République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 8 Mai 1945 Guelma

Faculté des Mathématiques et de l'Informatique
et des Sciences de la Matière
Département de Mathématiques

Mémoire

Présenté en vue de l'obtention du diplôme de

Master Académique en Mathématiques

Option : **Equations aux Dérivées Partielles**

Et analyse numérique

Présenté Par :

ABDEL-KANI IBRAHIM ANNOUR

Intitulé

Sur les Matrices à Coefficients Entiers

Dirigé par :
Dr. Djamel Bellaouar

Devant le jury

PRESIDENT	**Dr. Noureddine Azzouza**	**MCA**	**Univ-Guelma**
EXAMINATEUR	**Dr. MOURAD KERBOUA**	**MCA**	**Univ-Guelma**

Session Septembre 2020

Remerciements

J'adresse ce travail
à mes chers parents mon père Ibrahim Annour et ma mère Aminé Mahamat pour leur soutien infaillible durant toute mes années d'étude.
Ainsi qu'à mes frères Oumar, Youssouf, Abdou daim et mes sœurs Fatima Zahra, Khadija, Kouzaifa.
Et à mon cher encadreur, Mr: Djamel Bellaouar.
Ainsi qu'a tous mes amis, en particulier collègues de la spécialité à l'université 08 Mai 1945 Guelma, Algérie.
Ainsi qu'à tous ceux qui me connaissent ; qui m'ont aidé et qui sont toujours
présents à mes côtés, avec qui j'ai partagé le bon et le mauvais,
Et a toute la famille IBRAHIM
ANNOUR.

Sur les Matrices Coefficients Entiers

ABDEL-KAN IBRAHIM ANNOUR (Tchad)
Université 8 Mai 1945 Guelma
Mémoire de Master en mathématiques
Option : EDP Et Analyse Numérique

13 Septembre 2020

Table des matières

Résumé

Ma thèse finale traite de quelques notions de théorie élémentaire des nombres pour les matrices à coefficients entiers. Tout d'abord, on donne quelques notions élémentaires et quelques définitions, et nous avons présenté la preuve du théorème de Cayley-Hamilton, et théorème de décomposition de Schur : pour toute matrice à coefficients dans $\mathbb{Z}$, on peut la factoriser comme produit de trois matrices PTP^{-1}, où T est triangulaire supérieure. Nous allons donner quelques propriétés des matrices unimodulaires. Nous allons compris que, si le nombre d divise tous les représentation décimales des ligne d'une matrice de $\mathcal{M}_n(\mathbb{Z})$, alors d divise le déterminant de cette matrice. On a donné les conditions nécessaires et suffisantes pour une matrice soit dans $GL_n(\mathbb{Z})$. Et on a donné la forme normale de Smith, et comment résoudre un système d'équations linéaires Diophantiennes par la méthode de Smith. Enfin, on a donné quelques exemples sur la représentation d'une matrice comme le produit de matrices élémentaires.

Mots clés. matrices à coefficients entiers, factorisation, matrices élémentaires, forme normale de Smith, Système d'équations linéaires Diophantiennes.

Abstract

The manuscript deals essentially with some arithmetical properties of matrices with integer entries. At first, basic notations and definitions are given as well as the proof of both Cayley-Hamilton theorem and the theorem of decomposition of Shuer. We have introduced the properties of unimodular matrices which are important on the factoring of invertible matrices over the ring of integers. Next, we have understood a result about divisibility properties involving some class of integer matrices and their determinants. Further, there are several necessary and sufficient conditions for which a given matrix has inverse with integer entries. Also we present Smith normal form for a given matrix by which we can solve a system of linear Diophantine equations. At the end, there are several types on the factorization as well as the product of elementary matrices.

Table des notations

Notation	**Explication**
$a \mid b$,	a divise b.
$a \nmid b$	a ne divise pas b.
$\mathcal{M}_n(\mathbb{Z})$	L'ensemble des matrices à coefficients entiers.
$GL_n(\mathbb{Z})$	L'ensemble des matrices inversibles à coefficients entiers.
$diag\{d_1, d_2, 0\}$	Matrice diagonale et ses éléments diagonaux sont d_1, d_2 et 0.
$lcm(a, b)$	Le plus petit commun multiple de a et b.
$\mathbb{Z}^n$	L'ensemble de tous les points entiers de $\mathbb{R}^n$
I_n ou E_n	La matrice identité de $\mathcal{M}_n(\mathbb{R})$
$E_{i,j}$	$E_{i,j} = (a_{ij})$, où $a_{ij} = 0$ sauf la i-ième ligne et j-ième colonne qui vaut 1
$SL_n(\mathbb{Z})$	L'ensemble des matrices à coefficients entiers et déterminant est égal à 1
$rg(A)$	Le rang de A
(a, b)	Le plus grand commun diviseur de a et b (ou $\gcd(a, b)$).
$\lfloor a \rfloor$	La partie entière d'un réel a
$\{a\}$	La partie fractionnaire de a
$\rfloor a \lfloor$	Le plus grand entier strictement inférieur à a.
$com(A)$	Comatrice de A
$\det(A)$	Déterminant de A
$adj(A)$	La matrice adjointe de A
$A \equiv B$	A et B sont équivalentes
$\mathcal{M}_n(\mathbb{F})$	L'ensemble des matrices à coefficients dans un corps $\mathbb{F}$.
FNS	Forme Normale de Smith
(d)	Un idéal engendré par d
$A \sim T$	La matrice A est similaire avec T
$p_A(X)$	Le polynôme caractéristique de A
$(e_i)_{1 \leq i \leq n}$	Une base canonique
$\begin{pmatrix} 0 & D \end{pmatrix}$	FNS (diagonale croissante pour la relation de divisibilité)
ω	Un entier positif suffisamment grand

Introduction

Le manuscrit traite essentiellement de quelques notions sur la théorie élémentaire des nombres pour les matrices. Notons que l'étude des matrices à coefficients entiers trouvées dans le domaine de l'Algèbre linéaire sur $\mathbb{Z}$ où nous pouvons travailler avec des vecteurs ayant des combinaisons linéaires à coefficients entiers, des modules sur $\mathbb{Z}$ ($\mathbb{Z}$-modules) et des systèmes d'équations linéaires Diophantiennes [10]. La théorie des matrices à coefficients entiers est importante car il est intéressant de voir dans quelle mesure les propriétés des entiers ordinaires sont susceptibles de généralisation.

Dans ce travail, on examine quelques exemples d'algorithmes d'algèbre linéaire sur les entiers [9]. Ici, nous allons travailler sur l'anneau des entiers $\mathbb{Z}$ et voir comment des problèmes concrets sur les entiers d'essence linéaire peuvent se résoudre de manière effective, qui est un domaine ancien et avait été créé à partir d'équations diophantiennes. D'autre part, l'étude des propriétés arithmétiques des matrices à coefficients dans un corps de nombres algébrique a été commencée par Siegel dans les années 30, dans le contexte des formes quadratiques et des fonctions modulaires de degré supérieur, voir [2] et [1]. Nous ne réintroduirons pas tout le vocabulaire très semblable à celui des espaces vectoriels : on parlera donc librement de matrices (à coefficients dans $\mathbb{Z}$) et en particulier du groupe $GL_n(\mathbb{Z})$ (groupe des matrices inversibles

dans $\mathbb{Z}$, on montre que ce sont les matrices dont le déterminant est inversible dans $\mathbb{Z}$, c'est-à-dire égal à ± 1).

La factorisation des matrices à coefficients entiers comme produits de matrices triangulaires, involutions, unimodulaires, idempotentes, nilpotentes et commutateurs constituent une partie importante de la théorie des matrices et de la théorie des groupes classiques (voir [7], [8], [3]). Dans la troisième section, un certain nombre de ces résultats sont présentés pour des matrices intégrales. Nous ne considérons que des matrices sur $\mathbb{Z}$, mais toutes les notions introduites ici s'étendent au cas d'un anneau principal. Bien que les matrices intégrales aient été intensivement étudiées (voir, par exemple, [10], [2]) et que certaines notions arithmétiques comme GCD et la divisibilité aient été introduites, l'ensemble des classes de diviseurs d'une matrice donnée reste encore mal compris.

Notons que pour une matrice donnée à coefficients entiers. On va adapter les méthodes de factorisation pour d'une part rester dans $\mathbb{Z}$.

Plan de travail

L'objet de ce travail est de voir dans quelle mesure les propriétés arithmétiques des entiers sont susceptibles de généralisation. Dans le chapitre 1, il y a quelques outils de base, quelques notations, la preuve du théorème de Cayley-Hamilton et du Théorème de décomposition de Schur. Aussi, quelques notes sur les matrices unimodilaires. Au chapitre 2, nous avons présenté une propriété de divisibilité. Plus précisément, si un entier d divise la représentation décimale de n'importe quelle ligne d'une matrice, alors d divise son

déterminant. Dans le chapitre 3, nous avons présenté quelques résultats de l'arithmétique matricielle qui inclut matrice inversible dont l'inverse appartien à $\mathcal{M}_n(\mathbb{Z})$, la forme normale de Smith et comment résoudre un système d'équations polynomiales dont on cherche les solutions en nombres entiers. Au chapitre 4, nous étudierons la représentation des matrices à coefficients entiers comme le produit de matrices élémentaires.

Chapitre 1

Notions élémentaires

Dans la section suivante, nous présentons les outils de base, définitions et notions dont nous avons besoin dans le reste de ce travail [9]. Nous présentons aussi la preuve de deux théorèmes principaux qui sont assez importants dans la théorie de l'analyse matricielle, qui ont été utilisées dans les Chapitres 3,4. Le premier s'appelle "*Théorème de Calley-Hamilton*" dit que chaque matrice est une racine de son polynôme caractéristique. Le second s'appelle "*Théorème de décomposition de Schur*" qui traite de la factorisation de toute matrice comme le produit de trois matrices ; matrice inversible P, matrice triangulaire supérieure T et l'inverse de P. Concernant les matrices sur $\mathbb{Z}$ il y a une factorisation similaire qui s'appelle "*Forme Normale de Smith*" (voir Chapitre 3).

1.1 Définitions et Notations

1. Soit $n \geq 1$ un entier. On appelle *point entier* de $\mathbb{R}^n$ un point dont toutes les coordonnées sont entières, c'est-à-dire un point de $\mathbb{Z}^n$.

2. Une *équation Diophantienne* est une équation polynomiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers.

3. On note $\mathcal{M}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ dont tous les coefficients sont entiers. On vérifie trivialement que $\mathcal{M}_n(\mathbb{Z})$ est un *sous-anneau* de $\mathcal{M}_n(\mathbb{R})$.

4. Si $A \in \mathcal{M}_n(\mathbb{K})$, on note pour tout entier n, A^n le produit n fois de A par elle-même.

5. On note I_n la matrice identité de $\mathcal{M}_n(\mathbb{R})$ et $E_{i,j}$ la matrice de $\mathcal{M}_n(\mathbb{R})$ dont tous les coefficients sont nuls sauf celui de la i-ième ligne et j-ième colonne qui vaut 1.

6. En algèbre linéaire, une matrice carrée A d'ordre n est dite *inversible* ou *régulière* ou encore *non singulière* s'il existe une matrice B d'ordre n, appelée matrice inverse de A et notée : $B = A^{-1}$ telle que $AB = BA = I_n$.

7. Si $M = (m_{i,j})$ est une matrice de $\mathcal{M}_n(\mathbb{Z})$, $m_{i,j}$ est le coefficient de la i-ème ligne et de la j-ième colonne.

8. On note $\begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}$ la matrice de $\mathcal{M}_n(\mathbb{Z})$ dont les colonnes sont les vecteurs $x_1, x_2, ..., x_n$ de $\mathbb{Z}^n$.

