: soit D la matrice diagonale. Par des opérations de colonnes on transforme D en $\tilde{D}$ avec

$$\tilde{D} = \begin{bmatrix} d_1 & 0 & 0 & 0 \\ \vdots & \ddots & 0 & 0 \\ d_r & 0 & d_r & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.29}$$

Par des opérations de lignes on peut alors mettre un PGCD des d_i en haut à gauche. Puis on utilise l'algorithme du lemme 2.2. Soit N la matrice obtenue; alors $n_{1,1}$ est un diviseur commun de *tous* les éléments de D [11]. Il ne reste plus qu'à diagonaliser la matrice extraite $\tilde{N}$ en $\tilde{S}$ par l'algorithme du lemme 2.3. Comme $n_{1,1}$ divisait tous les éléments de N, $n_{1,1}$ (qui est le premier élément de $\tilde{S}$) divise tous les éléments de $\tilde{S}$.

Théorème 2.10 (Forme de Smith) *Toute matrice euclidienne est équivalente à une matrice S de la forme*

$$S = \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & s_r & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.30}$$

où r est le rang de M, et où s_i divise s_{i+1}, pour $i = 1$ à $r-1$.

Une telle matrice équivalente à M est dite forme de Smith *de M.*

Remarque: par définition, toutes les formes de Smith d'une matrice sont donc équivalentes.

Preuve: on commence par se ramener à une forme diagonale D (lemme 2.3). Puis on utilise récursivement l'algoritme du lemme 2.4 en "descendant" le long de la diagonale.

Remarque: là encore, la preuve est constructive à partir du moment où l'on dispose d'un algorithme de dividion euclidienne. L'algorithme de calcul de la forme de Smith est en fait un algorithme de pivot de Gauss-Jordan.

---

[10] c'est-à-dire composée d'une matrice carrée diagonale et de zéros autre part

[11] c'est en fait un PGCD des éléments de D, puisque les éléments de tout produit AB sont des éléments de $\mathcal{I}_A$ et de $\mathcal{I}_B$, où $\mathcal{I}_M$ est l'idéal engendré par les éléments de la matrice M.

le résultat est évidemment valable dans un anneau principal.

Lemme 2.5 Soit, pour une matrice entière M, $r_i(M)$ le PGCD de tous les mineurs d'ordre i de M. Alors $r_i(M)$ est inchangé (à un élément inversible près) lorsqu'on remplace M par le produit à gauche ou à droite de M par une unimodulaire.

Preuve: On commencera par traiter le cas où M est carrée.

Soit une matrice C de la forme AB, où A, B et C sont carrées, et $C_{l_1\dots l_m}^{k_1\dots k_m}$ la matrice extraite de C en sélectionnant les lignes $(k_1 \dots k_m)$ et les colonnes $(l_1 \dots l_m)$. Alors

$$\det C_{l_1\dots l_m}^{k_1\dots k_m} = \sum_{(i_1\dots i_m)} \det A_{i_1\dots i_m}^{k_1\dots k_m} \det B_{l_1\dots l_m}^{i_1\dots i_m} \tag{2.31}$$

On en déduit que les diviseurs communs des mineurs d'ordre m de A ou B sont des diviseurs communs des mineurs d'ordre m de C.

Si U est une matrice unimodulaire, on a donc $r_i(M)$ qui divise $r_i(UM)$ et $r_i(MU)$. Les matrices unimodulaires étant inversibles dans l'anneau, on en déduit que ces trois PGCD sont égaux à un inversible près, ce qui prouve le résultat pour M carrée.

Considérons maintenant le cas où M est rectangulaire de taille $p \times q$. On ne traitera que le cas de l'équivalence à gauche.

Dans le cas où on a $p > q$, on complète M en $\tilde{M} = [M|0]$. En notant $\sim$ l'equivalence dans l'anneau, on a alors $r_i(M) \sim r_i(\tilde{M}) \sim r_i(U\tilde{M}) \sim r_i([UM|0]) \sim r_i(UM)$.

Dans le cas où $p < q$ on complète M en $\tilde{M} = \begin{bmatrix} M \\ 0 \end{bmatrix}$ et U en $\tilde{U} = \begin{bmatrix} U & 0 \\ 0 & Id \end{bmatrix}$. On a alors $r_i(M) \sim r_i(\tilde{M}) \sim r_i(\tilde{U}\tilde{M}) \sim r_i(\begin{bmatrix} UM \\ 0 \end{bmatrix}) \sim r_i(UM)$.

Théorème 2.11 (Unicité de la forme de Smith) *La forme de Smith d'une matrice entière (en particulier euclidienne) est unique au produit des s_i par un inversible près.*

Preuve: pour $i > 1$, on a $s_i = \frac{r_i(S)}{r_{i-1}(S)} \sim \frac{r_i(M)}{r_{i-1}(M)}$ pour toute forme de Smith S de M; quant à s_1, il est visiblement égal à $r_1(S)$, qui est équivalent à $r_1(M)$.

La forme de Smith est donc une forme *canonique* des matrices entières. C'est donc un outil théorique important. Malheureusement, son calcul est assez complexe. Cela n'est pas gênant dans la mesure où, comme nous le verrons par la suite, la plupart des résultats pratiques s'obtiennent à partir des formes d'Hermite, plus simples à calculer.

2.3 Exercices

Exercice 2.1 Soient a et b deux éléments premiers entre eux dans un anneau principal $\mathcal{A}$, x et y dans l'anneau tels que $ax + by = 1$. Monter que les matrices $\begin{bmatrix} a & b \\ y & -x \end{bmatrix}$ et $\begin{bmatrix} a & y \\ b & -x \end{bmatrix}$ sont unimodulaires; calculer leur inverse.

Exercice 2.2 On considère le corps des fractions rationnelles $\mathbb{R}(s)$ et, dans ce corps, l'anneau $\mathcal{P}$ des fractions rationnelles *propres*, c'est-à-dire les fractions dont le degré du dénominateur est supérieur à celui du numérateur.

1. Montrer que le corps des fractions associé à $\mathcal{P}$ est identique au corps des fractions rationnelles.
2. On définit le degré d'une fraction propre de représentant $\frac{p}{q}$ comme étant le degré de q moins celui de p.
   - montrer que la définition précédente du degré est indépendante du représentant choisi.
   - soit r_1 et r_2 deux fractions rationnelles propres. Montrer que r_1 divise r_2 si et seulement si le degré de r_1 est inférieur à celui de r_2.
   - en déduire que $\mathcal{P}$ est un anneau euclidien
   - montrer que la division euclidienne n'est pas unique
   - montrer qu'une fraction propre de degré minimal dans une liste $(r_1, \ldots, r_n)$ est un PGCD de $(r_1, \ldots, r_n)$.
3. On dit que deux éléments d'un anneau sont équivalents s'ils sont égaux à un élément inversible près. On note $\overline{\mathcal{P}}$ le quotient de $\mathcal{P}$ par cette relation d'équivalence. Montrer que $\overline{\mathcal{P}}$ muni des opérations de PGCD et de produit sur deux fractions est isomorphe à $(\mathbf{N}, min, +)$, où $\mathbf{N}$ est l'ensemble des entiers naturels.

Exercice 2.3 Calculer une forme d'Hermite supérieure pour la matrice M donnée en exemple.

Exercice 2.4 On définit les *opérations de lignes par bloc* de la manière suivante:

- permutation de deux blocs de lignes
- multiplication à gauche d'un bloc de lignes par une matrice unimodulaire
- ajout à un bloc-lignes du produit d'un bloc-lignes disjoint par une matrice de taille adéquate

On définit de manière analogue au cas scalaire la bloc-lignes équivalence.

Montrer que, dans un anneau euclidien, deux matrices sont bloc-lignes équivalentes si et seulement si elles sont lignes équivalentes.

Chapitre 3

Divisibilité de matrices euclidiennes

Comme son nom l'indique, ce chapitre est consacré à l'étude des relations de divisibilité entre matrices euclidiennes. Il constitue essentiellement une extension des résultats scalaires au cas matriciel.

Après quelques définitions évidentes, on montrera que deux matrices se divisent mutuellement si et seulement si elles sont égales à un inversible près. Là encore, on distinguera divisibilité à gauche et à droite.

La notion de divisibilité conduira naturellement à définir les PGCD de deux matrices entières. On montrera qu'en juxtaposant les deux matrices et en calculant une forme d'Hermite de la matrice obtenue, on obtient un PGCD des deux matrices, ce qui prouvera l'existence du (des) PGCD dans le cas matriciel. Puis on reliera PGCD et identité de Bezout. On donnera ensuite l'expression générale des coefficients de Bezout de manière tout à fait analogue à ce qui se passe dans le cas scalaire.

Grâce à l'étude du cas matriciel, on montrera que le calcul de l'identité de Bezout dans le cas premiers entre eux est en fait une inversion partielle de matrice unimodulaire.

On terminera en faisant le lien entre calcul de PGCD et quelques questions de calcul vectoriel.

Résumé des épisodes précédents

Nous avons défini les notions de matrice entière, de matrice unimodulaire et de matrice euclidienne.

