MATRICES

JEAN-MARC COUVEIGNES

RÉSUMÉ. On rassemble quelques définitions et résultats élémentaires de calcul matriciel.

TABLE DES MATIÈRES

1. MATRICE D'UNE APPLICATION LINÉAIRE ENTRE DEUX MODULES LIBRES

Soit A un anneau commutatif. On note $\mathcal{M}_{m,n}(A)$ l'ensemble des matrices $m \times n$ à coefficients dans A. C'est un A-module. On souhaitera parfois considérer des matrices à coefficients dans un A-module M. Si M est un A-module on note donc $\mathcal{M}_{m,n}(M)$ le A-module des matrices $m \times n$ à coefficients dans M. La multiplication des matrices définit une application bilinéaire de $\mathcal{M}_{m,n}(A) \times \mathcal{M}_{n,p}(M)$ dans $\mathcal{M}_{n,p}(M)$ et une autre application bilinéaire de $\mathcal{M}_{m,n}(M) \times \mathcal{M}_{n,p}(A)$ dans $\mathcal{M}_{n,p}(M)$.

On note $\mathrm{GL}_n(A)$ le groupe des matrices inversibles.

Soit M un A-module libre de rang r. Soit $B = (b_1, \dots, b_r)$ une base de M. On peut regarder B comme une matrice dans $\mathcal{M}_{1,r}(M)$.

Soit m un élément de M. Avec les coordonnées de m dans la base B on peut former un vecteur colonne $m_B \in \mathcal{M}_{r,1}(A)$ tel que le produit matriciel Bm_B soit égal à la matrice 1×1 dont le seul coefficient est m. On écrit abusivement

$$Bm_B = m.$$

Date: 3 octobre 2018.

Soit $B' = (b'_i)_{1\leqslant i\leqslant r}$ une autre base de M. La **matrice de passage** de B dans B' est la matrice formée des coordonnées colonnes des vecteurs de B' dans la base B. On la note $\mathbf{P}_{B,B'}$. On a

$$B' = B\mathbf{P}_{B,B'}.$$

Si m est un élément de M et si m_B et $m_{B'}$ sont les colonnes formées des coordonnées de m dans B et B' respectivement alors on a $m = Bm_B = B'm_{B'} = B\mathbf{P}_{B,B'}m_{B'}$ donc

$$m_B = \mathbf{P}_{B,B'}m_{B'}.$$

C'est la formule de changement de base.

Soit maintenant N un A-module libre de rang s. Soit $C = (c_1, \dots, c_s)$ une base de N. Soit

$$f : N \to M$$

une application linéaire. La matrice de f dans les bases C et B est formée des colonnes coordonnées des $f(c_j)$ dans la base B. On la note $\mathbf{M}(f, B, C) \in \mathcal{M}_{r,s}(A)$. On a donc

$$B\mathbf{M}(f, B, C) = f(C)$$

où B est la ligne $(b_i)_{1\leqslant i\leqslant r}$ et $f(C)$ est la ligne $(f(c_j))_{1\leqslant j\leqslant s}$.

Soit maintenant $C' = (c'_j)_{1\leqslant j\leqslant s}$ une autre base de N. La matrice de passage de C dans C' est la matrice des coordonnées colonnes des vecteurs de C' dans la base C. On la note $\mathbf{P}_{C,C'}$. On a

$$C' = C\mathbf{P}_{C,C'}.$$

On a

$$B'\mathbf{M}(f, B', C') = f(C') = f(C\mathbf{P}_{C,C'}) = f(C)\mathbf{P}_{C,C'} = B\mathbf{M}(f, B, C)\mathbf{P}_{C,C'}$$

donc

$$B\mathbf{P}_{B,B'}\mathbf{M}(f, B', C') = B\mathbf{M}(f, B, C)\mathbf{P}_{C,C'}$$

donc $\mathbf{P}_{B,B'}\mathbf{M}(f, B', C') = \mathbf{M}(f, B, C)\mathbf{P}_{C,C'}$ soit

$$\mathbf{M}(f, B', C') = \mathbf{P}^{-1}_{B,B'}\mathbf{M}(f, B, C)\mathbf{P}_{C,C'} = \mathbf{P}_{B',B}\mathbf{M}(f, B, C)\mathbf{P}_{C,C'}.$$

On passe de $\mathbf{M}(f, B, C)$ à $\mathbf{M}(f, B', C')$ en multipliant à gauche par une matrice de $\mathrm{GL}_r(A)$ et à droite par une matrice de $\mathrm{GL}_s(A)$.