9. Pour des entiers $a_1, a_2, ..., a_k$ non tous nuls, on note $pgcd\,(a_1, a_2, ..., a_k)$ ou $(a_1, a_2, ..., a_k)$ le plus grand entier (strictement positif) qui divise tous les a_i.

10. On note $\lfloor a \rfloor$ la *partie entière* d'un réel a : c'est le plus grand entier inférieur ou égal à a ; et $\{a\} = a - \lfloor a \rfloor \in [0, 1[$ la *partie fractionnaire* de a. On note $\rfloor a \lfloor$ le plus grand entier strictement inférieur à a.
11. Une matrice *idempotente* est une matrice (carrée mais pas nécessairement symétrique) telle que $A^2 = A$. Notons que le rang d'une matrice idempotente symétrique est égal à sa trace. La seule matrice idempotente symétrique de plein rang est la matrice d'identité. De plus, toutes les matrices idempotentes symétriques, sauf la matrice d'identité, sont singulières.
12. J est une *involution* dans $\mathcal{M}_n(\mathbb{Z})$, c'est-à-dire $J^2 = I_n$.
13. $GL_n(\mathbb{Z}) = \{A \in \mathcal{M}_n(\mathbb{Z}) ;\ \det A = \pm 1\}$.
14. $SL_n(\mathbb{Z}) = \{A \in \mathcal{M}_n(\mathbb{Z}) ;\ \det A = 1\}$.
15. Une matrice A a un *commutateur* s'il existe une matrice L non nulle telle que $AL - LA = 0$.
16. Soit A un anneau. Un A-*module* est un groupe abélien $(M, +)$ muni d'une loi externe $A \times M \to M$ vérifiant les mêmes axiomes que ceux d'un espace vectoriel. Le terme $\mathbb{Z}$-module est simplement un autre nom pour un groupe abélien additif.

Définition 1.1.1 Un $\mathbb{Z}$-module libre (de rang n) L est un $\mathbb{Z}$-module tel qu'il existe une suite $(e_1, ..., e_n)$ (appelée base) de n éléments de L vérifiant : tout élément de L s'écrit comme combinaison linéaire de $(e_1, e_2, ..., e_n)$, de manière unique.

Définition 1.1.2 (Plus grand commun diviseur) Soit $a, b \in \mathbb{Z} - \{0\}$. Le

plus grand commun diviseur (ou pgcd, gcd) de a et b, noté (a, b), est l'entier positif d qui satisfait aux deux conditions

(i) $d \mid a$ et $d \mid b$,

(ii) Si $c \mid a$ et $c \mid b$, alors $c \leq d$.

De même, si $a_1, a_2, ..., a_r \in \mathbb{Z}-\{0\}$, alors le plus grand commun diviseur de $a_1, a_2, ..., a_r$, noté $(a_1, a_2, ..., a_r)$, est l'entier positif d qui satisfait aux deux conditions

(i) $d \mid a_i$ pour $i = 1, 2, ..., r$

(ii) Si $c \mid a_i$ pour $i = 1, 2, ..., r$, alors $c \leq d$.

Théorème 1.1.1 *Soit $a_1, a_2, ..., a_r \in \mathbb{Z}-\{0\}$. Alors il existe des entiers $x_1, x_2, ..., x_r$ tels que*

$$(a_1, a_2, ..., a_r) = a_1x_1 + a_2x_2 + ... + a_rx_r.$$

Définition 1.1.3 Une matrice est dite élémentaire lorsqu'elle est obtenue en appliquant une seule opération élémentaire sur les lignes de la matrice identité.

Les opérations élémentaires sur les lignes d'une matrice sont les suivantes :

1. Permuter deux lignes entre elles ;
2. Ajouter un multiple d'une ligne à une autre ligne ;
3. Multiplier une ligne par un scalaire non nul.

1.2 Théorème de Calley-Hamilton et Théorème de décomposition de Schur

Commençons par l'énocé du trés classique théorème de Calley-Hamilton, voir [9].

Théorème 1.2.1 *Soient $A \in \mathcal{M}_n(\mathbb{C})$ et $p_A(x)$ son polynôme caractristique, alors $p_A(A) = 0$.*

Lemme 1.2.1 *Pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$, on a*

$$A(com(A))^t = \det(A) I_n.$$

Par exemple, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$, on a

$$\begin{aligned} A(com(A))^t &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= (ad-bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \det(A) I_n. \end{aligned}$$

Preuve du théoirème de Cayley-Hamilton. Soit

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix}.$$

De plus, supposons que $p_A(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + cx + c_0$. En appliquant le Lemme 1.2.1 pour la matrice $xI_n - A$, on obtient

$$(xI_n - A) com(xI_n - A)^t = \det(xI_n - A) I_n,$$

où

$$xI_n - A = \begin{pmatrix} x - a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & x - a_{22} & ... & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & ... & x - a_{nn} \end{pmatrix}.$$

Posons

$com(xI_n - A)^t = B_0 + xB_1 + x^2B_2 + ... + x^{n-1}B_{n-1}$, où $(B_i)_{i=1,2,...,n-1} \in \mathcal{M}_n(\mathbb{R})$.

On en déduit alors

$$\begin{aligned} & (xI_n - A)(B_0 + xB_1 + x^2B_2 + ... + x^{n-1}B_{n-1}) \\ = \ & \det(xI_n - A).I_n = x^nI_n + c_{n-1}x^{n-1}I_n + ... + cxI_n + cI_n, \end{aligned}$$

il vient aussi

$$\begin{aligned} & x^nB_{n-1} + x^n(B_{n-2} - AB_{n-1}) + ... + x(B_0 - AB_1) - AB_0 \\ = \ & x^nI_n + c_{n-1}x^{n-1}I_n + c_{n-2}x^{n-2}I_n + ... + c_1xI_n + c_0I_n. \end{aligned}$$

Donc

$$\begin{cases} B_{n-1} = I_n, \\ B_{n-2} - AB_{n-1} = c_{n-1}I_n, \\ ... = ... \\ B_0 - AB_1 = c_1I_n, \\ -AB_0 = c_0I_n. \end{cases} \tag{1.1}$$

En utilisant (1.1), il vient

$$\begin{aligned} p_A(A) &= A^n + c_{n-1}A^{n-1} + c_{n-2}A^{n-2} + ... + c_1A + c_0I_n \\ &= A^nB_{n-1} + A^{n-1}(B_{n-2} - AB_{n-1}) + ... + A(B_0 - AB_1) - AB_0 \\ &= A^nB_{n-1} + A^{n-1}B_{n-2} - A^nB_{n-1} + ... + AB_0 - A^2B_1 - AB_0 \\ &= 0. \end{aligned}$$

Ce qui conclut la démonstration. ■

Nous montrons que toute matrice à coefficients complexes est trigonalisable, c'est-à-dire semblable a une matrice triangulaire supérieure. Notons que l'une des premières applications de la trigonalisation des matrices avec le calcul des puissances des matrices et la résolution de systèmes d'équations différentielles linéaires.

Théorème 1.2.2 (Théorème de décomposition de Schur) *Toute matrice à coefficients complexes est trigonalisable dans* $\mathcal{M}_n(\mathbb{C})$. *C'est-à-dire, pour toute matrice* $A \in \mathcal{M}_n(\mathbb{C})$ *ils existent une matrice* P *inversible et une matrice triangulaire supérieure* T *telles que* $A = PTP^{-1}$.

Preuve. Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrons que A est trigonalisable dans $\mathcal{M}_n(\mathbb{C})$. La démonstration se fait par récurrence sur n. En effet, pour $n = 1$ on a $A = a_{11}$, où $a_{11} \in \mathbb{C}$. Dans ce cas on peut écrire

$$A = I(a_{11})I^{-1} = PTP^{-1} \text{ avec } P = I = (1) \text{ et } T = (a_{11}) = A.$$

Supposons que toute matrice $A_1 \in \mathcal{M}_n(\mathbb{C})$ est trigonalisable. Soient (λ, x) un élément propre de A et $\{x, u_2, ..., u_n\}$ une base de $\mathbb{C}^n$. Posons $U = (x, u_2, ..., u_n)$, alors

$$AU = \begin{pmatrix} Ax & Au_2 & \dots & Au_n \end{pmatrix} = \begin{pmatrix} \lambda x & Au_2 & \dots & Au_n \end{pmatrix}$$

Maintenant, calculons $U^{-1}AU$. En effet, on a

$$U^{-1} = U^{-1}Ue_1 = e_1,$$

où $e_1 = (1, 0, ..., 0)$. D'où

$$U^{-1}AU = U^{-1}\begin{pmatrix} \lambda x & Au_2 & \dots & Au_n \end{pmatrix} = \begin{pmatrix} \lambda e_1 & U^{-1}Au_2 & \dots & U^{-1}Au_n \end{pmatrix}$$

On obtient aussi

$$U^{-1}AU = \begin{pmatrix} \lambda & \times & ... & \times \\ 0 & * & ... & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & ... & * \end{pmatrix} = \begin{pmatrix} \lambda & C \\ 0 & A_1 \end{pmatrix} = T_1,$$

où $C \in \mathcal{M}_{1,n-1}(\mathbb{C})$ et $A_1 \in \mathcal{M}_{n-1}(\mathbb{C})$. D'après l'hypothèse de la récurrence, il existe donc une matrice inversible W telle que

$$\begin{pmatrix} 1 & 0 \\ 0 & W^{-1} \end{pmatrix} \begin{pmatrix} \lambda & C \\ 0 & A_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix} = \begin{pmatrix} \lambda & CW \\ 0 & W^{-1}A_1W \end{pmatrix} = \begin{pmatrix} \lambda & CW \\ 0 & T' \end{pmatrix}.$$

Il vient

$$A \sim T_1 \sim \begin{pmatrix} \lambda & CW \\ 0 & T' \end{pmatrix} = T,$$

où T est triangulaire sépurieure. Ainsi, $A \sim T$. ■

Dans l'anneau $\mathbb{Z}$, nous avons une relation binaire similaire donnée par la définition suivante :

Définition 1.2.1 Deux matrices A et B sur $\mathbb{Z}$ de type $m \times n$ sont dites équivalentes et on écrit $A \equiv B$ s'il existent une matrice P de type $m \times m$ et une matrice Q de type $n \times n$, les deux inversibles sur $\mathbb{Z}$, telles que

$$PAQ^{-1} = B.$$

Il s'agit d'une relation d'équivalence sur chaque ensemble de matrices d'une taille donnée.

1.3 Matrices unimodulaires

Définition 1.3.1 Une matrice *unimodulaire* sur l'anneau des entiers relatifs

est une matrice carrée à coefficients entiers dont le déterminant vaut $+1$ ou -1. Plus généralement, une matrice unimodulaire sur un anneau commutatif A est une matrice inversible à coefficients dans A, dont l'inverse est aussi à coefficients dans A. Le groupe général linéaire $GL_n(A)$ des matrices unimodulaires de taille n sur l'anneau A est donc constitué des matrices dont le déterminant est inversible dans A.

1.3.1 Propriétés des matrices unimodulaires

Les matrices unimodulaires d'ordre n forment un groupe pour le produit, c'est-à-dire que les matrices suivantes sont unimodulaires :

1. La matrice unité ;
2. L'inverse d'une matrice unimodulaire ;
3. Le produit de deux matrices unimodulaires.

De plus, le produit de Kronecker de deux matrices unimodulaires est unimodulaire.