Nous avons montré que toute matrice entière est équivalente à gauche (ligne équivalente dans le cas euclidien) à une forme d'Hermite triangulaire supérieure; et équivalente à droite (resp. colonne équivalente) à une forme d'Hermite triangulaire inférieure.

Nous en avons déduit que, dans le cas euclidien, les matrices unimodulaires peuvent s'exprimer comme produit de matrices d'opérations élémentaires.

Enfin nous avons montré que toute matrice entière est bi-équivalente (équivalente dans le cas euclidien) à une forme diagonale dite de Smith.

3.1 Divisibilité

Définition 3.1 (Diviseurs) *Une matrice entière B divise une autre matrice entière A à droite (resp. à gauche) s'il existe une matrice entière Q telle que $A = QB$ (resp. $A = BQ$).*

Remarque: si B divise A à droite (resp. à gauche), alors A et B ont le même nombre de colonnes (resp. de lignes).

Définition 3.2 (Multiples) *Une matrice entière A est multiple d'une autre matrice entière B à gauche (resp. à droite) si B divise A à droite (resp. à gauche).*

Les definitions ci-dessus sont assez logiques si l'on se souvient qu'un diviseur à droite est placé *à droite* dans le produit, et que pour obtenir un multiple à gauche, on multiplie *à gauche*.

Nous allons maintenant nous intéresser aux conditions dans lesquelles deux matrices de même taille se divisent mutuellement. On commencera par étudier le cas des matrices carrées.

Lemme 3.1 Deux matrices entières carrées de rang plein se divisent mutuellement à droite (resp. à gauche) si et seulement si elles sont équivalentes à gauche (resp. à droite).

Preuve: la condition suffisante est triviale. Réciproquement, si on a $A = QB$ et $B = RA$, on en deduit que $\det(A)(1-\det(Q)\det(R)) = 0$; A étant de rang plein et l'anneau étant intègre, on en déduit que Q et R sont unimodulaires.

Nous allons maintenant lever l'hypothèse de rang plein sur les matrices carrées.

Lemme 3.2 Deux matrices entières carrées se divisent mutuellement à droite (resp. à gauche) si et seulement si elles sont équivalentes à gauche (resp. à droite).

Preuve: on s'occupera de la divisibilité à droite.

On commence par remarquer que deux matrices se divisent mutuellement si et seulement si leurs formes d'Hermite se divisent mutuellement. On se ramènera donc au cas de matrices triangulaires supériures.

La démonstration procède par récurrence sur la taille n des matrices, le résultat étant trivial pour $n = 1$. On considère maintenant deux matrices entières A et B, triangulaires supérieures, de taille $n+1$, et se divisant mutuellement à droite. Elles sont alors de même rang. Si ce rang vaut $n+1$, le résultat découle du lemme précédent.

Dans le cas contraire, on commence par remarquer que, du fait de la structure triangulaire et de la divisibilité réciproque, les $a_{i,i}$ et $b_{i,i}$ sont soit égaux à un inversible près, soit simultanément nuls. Notons i_0 le premier indice i tel $a_{i,i}$ soit nul. Trois cas sont à distinguer:

- $i_0 = 1$. Alors A est de la forme $\left[\begin{array}{cc} 0 & \tilde{A} \end{array}\right]$; il est de même pour B. On peut alors, en calculant une forme d'Hermite supérieure de $\tilde{A}$, se ramener au cas où A est de la forme:

$$A = \left[\begin{array}{cc} 0 & A_1 \\ 0 & 0 \end{array}\right] \tag{3.1}$$

On fait de même pour B. On voit facilement que A_1 et B_1 se divisent mutuellement à droite. Par récurrence, il existe donc U_1 unimodulaire telle que $U_1 A_1 = B_1$, d'où

$$\begin{bmatrix} U_1 & 0 \\ 0 & Id \end{bmatrix} \begin{bmatrix} 0 & A_1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & B_1 \\ 0 & 0 \end{bmatrix} \tag{3.2}$$

ce qui prouve la récurrence.

- $i_0 = n$. A est donc de la forme

$$A = \begin{bmatrix} A_1 & A_2 \\ 0 & 0 \end{bmatrix} \tag{3.3}$$

avec A_1 carrée, triangulaire supérieure, de rang plein; de même pour B. Il est alors facile de voir que A_1 et B_1 se divisent mutuellement. Soit Q telle que $QA = B$. En décomposant Q comme A et B, on a $Q_{1,1}A_1 = B_1$. Or, par définition de i_0, A_1 et B_1 sont carrés de rang plein; on en déduit que $Q_{1,1}$ est unimodulaire. Il ne reste plus qu'à poser

$$U = \begin{bmatrix} Q_{1,1} & 0 \\ Q_{2,1} & 1 \end{bmatrix} \tag{3.4}$$

pour prouver la récurrence.

- $1 < i_0 < n$. Alors A a la structure suivante:

$$A = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ 0 & 0 & A_{2,3} \\ 0 & 0 & A_{3,3} \end{bmatrix} \tag{3.5}$$

Par le produit à gauche d'une unimodulaire on se ramène au cas où $A_{2,3} = 0$ (forme d'Hermite sur les blocs colonnes de droite); on procède de manière analogue sur B. Soit Q telle que $QA = B$ et R telle que $RB = A$; on décompose Q et R comme A et B. On remarque que $Q_{2,1}A_{1,1}$ et $Q_{3,1}A_{1,1}$ sont nuls; $A_{1,1}$ étant carrée de rang plein, on en déduit que $Q_{2,1}$ et $Q_{3,1}$ sont nulles. $B_{1,2}$ (et $A_{1,2}$ par un raisonnement symétrique) est donc nulle. Soient d'autre part $\tilde{A}$ et $\tilde{B}$ les matrices extraites de A et B en rayant la i_0^{eme} colonne et la i_0^{eme} ligne (ligne et colonne "du milieu"). On constate alors assez facilement que $\tilde{A}$ et $\tilde{B}$ se divisent mutuellement à droite; il existe donc une unimodulaire $\tilde{U}$, que nous décomposerons en

$$\tilde{U} = \begin{bmatrix} U_{1,1} & U_{1,2} \\ U_{2,1} & U_{2,2} \end{bmatrix} \tag{3.6}$$

telle que $U\tilde{A} = \tilde{B}$. $A_{1,1}$ étant de rang plein, on a nécessairement $U_{2,1} = 0$.
Il ne reste plus qu'à poser

$$U = \begin{bmatrix} U_{1,1} & 0 & U_{1,2} \\ 0 & 1 & Q_{2,3} \\ 0 & 0 & U_{2,2} \end{bmatrix} \tag{3.7}$$

U est alors unimodulaire, et on a $UA = B$.

Théorème 3.1 (Divisibilité réciproque et équivalence) *Deux matrices entières A et B de même taille se divisent mutuellement à droite (resp. à gauche) si et seulement si elles sont équivalentes à gauche (resp. à droite).*

Preuve: on fera la preuve pour la division à droite. Deux cas sont à considérer:

- il ya plus de lignes que de colonnes.
  On se ramène alors à des formes d'Hermite supérieures. On notera T_M la partie triangulaire carrée de la forme d'Hermite de M. Il existe donc deux matrices Q et $\tilde{Q}$ telles que

$$\begin{bmatrix} T_A \\ 0 \end{bmatrix} = Q \begin{bmatrix} T_B \\ 0 \end{bmatrix} \quad \begin{bmatrix} T_B \\ 0 \end{bmatrix} = \tilde{Q} \begin{bmatrix} T_A \\ 0 \end{bmatrix} \tag{3.8}$$

  soit, en décomposant Q et $\tilde{Q}$ de manière adéquate:

$$\begin{bmatrix} T_A \\ 0 \end{bmatrix} = \begin{bmatrix} Q_{1,1}T_B \\ Q_{2,1}T_B \end{bmatrix} \quad \begin{bmatrix} T_B \\ 0 \end{bmatrix} = \begin{bmatrix} \tilde{Q}_{1,1}T_A \\ \tilde{Q}_{2,1}T_A \end{bmatrix} \tag{3.9}$$

  On en déduit, d'après le lemme précédent, qu'il existe une matrice unimodulaire U_1 telle que $T_A = U_1 T_B$. Il suffit alors de poser

$$U = \begin{bmatrix} U_1 & 0 \\ Q_{2,1} & Id \end{bmatrix} \tag{3.10}$$

  pour aboutir au résultat.

- il y a moins de lignes que de colonnes.
  On note S une forme de Smith de B. Il existe donc deux matrices Q et $\tilde{Q}$, deux unimodulaires U_1 et V_1 telles que

$$A = QB \quad B = \tilde{Q}A \quad B = U_1 S V_1 \tag{3.11}$$

  Posons $\tilde{A} = AV_1^{-1}$. On a alors

$$\tilde{A} = QU_1 S \quad S = U_1^{-1}\tilde{Q}\tilde{A} \tag{3.12}$$

  En décomposant $\tilde{A}$ en $[A_1, A_2]$ et S en $[S_1, 0]$, avec A_1 et S_1 carrées, les égalités précédentes sont équivalentes à:

$$A_2 = 0 \quad A_1 = QU_1 S_1 \quad S_1 = U_1^{-1}\tilde{Q}A_1 \tag{3.13}$$

  Il existe donc une unimodulaire U telle que $A_1 = US_1$, d'où $\tilde{A} = US$, soit encore $A = UU_1^{-1}B$.