L'application qui à une application linéaire $f : N \to M$ associe sa matrice dans les bases C et B est un isomorphisme de A-modules entre $\mathrm{Hom}_A(N, M)$ et $\mathcal{M}_{r,s}(A)$.

Soit O un A-module libre de rang t et $D = (d_1, \dots, d_t)$ une base de O. Soit $g : O \to N$ une application linéaire. On vérifie que

$$\mathbf{M}(f \circ g, B, D) = \mathbf{M}(f, B, C) \times \mathbf{M}(g, C, D).$$

On peut maintenant énoncer une version matricielle du théorème des facteurs invariants.

Théorème 1. *Soit A un anneau principal. Soient r et s deux entiers $\geqslant 1$. Soit M une matrice dans $\mathcal{M}_{r,s}(A)$. Il existe un entier $k \leqslant \min(r, s)$, deux matrices $P \in \mathrm{GL}_r(A)$ et $Q \in \mathrm{GL}_s(A)$ et des scalaires non-nuls a_1, a_2, …, a_k tels que $a_1|a_2|\dots|a_k$ et $M = PDQ^{-1}$ avec $D = \mathrm{Diag}(a_1, \dots, a_k, 0, 0, \dots, 0)$ dans $\mathcal{M}_{r,s}(A)$.*

Soit $f : A^s \to A^r$ l'application linéaire qui envoie la colonne c sur Mc. Soit C la base canonique de A^s et B la base canonique de A^r. La matrice de f dans les bases C et B est $\mathcal{M}(f, B, C) = M$.

Soit $K \subset A^s$ le noyau de f. C'est un sous-module de A^s. Le quotient A^s/K est isomorphe à l'image de f. Il est donc sans-torsion car A^r est sans torsion. Donc K admet un supplémentaire L dans A^s.

La restriction F de f à L est une bijection entre L et son image $f(L) \subset A^r$.

On applique le théorème de la base adaptée à l'inclusion $f(L) \subset A^r$. Il existe une base $B' = (b'_1, \ldots, b'_r)$ de A^r et des éléments $a_1, \ldots, a_r$ de A tels que $a_1 A \supset a_2 A \supset \cdots \supset a_r A$ et

$$f(L) = a_1 b'_1 \oplus \cdots \oplus a_r b'_r.$$

Soit k le plus grand entier tel que a_k soit non-nul.

Soient c'_1 l'unique antécédent de $a_1 b'_1$ par F. On définit de même $c'_2, \ldots, c'_k$. On obtient ainsi une base de L que l'on complète avec une base de K pour obtenir une base $C' = (c'_1, c'_2, \ldots, c'_s)$ de A^s. La matrice de f dans les bases C' et B' est $D = \mathrm{Diag}(a_1, \ldots, a_k, 0, 0, \ldots, 0)$, ce qui prouve le théorème. □

2. Matrices élémentaires

Soit A un anneau commutatif et $n \geqslant 1$ un entier.

2.1. Matrices $E_{i,j}$. On note $E_{i,j} \in \mathcal{M}_n(A)$ la matrice $n \times n$ dont toutes les entrées sont nulles sauf celle à l'intersection de la ligne i et de la colonne j, qui vaut 1. On vérifie que

$$E_{i,j} E_{k,l} = \delta_{j,k} E_{i,l}.$$

Donc si $M = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ on a $M = \sum_{1 \leqslant i,j \leqslant n} m_{i,j} E_{i,j}$ et

$$E_{i,j} M E_{k,l} = m_{j,k} E_{i,l}.$$

On en déduit une description des idéaux bilatères de $\mathcal{M}_n(A)$.

Théorème 2. *Soit A un anneau commutatif et $n \geqslant 2$ un entier. Soit I un idéal bilatère de $\mathcal{M}_n(A)$. Soit J l'idéal de A engendré par tous les coefficients de toutes les matrices dans I. Alors I est l'ensemble $\mathcal{M}_n(J)$ des matrices à coefficients dans J.*

L'inclusion $I \subset \mathcal{M}_n(J)$ est évidente. Si $M = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ est dans I alors

$$E_{1,i} M E_{j,1} = m_{i,j} E_{1,1} \in I.$$

On en déduit que $J E_{1,1} \subset I$. On montre de même que $J E_{k,l} \subset I$ pour tous $1 \leqslant k, l \leqslant n$. □

On classifie de même les idéaux à gauche de $\mathcal{M}_n(A)$.