Définition 1.3.2 Une matrice totalement unimodulaire (TUM) est une matrice (non nécessairement carrée) à coefficients entiers dont chaque sous-matrice carrée de déterminant non nul est unimodulaire. On déduit de cette définition que les éléments d'une TUM peuvent uniquement être -1, 0 ou $+1$.

La matrice suivante est totalement unimodulaire :

$$A = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}$$

1.3.2 Condition suffisante pour être totalement unimodulaire

Une condition suffisante mais pas nécessaire pour qu'une matrice A soit totalement unimodulaire :

Soit A une matrice rectangulaire dont les lignes sont partitionnées en 2 ensembles disjoints B et C avec les propriétés suivantes :

1. Chaque colonne de A contient au plus 2 éléments non nuls ;
2. Chaque élément de A vaut -1, 0 ou $+1$;
3. Si 2 éléments d'une colonne de A ont le même signe, alors la ligne de l'un est dans B, l'autre dans C ;
4. Si 2 éléments d'une colonne de A ont des signes opposés, alors les lignes des 2 éléments sont dans B ou toutes les 2 dans C ;

alors les déterminants des sous-matrices de A sont -1, 0 ou $+1$.

1.3.3 Question

Soit $A \in \mathcal{M}_n(\mathbb{Z})$. Est-ce-que A peut toujours être représentée comme le produit de matrices unimodulaires ?

Chapitre 2

Divisibilité du Déterminant d'une classe de matrices à coefficients entiers

2.1 Introduction

Dans la section suivante on présente une propriété sur la divisibilité entre le déterminant d'une classe de matrices à coefficients entiers et l'écriture décimale d'un entier positif (voir [5]). En effet, Soit $b_i = \sum_{j=1}^{n} a_{ij}10^{n-j}$, où $i = 1, ..., n$ et $a_{ij} \in \mathbb{Z}$. Soient $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{Z})$ et $k \in \mathbb{Z}^*$. On a

Théorème 2.1.1 *Si chaque b_i est divisible par k, alors le déterminant de la maxtrice A est également divisible par k, i.e.,*

$$Si\ k \mid b_i,\ pour\ i = 1, ..., n \Rightarrow k \mid \det(A).$$

On sait que les nombres 14529, 15197, 20541, 38911 et 59619 sont des multiples de 167. Sans calculer réellement, le déterminant de la matrice $A \in$

$\mathcal{M}_5(\mathbb{Z})$ est également un multiple de 167, où

$$A = \begin{bmatrix} 1 & 4 & 5 & 2 & 9 \\ 1 & 5 & 1 & 9 & 7 \\ 2 & 0 & 5 & 4 & 1 \\ 3 & 8 & 9 & 1 & 1 \\ 5 & 9 & 6 & 1 & 9 \end{bmatrix}.$$

En effet, on a $\det(A) = 13\,861 = 83 \times 167$.

Dans ce problème, nous avons donné une matrice de type 5×5 et le calcul de son déterminant à la main est fastidieux. Nous examinons un problème similaire, mais avec une dimension plus petite. Tout d'abord, nous examinons des exemples impliquant des matrices 2×2 pour savoir si ce cas est valable : si on donne des entiers à deux chiffres (disons, $x = a_1a_2$ et $y = b_1b_2$) et si ces entiers sont divisibles par un entier donné k, est-il vrai que k divise aussi le déterminant de la matrice $\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$?

Nous enquêtons sur ce cas et voyons s'il s'étend à des dimensions plus élevées, c'est-à-dire au cas 3×3, au cas 4×4, et en général, au cas $n \times n$. Bien que le problème d'origine ait donné une matrice très spécifique, nous résolvons une généralisation de ce problème et examinons également d'autres problèmes concernant le déterminant d'une matrice.

Soit $\mathbb{Z}$ l'ensemble de tous les entiers, $\mathbb{N}$ l'ensemble de tous les nombres naturels, et nous laissons $\mathcal{M}_n(\mathbb{Z})$ l'ensemble de toutes les matrices $n \times n$ à coefficients entiers. On note également le déterminant d'une matrice A par $\det(A)$.

Un nombre naturel à deux chiffres ab est vraiment $a(10)+b$, et un nombre naturel à trois chiffres abc est en fait $a(10^2)+b(10^1)+c(10^0)$. En général, un nombre naturel à n chiffres $a_1a_2a_3...a_{n-1}a_n$ peut s'écrire sous la forme :

$$a_1(10^{n-1}) + a_2(10^{n-2}) + a_3(10^{n-3}) + ... + a_{n-1}(10^1 + a_n(10^0),$$

où $0 \leq a_i \leq 9$ pour tout $i = 1, 2, ..., n$ avec $a_1 \neq 0$.

2.2 Exemples sur $\mathcal{M}_2(\mathbb{Z})$ et $\mathcal{M}_3(\mathbb{Z})$

Exemple 2.2.1 *Les nombres* 72 *et* 18 *sont divisibles par* 3. *La matrice*

$$\begin{bmatrix} 7 & 2 \\ 1 & 8 \end{bmatrix}$$

a le déterminant $7(8) - 2(1) = 54$, *qui est également divisible par* 3.

Exemple 2.2.2 Les nombres 16 et 36 sont divisibles par 4. La matrice

$$\begin{bmatrix} 1 & 6 \\ 3 & 6 \end{bmatrix}$$

a le déterminant $1(6) - 6(3) = -12$, qui est également divisible par 4.

Dans ces exemples, nous voyons que si deux nombres entiers positifs a_1a_2 et b_1b_2 sont des multiples d'un entier positif k, alors le déterminant de la matrice $A = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$ (lequel est $a_1b_2 - a_2b_1$), est également divisible par k. Notons que même lorsque le déterminant de A est 0, alors k également divise le déterminant de A.

Proposition 2.2.1 *Soient* $e, f \in \mathbb{N}$ *deux entiers à deux chiffres, i.e.,* $e = 10a + b$ *et* $f = 10c + d$ *, et soit* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. *Si* k *(un entier positif) divise à la fois* e *et* f, *alors* k *divise* $\det(A)$.

Preuve. Nous avons les deux équations

$$10a + b = e, \tag{2.1}$$

$$10c + d = f. \tag{2.2}$$

En multipliant l'équation (2.1) par $-c$ et l'équation (2.2) par a et en ajoutant ces équations, on obtient

$$ad - bc = af - ce$$

Maintenant, $e = kr$ et $f = kg$, où r et g sont des entiers. Ainsi, $ad - bc = a(kg) - c(kr) = k(ag - cr)$, pour que k divise $(ab - bc)$. Par suite, k divise $\det(A)$. ■

Ensuite, nous examinons un exemple particulier sur une matrice de type 3×3.

Exemple 2.2.3 Les nombres 156, 228 et 276 sont des multiples de 12. Un calcul simple montre que le déterminant de la matrice $\begin{bmatrix} 1 & 5 & 6 \\ 2 & 2 & 8 \\ 2 & 7 & 6 \end{bmatrix}$ est 36, qui est également un multiple de 12.

Regardons maintenant de plus près le cas $n = 3$. Soit

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

et notons que $\det(A) = aei - afh + bfg - bdi + cdh - ceg$.

Supposons que m, n et p sont des entiers à trois chiffres, i.e., $m = 100a + 10b + c$, $n = 100d + 10e + f$, et $p = 100g + 10h + i$. Supposons que m, n et p soient divisibles par k. On montre que k divise $\det(A)$.

Nous avons le système d'équations suivant :

$$100a + 10b + c = m, \tag{2.3}$$

$$100d + 10e + f = n, \tag{2.4}$$

$$100g + 10h + i = p. \tag{2.5}$$

Si $a = d = g = 0$, alors $\det(A) = 0$, qui est divisible par k. Ainsi, nous pouvons supposer que l'un des nombres a, d ou g est différent de zéro. Sans perte de généralité, supposons que $d \neq 0$. En multipliant (2.3) par d des deux côtés, en multipliant (2.4) par $-a$ et en ajoutant ces équations, on obtient

$$10(bd - ea) + cd - fa = md - na. \tag{2.6}$$

De même si nous multiplions (2.4) par g et si nous multiplions (2.5) par $-d$ et ajoutons ces équations, on obtient aussi

$$10(ge - hd) + gf - id = gn - pd. \tag{2.7}$$

Multiplions (2.6) par $-(ge - hd)$, multiplions (2.7) par $(bd - ea)$ et ajoutons ces deux équations : $(bd-ea)(gf-id)-(cd-fa)(ge-hd) = (bd-ea)(gn-pd)-(md-na)(ge-hd)$. En simplifiant le côté gauche, nous obtenons

$$d(aei - afh + bfg - bdi + cdh - ceg),$$

mais sur le côté droit, nous avons

$$d(dhm - egm - ahn + bdp - bgn - aep).$$

Lorsque $d \neq 0$, on peut diviser par d pour obtenir

$$aei - afh + bfg - bdi + cdh - ceg = dhm - egm - ahn + bdp - bgn - aep.$$

Le côté gauche de cette équation est $\det(A)$. Lorsque m, n, et p sont divisibles par k, alors chacune des sommes du côté droit est divisible par k. On en déduit que k divise $\det(A)$.

Notons bien que cette méthode fonctionne, elle peut devenir très fastidieuse lorsque la taille de la matrice devient grande. Cela nécessite de rechercher une approche différente.

Avant d'examiner le cas général de ce problème, nous définissons une terminologie et des faits importants sur les matrices.

Soit $A = (a_{ij})$ une matrice de type $n \times n$ et soit M_{ij} la matrice de type $(n-1) \times (n-1)$ obtenue à partir de A en supprimant la ligne et la colonne contenant a_{ij}. Le déterminant de M_{ij} est appelé le mineur de a_{ij}. Le cofacteur de a_{ij} [9, page 102-103] est

$$A_{ij} = (-1)^{i+j} \det(M_{ij}).$$

L'adjoint de A est

$$adj(A) = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix}.$$

Exemple 2.2.4 Par exemple, supposons que $A = \begin{bmatrix} 3 & 8 & 7 \\ 2 & 6 & 0 \\ 5 & 4 & 3 \end{bmatrix}$. Alors

$$A_{11} = \begin{vmatrix} 6 & 0 \\ 4 & 3 \end{vmatrix} = 18,\ A_{12} = -\begin{vmatrix} 2 & 0 \\ 5 & 3 \end{vmatrix} = -6,\ldots, \text{ et } A_{33} = \begin{vmatrix} 3 & 8 \\ 2 & 6 \end{vmatrix} = 2,$$

$$adj(A) = \begin{bmatrix} 18 & -6 & -22 \\ 4 & -26 & 28 \\ -42 & 14 & 2 \end{bmatrix}, \text{ et}$$

$$\det(A) = 3(18) - 8(6) + 7(-22) = -148.$$

Si $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{Z})$ alors $adj(A) \in M_n(\mathbb{Z})$ puisque $adj(A)$ est calculé en ajoutant, en soustrayant et en multipliant les coefficients de$A$. Ce qui suit

est une connexion entre une matrice non singulière et son adjoint [9, page 116].

Lemme 2.2.1 *Soit A une matrice non singulière de type $n \times n$. Alors* $A^{-1} = \frac{1}{\det(A)} adj(A)$.

Maintenant, nous sommes prêts à résoudre le problème précédent.

2.3 Preuve du Théorème 2.1.1

Preuve. Soit

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in \mathcal{M}_n(\mathbb{Z})$$

une matrice donnée. Tout d'abord, notons que si A est singulière, alors $\det(A) = 0$ est divisible par k. Ainsi, on peut supposer que A est non singulière. De plus, si $k = 1$ alors k divise $(b_i)_{1 \leq i \leq n}$ et k divise $\det(A)$.