3.2 PGCD

Définition 3.3 (diviseurs communs, PGCD) *Une matrice entière R est un diviseur commun à droite (resp. à gauche) de deux matrices entières A et B si et seulement si R divise A et B à droite (resp. à gauche).*

R est un PGCD à droite (resp. à gauche) de A et B si et seulement si R est un diviseur commun à droite (resp. à gauche) de A et B, multiple à gauche (resp. à droite) de tous les autres.

A et B sont premières entre elles à droite (resp. à gauche) si et seulement si l'identité est un PGCD à droite (resp. à gauche) de A et B.

Lemme 3.3 Si R est un diviseur commun à droite (resp. à gauche) de A et B et si il existe X et Y tels que $XA+YB$ (resp. $AX+BY$) $= R$, alors R est un PGCD à droite (resp. à gauche) de A et B.

Preuve: procéder comme dans le cas d'un anneau.

Théorème 3.2 (Hermite = PGCD) *Soient A et B deux matrices entières. Alors toute forme d'Hermite supérieure (resp. inférieure) de $\begin{bmatrix} A \\ B \end{bmatrix}$ (resp. $[A, B]$) est un PGCD à droite (resp. à gauche) de A et B.*

Preuve: comme d'habitude, on ne traitera que la division à droite.

Soit H une forme d'Hermite de $\begin{bmatrix} A \\ B \end{bmatrix}$. Alors il existe une unimodulaire U telle que

$$U \begin{bmatrix} A \\ B \end{bmatrix} = H \tag{3.14}$$

En décomposant U en $[U_1, U_2]$, on obtient

$$U_1 A + U_2 B = H \tag{3.15}$$

D'autre part, en décomposant U^{-1} en $\begin{bmatrix} V_1 \\ V_2 \end{bmatrix}$, on a visiblement

$$A = V_1 H \quad B = V_2 H \tag{3.16}$$

d'où le résultat.

Remarques:

- ce résultat prouve l'existence de PGCD pour deux matrices entières quelconques.
- dans le cas où la matrice $\begin{bmatrix} A \\ B \end{bmatrix}$ (resp. $[A, B]$) compte plus de lignes que de colonnes (resp. plus de colonnes que de lignes), toute forme d'Hermite supérieure (resp. inférieure) H est de la forme $\begin{bmatrix} R \\ 0 \end{bmatrix}$ (resp. $[R, 0]$).

  Il est alors facile de voir que R **est un PGCD carré** de A et B, et que tous les PGCD carrés à droite (resp. à gauche) sont équivalents à gauche (resp. à droite), puisqu'ils sont de même taille et se divisent mutuellement à droite (resp. à gauche). On peut donner dans ce cas un sens à l'unicité du PGCD en se limitant aux PGCD carrés, l'unicité étant de toute façon toujours entendue à une unimodulaire près.

- bien qu'en fait on établisse ici des résultats classiques d'anneaux principaux, nous n'avons pas cherché à mettre une structure explicite d'anneau sur les matrices entières. En effet, il nous faudrait nous limiter au cas des matrices carrées de taille fixe. Ceci n'est absolument pas réaliste dans la mesure où tout l'intérêt des changements de formes opérateur consiste justement à faire varier la taille des matrices; de plus, les matrices en question sont rarement carrées. Enfin, et comme on a pu le constater, les résultats en question se laissent montrer sans difficulté supplémentaire dans le cas général.

Théorème 3.3 (Identité de Bezout) *R est un PGCD à droite (resp. à gauche) de A et B si et seulement si R est un diviseur commun à droite (resp. à gauche) de A et B et si il existe X et Y tels que $XA+YB$ (resp. $AX+BY$) $= R$.*

Preuve: la condition suffisante à été vue.

Pour la condition nécessaire (on considère encore la division à droite), il suffit de considérer une forme d'Hermite supérieure H de $\begin{bmatrix} A \\ B \end{bmatrix}$. Il existe alors X et Y tels que $XA+YB = H$. Si R est un PGCD à droite de A et B, H, en tant que diviseur commun, divise R à droite. Il existe donc T tel que $R = TH$, d'où

$$TXA + TYB = TH = R \tag{3.17}$$

d'où le résultat.

Corollaire 3.1 A et B sont donc premiers entre eux à droite (resp. à gauche) si et seulement si il existe X et Y tels que $XA+YB = Id$ (resp. $AX+BY = Id$).

Remarque: si A et B sont premiers entre eux à droite , alors la matrice $\begin{bmatrix} A \\ B \end{bmatrix}$ est nécessairement injective[1], puisqu'on a $XA+YB = Id$. En particulier cette matrice doit contenir plus de lignes que de colonnes. De même, si A et B sont premiers entre eux à gauche, alors la matrice $[A, B]$ est surjective, et doit donc contenir plus de colonnes que de lignes.

3.3 Variations sur l'identité de Bezout

Théorème 3.4 (Sous-matrices d'une unimodulaire) *Soit $U = \begin{bmatrix} U_{1,1} & U_{1,2} \\ U_{2,1} & U_{2,2} \end{bmatrix}$ une matrice unimodulaire. Alors*

- *$U_{1,1}$ et $U_{2,1}$ sont premières entre elles à droite*
- *$U_{1,2}$ et $U_{2,2}$ sont premières entre elles à droite*
- *$U_{1,1}$ et $U_{1,2}$ sont premières entre elles à gauche*
- *$U_{2,1}$ et $U_{2,2}$ sont premières entre elles à gauche*

Preuve: Il suffit d'appliquer l'identité de Bezout en utilisant l'inverse de U.

Théorème 3.5 *A et B sont premières entre elles à droite (resp. à gauche) si et seulement si il existe une unimodulaire U telle que $U \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} Id \\ 0 \end{bmatrix}$ (resp. $[A, B]U = [Id, 0]$)*

[1] on plonge l'anneau dans le corps des fractions

Preuve: la partie suffisante résulte de Bezout.

Quant à la partie nécessaire, on sait que A et B ont nécessairement suffisamment de lignes (resp. de colonnes) pour que les formes d'Hermite de $\begin{bmatrix} A \\ B \end{bmatrix}$ (resp. $[A, B]$) soient de la forme $\begin{bmatrix} R \\ 0 \end{bmatrix}$ (resp. $[R, 0]$), où R est un PGCD carré. Tous les PGCD carrés étant équivalents du bon côté, on en déduit que R est unimodulaire. Il suffit alors de multiplier par $\begin{bmatrix} R^{-1} & 0 \\ 0 & Id \end{bmatrix}$ pour conclure.

Corollaire 3.2 soit A et B première entre elles à droite (resp. à gauche). Alors il existe $\tilde{A}$ et $\tilde{B}$, premières entre elles à gauche (resp. à droite) telles que $\tilde{B}A = \tilde{A}B$ (resp. $B\tilde{A} = A\tilde{B}$).

Preuve: considérer le bloc ligne inférieur (resp. bloc colonne droit) de l'unimodulaire U.

Théorème 3.6 (Bezout = inversion) *A et B sont premières entre elles à droite (resp. à gauche) si et seulement si il existe $\tilde{X}$ et $\tilde{Y}$ tels que $\begin{bmatrix} A & -\tilde{Y} \\ B & \tilde{X} \end{bmatrix}$ (resp. $\begin{bmatrix} A & B \\ -\tilde{Y} & \tilde{X} \end{bmatrix}$) soit unimodulaire.*

Preuve: la partie suffisante résulte du théorème 3.4.

Partie nécessaire: on considèrera la division à droite. On sait (théorème 3.5) qu'il existe une unimodulaire U telle que $U \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} Id \\ 0 \end{bmatrix}$. Soit V l'inverse de U, qu'on décompose en $\begin{bmatrix} V_{1,1} & V_{1,2} \\ V_{2,1} & V_{2,2} \end{bmatrix}$ de manière cohérente avec A et B. On vérifie alors sans peine que $-\tilde{Y} = V_{1,2}$ et $\tilde{X} = V_{2,2}$ répondent à question, la matrice ainsi constituée à partir de A et B étant égale à V, l'inverse de U.

Remarque: ce théorème montre bien que le calcul de l'identité de Bezout (lorsque les matrices sont premières entre elles) est bien un calcul d'*inverse*; en effet, une partie de l'inverse de la matrice unimodulaire "contenant" A et B est constituée des coefficients de Bezout sur ces deux matrices. En fait, l'identité de Bezout scalaire peut être elle-même considérée comme une inversion partielle de matrices 2×2 (c.f. entiers de Gauss).