Théorème 3. *Soit A un anneau commutatif et $n \geqslant 2$ un entier. Soit I un idéal à gauche de $\mathcal{M}_n(A)$. Soit J le sous-module de A^n engendré par toutes les lignes de toutes les matrices dans I. Alors I est l'ensemble L des matrices qui ont toutes leurs lignes dans J.*

L'inclusion $I \subset L$ est évidente. Si $M = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ est dans I alors $E_{1,i}M \in I$. C'est la matrice dont toutes les lignes sont nulles sauf la première qui est égale à la i-ième ligne de M. On en déduit que tout matrice qui a sa première ligne dans J et toutes ses autres lignes nulles est dans I. On montre de même que tout matrice qui a sa k-ième ligne dans J et toutes ses autres lignes nulles est dans I. Donc $L \subset I$. □

Exercice 1 : Soit A un anneau commutatif et $n \geqslant 1$. Montrer que le centre de $\mathcal{M}_n(A)$ est formé des matrices scalaires. Autrement dit $Z(\mathcal{M}_n(A)) = AI_n$.

Soit M une matrice dans le centre de $\mathcal{M}_n(A)$. La matrice $E_{i,i}M$ est obtenue en annulant toutes les lignes de M sauf la i-ième. La matrice $ME_{i,i}$ est obtenue en annulant toutes les colonnes de M sauf la i-ième. Comme $E_{i,i}M = ME_{i,i}$ on déduit que la i-ième ligne se réduit à son terme diagonal. Donc la matrice M est diagonale. On peut écrire $M = \sum_{1 \leqslant k \leqslant n} a_k E_{k,k}$. On vérifie que $E_{1,i}M = a_i E_{1,i}$ et $ME_{1,i} = a_1 E_{1,i}$. Donc $a_i = a_1$ pour tout i et la matrice est scalaire.

2.2. **Matrices de permutations.** Soit σ une permutation dans S_n. Soit

$$P_\sigma = (\delta_{i,\sigma(j)})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(A).$$

On vérifie que P_σ est la matrice dans la base canonique $(e_1, \dots, e_n)$ de l'endomorphisme u_σ qui envoie e_i sur $e_{\sigma(i)}$ pour tout $1 \leqslant i \leqslant n$. On en déduit que

$$P_{\sigma\tau} = P_\sigma P_\tau$$

puisque $u_{\sigma\tau} = u_\sigma \circ u_\tau$.

Soit M une matrice $m \times n$. La matrice MP_σ a les mêmes colonnes que M mais elles sont permutées selon σ. Plus précisément la colonne i de MP_σ est la colonne $\sigma(i)$ de M.

Soit maintenant M une matrice $n \times m$. La matrice $P_\sigma M$ a les mêmes lignes que M mais elles sont permutées selon σ^{-1}. Plus précisément la ligne i de $P_\sigma M$ est la ligne $\sigma^{-1}(i)$ de M.

2.3. **Matrices $F_{i,j}(a)$.** Si $1 \leqslant i, j \leqslant n$ et $a \in A$ on note $F_{i,j}(a)$ la matrice $I_n + aE_{i,j}$. C'est une matrice inversible. Son inverse est $F_{i,j}(-a)$.

Soit M une matrice $m \times n$. La matrice $MF_{i,j}(a)$ est obtenue à partir de M en ajoutant à la j-ième colonne de M le produit de a par sa i-ième colonne.

Soit maintenant M une matrice $n \times m$. La matrice $F_{i,j}(a)M$ est obtenue à partir de M en ajoutant à la i-ième ligne de M le produit de a par sa j-ième ligne.

2.4. **Matrices $E_i(u)$.** Si u est une unité de A on note $E_i(u)$ la matrice diagonale dont les entrées diagonales sont toutes égales à 1 sauf celle en position (i, i) qui vaut u.

Soit M une matrice $m \times n$. La matrice $ME_i(u)$ est obtenue à partir de M en multipliant la i-ième colonne par u.

Soit maintenant M une matrice $n \times m$. La matrice $E_i(u)M$ est obtenue à partir de M en multipliant la i-ième ligne par u.

2.5. **Opérations élémentaires.** La définition suivante est souvent admise.