Maintenant, supposons que $k \geq 2$. Soit $z = \begin{pmatrix} 10^{n-1} & 10^{n-2} & \cdots & 10^0 \end{pmatrix}^t$, il vient

$$Az = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} 10^{n-1} \\ 10^{n-2} \\ \vdots \\ 10^0 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = b.$$

Nous avons donné cela pour chaque $i = 1, ..., n$, nous avons aussi $b_i = kr_i$ pour un certain $r_i \in \mathbb{Z}$. Posons $r = \begin{pmatrix} r_1 & ... & r_n \end{pmatrix}^t$. Alors $b = kr$. Maintenant, $A^{-1} = \frac{1}{\det(A)} adj(A)$. Par conséquent

$$z = A^{-1}b = \frac{1}{\det(A)} adj(A)b = \frac{1}{\det(A)} adj(A)kr$$

Ce qui donne

$$\frac{\det(A)}{k}z = adj(A)r. \tag{2.8}$$

Comme $adj(A)r \in \mathbb{Z}$, alors (2.8) donne $\dfrac{\det(A)}{k} \in \mathbb{Z}$. Ainsi $\det(A)$ est divisible par k, puisque $k \nmid z$. ■

Une question naturelle à se poser est : pour $A \in \mathcal{M}_n(\mathbb{Z})$, quand est $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$?

Proposition 2.3.1 *Soit $A \in \mathcal{M}_n(\mathbb{Z})$ une matrice non singulière. Alors $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$ si et seulement si $\det(A) = \pm 1$.*

Preuve. Soit $A \in \mathcal{M}_n(\mathbb{Z})$. Alors $\det(A) \in \mathbb{Z}$ parce que le déterminant est calculé en ajoutant, en soustrayant et en multipliant les coefficients d'une matrice.

Si $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$, alors $\det(A^{-1}) \in \mathbb{Z}$. Mais, $\det(A^{-1}) = \dfrac{1}{\det(A)}$. Par conséquent, $\dfrac{1}{\det(A)}$ est également un entier et par suite, $\det(A) = \pm 1$.

Réciproquement, si $\det(A^{-1}) = \dfrac{1}{\det(A)} adj(A) \in \mathcal{M}_n(\mathbb{Z})$ puisque $adj(A) \in \mathcal{M}_n(\mathbb{Z})$. ■

Chapitre 3

Quelques résultats de l'arithmétique matricielle

3.1 Matrice inversible dont l'inverse appartient à $\mathcal{M}_n(\mathbb{Z})$

Dans la section suivante, nous présentons quelques conditions nécessaires et suffisantes pour lesquelles $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

Proposition 3.1.1 *Soit $A \in \mathcal{M}_n(\mathbb{Z})$ une matrice inversible et à coefficients entiers. Alors A^{-1} est à coefficients rationnels.*

Preuve. On a $\mathcal{M}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Q})$. Donc si A est inversible elle est inversible en tant que matrice à coefficients dans le corps $\mathbb{Q}$. Son inverse A^{-1} est donc encore à coefficients rationnels. On sait que $A^{-1} = \dfrac{1}{\det(A)} C^t$, où $C^t = (comA)^t$ est la transposée de la matrice des cofacteurs de A. Comme le déterminant de A est entier et ses cofacteurs aussi (ce sont tous des déterminants de matrices à coefficients entiers), A^{-1} est bien à coefficients rationnels.

■

Nous avons :

$$A \in \mathcal{M}_n(\mathbb{Z}) \cap GL_n(\mathbb{R}) \Rightarrow A^{-1} \in \mathcal{M}_n(\mathbb{Q}).$$

Montrons l'équivalence des propositions suivantes :

1. A^{-1} est à coefficients entiers.
2. $\det(A)$ vaut -1 ou 1.

Si $A \in \mathcal{M}_n(\mathbb{Z})$ est inversible telle que A et A^{-1} sont à coefficients entiers, alors $\det(A)$ et $\det(A^{-1})$ sont dans $\mathbb{Z}$ tels que

$$1 = \det(I_n) = \det(A) \det\left(A^{-1}\right).$$

Donc $\det(A)$ est un diviseur de 1, i.e., vaut -1 ou 1. Si $A \in \mathcal{M}_n(\mathbb{Z})$ est telle que $\det(A) \in \{-1, 1\}$, comme on a déjà dit que si A est à coefficients entiers, alors il en est de même de A^t et en divisant par 1 ou par -1, $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

On a

$$\text{Pour } A \in \mathcal{M}_n(\mathbb{Z}),\ A^{-1} \in \mathcal{M}_n(\mathbb{Z}) \Leftrightarrow \det(A) = \pm 1.$$

Dans la suite on note $GL_n(\mathbb{Z})$ l'ensemble des matrices carrées de taille n à coefficients entiers et de déterminant ± 1. C'est un sous-groupe de $GL_n(\mathbb{R})$. On remarque que pour $i \neq j$ et $c \in \mathbb{Z}$, la matrice $I_n + cE_{i,j}$ appartient à $GL_n(\mathbb{Z})$. En effet, comme I_n commute avec tout le monde et puisque $i \neq j \Rightarrow E_{i,j}^2 = 0$. De plus, on a

$$(I_n + cE_{i,j})(I_n - cE_{i,j}) = I_n - c^2 E_{i,j}^2 = I_n.$$

Donc $I_n + cE_{i,j} \in GL_n(\mathbb{Z})$. On peut aussi dire que le déterminant d'une telle matrice vaut 1.

Maintenant, on considère le théorème suivant :

Théorème 3.1.1 *Soit* $A = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \in GL_n(\mathbb{R})$. *Alors*

$$A \in GL_n(\mathbb{Z}) \text{ si et seulement si } A(\mathbb{Z}^n) = \mathbb{Z}^n. \tag{3.1}$$

Preuve. Commençons par remarquer que si $A \in \mathcal{M}_n(\mathbb{Z})$ alors pour toute colonne (ou vecteur) x à coefficients entiers Ax est encore à coefficients entiers. Ainsi $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$ et c'est l'inclusion contraire qui pose problème ...

- Supposons que $A(\mathbb{Z}^n) = \mathbb{Z}^n$. Notons que $e_1, e_2, ..., e_n \in \mathbb{Z}^n = A(\mathbb{Z}^n)$, donc l'image de A (en tant qu'endomorphisme de $\mathbb{R}^n$ ou $\mathbb{Q}^n$) contient une base de $\mathbb{R}^n$ (ou de $\mathbb{Q}^n$) et A est surjectif, donc bijectif. Cela prouve que $A \in GL_n(\mathbb{R})$. Par hypothèse, pour tout $j = 1, 2, ..., n$, il existe $y_j \in \mathbb{Z}^n$ tel que $Ay_j = e_j$. Comme $A \in GL_n(\mathbb{Z})$, on a en fait $y_j = A^{-1}e_j$ et on vient donc de montrer que pour tout j, la $j^{\text{ème}}$ colonne de A^{-1} est à coefficients entiers. Ainsi $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Donc A et A^{-1} sont à coefficients entiers et $A \in GL_n(\mathbb{Z})$.
- Si $A \in GL_n(\mathbb{Z})$. A et A^{-1} sont à coefficients entiers. Alors pour tout vecteur $y \in \mathbb{Z}^n$, le vecteur $x = A^{-1}y$ est à coefficients entiers et $Ax = y$. Cela prouve que contient $A(\mathbb{Z}^n)$ contient $\mathbb{Z}^n$ et comme on a dit que $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$ est triviale, on a $A(\mathbb{Z}^n) = \mathbb{Z}^n$. Ce qui preuve (3.1). Ce que l'on peut aussi écrire

  $$A \in GL_n(\mathbb{Z}) \Leftrightarrow (x \in \mathbb{Z}^n \Leftrightarrow Ax \in \mathbb{Z}^n),$$

  car si $A \in GL_n(\mathbb{Z})$ on a banalement $x \in \mathbb{Z}^n \Rightarrow Ax \in \mathbb{Z}^n$ et on a aussi $Ax \in \mathbb{Z}^n \Rightarrow x = A^{-1}(Ax) \in \mathbb{Z}^n$.

■

Théorème 3.1.2 *Les deux propositions suivantes sont équivalentes :*

1. $A \in GL_n(\mathbb{Z})$.
2. *Les points entiers du parallélépipède*

$$\mathfrak{p} = \left\{ \sum_{i=1}^{n} t_i x_i \; ; \; \forall \; i \in \{1, 2, ..., n\} \, , t_i \in [0, 1] \right\}$$

sont exactement les 2^n *points* $\sum_{i=1}^{n} \varepsilon_i x_i$, *où* $\varepsilon_i \in \{0, 1\}$ *pour tout* $i \in \{1, 2, ..., n\}$.

Preuve. $1 \Rightarrow 2)$ On suppose donc que l'on a $A \in GL_n(\mathbb{Z})$. Pour $t = (t_1, t_2, ..., t_n)$, on a

$$\sum_{j=1}^{n} t_j x_j = \sum_{j=1}^{n} t_j A e_j = A \sum_{j=1}^{n} t_j e_j = At.$$

Donc, par le résultat (3.1), $t \in \mathbb{Z}^n \Leftrightarrow A(t) = \sum_{j=1}^{n} t_j x_j \in \mathbb{Z}^n$. Si pour tout $j \in \{1, 2, ..., n\}$ on a $t_j \in [0, 1]$ alors $\sum_{j=1}^{n} t_j x_j \in \mathbb{Z}^n$ si et seulement si chaque t_j est entier donc vaut 0 ou 1, ce qui fait donc 2^n listes possibles et 2^n points, car la famille $(x_1, x_2, ..., x_n)$ est une base de $\mathbb{R}^n$ (image de la base canonique par M inversible) et donc des listes de coordonnées différentes donnent des points différents.

$2 \Rightarrow 1)$ En prenant tous les t_i nuls sauf l'un qui vaut 1, l'hypothèse entraîne que les vecteurs $x_1, x_2, ..., x_n$ sont tous des points entiers et $A \in \mathcal{M}_n(\mathbb{Z})$. Réciproquement, soit $j \in \{1, 2, ..., n\}$ et $z = A^{-1} e_j \in \mathbb{R}^n$. On a donc $Az = e_j$. On peut écrire :

$$z = (z_1, z_2, ..., z_n) = (\lfloor z_1 \rfloor, \lfloor z_2 \rfloor, ..., \lfloor z_n \rfloor) + (\{z_1\}, \{z_2\}, ..., \{z_n\})$$

et chaque $\{z_i\}$ appartient à $[0, 1]$. En notant $\lfloor z \rfloor = (\lfloor z_1 \rfloor, \lfloor z_2 \rfloor, ..., \lfloor z_n \rfloor)$ et $\{z\} = (\{z_1\}, \{z_2\}, ..., \{z_n\})$, on a donc :

$$A\{z\} = Az - A\lfloor z \rfloor = e_j - A\lfloor z \rfloor .$$

Comme $\lfloor z \rfloor$ est à coefficients entiers, il en est de même de $A \lfloor z \rfloor$ et donc $A \{z\} = \sum_{j=1}^{n} \{z_j\} x_j$ est à coefficients entiers, les $\{z_j\}$ valent tous 0, ce qui prouve z est à coefficients entiers. On vient donc de montrer que les colonnes de A^{-1} sont à coefficients entiers et $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Ainsi A et A^{-1}sont à coefficients entiers et $A \in GL_n(\mathbb{Z})$. ■

3.2 Forme normale de Smith

Commençons par la notion d'une matrice échelonnée suivant les lignes, voir [2].