Théorème 3.7 *Soient A, B, $\tilde{A}$, $\tilde{B}$ quatre matrices entières. Les deux propositions suivantes sont équivalentes:*

- – *A et B sont premières entre elles à droite*
  – *$\tilde{A}$ et $\tilde{B}$ sont premières entre elles à gauche*
  – *$\tilde{B}A = \tilde{A}B$*
- *il existe X, Y, $\tilde{X}$ et $\tilde{Y}$ tels que*

$$\begin{bmatrix} X & Y \\ -\tilde{B} & \tilde{A} \end{bmatrix} \begin{bmatrix} A & -\tilde{Y} \\ B & \tilde{X} \end{bmatrix} = \begin{bmatrix} Id & 0 \\ 0 & Id \end{bmatrix} \tag{3.18}$$

Preuve: condition suffisante: on a visiblement $\tilde{A}B = \tilde{B}A$; le reste découle de Bezout.

condition nécessaire: il existe X et Y, $\tilde{X}_1$, $\tilde{Y}_1$ tels que $XA + YB = Id$, $\tilde{A}\tilde{X}_1 + \tilde{B}\tilde{Y}_1 = Id$. On a alors

$$\begin{bmatrix} X & Y \\ -\tilde{B} & \tilde{A} \end{bmatrix} \begin{bmatrix} A & -\tilde{Y}_1 \\ B & \tilde{X}_1 \end{bmatrix} = \begin{bmatrix} Id & C \\ 0 & Id \end{bmatrix} \tag{3.19}$$

où C est une matrice entière. On en déduit le résultat en inversant la matrice de droite et en prenant $\tilde{X} = \tilde{X}_1 - BC$, $\tilde{Y} = \tilde{Y}_1 + AC$.

3.4 Solution générale de l'Identité de Bezout

Théorème 3.8 *Soit A et B premières entre elles à droite (resp. à gauche), et $U = \begin{bmatrix} U_1 & U_2 \\ U_3 & U_4 \end{bmatrix}$ unimodulaire telle que $U \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} Id \\ 0 \end{bmatrix}$ (resp. $\begin{bmatrix} A & B \end{bmatrix} U = \begin{bmatrix} Id & 0 \end{bmatrix}$)*

Alors X et Y sont solution de l'identité de Bezout $XA + YB = Id$ (resp. $AX + BY = Id$) si et seulement si il existe une matrice entière Π telle que

$$\begin{array}{rcl} X & = & U_1 + \Pi U_3 \\ Y & = & U_2 + \Pi U_4 \end{array} \tag{3.20}$$

(resp.

$$\begin{array}{rcl} X & = & U_1 + U_2 \Pi \\ Y & = & U_3 + U_4 \Pi \end{array} \tag{3.21}$$

)

Preuve: On traitera le cas de matrices premières entre elles à droite.

Décomposons $\begin{bmatrix} X & Y \end{bmatrix} U^{-1}$ en $\begin{bmatrix} R & \Pi \end{bmatrix}$. Alors X et Y vérifient $XD + YN = Id$ si et seulement si

$$\begin{bmatrix} R & \Pi \end{bmatrix} U \begin{bmatrix} A \\ B \end{bmatrix} = Id \tag{3.22}$$

c'est-à-dire $R = Id$. On en déduit que $\begin{bmatrix} X & Y \end{bmatrix} = \begin{bmatrix} Id & \Pi \end{bmatrix} U$, d'où le résultat.

Théorème 3.9 *Soit A et B premières entre elles à droite (resp. à gauche). Soit X_0 et Y_0 une solution particulière de l'identité de Bezout associée. Alors*

- *il existe $\tilde{A}$ et $\tilde{B}$ premières entre elles à gauche (resp. à droite) telles que $\tilde{B}A = \tilde{A}B$ (resp. $B\tilde{A} = A\tilde{B}$)*
- *soient $\tilde{A}$ et $\tilde{B}$ un couple de matrices satisfaisant à la condition précédente; un couple (X, Y) de matrices entières est solution de l'identité de Bezout associée à A et B si et seulement si il existe Π entière telle que*

$$\begin{array}{rcl} X & = & X_0 + \Pi \tilde{B} \\ Y & = & Y_0 - \Pi \tilde{A} \end{array} \tag{3.23}$$

(resp.

$$\begin{array}{rcl} X & = & X_0 + \tilde{B} \Pi \\ Y & = & Y_0 - \tilde{A} \Pi \end{array} \tag{3.24}$$

)

Preuve: On traitera le cas de matrices premières entre elles à droite.

L'existence de $\tilde{A}$ et $\tilde{B}$ résulte du corollaire 3.2; on peut la prouver de manière indépendante lorsque A est carrée de rang plein en factorisant à gauche la fraction BA^{-1} (c.f. chapitre suivant).

En utilisant la preuve du théorème 3.7 on déduit que $\begin{bmatrix} X_0 & Y_0 \\ -\tilde{B} & \tilde{A} \end{bmatrix}$ est une unimodulaire telle que $U \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} Id \\ 0 \end{bmatrix}$.

La preuve découle alors directement du théorème 3.8.

3.5 Rang du PGCD

Théorème 3.10 *soit R un PGCD à droite (resp. à gauche) de deux matrices entières P et Q. On plonge l'anneau dans son corps des fractions*[2]*. Alors:*

- $\ker R = \ker P \cap \ker Q = \ker \begin{bmatrix} P \\ Q \end{bmatrix}$
- *le rang de* $\begin{bmatrix} P \\ Q \end{bmatrix}$ *est égal au rang de* R.

(resp.

- $Im\ R = Im\ P + Im\ Q = Im \begin{bmatrix} P & Q \end{bmatrix}$
- *le rang de* $\begin{bmatrix} P & Q \end{bmatrix}$ *est égal au rang de* R.

)

Preuve: On se limitera à la division à droite.

Comme R divise P et Q à droite, tout élément du noyau de R est dans le noyau de P et dans le noyau de Q. L'inclusion inverse se déduit de l'identité de Bezout. On a donc

$$\ker R = \ker P \cap \ker Q = \ker \begin{bmatrix} P \\ Q \end{bmatrix} \tag{3.25}$$

Comme R et $\begin{bmatrix} P \\ Q \end{bmatrix}$ ont nécessairement le même nombre de colonnes, on conclut à l'égalité des rangs.

Pour la division à gauche, on transpose tout.

Remarque: la propriété précédente n'est en aucun cas caractéristique de R; pour s'en convaincre, on peut se reporter à l'exemple cité à propos du corollaire qui suit.

Corollaire 3.3 On se donne un corps commutatif $\mathcal{K}$ et on prend comme anneau l'anneau euclidien $\mathcal{K}[s]$ des polynômes à coefficients dans $\mathcal{K}$. On suppose que les matrices polynômiales $P(s)$ et $Q(s)$ sont telles que $\begin{bmatrix} P \\ Q \end{bmatrix}$ ait plus de lignes que de colonnes (pour la division à droite) ou telles que $\begin{bmatrix} P & Q \end{bmatrix}$ ait plus de colonnes que de lignes (pour la division à gauche); c'est le cas si P est carrée. Soit R un PGCD carré à droite (resp. à gauche) de P et Q, s un élément de $\mathcal{K}$. Alors les deux conditions suivantes sont équivalentes:

- s est un zéro de $\det(R)$
- $\begin{bmatrix} P(s) \\ Q(s) \end{bmatrix}$ (resp. $\begin{bmatrix} P(s) & Q(s) \end{bmatrix}$), en tant que matrice à éléments dans $\mathcal{K}$, n'est pas de rang plein.

En particulier, P et Q sont premières entre elles à gauche (resp. à droite) si et seulement si $\begin{bmatrix} P(s) & Q(s) \end{bmatrix}$ (resp. $\begin{bmatrix} P(s) \\ Q(s) \end{bmatrix}$) est de rang plein pour tout s.

Remarque: Il n'y par contre aucun rapport entre l'ordre de multiplicité du zéro s et la dimension du noyau. Pour s'en convaincre, il suffit de remarquer que l'ordre de multiplicité en question n'est nullement borné par la taille des matrices. Ainsi, dans le cas scalaire, en prenant

[2] pour simplifier les choses, on ignore les modules dans ce cours

$p(s) = q(s) = (s-1)^2$, $(s-1)^2$ est un PGCD carré dont 1 est un zéro double, alors que la dimension du noyau ne peut depasser 1. On remarquera d'ailleurs que tout polynôme ayant 1 comme zéro vérifie les propriétés du théorème et du corollaire précédents.

Il est par contre vrai que le rang de $R(s)$ est toujours égal à celui de $\begin{bmatrix} P(s) \\ Q(s) \end{bmatrix}$.

Chapitre 4

Matrices rationnelles

Après avoir étudié les matrices entières, c'est-à-dire à éléments dans un anneau, nous allons passer dans ce chapitre à l'étude des matrices *rationnelles*, c'est-à-dire à éléments dans le corps des fractions associé. On commencera par montrer que ces *matrices de fractions* sont également des *fractions de matrices entières* en mettant celles-ci sous la forme ND^{-1}, $D^{-1}N$ et $N_gD^{-1}N_d$.

Puis on montrera l'existence de représentants irréductibles de ces fractions; on montrera que ces réprésentations irréductibles sont uniques à un inversible près, tout au moins en ce qui concerne les représentations unilatérales.