Definition 1. *On appelle* **matrices élémentaires** *les matrices définies ainsi :*

— *les matrices P_σ pour σ dans S_n,*
— *les matrices $E_i(u)$ pour $1 \leqslant i \leqslant n$ et $u \in A^*$,*
— *les matrices $F_{i,j}(a)$ pour $1 \leqslant i, j \leqslant n$ et $a \in A$.*

Les **opérations élémentaires** sur les lignes d'une matrice M à coefficients dans A sont obtenues en multipliant M à gauche par une matrice élémentaire.

Les **opérations élémentaires** sur les colonnes de M sont obtenues en multipliant M à droite par une matrice élémentaire.

Toutes les matrices élémentaires d'ordre n sont dans $\mathrm{GL}_n(A)$ le groupe des matrices inversibles dans $\mathcal{M}_n(A)$.

2.6. **Algorithme de réduction.** On suppose que A est euclidien. Il existe donc une application $v : A \smallsetminus \{0_A\} \to \mathbf{N}$ telle que

(1) Si $a, b \in A$ et $b \neq 0_A$ il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0_A$ ou $v(r) < v(b)$.
(2) Si $a, b \in A \smallsetminus \{0_A\}$ alors $v(ab) \geqslant v(a)$.

On se donne M une matrice $r \times s$ à coefficients dans A. On sait qu'il existe des matrices $P \in \mathrm{GL}_r(A)$ et $Q \in \mathrm{GL}_s(A)$ et des scalaires non-nuls a_1, a_2, $\ldots$, a_k tels que $a_1|a_2|\ldots|a_r$ et $M = PDQ$ avec $D = \mathrm{Diag}(a_1, \ldots, a_k, 0, 0, \ldots, 0)$ dans $\mathcal{M}_{r,s}(A)$.

On cherche P et Q sous la forme de produits de matrices élémentaires. Autrement dit on cherche une succession d'opérations élémentaires sur les lignes et les colonnes qui diagonalisent M. On suppose que M n'est pas nulle. L'algorithme de réduction procède de la façon suivante.

(1) Soit $m_{i,j}$ celui des coefficients non-nuls de M où v prend sa plus petite valeur. On échange les lignes 1 et i. On échange les colonnes 1 et j.
(2) Pour tout $j > 1$ on écrit $m_{1,j} = m_{1,1}q + r$ la division euclidienne de $m_{1,j}$ par $m_{1,1}$. On retranche q fois la première colonne à la j-ième colonne.
(3) Pour tout $i > 1$ on écrit $m_{i,1} = m_{1,1}q + r$ la division euclidienne de $m_{i,1}$ par $m_{1,1}$. On retranche q fois la première ligne à la i-ième ligne.
(4) S'il existe un élément non-nul autre que $m_{1,1}$ dans la première ligne (resp. dans la première colonne) on le fait remonter en position $(1, 1)$ en échangeant sa ligne (resp. sa colonne) avec la première. On repars à l'étape 2.
(5) On a maintenant une matrice M de la forme $\begin{pmatrix} m_{1,1} & 0_{1,p} \\ 0_{n-1,1} & N_{n-1,p-1} \end{pmatrix}$.

   Si $m_{1,1}$ divise tous les coefficients de N, on applique l'algorithme à N récursivement, ce qui n'affecte pas la première ligne ni la première colonne de M.

   S'il existe au contraire un coefficient dans N qui n'est pas divisible par $m_{1,1}$, on ajoute la ligne qui contient ce coefficient à la première ligne de M et on repars à l'étape 1.

Une conséquence théorique de cet algorithme est que les matrices élémentaires engendrent $\mathrm{GL}_n(A)$ si A est euclidien.

Théorème 4. *Soit A un anneau euclidien et $n \geqslant 2$ un entier. L'ensemble des matrices élémentaires telles que définies à la définition 1 engendre* $\mathrm{GL}_n(A)$.

En effet si $M \in \mathrm{GL}_n(A)$ on peut lui appliquer l'algorithme de réduction et trouver deux produits de matrices élémentaires G et D tels que GMD soit diagonale. On note $N = GMD$. Comme M est inversible, N est inversible elle aussi. Donc les entrées de N sont des unités de A. On peut donc écrire $N = \prod_{1 \leqslant i \leqslant n} E_i(n_{i,i})$. Donc

$$M = G^{-1}\left(\prod_{1\leqslant i\leqslant n} E_i(n_{i,i})\right)D^{(-1)}$$

est un produit de matrices élémentaires. □

2.7. **Déterminant.** Le **déterminant** de M est le scalaire

$$\det(M) = \sum_{\sigma \in S_n} \epsilon(\sigma) m_{\sigma(1),1} m_{\sigma(2),2} \dots m_{\sigma(n),n}.$$

Exercice 2 : Montrer que si une matrice a deux colonnes égales alors son déterminant est nul.