Définition 3.2.1 Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$ une matrice à m lignes et n colonnes à coefficients $a_{i,j}$. Pour i allant de 1 à m, posons $p(i)$ le plus petit indice j tel que $a_{i,j} \neq 0$ (avec la convention $p(i) = \infty$ si la i-ème ligne est nulle). Alors la matrice A est dite échelonnée suivant les lignes quand on a, pour tout $i = 2, ..., m$, $p(i) = \infty$ ou $p(i-1) < p(i)$. Autrement dit, le premier coefficient non nul d'une ligne est toujours strictement à droite du premier coefficient non nul de la ligne précédente.

Le résultat de base pour l'échelonnement est le suivant :

Proposition 3.2.1 *Soit (a, b) un vecteur de $\mathbb{Z}^2$, $d = \gcd(a, b)$. Alors on peut calculer une matrice $A \in GL_2(\mathbb{Z})$ telle que*

$$A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Preuve. On suppose a et b non tous les deux nuls (car sinon il suffit de prendre $A = I_2$), on a alors $d \neq 0$. Grâce à l'algorithme d'Euclide étendu, on

peut calculer des entiers relatifs u et v tels que $au + bv = d$. Soient a' et b' les entiers relatifs définis par $a = da'$ et $b = db'$. On prend alors

$$A = \begin{pmatrix} u & v \\ -b' & a' \end{pmatrix}.$$

Dans ce cas, on a

$$A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} u & v \\ -b' & a' \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Notons que que $A \in GL_2(\mathbb{Z})$; sinon $a'u = -b'v$ et par suite, $da'u + db'v = 0$, i.e., $au + bv = 0$. Une contradiction. ■

On peut appliquer la proposition 2 à des vecteurs de longueur $n > 2$, quand on veut en modifier deux des composantes d'indices i et j. On « gonfle » alors les matrices 2×2 en remplaçant par leurs coefficients les coefficients d'indices (i, i), (i, j), (j, i) et (j, j) de la matrice identité I_n. En utilisant plusieurs fois la proposition ainsi étendue, on obtient sans peine le résultat suivant :

Corollaire 3.2.1 *Soit $(a_1, a_2, ..., a_n)$ un vecteur de $\mathbb{Z}^n$, $d = \gcd(a_1, a_2, ..., a_n)$. Alors on peut calculer une matrice $A \in GL_n(\mathbb{Z})$ telle que*

$$A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Le calcul successif d'identités de Bézout entre deux coefficients n'est sans doute pas le procédé le plus efficace pour trouver la matrice A du corollaire. On peut plutôt répéter l'opération qui consiste à choisir un coefficient du vecteur de valeur absolue non nulle minimale, et à faire la division euclidienne

des autres coefficients par celui-ci. Remarquez que chaque division euclidienne se fait par multiplication à gauche par une matrice élémentaire à coefficients entiers. A la fin, on peut multiplier à gauche par une matrice de transposition pour amener le pgcd obtenu en première position.

Nous considérons l'effet de l'application d'opérations élémentaires sur les lignes (eros) sur $\mathbb{Z}$ et colonne élémentaire opérations (ecos) sur $\mathbb{Z}$ à la matrice A, c'est-à-dire des opérations des types suivants :

(i) échange de deux lignes ou deux colonnes

(ii) changer le signe d'une ligne ou d'une colonne

(iii) ajout d'un multiple entier d'une ligne / colonne à une ligne / colonne différente.

Soit A une matrice de type $m \times n$ sur $\mathbb{Z}$. Notre but dans cette section est de montrer que A peut être réduite à une seule matrice D sous la forme normale de Smith.

Proposition 3.2.2 *Soit A une matrice diagonale de type 2×2 sur $\mathbb{Z}$ à coefficients non nuls. Alors A peut être changé en forme normale de Smith D en utilisant au plus cinq opérations élémentaires de type (iii).*

Preuve. Supposons que $A = diag\{l, m\}$. Dans le cas $l|m$, il n'y a rien à faire car $A = D$. Sinon on pose $d = \gcd\{l, m\}$. Alors $d > 0$ et il y a des entiers a, b avec $al + bm = d$. La suite suivante d'opérations élémentaires de type (iii)

change A en D :

$$\begin{aligned} A &= \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix}_{c_2+ac_1} \equiv \begin{pmatrix} l & al \\ 0 & m \end{pmatrix}_{r_1+br_2} \equiv \begin{pmatrix} l & d \\ 0 & m \end{pmatrix}_{c_1-\left(\frac{1}{d}-1\right)c_2} \\ &\equiv \begin{pmatrix} d & d \\ -lm\ /d+m & m \end{pmatrix}_{c_2-c_1} \equiv \begin{pmatrix} d & 0 \\ -lm\ /d+m & lm\ /d \end{pmatrix}_{r_2+\left(\frac{m}{d}\right)\left(\frac{l}{d}l-1\right)r_1} \\ &\equiv \begin{pmatrix} d & 0 \\ 0 & lm\ /d \end{pmatrix} = D. \end{aligned}$$

■

En appliquant la Proposition 3.2.2 posons $l = 21$, $m = 35$. Alors $2 \times 21 + (-1) \times 35 = 7 = d$ et par suite $a = 2, b = -1$. C'est-à-dire $\gcd\{21, 35\} = 7$ et $lcm\{21, 35\} = (21 \times 35)/7 = 105$. Ainsi

$$\begin{aligned} A &= \begin{pmatrix} 21 & 0 \\ 0 & 35 \end{pmatrix}_{c_2+2c_1} \equiv \begin{pmatrix} 21 & 42 \\ 0 & 35 \end{pmatrix}_{r_1-r_2} \equiv \begin{pmatrix} 21 & 7 \\ 0 & 35 \end{pmatrix}_{c_1-2c_2} \\ &\equiv \begin{pmatrix} 7 & 7 \\ -70 & 35 \end{pmatrix}_{c_2-c_1} \equiv \begin{pmatrix} 7 & 0 \\ -70 & 105 \end{pmatrix}_{r_2+10r_1} \equiv \begin{pmatrix} 7 & 0 \\ 0 & 105 \end{pmatrix} = D. \end{aligned}$$

Nous sommes maintenant prêts pour le théorème principal de la Section 3.

Théorème 3.2.1 (L'existence de la forme normale de Smith sur $\mathbb{Z}$) *Toute matrice A de type $m \times n$ sur $\mathbb{Z}$ peut être réduite à une matrice D de type $m \times n$ sous la forme normale de Smith en utilisant des opérations élémentaires sur $\mathbb{Z}$.*

Corollaire 3.2.2 *Soit A une matrice de type $m \times n$ sur $\mathbb{Z}$. Il existe des matrices inversibles P et Q sur $\mathbb{Z}$ telles que $PAQ^{-1} = D$, où D est sous la forme normale de Smith.*

Exemple 3.2.1 Soit $A = \begin{pmatrix} 4 & 6 \\ 8 & 10 \end{pmatrix}$. Nous nous concentrons d'abord sur la ligne une en appliquant les opérations élémentaires suivantes sur A :

$$\begin{aligned} A &= \begin{pmatrix} 4 & 6 \\ 8 & 10 \end{pmatrix}_{c_2-c_1} \equiv \begin{pmatrix} 4 & 2 \\ 8 & 2 \end{pmatrix}_{c_1-2c_2} \equiv \begin{pmatrix} 0 & 2 \\ 4 & 2 \end{pmatrix}_{c_1 \leftrightarrow c_2} \\ &\equiv \begin{pmatrix} 2 & 0 \\ 2 & 4 \end{pmatrix}_{r_2-r_1} \equiv \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = D. \end{aligned}$$

Ainsi, $A \equiv D$.

Définition 3.2.2 Une matrice $(0 \mid D)$ ou $\begin{pmatrix} 0 \\ D \end{pmatrix}$ est dans une forme normale de Smith (FNS) si D est diagonale, de diagonale $d_1, ..., d_n$ formée d'entiers positifs telle que $d_n \mid \ldots \mid d_1$ (en terme d'idéaux, telle que $(d_1) \subset (d_2) \subset ...$).

Théorème 3.2.2 *Si A est une matrice $n \times n$ à coefficients dans $\mathbb{Z}$ non singulière, il existe des matrices U et V unimodulaires (à coefficients dans $\mathbb{Z}$ de déterminant 1) tels que UAV soit une matrice diagonale à coefficients dans $\mathbb{Z}$, de diagonale $d_1, ..., d_n$ tels que $d_n \mid \ldots \mid d_1$.*

Théorème 3.2.3 *Soit A une matrice entière $n \times m$. Il existe des matrices U et V unimodulaires et une unique matrice S de Smith telles que*

$$UAV = S = \begin{pmatrix} 0 & 0 \\ 0 & D \end{pmatrix},$$

avec U carrée d'ordre n, V carrée d'ordre m, D diagonale de diagonale $(d_1, ..., d_r)$ avec $d_r \mid \ldots \mid d_1$, $d_i > 0$.

3.2.1 Comment calculer la forme de Smith

Regardons simplement le cas des matrices 2×2, qui montre bien les difficultés. Notons que l'opération de réinterpréter les multiplications par des

matrices comme des opérations sur les lignes ou les colonnes pour comprendre ce qu'on fait.

On considère la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Soit d_1 le pgcd de b et d. Si $d_1 = d$, c'est-à-dire si d divise b, on multiplie à gauche par la matrice $\begin{pmatrix} 1 & -\frac{b}{d} \\ 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} 1 & -\frac{b}{d} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ c & d \end{pmatrix}.$$

Si d_1 est différent de d (on a donc $d_1 \leq d$), en utilisant $bu + dv = d_1$, $s = \dfrac{-b}{d_1}$, $t = \dfrac{d}{d_1}$ on obtient

$$\begin{pmatrix} t & s \\ u & v \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}.$$

(on remplace donc la colonne $\begin{pmatrix} b \\ d \end{pmatrix}$ par $\begin{pmatrix} 0 \\ d_1 \end{pmatrix} = \begin{pmatrix} 0 \\ p\gcd(b,d) \end{pmatrix}$. Si d_1 divise c_1, on multiplie à droite par $\begin{pmatrix} 1 & 0 \\ \frac{-c_1}{d_1} & 1 \end{pmatrix}$ pour obtenir une matrice diagonale $\begin{pmatrix} * & 0 \\ 0 & d_1 \end{pmatrix}$. Sinon, soit d_2 le pgcd de d_1 et c_1 :

$$\begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} t' & u' \\ s' & v' \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & d_2 \end{pmatrix}$$

On a peut-être perdu le zéro sur la première ligne ... Mais on a quand même gagné un peu car d_2 divise strictement d. En recommençant ces opérations autant de fois qu'il le faut, on obtient au bout d'un certain temps une matrice diagonale :

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

On veut maintenant obtenir la matrice $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ avec d le pgcd de a et b et $d \mid c$ (le déterminant de ces matrices est inchangée au signe près, on a alors nécessairement $c = \pm\frac{ab}{d}$). Pour cela, soient u et v tels que $au + bv = d$, on a

$$\begin{pmatrix} \frac{b}{d} & \frac{-au}{d} \\ 1 & v \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{bv}{d} & u \\ \frac{-a}{d} & 1 \end{pmatrix} = \begin{pmatrix} \frac{ab}{d} & 0 \\ 0 & d \end{pmatrix}$$

Ces matrices sont composées d'opérations élémentaires comme le montrent les produits suivants :

$$\begin{pmatrix} \frac{bv}{d} & u \\ \frac{-a}{d} & 1 \end{pmatrix} = \begin{pmatrix} \frac{bv}{d} & u \\ \frac{-a}{d} & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{-a}{d} & 1 \end{pmatrix}$$

et

$$\begin{pmatrix} \frac{b}{d} & \frac{-au}{d} \\ 1 & v \end{pmatrix} = \begin{pmatrix} 1 & \frac{b}{d} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}.$$

En pratique, on commence par amener par des permutations de lignes ou de colonnes l'élément de plus petite valeur absolue en bas à droite et on refait cette opération avant de recommencer.