On montrera, dans le cas polynômial, que les pôles des *éléments* d'une matrice rationnelle sont exactement les valeurs qui rendent singulier le dénominateur des factorisations irréductibles, mettant ainsi en évidence la correspondance entre les singularités des matrices de fractions et celles des fractions de matrices.

Le reste du chapitre est consacré à l'étude, dans le cas euclidien et plus spécialement polynômial, des *fractions rationnelles propres*: ce sont des fractions rationnelles dont le degré du dénominateur est supérieur à celui du numérateur. Cette propriété est liée, en théorie des systèmes, à des problèmes de régularité ou de causalité : on exige en général d'un transfert qu'il soit propre pour considérer qu'il représente bien un processus physique. Comme nous le verrons plus tard, cette propriéré est équivalente à l'existence d'une forme d'état (au sens classique du terme) possédant ce transfert. Bien qu'il n'existe pas de notion satisfaisante de degré pour les matrices euclidiennes, on définira une *division euclidienne* sur les matrices, en exigeant du reste qu'il soit strictement propre. En un sens, on aura alors une notion affaiblie de degré qui, au lieu d'induire un ordre total, reposera sur un ordre partiel.

Puis on étudiera, dans le cas polynômial, comment caractériser les matrices rationnelles propres (qui sont alors vues comme matrices de fractions) lorsque celles-ci sont représentées sous forme de fractions de matrices. Alors que cette caractérisation, dans le cas scalaire, repose sur la simple comparaison des degrés des deux termes de la fraction, il convient de comparer, dans le cas matriciel, deux n^{uples} de degrés[1]. On ne peut donc dans ce cas s'abstraire de la géométrie propre aux matrices considérées.

[1] la comparaison s'effectuant terme à terme, il s'agit donc bien d'un ordre partiel

4.1 Matrices rationnelles dans le cas général

4.1.1 Définition

Définition 4.1 (matrices rationnelles) *Une matrice rationnelle est une matrice dont les éléments sont dans le corps des fractions rationnelles associé à l'anneau $\mathcal{A}$ (principal ou euclidien suivant les cas).*

4.1.2 Factorisation

Théorème 4.1 (factorisation) *Toute matrice rationnelle T peut se factoriser à gauche (resp. à droite) sous la forme $D^{-1}N$ (resp. ND^{-1}), où N et D sont des matrices entières, et où D est carrée de rang plein.*

Preuve: il suffit de considérer un dénominateur commun d à tous les éléments de T, et de prendre $N = dT$ et $D = d \times Id$.

Remarque: en un sens, on définit ici la notion de *fraction matricielle* par la paire (N, D). Nous allons passer une bonne partie de ce chapitre à étudier les relations liant les représentations d'une matrice rationnelle sous forme de matrice de fractions et ses représentations sous forme de fraction de matrices.

Corollaire 4.1 Toute matrice rationnelle T peut se factoriser sous la forme $N_d D^{-1} N_g$, où N_g, N_d et D sont des matrices entières, et où D est carrée de rang plein. On parle de bifactorisation.

Preuve: : prendre un des deux numérateurs égal à l'identité.

Théorème 4.2 (factorisation irréductible) *Toute matrice rationnelle T peut se factoriser à gauche (resp. à droite) sous la forme $D^{-1}N$ (resp. ND^{-1}), où N et D sont des matrices entières, D carrée de rang plein, avec N et D premières entre elles à gauche (resp. à droite).*

La première forme est dite factorisation irréductible à gauche, la seconde, factorisation irréductible à droite.

Preuve: il suffit de calculer un PGCD des N et D précédents et de simplifier.

Corollaire 4.2 Toute matrice rationnelle T peut se bifactoriser sous la forme $N_d D^{-1} N_g$, où N_d et D sont premières entre elles à droite, et N_g et D sont premières entre elles à gauche. On parle de bifactorisation irréductible.

Théorème 4.3 (unicité des factorisations irréductibles) *Soit $D^{-1}N$ (resp. ND^{-1}) une factorisation irréductible à gauche (resp. à droite) de T. Alors $D_1^{-1}N_1$ (resp. $N_1 D_1^{-1}$) est une factorisation irréductible à gauche (resp. à droite) de T si et seulement si il existe une matrice unimodulaire U telle que $N_1 = UN$ et $D_1 = UD$ (resp. $N_1 = NU$ et $D_1 = DU$).*

Preuve: : la partie suffisante est triviale.

La partie nécessaire se montre à peu près comme dans le cas scalaire. On considère deux factorisations à droite irréductibles ND^{-1} et $N_1 D_1^{-1}$. Il existe alors X et Y tels que $XN + YD = Id$. On en déduit que $DXND^{-1} + DY = Id$, d'où $DXN_1 + DYD_1 = D_1$; D divise donc D_1 à gauche; un raisonnement symétrique montre que D_1 divise D à gauche. D et D_1 sont donc équivalentes à droite, et il existe alors une unimodulaire U telle que $D_1 = DU$. De $ND^{-1} = N_1 D_1^{-1}$ on déduit alors que $N_1 = NU$.

Attention: ce resultat ne se transpose pas au cas de la bifactorisation. En effet, la latitude qui nous est laissée de répartir des termes entre la gauche et la droite est un obstacle à l'unicité au sens habituel d'un anneau. Pour prendre un exemple trivial, une matrice entiere M se

bifactorise de manière irréductible en $M.Id^{-1}.Id$ et $Id.Id^{-1}.M$, alors que M peut très bien ne pas être carrée, *a fortiori* unimodulaire. Plus généralement, les factorisations irréductibles à gauche et à droite *sont* des bifactorisations irréductibles.

Une conséquence intéressante de cette remarque réside dans le fait que le problème de la bifactorisation (irréductible ou non) ne se ramène pas au cas de la factorisation simple.

Théorème 4.4 (factorisation irréductible d'une matrice entière) *Soit T une matrice rationnelle et $D^{-1}N$ (resp. ND^{-1}) une factorisation irréductible à gauche (resp. à droite) de T. Alors T est entière si et seulement si D est unimodulaire.*

Preuve: elle suit le cas scalaire.

La condition suffisante est triviale.

Réciproquement, soit une factorisation à gauche irréductible $D^{-1}N$ de T. Il existe alors X et Y telles que $DX + NY = Id$. On en déduit que $D^{-1} = X + TY$; D^{-1} est donc entière, ce qui prouve le résultat.

Théorème 4.5 (bifactorisation irréductible d'une matrice entière) *Soit T une matrice rationnelle et $N_d D^{-1} N_g$ une bifactorisation irréductible de T. Alors T est entière si et seulement si D est unimodulaire.*

Preuve: analogue à la précédente. On commence par écrire les identités de Bezout $X_d D + Y_d N_d = Id$ et $DX_g + N_g Y_g = Id$, pour en déduire que $X_d + Y_d N_d X_g + Y_d T Y_g = D^{-1}$.

4.1.3 Pôles d'une matrice rationnelle (cas polynômial)

On suppose dans cette section que l'anneau utilisé est un anneau de polynômes sur un corps $\mathcal{K}$.

On rappelle que, dans le cas scalaire, un élément s_0 du corps $\mathcal{K}$ est un pôle d'une fraction rationnelle $r(s)$ si s_0 est une racine du dénominateur q d'une représentation irréductible $\frac{p(s)}{q(s)}$ de $r(s)$; cette définition est d'ailleurs indépendante du choix de la représentation irreductible[2]. Etendons cette définition au cas matriciel:

Définition 4.2 (Pôles d'une matrice rationnelle) *Soit $T(s)$ une matrice rationnelle sur $\mathcal{K}(s)$. Un élément s_0 de $\mathcal{K}$ est un pôle de T si s_0 est un pôle d'un des éléments de T.*

Cette définition utilise la représentation d'une matrice rationnelle comme "matrice de fractions". Nous allons montrer que cette définition à un analogue lorsqu'on passe au point de vue "fraction de matrices", et ce, par le biais des factorisations irréductibles. Commençons par un lemme:

Lemme 4.1 Soit P une matrice polynômiale carrée de rang plein. Alors un élément s_0 de $\mathcal{K}$ est un pôle de P^{-1} si et seulement si s_0 est un zéro de $\det P$.

Preuve:

- condition nécessaire: P^{-1} est égal au quotient d'une matrice polynômiale par $\det P$. L'ensemble des pôles de P^{-1} est donc contenu dans l'ensemble des zéros de $\det P$.
- condition suffisante: on a $\det P \det P^{-1} = 1$. D'autre part, P^{-1} est égal aux quotient de P_c^T, matrice transposée des cofacteurs de P, qui est polynômiale, par $\det P$, soit

$$P^{-1} = \det(P^{-1}) P_c^T \tag{4.1}$$

[2]puisqu'elles sont toutes égales à une constante près

On en déduit que P_c^T est unimodulaire. En particulier, s_0 ne peut être un zéro commun à tous les éléments de P_c^T. On en déduit que s_0 est un pôle d'au moins un des éléments de P^{-1}, c'est-à-dire un pôle de P^{-1}.