Exercice 3 : Montrer que M et sa transposée ${}^tM$ on le même déterminant.

Exercice 4 : Calculer le déterminant de P_σ et de $E_{i,j}(a)$.

---

3. Formes multilinéaires

Soit A un anneau commutatif. Soit $p \geqslant 1$ un entier et $F_1, \dots, F_p$ des A-modules. Soit E un A-module. Une application $f : F_1 \times \dots \times F_p \to E$ est dite **multilinéaire** si pour tout $1 \leqslant i \leqslant p$ et pour tous éléments $y_j \in F_j$ pour $j \neq i$ l'application $x \mapsto f(y_1, y_2, \dots, y_{j-1}, x, y_{j+1}, \dots, y_p)$ est une application linéaire de F_i dans E. Autrement dit f est linéaire en chacun de ses arguments.

Une application multilinéaire $f : N^p \to A$ est appelée **forme p-linéaire**. Une telle application est dite **alternée** si pour tous $(y_1, \dots, y_p) \in N^p$ tels que $y_i = y_j$ pour deux indices i et j distincts on a $f(y_1, \dots, y_p) = 0$.

L'ensemble des formes p-linéaires alternées sur N est un A-module.

Soit maintenant N un module libre de rang n et soit $B = (b_1, \dots, b_n)$ une base de N. On définit une application de $f_B : N^n \to A$ de la façon suivante. Pour $(v_1, \dots, v_n) \in N^n$ on forme une matrice V en juxtaposant les colonnes coodonnées de $v_1, \dots, v_n$ dans la base B et on pose $f_B(v_1, \dots, v_n) = \det(V)$. Il est facile de vérifier que cette application est une forme n-linéaire alternée. Cette forme n'est pas identiquement nulle.

Soit maintenant $f : N^n \to A$ une forme n-linéaire alternée. On vérifie que pour tous $v_1, \dots, v_n$

$$f(v_1, \dots, v_n) = f_B(v_1, \dots, v_n) \times f(e_1, \dots, e_n).$$

Donc l'ensemble des formes n-linéaire sur N est un module libre de rang 1.

Soit maintenant u un endomorphisme du A-module N. À toute forme n-linéaire f de N on associe une forme n-linéaire f^u définie par

$$f^u(v_1, \dots, v_n) = f(u(v_1), \dots, u(v_n)).$$

Comme le module des formes n-linéaires alterné est libre de rang 1. Il existe un scalaires noté $\det(u)$ tel que pour tout f on ait $f^u = \det(u).f$.

On vérifie que $\det(u)$ est le déterminant de la matrice de u dans n'importe quelle base de N. Il résulte de la définition que $\det(u \circ v) = \det(u) \times \det(v)$ pour tous endomorphismes u et v de N. On en déduit que $\det(M_1 M_2) = \det(M_1)\det(M_2)$ pour toutes matrices M_1 et M_2 dans $\mathcal{M}_{n\times n}(A)$. En particulier, si une matrice est inversible, son déterminant est une unité.

Si M est une matrice carrée dans $\mathcal{M}_{n\times n}(A)$ on note $M_{i,j}$ la matrice de $\mathcal{M}_{(n-1)\times(n-1)}(A)$ obtenue en retirant la i-ième ligne et la j-ième colonne de M. On dit que $M_{i,j}$ est une **sous-matrice** de M.

On a

$$\det(M) = \sum_{1\leqslant k\leqslant n} (-1)^{i+k} m_{i,k} \det(M_{i,k}) = \sum_{1\leqslant k\leqslant n} (-1)^{i+k} m_{k,i} \det(M_{k,i}).$$

On dit que les $(-1)^{i+j}\det(M_{i,j})$ sont les **cofacteurs** de M. On note $\tilde{M} = ((-1)^{i+j}\det(M_{i,j}))_{1\leqslant i,j\leqslant n}$ la matrice des cofacteurs. On l'appelle la **comatrice** de M. On a

$$M^t\tilde{M} = {}^t\tilde{M}M = \det(M)\mathrm{I}_n.$$

On en déduit qu'une matrice carrée est inversible si et seulement si son déterminant est une unité de A.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, BORDEAUX INP, INRIA, CNRS, UMR 5251, F-33400 TALENCE, FRANCE.

E-mail address: Jean-Marc.Couveignes@u-bordeaux.fr