Remarque 3.2.1 La discussion ci-dessus montre que chaque élément de $SL_n(\mathbb{Z})$ peut être écrit comme un produit de matrices élémentaires. Par exemple, pour $A = \begin{pmatrix} 13 & 9 \\ 36 & 25 \end{pmatrix}$, on voit que $\det A = 1$. De plus, on a

$$A = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Notons que $A \equiv B$ si et seulement si A peut être obtenu à partir de B par des opérations élémentaires.

3.2.2 Les unités

En raison de la non-commutativité de la multiplication et de l'existence de matrices singulières, les unités pour la multiplication sont unilatérales et dépendent du rang. Une matrice idempotente (les matrices idempotentes sont égales à leurs carrés) G de même rang qu'une matrice donnée A et qui satisfait la condition $AG = A$ est appelée une unité à droite pour A. Si les coefficients de G appartiennent à $\mathbb{Q}$, nous dirons que G est une unité fractionnaire à droite, mais si ces coefficients appartiennent à $\mathbb{Z}$, nous l'appellerons une unité entière à droite, souvent écourté en unité à droite. Comme exemple, nous constatons que

$$\begin{pmatrix} 1 & 0 & 8 \\ 0 & 1 & -13 \\ 0 & 0 & 0 \end{pmatrix}$$

est une unité à droite de la matrice $\begin{pmatrix} 2 & 1 & 3 \\ 5 & 3 & 1 \end{pmatrix}$. De façon similaire, si $G^{*^2} = G^*$, si $rg(G^*) = rg(A)$ et si $G^*A = A$, nous dirons que G^* est une unité à gauche pour A. Elle est fractionnaire ou entière selon que ses coefficients appartiennent à $\mathbb{Q}$ ou à $\mathbb{Z}$. En ce qui concerne les matrices non-singulières, leurs seules unités sont l'identité usuelle, c'est-à-dire

$$E_r = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix},$$

où r est le nombre de lignes (ou de colonnes).

3.2.3 Décomposition en produit

Nous considérons une décomposition $A = MN$ comme licite si le nombre de colonnes de M égale le nombre de lignes de N et si il existe une unité

(entière) à droite pour M qui soit aussi une unité à gauche pour N. Nous dirons alors que M et N admettent une unité simultanée (attention cette notion n'est pas symétrique !). Cette condition, qui n'apparaît pas sur des anneaux intègres, est nécessaire ici pour tenir compte des diviseurs de 0. A partir des idées présentées dans ce mémoire, il est possible de montrer que, si une unité simultanée existe, alors elle est unique. Deux matrices de même rang ayant une unité fractionnaire simultanée peuvent ne pas avoir d'unité simultanée et la factorisation résultante n'est pas considérée comme étant licite. Par exemple,

$$A = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 1 & 0 \end{pmatrix} = MN.$$

Mais, il n'y a aucune unités entières simultanées entre M et N (Il est facile de voir que les unités à droite de M sont de la forme $\begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix}$; si cette matrice doit aussi être une unité à gauche pour N, alors il faut prendre $x = 1/3$). Laffey a montré [8] que toute matrice singulière s'écrit comme produit d'idempotents sur un anneau euclidien, ce qui montre clairement qu'une condition est nécessaire pour que le produit MN soit arithmétiquement intéressant. Remarquons finalement que dans le cas de matrices non-singulières, la condition d'existence d'une unité simultanée est automatiquement satisfaite.

3.2.4 Inverses de Siegel et matrices primitives

Nous nous tournons maintenant vers une notion assez courante en mathématiques, qui est celle d'inverse généralisé. L'inverse généralisé de Moore-Penrose par exemple est bien expliqué dans [12]. Nous considérons un inverse

bien adapté à notre situation : l'inverse de Siegel. Cet inverse dépend d'un choix d'unités à droite et à gauche.

Plus précisément, supposons que les deux matrices entières A et X aient une unité simultanée G et que X et A aient une unité simultanée G^*. Supposons en outre que $XA = G$ et que $AX = G^*$. Alors nous appelons X l'inverse de Siegel de A (relativement aux unités G et G^*). Remarquons que la liste suivante d'égalités est satisfaite : $G^2 = G$, $G^{*^2} = G^*$, $AG = A$, $G^*A = A$, $XG^* = X$, $GX = X$, $AX = G^*$ et $XA = G$. Si A admet un inverse de Siegel, A est dite primitive. Bien que X dépende de G et de G^*, son existence et le fait qu'elle soit entière sont eux indépendants des unités choisis. En ce qui concerne les matrices nonsingulières, l'inverse de Siegel est l'inverse usuel et les matrices primitives sont les matrices unimodulaires. Voici deux exemples : la matrice

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

est primitive ; en prenant $G^* = E_2$ et

$$G = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

qui sont des unités respectivement à gauche et à droite de A, la matrice

$$X = \begin{pmatrix} 0 & 0 \\ 1 & -1 \\ -1 & 2 \end{pmatrix}$$

est son inverse de Siegel. Par contre la matrice $B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}$ n'est pas primitive car, étant données des unités $G = E_2$ et $G^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, il n'y

a aucun inverse entier bien qu'un inverse fractionnaire $X = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \end{pmatrix}$ existe. Nous pouvons établir que les matrices primitives ont un discriminant égal à 1 et que les matrices primitives de rang maximal sont précisément celles qui peuvent être complétées en des matrices unimodulaires, i.e., $P \in \mathcal{M}_{m,n}(\mathbb{Z})$ de rang maximal est primitive si il existe une matrice $M \in \mathcal{M}_{m,m-n}(\mathbb{Z})$ (ou dans $\mathcal{M}_{n-m,n}(\mathbb{Z})$ selon que $m \geq n$ ou que $m < n$) telle que la matrice $\begin{pmatrix} P \\ M \end{pmatrix}$ (ou $\begin{pmatrix} P & M \end{pmatrix}$) soit dans $GL_m(\mathbb{Z})$ (resp. dans $GL_n(\mathbb{Z})$). Dans les exemples précédents, nous remarquons que $\begin{pmatrix} A \\ M \end{pmatrix}$ avec $M = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ est unimodulaire, mais il n'y a aucune matrice M entière telle que $\begin{pmatrix} B & M \end{pmatrix}$ soit dans $GL_3(\mathbb{Z})$.

3.3 Système d'équations linéaires Diophantiennes

Une équation Diophantienne, en mathématiques, est une équation polynomiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers. Nous traitons ici avec des système d'équations polynomiales dont on cherche les solutions en nombres entiers. Bien sûr, les polynômes sont à coefficients entiers. On peut soit vouloir seulement connaître l'existence de solutions, soit demander une description complète de l'ensemble des solutions. Nous présentons ici une première application de la forme normale de Smith des matrices ; c'est la résolution de systèmes d'équations linéaires Diophantiennes.

Étant donné un système d'équations linéaires $Ax = b$, où $A = (a_{i,j})$ est une matrice de type $m \times n$ à coefficients entiers, et b est un vecteur colonne de type $m \times 1$ avec des composants entiers, le système a-t-il une solution

entière, c'est-à-dire un vecteur solution x de type $n \times 1$ avec des composants entiers ? Comment savoir si un système d'équations Diophantiennes linéaires a un Solution ? Si des solutions existent, comment peut-on en trouver une ou toutes ? (*)

Notons que pour résoudre un système linéaire $AX = b$, où $A \in \mathcal{M}_{m,n}(\mathbb{Z})$, $B \in \mathcal{M}_{m,1}(\mathbb{Z})$ et $X \in \mathcal{M}_{n,1}(\mathbb{Z})$ on peut commencer par trouver $P \in GL_m(\mathbb{Z})$, $Q \in GL_n(\mathbb{Z})$ et $D \in M_{m,n}(\mathbb{Z})$ diagonale (avec diagonale croissante pour la relation de divisibilité) telles que $LAR = D$. Il y a un algorithme pour cela. Donc, $AX = B$ équivaut à $LAX = LB$, $LARR^{-1}X = LB$, i.e., l'équation s'écrit $DX' = B'$ où $X' = R^{-1}X$ (changement d'inconnue). Comme D est diagonale, c'est trivial à résoudre.

Théorème 3.3.1 (Théorème de Van Der Waerden) *Une solution entière du système existe si et seulement si, pour chaque vecteur ligne v avec des composants rationnels tels que vA a des composants entiers, vb est un entier.*

Soit $\mathbb{Z}$ l'anneau des nombres entiers, $\mathcal{M}_{m,m-n}(\mathbb{Z})$, $1 \leq m \leq n$, l'anneau de toutes les matrices entières de type $m \times n$, $GL_k(\mathbb{Z})$ l'ensemble de toutes les matrices carrées de type $k \times k$ à coefficients entiers et déterminant 1 ou -1 (matrices nimodulaires). On note par $D = diag(d_1, d_2, ..., d_m) \in \mathcal{M}_{m,m-n}(\mathbb{Z})$ la matrice diagonale qui a un entier d_i dans la position (i, i), $i = 1, ..., m$ et zéros ailleurs. Ensuite on a :

Théorème 3.3.2 *Soit $A \in \mathcal{M}_{m,m-n}(\mathbb{Z})$. Ils existent $L \in GL_m(\mathbb{Z})$ et $R \in GL_n(\mathbb{Z})$ telles que*

$$LAR = D = diag(d_1, d_2, ..., d_s, 0, ..., 0),$$

où $d_i > 0$, $i = 1, ..., s$, *et* $d_i \mid d_{i+1}$, $i = 1, ..., s-1$.

De plus, si A *est une matrice à coefficients dans cet anneau, il existe* $d_1, d_2, ..., d_s$ *éléments non nuls tels que* d_i *divise* d_{i+1} *et* A *est similaire à*

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & 0 \\ \vdots & \cdots & d_r & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Une preuve peut être trouvée, par exemple, dans [11].

L'idée est d'utiliser des opérations élémentaires de lignes et les colonnes de A. Les matrices L et R correspondent aux compositions de ces opérations. Bien que les matrices L et R dans le théorème 1 peuvent varier, la matrice D est définie uniquement par A et elle est appelée "forme normale de Smith" de la matrice A.

Notons tout de suite que le Théorème 1 peut être utilisé pour répondre à la question (*). Étant donné $Ax = b$, réécrivez-le comme $Dy = c$ avec $Ry = x$, $LAR = D$ et $c = Lb$. Mais la solution au système diagonal $Dy = c$ est facile. Plus de détails et une application numérique sont donnés dans l'Exemple 3.3.2.

Notre première application est liée à la question (*). Il contient également une preuve du théorème de Van Der Waerden. Soit $\mathbb{Q}$ le corps des nombres rationnels.

Théorème 3.3.3 . *Soit* A, L, R, D *comme dans le Théorème 3.3.2,* $b \in \mathbb{Z}^n$ *et* $c = Lb$. *Les quatre propositions suivantes sont équivalentes :*

1. *Le système d'équations linéaires* $Ax = b$ *a une solution entière,*

2. *Le système d'équations linéaires $Dy = c$ a une solution entière,*
3. *Pour tout vecteur rationnel u tel que uA est un vecteur entier, le nombre ub est un entier,*
4. *Pour tout vecteur rationnel v tel que vD est un vecteur entier, le nombre vc est un entier.*

Preuve. (1) $\Leftrightarrow$ (2). En effet on a, $Ax = b \Leftrightarrow (L^{-1}DR^{-1})x = b \Leftrightarrow D(R^{-1}x) = c \Leftrightarrow Dy = c$, où $y = R^{-1}x$. Comme $R \in GL_m(\mathbb{Z})$, alors $R^{-1} \in GL_m(\mathbb{Z})$. Par suite $x \in \mathbb{Z}^n \Leftrightarrow y = R^{-1}x \in \mathbb{Z}^n$.