Passons au vif du sujet:

Théorème 4.6 (Pôles et factorisations irréductibles) *Soit T une matrice rationnelle sur $\mathcal{K}(s)$ et $D^{-1}N$ (resp. ND^{-1}) une factorisation irréductible à gauche (resp. à droite) de T. Alors un élément s_0 de $\mathcal{K}$ est un pôle de T si et seulement si s_0 est un zéro du déterminant de D.*

Preuve: on traitera la factorisation à gauche. On sait qu'il existe deux matrices polynômiales X et Y telle que la matrice

$$\begin{bmatrix} D & N \\ X & Y \end{bmatrix} \tag{4.2}$$

soit unimodulaire. Or on a

$$\begin{bmatrix} Id & D^{-1}N \\ X & Y \end{bmatrix} = \begin{bmatrix} D^{-1} & 0 \\ 0 & Id \end{bmatrix} \begin{bmatrix} D & N \\ X & Y \end{bmatrix} \tag{4.3}$$

le produit de droite étant par ailleurs l'inverse d'une matrice polynômiale carrée dont le déterminant est égal à celui de D; ses pôles sont donc les zéros de $\det D$. D'autre part, les pôles de la matrice de gauche sont visiblement ceux de T: cela prouve le résultat.

4.2 Matrices rationnelles dans le cas euclidien

4.2.1 Préliminaires

Lemme 4.2 soit $\mathcal{A}$ un anneau euclidien, $\mathcal{K}$ le corps des fractions associé, r un élément non nul de $\mathcal{K}$, $\frac{p_1}{q_1}$ et $\frac{p_2}{q_2}$ deux représentations irréductibles de r. Alors p_1 et p_2 sont égaux à un inversible près, q_1 et q_2 sont égaux à un inversible près.

Preuve: : laissée au lecteur.

On en déduit que sur l'ensemble des représentations irréductibles de r, les degrés du numérateur et du dénominateur sont constants. On appelera ceux-ci respectivement "degré du numérateur" et "degré du dénominateur" de r.

Définition 4.3 (fraction rationnelle scalaire propre) *Une fraction rationnelle non nulle de $\mathcal{K}$ est dite (strictement) propre si le degré de son dénominateur est supérieur (strictement) à celui de son numérateur.*

Par convention, 0 est propre et strictement propre[3]*.*

Si $\mathcal{A}$ est un anneau de polynômes, les fractions rationnelles propres forment un anneau euclidien (voir exercice).

Dans le cas où $\mathcal{A} = \mathrm{R}[s]$ ou $\mathrm{C}[s]$, une fraction rationnelle est propre (resp. strictement propre) si et seulement si elle est bornée (resp. nulle) à l'infini.

Théorème 4.7 *La seul entier strictement propre est 0.*

Preuve: soit n un entier; $\frac{n}{1}$ est une représentation irréductible de n; si n est non nul, on a $\deg(n) \geq 0 = \deg(1)$.

Ces quelques résultats étant présentés, nous pouvons passer à la définition des *matrices* rationnelles propres.

[3]ce qui logique si on convient d'affecter le degré $-\infty$ à 0

4.2.2 Définition

Définition 4.4 (matrices rationnelles propres) *Une matrice rationnelle (strictement) propre est une matrice dont les éléments sont des fractions rationnelles (strictement) propres.*

4.2.3 Division euclidienne de matrices

Nous n'avons pas défini le degré d'une matrice. En fait il n'existe pas de notion satisfaisante de degré dans ce cas. Il existe par contre une notion de "division euclidienne", que nous allons présenter ici.

Théorème 4.8 (Division euclidienne de matrices) *Soit D une matrice euclidienne carrée régulière, N une matrice euclidienne ayant le même nombre de colonnes (resp. de lignes) que D. Alors il existe un couple de matrices entières (Q, R) tel que:*

- $N = QD + R$
- RD^{-1} *est strictement propre*

(resp.

- $N = DQ + R$
- $D^{-1}R$ *est strictement propre*

)

Dans le cas polynômial[4]*, le couple (Q, R) est unique.*
On parle de division euclidienne à droite (resp. à gauche).

Preuve: on traitera la division à droite.

a) existence: soit $T = ND^{-1}$, d'élément courant $\frac{\alpha_{i,j}}{\beta_{i,j}}$, la représentation précédente étant choisie irréductible. Posons une division euclidienne de $\alpha_{i,j}$ par $\beta_{i,j}$, soit $\alpha_{i,j} = q_{i,j}\beta_{i,j} + r_{i,j}$, c'est-à-dire $\frac{\alpha_{i,j}}{\beta_{i,j}} = q_{i,j} + \frac{r_{i,j}}{\beta_{i,j}}$. Notons T_{sp} la matrice rationnelle d'élément courant $\frac{r_{i,j}}{\beta_{i,j}}$. Alors T_{sp} est strictement propre, puisque $\frac{r_{i,j}}{\beta_{i,j}}$ est irréductible ou nulle, et que le degré de $r_{i,j}$[5] est inférieur strict à celui de $\beta_{i,j}$. Il suffit alors de poser Q la matrice d'élement courant $q_{i,j}$ et $R = T_{sp}D$; on a $ND^{-1} = Q + T_{sp}$, soit $N = QD + R$, avec RD^{-1} strictement propre et R entière puisque N et QD le sont.

b) unicité: soit deux divisions euclidiennes

$$N = Q_1D + R_1 \tag{4.4}$$
$$N = Q_2D + R_2 \tag{4.5}$$

On a alors $(R_1 - R_2)D^{-1}$ qui est strictement propre (dans le cas présent, les strictement propres forment un groupe additif) et entière, car égale à $Q_1 - Q_2$; d'où $R_1 = R_2$, $Q_1 = Q_2$.

Remarque: dans le cas où la dividion euclidienne est obtenue par la méthode précédente, $r_{i,j}$ ne peut être nul lorsque $\alpha_{i,j}$ ne l'est pas, puisque la fraction $\frac{\alpha_{i,j}}{\beta_{i,j}}$ est irréductible. C'est évidemment vrai dans le cas pôlynomial, puisque le reste est unique.

[4] il suffit en fait que les fractions rationnelles propres forment un groupe additif; on trouvera un exemple de conditions suffisantes en exercice

[5] pour $r_{i,j}$ non nul

On se donne maintenant un corps commutatif $\mathcal{K}$, et dans tout ce qui suit on prend comme anneau euclidien l'anneau des polynômes $\mathcal{K}[s]$, auquel on associe le corps des fractions rationnelles $\mathcal{K}(s)$. Par matrice rationnelle on entendra désormais une matrice à éléments dans $\mathcal{K}(s)$.

4.3 Matrices polynômiales propres

4.3.1 Définitions

Définition 4.5 (matrices par degré) *Soit M une matrice polynômiale. Le i^{eme} degré ligne (resp. colonne) de M est le degré maximal des éléments de la i^{eme} ligne (resp. colonne) de M; on le notera ∂l_i (resp. ∂c_i).*

La matrice par degrés ligne (resp. colonne) extraite de M est la matrice dans laquelle on a remplacé l'élément courant $m_{i,j}$ de M par le coefficient du terme de degré ∂l_i (resp. ∂c_i) de $m_{i,j}$. C'est une matrice à éléments dans $\mathcal{K}$.

Remarques:

- lorsqu'une ligne (ou une colonne) est nulle, on convient de lui attribuer le degré 0. La ligne correspondante de la matrice par degrés ligne (ou colonne) est alors nulle.
- la définition de degré ligne et de degré colonne s'étend bien sûr au cas d'un anneau euclidien général.

Définition 4.6 (matrices propres) [6] *Une matrice polynômiale carrée est dite ligne (resp. colonne) propre si sa matrice par degrés ligne (resp. colonne) est de rang plein.*

Exemple: soit la matrice polynômiale

$$M(s) = \begin{bmatrix} s^2-3 & 1 & 2s \\ 4s+2 & 2 & 0 \\ -s^2 & s+3 & -3s+2 \end{bmatrix} \tag{4.6}$$

On a

$$\begin{array}{lll} \partial l_1 = 2 & \partial l_2 = 1 & \partial l_3 = 2 \\ \partial c_1 = 2 & \partial c_2 = 1 & \partial c_3 = 1 \end{array} \tag{4.7}$$

Les matrices par degrés ligne Γ_l et par degrés colonne Γ_c valent

$$\Gamma_l = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \quad \Gamma_c = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ -1 & 1 & -3 \end{bmatrix} \tag{4.8}$$

M n'est donc ni ligne propre, ni colonne propre; elle est pourtant de rang plein, puisque son déterminant (à une constante près) vaut $3s^3 + 22s^2 + 14s - 8$.

Remarque: on notera par la suite Γ_l (resp. Γ_c) les matrices par degrés ligne (resp. colonne).

[6] Nous sommes bien conscient du risque de confusion qui existe entre matrices polynômiales propres et matrices rationnelles propres; il s'agit malheureusement de la terminologie consacrée.