(3) $\Leftrightarrow$ (4). En effet, $vD \in \mathbb{Z}^n \Leftrightarrow v(LAR) \in \mathbb{Z}^n \Leftrightarrow (vL)AR \in \mathbb{Z}^n \Leftrightarrow (vL)A \in \mathbb{Z}^n R^{-1} = \mathbb{Z}^n \Leftrightarrow uA \in \mathbb{Z}^n$, où $u = vL$. Comme $L \in GL_n(\mathbb{Z})$, alors $u \in Q^m \Leftrightarrow v \in Q^m$, et par (3), $ub \in Z$. Mais $ub \in \mathbb{Z} \Leftrightarrow (vL)(L^{-1}c) \in \mathbb{Z} \Leftrightarrow vc \in \mathbb{Z}$. Donc (3) implique (4). En inversant l'ordre de l'argument, on obtient $uA \in \mathbb{Z}^n \Leftrightarrow vD \in \mathbb{Z}^n$ et $vc \in \mathbb{Z} \Leftrightarrow ub \in \mathbb{Z}$. Donc (4) implique (3).

(2) $\Leftrightarrow$ (4). $Dy = c$ implique $v(Dy) = vc$ pour tout $v \in Qm$, par conséquent $(vD)y = vc$. Si $vD \in \mathbb{Z}^n$, alors $vc \in \mathbb{Z}$. Ainsi (2) implique (4). Afin de prouver que (4) implique (2), nous observons d'abord que $c = (c_1, ..., c_s, 0, ..., 0)$. Pour supposer $c_j \neq 0, j > s$. Posons $v = (0, ..., 0, \frac{1}{2c_j}, 0, ..., 0)$, où $\frac{1}{2c_j}$ apparaît en j-ième position. Puisque $vD = 0 \in \mathbb{Z}^n$, alors d'après (4) $vc = \frac{1}{2} \in \mathbb{Z}$, et nous arrivons à une contradiction. Ainsi $c_j = 0$ pour $j > s$. Ensuite, pour $i = 1, ..., s$, nous considérons des vecteurs $v_i = (0, ..., 0, \frac{1}{d_i}, 0, ..., 0)$. Comme $v_iD \in \mathbb{Z}^n$, alors d'après (4), $v_ic \in \mathbb{Z}$ et donc $\frac{c_i}{d_i} \in \mathbb{Z}$. Soit $y = (y_1, ..., y_s, 0..., 0)$, où $y_i = \frac{c_i}{d_i}$, $i = 1, ..., s$. Alors $y \in \mathbb{Z}^n$, et $Dy = c$. ■

Avec des notations comme dans la proposition 3.3.3, on peut réduire la solution du système $Ax = b$ à une solution de $Dy = c$ en effectuant des

transformations élémentaires (sur $\mathbb{Z}$) de lignes et de colonnes d'une matrice A augmenté de vecteur b. Les matrices L et R peuvent être construites en multipliant les matrices correspondant à ces transformations. Le système $Dy = c$ a une solution si et seulement si $c_{s+1} = ... = c_m = 0$, et $d_i|c_i$ pour $i = 1, ..., s$. Une solution générale de $Dy = c$ peut être donné sous la forme $y = (y_1, ..., y_s, t_1..., t_{m-s})$, où $y_i = \frac{c_i}{d_i}$, $i = 1, ..., s$, et $t_1..., t_{m-s}$ sont des paramètres entiers libres. Puis la solution générale de $Ax = b$ est juste Ry. De toute évidence, nous pouvons supposer que chaque équation est réduite du plus grand diviseur commun des coefficients des variables.

Exemple 3.3.1 Calculer l'ensemble des solutions entières du système diophantien $AX = B$ avec A et B des matrices à coefficients dans $\mathbb{Z}$. Ici, X est un vecteur colonne.

Il s'agit de calculer l'ensemble des solutions entières d'un système $AX = B$. Si B est nul, c'est aussi le noyau de l'application linéaire de $\mathbb{Z}$-modules donnée par A dans la base canonique.

Utilisons la forme normale de Smith. Soit $UAV = S$ la forme normale de Smith. Résoudre en entiers $AX = B$ est équivalent à résoudre $SY = C$ en entiers avec $C = UB$, le lien étant donné par $X = VY$. Le système $SY = C$ est de la forme :

$$\begin{cases} d_1 y_{n-t+1} = c_{n-t+1} \\ \quad ... = ... \\ d_t y_n = c_n \end{cases}$$

Lorsqu'une solution existe, ce qui se vérifie facilement sur C, il est maintenant facile de finir la résolution.

Exemple 3.3.2 Résoudre le système d'équations diophantiennes $Ax = b$, où

$$A = \begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix}, \; x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ et } b = \begin{pmatrix} 17 \\ -13 \end{pmatrix}.$$

Solution. Considérons une suite de transformations élémentaires de lignes et de colonnes de A. Il est bien connu qu'elles peuvent être réalisées en multipliant A par des matrices unimodulaires. Représentons la transformation des lignes par matrices L_i de type 2×2 et celles des colonnes par matrices R_j de type 3×3, où les indices inférieurs reflètent l'ordre des multiplications. Nous considérons les transformations (matrices) suivantes :

$$\begin{aligned} R_1 &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, R_2 = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, R_3 = \begin{pmatrix} 1 & 0 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ L_4 &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -5 & 1 \end{pmatrix}, R_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Soit $L = L_4$ et $R = R_1R_2R_3R_5R_6$. Alors

$$D = LAR = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 1 & 18 & 32 \\ 0 & -5 & -9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

et $c = Lb = \begin{pmatrix} 17 \\ -47 \end{pmatrix}$. Résoudre $Dy = c$. En posant $x = Ry$, on trouve

$$x = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 18 & 32 \\ 0 & -5 & -9 \end{pmatrix} \begin{pmatrix} 17 \\ -47 \\ t_1 \end{pmatrix} = \begin{pmatrix} 2t_1 - 47 \\ 32t_1 - 829 \\ 235 - 9t_1 \end{pmatrix}, \; t_1 \in \mathbb{Z}.$$

Chapitre 4

Quelques types de factorisation

Nous présentons une section importante dans la théorie de l'analyse matricielle traite de la factorisation des matrices entières comme le produit de matrices élémentaires. Dans certaines applications, on a besoin d'une matrice P telle que $A^{-1} = PP^t$, la décomposition spectrale, la factorisation de Cholesky d'une matrice définie positive symétrique est une représentation alternative très utile dans l'analyse de régression. Toute matrice définie positive symétrique A peut-être écrite comme le produit d'une matrice triangulaire inférieure L et sa transposée (qui est une matrice triangulaire supérieure) $L^t = U$. Ainsi, $A = LU$. En général, ces méthodes de factorisation LU ou QR ne sont pas utilisés de la même manière avec l'anneau $\mathbb{Z}$; car les éléments de L, U doivent être dans $\mathbb{Z}$. En général, i.e., le cas $n \times n$, il est très difficile de factoriser une matrice $A \in \mathcal{M}_n(\mathbb{Z})$ sous la forme LU ou QR, où L, U ou Q, R sont unimodulaires dans $\mathcal{M}_n(\mathbb{Z})$. Cependant, pour toute matrice carrée symétrique inversible à coefficients complexes A, on peut démontrer qu'il existe une matrice P tell que $A = PP^t$. Mais, cette dernière propriété tient avec peu de matrices à coefficients entiers. Comme nous l'avons vu à propos

de la factorisation des entiers dans le produit de puissances premières distinctes ; dans cette section, nous visons à voir des résultats similaires sur la factorisation des matrices à coefficients entiers comme le produit des matrices idempotents, nilpotents, unimodulaires,... Etc.

D'abord ; on parle de la factorisation d'une matrice $A \in \mathcal{M}_n(\mathbb{Z})$ comme le produit de deux matrices $W_1, W_2 \in \mathcal{M}_n(\mathbb{Z})$, qui ont des éléments suffisamment grands. Voici quelques exemples :

4.1 Exemples sur le produit de deux matrices ayant des éléments suffisamment grands

Exemple 4.1.1 On Considère la matrice suivante

$$A = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}.$$

Alors A^ω peut s'écrire sous la forme $S + W_1W_2$, où $W_1, W_2 \in \mathcal{M}_2(\mathbb{Z})$ sont en fonction de ω et $S \in \mathcal{M}_2(\mathbb{Z}^*)$ indépendant de ω.

En effet, d'aprés un calcul simple, on obtient

$$\begin{aligned} A^\omega &= \begin{pmatrix} 2^{\omega+1}-1 & 2^\omega-1 \\ 2-2^{\omega+1} & 2-2^\omega \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 2 & 2 \end{pmatrix} + 2^\omega \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & -1 \\ 2 & 2 \end{pmatrix} + 2^\omega \begin{pmatrix} 2 & 0 \\ -2 & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix} \\ &= \begin{cases} \begin{pmatrix} -1 & -1 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 2^{\frac{\omega}{2}+1} & 0 \\ -2^{\frac{\omega}{2}+1} & 0 \end{pmatrix} \begin{pmatrix} 2^{\frac{\omega}{2}} & 2^{\frac{\omega}{2}-1} \\ 0 & 2^{\frac{\omega}{2}} \end{pmatrix}, \text{ si } \omega \text{ est pair} \\ \begin{pmatrix} -1 & -1 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 2^{\frac{\omega-1}{2}+2} & 0 \\ -2^{\frac{\omega-1}{2}+2} & 0 \end{pmatrix} \begin{pmatrix} 2^{\frac{\omega-1}{2}} & 2^{\frac{\omega-1}{2}-1} \\ 0 & 2^{\frac{\omega-1}{2}} \end{pmatrix}, \text{ si } \omega \text{ est impair.} \end{cases} \end{aligned}$$

Remarque 4.1.1 Soit A la matrice de l'Exemple 4.1.1. Dans le cas où ω est

pair, on voit que

$$\begin{aligned} A^{\omega} &= I + \left(A^{\frac{\omega}{2}} - I\right)\left(A^{\frac{\omega}{2}} + I\right) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2^{\frac{\omega}{2}+1} - 2 & 2^{\frac{\omega}{2}} - 1 \\ 2 - 2^{\frac{\omega}{2}+1} & 1 - 2^{\frac{\omega}{2}} \end{pmatrix} \begin{pmatrix} 2^{\frac{\omega}{2}+1} & 2^{\frac{\omega}{2}} - 1 \\ 2 - 2^{\frac{\omega}{2}+1} & 3 - 2^{\frac{\omega}{2}} \end{pmatrix}. \end{aligned}$$

Dans le cas où ω est impair, on voit aussi que

$$\begin{aligned} A^{\omega} &= A + A\left(A^{\frac{\omega-1}{2}} - I\right)\left(A^{\frac{\omega-1}{2}} + I\right) \\ &= \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix} + \begin{pmatrix} 2^{\frac{\omega-1}{2}+1} - 2 & 2^{\frac{\omega-1}{2}} - 1 \\ 2 - 2^{\frac{\omega-1}{2}+1} & 1 - 2^{\frac{\omega-1}{2}} \end{pmatrix} \begin{pmatrix} 2^{\frac{\omega-1}{2}+1} & 2^{\frac{\omega-1}{2}} - 1 \\ 2 - 2^{\frac{\omega-1}{2}+1} & 3 - 2^{\frac{\omega-1}{2}} \end{pmatrix}. \end{aligned}$$