4.3.2 Propriétés

Théorème 4.9 (degré du déterminant) *Soit M une matrice polynômiale carrée. On a alors*[7]

$$\begin{array}{l} \deg(\det(M)) \leq \sum \partial l_i \\ \deg(\det(M)) \leq \sum \partial c_j \end{array} \tag{4.9}$$

et le terme de degré $\sum \partial l_i$ (resp. $\sum \partial c_j$) du déterminant de M est égal au déterminant de Γ_l (resp. Γ_c); soit:

- $\det(M(s)) = \det \Gamma_l \times s^{\sum \partial l_i}$ *+ termes de degrés inférieurs*
- $\det(M(s)) = \det \Gamma_c \times s^{\sum \partial c_j}$ *+ termes de degrés inférieurs*

Preuve: On ne traitera que les degrés ligne.

Soit n la taille de M; on suppose le résultat vrai pour $n-1$ et on developpe le déterminant de M suivant la première colonne. Pour cela, on pose:

- k_i le coefficient de degré ∂l_i de $m_{i,1}(s)$
- M_i la matrice extraite de M en rayant i^{eme} ligne et première colonne
- $d_{i,j}$ le degré de la j^{eme} ligne de M_i
- Γ_l la matrice par degrés ligne de M
- Γ_{l_i} la matrice extraite de Γ_l en rayant i^{eme} ligne et première colonne
- $\Gamma_l(M_i)$ la matrice par degrés ligne de M_i

On a alors

$$\begin{aligned} \det(M(s)) &= \sum_{i=1}^{i=n} (-1)^{i-1} m_{i,1}(s) \det(M_i(s)) \\ &= \sum_{i=1}^{i=n} (-1)^{i-1} k_i \det(\Gamma_l(M_i)) s^{\partial l_i + \sum_{j \neq i} d_{i,j}} + \textit{degrés inférieurs} \end{aligned}$$

On a toujours $\partial l_i + \sum_{j \neq i} d_{i,j}$ qui est inférieur à $\sum_{i=1}^{i=n} \partial l_i$, et l'égalité est réalisée si et seulement si on a $d_{i,j} = \partial l_j$ pour tous les j différents de i. Dans l'affirmative, on a alors $\Gamma_l(M_i) = \Gamma_{l_i}$; dans la négative, on a alors Γ_{l_i} qui contient une ligne nulle, et son déterminant est donc également nul. On en déduit que:

$$\begin{aligned} \det(M(s)) &= \sum_{\substack{i=1 \\ d_{i,j} = \partial l_j \ \forall j \neq i}}^{i=n} (-1)^{i-1} k_i \det(\Gamma_{l_i}) s^{\sum_{i=1}^{1=n} \partial l_i} + \textit{degrés inférieurs} \\ &= \sum_{i=1}^{i=n} (-1)^{i-1} k_i \det(\Gamma_{l_i}) s^{\sum_{i=1}^{1=n} \partial l_i} + \textit{degrés inférieurs} \\ &= \det \Gamma_l \times s^{\sum \partial l_1} + \textit{degrés inférieurs} \end{aligned}$$

Corollaire 4.3 une matrice carrée de rang plein est ligne (resp. colonne) propre si et seulement si le degré de son déterminant est égal à la somme de ses degrés de lignes (resp. colonne).

[7] si M n'est pas de rang plein, on convient de dire que $\deg(\det M)=0$

Théorème 4.10 ("lavage" de matrices) *Toute matrice polynômiale carrée de rang plein est*

- *ligne équivalente à une matrice ligne propre*
- *colonne équivalente à une matrice ligne propre*
- *ligne équivalente à une matrice colonne propre*
- *colonne équivalente à une matrice colonne propre*

Remarque: d'après le théorème précédent, la condition de rang plein est nécessaire.

Preuve: on ne traitera que la ligne équivalence.

Obtention d'une matrice colonne propre: le passage à une forme d'Hermite supérieure convient.

Obtention d'une matrice ligne propre: on utilise l'algorithme suivant:

a) $i = 0$, $M_0 = M$

b) si M_i est ligne propre ou si M_i n'est pas de rang plein, STOP.
Sinon, il existe une combinaison linéaire non triviale $\sum_{j=1}^{j=n} \lambda_j L_j$ des lignes L_j de $\Gamma_l(M_i)$ qui soit égale à zéro. On note l_j la j^{eme} ligne de M_i, ∂_{max} le plus grand degré ∂l_j tel que λ_j soit non nul, et on se donne j_0 tel que $\partial l_{j_0} = \partial_{max}$.
Remarquons que ∂_{max} est positif strict. En effet, si ce n'était pas le cas, alors toutes les lignes L_j telles que $\lambda_j \neq 0$ seraient égales aux lignes l_j correspondantes de M_i; on aurait alors $\sum_{j=1}^{j=n} \lambda_j l_j = 0$, et M_i ne serait pas de rang plein.
A la ligne l_{j_0} de M_i on ajoute alors la combinaison linéaire[8]
$\sum_{j \neq j_0} s^{\partial_{max} - \partial l_j} \frac{\lambda_j}{\lambda_{j_0}} l_j$.
Ceci est réalisable par opérations de lignes[9]. La ligne obtenue n'est pas nulle, puisque M_i est de rang plein. On a alors fait baisser strictement le degré de la ligne lj_0 en éliminant les termes de degré $\partial_{max} = \partial l_{j_0}$ de l_{j_0}. On a par ailleurs laissé inchangés les autres degrés ligne; on a donc fait baisser strictement la somme des degrés ligne.
On note M_{i+1} la matrice obtenue; M_{i+1} est de rang plein, car ligne équivalente à M_i. On fait ensuite $i = i + 1$, et on retourne en b).
Cet algorithme s'arrête en un nombre fini de coups; comme M_i est toujours de rang plein, cela prouve le résultat.

Interprétation: on prend $\mathcal{K} = \mathrm{R}$, et à l'indéterminée s on substitue l'opérateur différentiel $\frac{d}{dt}$. Si M n'est pas ligne propre ou colonne propre, cela signifie qu'on peut, soit par changements de variables différentiellemnt réversibles, soit par des combinaisons différentiellement réversibles d'équations, faire baisser l'ordre des opérateurs (ou des équations) différentiel(le)s.

Exemple: reprenons l'exemple présenté en début de section. On a

$$M(s) = \begin{bmatrix} s^2 - 3 & 1 & 2s \\ 4s + 2 & 2 & 0 \\ -s^2 & s + 3 & -3s + 2 \end{bmatrix} \quad \Gamma_l = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \tag{4.10}$$

La matrice Γ_l est singulière, avec $L_1 + L_3 = 0$. Les degrés ligne étant égaux, on remplace l_1 par $l_1 + l_3$ dans $M(s)$. On obtient:

$$M(s) = \begin{bmatrix} -3 & s + 4 & -s + 2 \\ 4s + 2 & 2 & 0 \\ -s^2 & s + 3 & -3s + 2 \end{bmatrix} \quad \Gamma_l = \begin{bmatrix} 0 & 1 & -1 \\ 4 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \tag{4.11}$$

[8] ∂l_j est toujours défini sans ambiguïté car aucune ligne ne peut être nulle, M_i étant de rang plein.

[9] pour $\lambda_j \neq 0$, on a $\partial l_j < \partial_{max}$

On a fait baisser le degré de la première ligne, mais Γ_l est encore singulière, puisqu'on a $L_2 + 4L_3 = 0$. La différence de degrés étant de 1 en faveur de l_3, on remplace cette dernière par $sl_2 + 4l_3$, et on obtient:

$$M(s) = \begin{bmatrix} -3 & s+4 & -s+2 \\ 4s+2 & 2 & 0 \\ 2s & 6s+12 & -12s+8 \end{bmatrix} \quad \Gamma_l = \begin{bmatrix} 0 & 1 & -1 \\ 4 & 0 & 0 \\ 2 & 6 & -12 \end{bmatrix} \tag{4.12}$$

ce qui fait baisser le degré de la troisième ligne. Γ_l est alors régulière et M ligne propre.

4.4 Caractérisation des matrices rationnelles propres

Il ne s'agit pas à proprement parler d'une caractérisation, dans la mesure où la condition suffisante est légèrement plus forte que la condition nécessaire; on y voit en particulier l'importance des matrices polynômiales propres.

Théorème 4.11 (Condition nécessaire) *Soit T une matrice (strictement) propre, et $D^{-1}N$ (resp. ND^{-1}) une factorisation à gauche (resp. à droite) de T. Alors chaque ligne (resp. colonne) non nulle de N a un degré (strictement) inférieur au degré de la ligne (resp. colonne) correspondante de D*[10].

Preuve: on traite la factorisation à gauche et le cas simplement propre; on laisse au lecteur le soin de substituer les signes d'inégalité pour le cas strictement propre.

On notera $m_{i,j}$ l'élément courant d'une matrice M.

Considérons la i^{eme} ligne de N, qu'on suppose non nulle, et $n_{i,j}$ un élément, également non nul, de cette ligne.

On a donc

$$n_{i,j} = \sum_k d_{i,k} t_{k,j} \tag{4.13}$$

Notons $I_{i,j}$ l'ensemble des indices k tels que $t_{k,j}$ et $d_{i,k}$ soient non nuls, et, pour un tel indice k, donnons-nous une représentation irréductible $\frac{p_{k,j}}{q_{k,j}}$ de $t_{k,j}$. Afin de ramener (4.13) à une expression polynômiale, on note $\tilde{q_j}$ le produit $\prod_k q_{k,j}$ et $\tilde{p}_{k,j}$ l'entier $t_{k,j}\tilde{q_j}$. On a alors

$$\tilde{p}_{k,j} q_{k,j} = p_{k,j} \tilde{q_j} \tag{4.14}$$

d'où

$$\begin{aligned} \deg(\tilde{p}_{k,j} q_{k,j}) &= \deg(p_{k,j}\tilde{q_j}) \\ &\leq \deg(q_{k,j}\tilde{q_j}) \end{aligned}$$

car toutes ces quantités sont non nulles; on en déduit que

$$\deg(\tilde{p}_{k,j}) \leq \deg(\tilde{q_j}) \tag{4.15}$$

On a d'autre part

$$n_{i,j}\tilde{q_j} = \sum_{k \in I_{i,j}} d_{i,k} \tilde{p}_{k,j} \tag{4.16}$$

[10]les degrés lignes (resp. colonne) de D sont définis, puisque D est de rang plein.

où toutes les quantiées mentionnées sont entières.

$$\begin{aligned}\deg(n_{i,j}) + \deg(\tilde{q}_j) &= \deg(\sum_{k\in I_{i,j}} d_{i,k}\tilde{p}_{k,j}) \\ &\leq \max_{k\in I_{i,j}}(\deg(d_{i,k}\tilde{p}_{k,j})) \\ &\leq \max_{k\in I_{i,j}}(\deg(d_{i,k}\tilde{q}_j)) \\ &\leq \partial l_i(D) + \deg(\tilde{q}_j)\end{aligned}$$

d'où $\deg(n_{i,j}) \leq \partial l_i(D)$, et le résultat en maximisant sur j.

Remarque: dans le cas strictement propre, on en déduit que $\partial l_i(D)$ est strictement positif lorsque la i^{eme} ligne de N est non nulle.

Théorème 4.12 (Condition suffisante) *On suppose D ligne (resp. colonne) propre. Alors la condition nécessaire précédente est aussi suffisante.*

Preuve: on traitera la factorisation à gauche.

Notons $D_{i,j}$ la matrice obtenue à partir de D en remplaçant la i^{eme} colonne par la j^{eme} colonne de N. On a alors

$$t_{i,j} = \frac{\det(D_{i,j})}{\det(D)} \tag{4.17}$$

Nous allons montrer que $t_{i,j}$ est propre. Si $t_{i,j}$ est nul, le résultat est trivial. Dans le cas contraire, on a $\det(D_{i,j})$ qui est non nul, avec

$$\deg(\det(D_{i,j})) \leq \sum_k \partial l_k(D_{i,j}) \tag{4.18}$$

$$\deg(\det(D)) = \sum_k \partial l_k(D) \tag{4.19}$$

puisque D est ligne propre. D'autre part, on a pour tout k:

$$\deg(n_{k,j}) \leq \partial l_k(N) \tag{4.20}$$

$$\leq \partial l_k(D) \tag{4.21}$$

On en déduit que, pour tout k,

$$\begin{aligned}\partial l_k(D_{i,j}) &= \max\left[\deg(n_{k,j}), \max_{\tilde{j}\neq j}(\deg(d_{k,\tilde{j}}))\right] \\ &\leq \max\left[\partial l_k(D), \max_{\tilde{j}\neq j}(\deg(d_{k,\tilde{j}}))\right] \\ &= \partial l_k(D)\end{aligned}$$

d'où l'on déduit que $\deg(\det(D_{i,j})) \leq \deg(\det(D))$, ce qui clôt la démonstration dans le cas simplement propre. Pour étudier le cas strictement propre, il convient de poursuivre l'analyse en distinguant deux cas:

- s'il existe k tel que $\partial l_k(D_{i,j}) < \partial l_k(D)$, le théorème est prouvé
- sinon on a $\partial l_k(D_{i,j}) = \partial l_k(D)$ pour tout k; or on a $\deg(n_{k,j}) < \partial l_k(D)$ par hypothèse. On en déduit que la i^{eme} colonne de $\Gamma_l(D_{i,j})$ est nulle, et que $D_{i,j}$ n'est pas ligne propre, d'où

$$\deg(\det D_{i,j}) < \sum_k \partial l_k(D_{i,j}) \tag{4.22}$$

$$\leq \sum_k \partial l_k(D) \tag{4.23}$$

$$= \deg(\det D) \tag{4.24}$$

ce qui prouve le résultat.

4.5 Exercices

Exercice 4.1 on se place dans le cadre d'un anneau principal $\mathcal{A}$.

a) Soit T une matrice rationnelle[11] de rang r, d'éléments $t_{i,j} = \frac{p_{i,j}}{q_{i,j}}$, où $\frac{p_{i,j}}{q_{i,j}}$ est une fraction irréductible. On note Λ un dénominateur commun des $q_{i,j}$. A partir de la forme de Smith S de $T\Lambda$, montrer qu'il existe U et V, matrices unimodulaires, et S_M rationnelle, vérifiant:

$$T = US_MV \tag{4.25}$$

$$S_M = \begin{pmatrix} S_1 & 0 \\ 0 & 0 \end{pmatrix} \tag{4.26}$$

où S_1 est carrée diagonale de taille r et d'éléments diagonaux $\frac{\epsilon_i}{\psi_i}$, où $\frac{\epsilon_i}{\psi_i}$ est irréductible, avec ϵ_i divise ϵ_{i+1} et ψ_{i+1} divise ψ_i.

Une matrice rationnelle équivalente à T possédant ces propriétés est dite *forme de Smith-Mac Millan* de T.

b) Monter que les ϵ_i et les ψ_i sont uniques à une constante près.

Exercice 4.2 On on considère un anneau euclidien $\mathcal{A}$ muni d'une fonction degré telle que, pour tout triplet (a, b, α) d'éléments non nuls de $\mathcal{A}$, on a:

$$\deg(a+b) \leq \max(\deg(a), \deg(b)) \tag{4.27}$$

$$\deg(a) < \deg(b) \iff \deg(\alpha a) < \deg(\alpha b) \tag{4.28}$$

$$\deg(a) = \deg(b) \iff \deg(\alpha a) = \deg(\alpha b) \tag{4.29}$$

1. Soit r une fraction rationnelle, et $\frac{n}{d}$ une représentation de r. Montrer que la quantité $\deg(d) - \deg(n)$ est indépendante du choix de la représentation.
2. Monter que l'ensemble des fractions rationnelles propres et l'ensemble des fractions rationnelles strictement propres sont des sous-anneaux du corps des fractions rationnelles.
3. Reprendre dans ce cas l'exercice 2.2.
4. Reprendre la preuve du théorème 4.11.

Exercice 4.3 Soit $(sId - A, B, C, D(s))$ une forme d'état généralisée.

1. Montrer que $sId - A$ est ligne propre et colonne propre quelque soit A
2. En déduire que $C(sId - A)^{-1}B$ est strictement propre

Exercice 4.4 Soit T une matrice entière et $N_dD^{-1}N_g$ une bifactorisation irréductible de T. Montrer qu'il existe deux unimodulaires U et V telles que

$$\begin{bmatrix} D^{-1} & 0 \\ 0 & 0 \end{bmatrix} = U \begin{bmatrix} D & N_g \\ N_d & T \end{bmatrix} V \tag{4.30}$$

En déduire une nouvelle preuve du théorème (4.5).

Exercice 4.5 Utiliser la division euclidienne de matrices pour exhiber un critère de divisibilité.

Exercice 4.6 (Séparation des entrées et sorties) On considère une matrice polynômiale M, de rang plein, *ayant plus de colonnes que de lignes*. On cherche des opérations de lignes et *de simples permutations de colonnes* qui mette M sous la forme $\begin{bmatrix} P & Q \end{bmatrix}$, avec P carré de rang plein et $P^{-1}Q$ propre.

[11] c'est-à-dire à éléments dans le corps des fractions associé à $\mathcal{A}$

1. On étend la définition des degrés-lignes, des matrices par degrés-lignes et des matrices ligne propres aux matrices "horizontales" comme M, en oubliant simplement de préciser que M doit être carrée. Montrer que l'algorithme de passage à une matrice ligne propre par opération de lignes, tel qu'il est décrit dans la preuve du théorème 4.10, donne les mêmes résultats dans le cas de matrices "horizontales".
2. On peut donc se ramener au cas où M est ligne propre. Il existe donc une matrice $\Gamma_l(P)$, extraite de $\Gamma_l(M)$ par sélection de colonnes, qui soit carrée de rang plein; on note P la matrice correspondante obtenue à partir de M par extraction de colonnes, et Q la matrice complémentaire dans M.
   (a) Montrer que les degrés lignes de P sont ceux de M.
   (b) En déduire que P est ligne propre, et que $P^{-1}Q$ est une matrice rationnelle propre.