Proposition 4.1.1 *Soit A une matrice de la forme*

$$A = \begin{pmatrix} d & & & a_{ij} \\ & d & & \\ & & \ddots & \\ a_{ji} & & & d \end{pmatrix},$$

où d est suffisamment petits et au moins un des a_{ij} est suffisamment grand, et soit $k \geq 2$. Alors A^k est de la forme $d^k I + W_1 W_2$, où $W_1, W_2 \in \mathcal{M}_n(\mathbb{Z})$ ont des éléments suffisamment grands. [1]

Preuve. Il est clair que

$$A = \begin{pmatrix} d & & & 0 \\ & d & & \\ & & \ddots & \\ 0 & & & d \end{pmatrix}_D + \begin{pmatrix} 0 & & & a_{ij} \\ & 0 & & \\ & & \ddots & \\ a_{ji} & & & 0 \end{pmatrix}_B,$$

1. Notons que si k est impair avec $k \geq 3$, alors A^k peut être écrit simultanément sous la forme $I + W_1 W_2$ et $-I + W_1 W_2$ pour toute matrice A de type $n \times n$, où I est la matrice d'identité et W_1, W_2 sont deux matrices qui ont des éléments suffisamment grands. En effet, ceci est effectué en factorisant $A^k \pm I$.

où D est une matrice diagonale et B a au moins un élément suffisamment grand. Puisque $D = dI$ et B commutent, en appliquant le théorème binomial, on a

$$A^k = \sum_{i=0}^{k} C_k^i D^i B^{k-i} = d^k I + B\left(\sum_{i=0}^{k-1} C_k^i D^i B^{k-i-1}\right), \tag{4.1}$$

où le côté droit entre parenthèses (4.1) est suffisamment grand puisque $k \geq 2$. Ce qui achève la démonstration. ■

Corollaire 4.1.1 *Soit ω un entier positif suffisamment grand et soit A une matrice carrée à coefficients entiers de la forme*

$$A_n = \begin{pmatrix} 1 & -\omega & & & \\ & 1 & -\omega & & \\ & & \ddots & \ddots & \\ & & & 1 & -\omega \\ & & & & 1 \end{pmatrix}.$$

Alors pour tout $k \in \mathbb{Z}^*$, A_n^{-k} est de la forme $S + W_1 W_2$, où $S \in \mathcal{M}_n(\mathbb{Z})$ et $W_1, W_2 \in \mathcal{M}_n(\mathbb{Z})$ sont en fonction de ω.

Preuve. Notons que pour tout entier $k \geq 1$, $A_n^{-k} \in \mathcal{M}_n^*(\mathbb{Z})$ car $\det(A_n) = 1$. En effet, d'après un calcul simple, on obtient

$$A_n^{-1} = \begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ & 1 & \omega & \cdots & \omega^{n-2} \\ & & \ddots & \ddots & \vdots \\ & & & 1 & \omega \\ & & & & 1 \end{pmatrix}.$$

Comme les éléments diagonaux de A_n^{-1} sont égaux à 1, alors le résultat suit immédiatement par Proposition 4.1.1 pour tout $k \geq 2$. Dans le cas où $k = 1$,

on voit que

$$\begin{aligned} A_n^{-1} &= \underbrace{\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}}_{I} + \begin{pmatrix} 0 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ & 0 & \omega & \cdots & \omega^{n-2} \\ & & \ddots & \ddots & \vdots \\ & & & 0 & \omega \\ & & & & 0 \end{pmatrix} \\ &= I + \begin{pmatrix} 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega & \cdots & \\ & & \ddots & \ddots & \vdots \\ 0 & 0 & & 0 & \omega \\ 0 & 0 & & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ & 1 & \omega & \cdots & \omega^{n-2} \\ & & \ddots & \ddots & \vdots \\ 0 & 0 & & 1 & \omega \\ 0 & 0 & & & 1 \end{pmatrix}. \end{aligned}$$

Ce qui achève la démonstration. ■

Corollaire 4.1.2 *Soit $N = A^k$ une matrice de type $n \times n$ contient des entiers positifs suffisamment grands avec $k \geq 2$. Alors N est de la forme $S + W_1 W_2$, où $S \in \mathcal{M}_n(\mathbb{Z})$ et $W_1, W_2 \in \mathcal{M}_n(\mathbb{Z})$ ont des éléments suffisamment grands.*

Preuve. En effet, il y a deux cas :

1. Supposons que A contient des entiers positifs suffisamment grands. On voit que

$$\begin{aligned} N &= I + A^k - I^k \\ &= I + (A - I)\left(A^{k-1} + A^{k-2} + ... + A + I\right), \end{aligned}$$

qui est de la forme $I + W_1 W_2$, où $W_1 = A - I, W_2 = A^{k-1} + A^{k-2} + ... + A + I$ ont des éléments suffisamment grands.

2. Supposons que A a des éléments suffisamment petits, i.e., k est suffisamment grand. Dans ce cas, si k est pair on a

$$A^k = I + \left(A^{\frac{k}{2}} - I\right)\left(A^{\frac{k}{2}} + I\right), \tag{4.2}$$

et si k est impair on a aussi

$$A^k = A + A\left(A^{\frac{k-1}{2}} - I\right)\left(A^{\frac{k-1}{2}} + I\right),$$

comme demandé.

■

Remarque 4.1.2 Soit $A \in \mathcal{M}_2(\mathbb{Z})$ une matrice contient des entiers positifs suffisamment grands avec $tr(A) = 1$ et $\det(A)$ est suffisamment petit. Alors A est de la forme $S + W_1W_2$, où $S \in \mathcal{M}_n(\mathbb{Z})$ et $W_1, W_2 \in \mathcal{M}_n(\mathbb{Z})$ ont des éléments suffisamment grands. En effet, d'après le théorème de Cayley-Hamilton nous avons

$$A^2 + A + \det(A) I = 0,$$

et d'après le corollaire 4.1.2, $A^2 = S + W_1W_2$ où $S, W_1, W_2 \in \mathcal{M}_2(\mathbb{Z})$ avec S a des éléments suffisamment petits et W_1, W_2 ont des éléments suffisamment grands. Ainsi, on obtient

$$A = -(S + \det(A) I) - W_1W_2.$$

Enfin, nous présentons quelques bons résultats sur la factorisation ci-dessus qui se trouvent dans de nouveaux articles publiés. Notons que leur preuve est peu de difficultés et nécessite trop de bagages.

4.2 Quelques résultats typiques sur un corps $\mathbb{F}$

1. (Gustafson, Halmos, Radja vi [7]) Si $A \in \mathcal{M}_n(\mathbb{F})$ avec $\det A = \pm 1$ alors $A = J_1J_2J_3J_4$, où chaque J_i est une *involution* dans $\mathcal{M}_n(\mathbb{F})$, (c'est-à-dire $J_i^2 = I$).

2. (Ballantine [7]) Si $A \in \mathcal{M}_n(\mathbb{F})$ et $\det A = 0$, alors A est le produit de n matrices idempotents.
3. Si $A \in GL_n(\mathbb{F})$ alors A est similaire à LU où L est triangulaire inférieure et U est triangulaire supérieure.
4. **Quelques résultats sur l'anneau** $\mathbb{Z}$:

Théorème 4.2.1 *Soit* $D = diag(d_1, d_2, ..., d_{n-1}, 0) \in \mathcal{M}_n(\mathbb{Z})$ *une matrice diagonale singulière. Alors* D *est le produit de* n *matrices idempotents dans* $\mathcal{M}_n(\mathbb{Z})$.

Dans $\mathcal{M}_2(\mathbb{Z})$, notons que

$$\begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d-1 & 0 \end{pmatrix}.$$

Théorème 4.2.2 *Soit* $A \in SL_n(\mathbb{Z})$ *avec* $n \geq 3$. *Alors* A *est le produit de* $(I + R_1)(I + R_2)...(I + R_k)$, *où* $k = 5n + 31$ *et* R_1, $R_2, ..., R_k$ *ont la trace* 0 *et rang au plus un.*

Théorème 4.2.3 (Yuan [7]) *Si* $\det A = 0$ *et* A *n'est pas similaire à* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, *alors* $A = N_1 N_2$ *où* N_1, N_2 *sont nilpotentes.*

En 1988 [7, p. 32], Vaserstein prouvé que si $A \in \mathcal{M}_2(\mathbb{Z})$ a la trace 0, alors $A = PQ - QP$ pour certains $P, Q \in M_2(\mathbb{Z})$ et a demandé si le résultat peut être étendu à $\mathcal{M}_n(\mathbb{Z})$ $(n \geq 3)$. En 1994 (après six ans), Reams et Laffey prouvé le théorème suivant :

Théorème 4.2.4 (voir [11]) *Si* $A \in \mathcal{M}_n(\mathbb{Z})$ *a la trace* 0, *alors* $A = PQ - QP$ *pour certains* $P, Q \in M_n(\mathbb{Z})$.

Théorème 4.2.5 *Soit* $n \geq 3$. *Chaque élément* $A \in \mathcal{M}_n(\mathbb{Z})$ *avec* $\det A = 0$ *peut s'écrire comme produit de* $36n + 217$ *matrices idempotentes et* $72n + 434$ *matrice nilpotentes dans* $\mathcal{M}_2(\mathbb{Z})$.

5. **Questions ouvertes, voir [11].**

– Supposons que R est un anneau euclidien (par exemple $C[x]$, $\mathbb{Q}[x]$) et $A \in \mathcal{M}_n(R)$ a trace 0. Est-ce-que $A = PQ - QP$ pour certains $P, Q \in \mathcal{M}_n(R)$?

– On considère l'équation

$$f(X) = A, \tag{P}$$

où $A, X \in \mathcal{M}_n(\mathbb{Z})$ et $f : \mathbb{Z} \to \mathbb{Z}$ est une fonction arithmétique (X c'est la matrice inconnue). Si A est unimodulaire, est-ce-que l'équation (P) est toujours possède une solution dans $\mathcal{M}_n(\mathbb{Z})$.

Bibliographie

[1] C. S. Ballantine, Products of idempotent matrices. Linear Algebra Appl. 19,(1978), 81–86.

[2] G. Bhowmik, Fonctions diviseurs de matrices, l'Université des Sciences et Technologies de Lille, (1998) http ://math.univ-lille1.fr/˜bhowmik/files/Memoire.pdf.

[3] D. Carter and G. Keller, Elementary expressions for unimodular matrices. Comm. Algebra, 12,(1984),379–389.

[4] H. Cohen, A course in computational algebraic number theory. Graduate Texts in Mathematics, 138,Springer-V erlag, Berlin, 1993.

[5] Problem Department, Pi Mu Epsilon Journal, 12 No. 8 (2008) 494-496.

[6] T.J. Laffey, Products of idempotent matrices, Lin. and Multilinear Algebra 14 (1983), pages 309–314.

[7] T.J. Laffey, Lectures on Integer, Matrices. https ://pdfs.semanticscholar.org/3dfe/57pdf

[8] T. J. Laffey, Factorizations of integer matrices as products of idempotents and nilpotents. Linear Algebra Appl, 120,(1989),81–94.

[9] S.J. Leon. Linear Algebra with Applications, Sixth Edition. Prentice Hall, Upper Saddle River,N.J, 2002.

[10] M. Newman, Integral Matrices. Academic Press, 1972.

[11] C. Norman, Finitely Generated Abelian Groups and Similarity of Matrices over a Field, Springer-Verlag London Limited, 2012.

[12] R.C. Radhakrishna ; M.S. Kumar, Generalized Inverse of Matrices and its Applications. New York : John Wiley & Sons, 1971.