Déterminant des matrices à coefficients dans un anneau

Cette note présente une relecture (complétée) d'un résultat que l'on trouve dans Leichtnam, Schauer, Exercices corrigés de Mathématiques posés aux oraux X-ENS, Algèbre 1, *Ellipses.* Il peut servir de développement pour la leçon :

- Déterminant. Exemples et applications.

Par ailleurs, comme les anneaux les plus importants au programme (mis à part les corps) sont les anneaux principaux, en insistant plus sur l'aspect ¡¡ matrices à coefficients dans un anneau principal ¿¿ on peut aussi imaginer une utilisation dans les leçons :

- Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- Anneaux principaux. Applications.

Soit donc A un anneau commutatif avec un élément unité noté 1.

Théorème : *Soit M une matrice de taille n à coefficients dans A, et $f : A^n \to A^n$ l'endomorphisme A-linéaire associé. Alors :*

(1) *f est surjectif ssi f est bijectif ssi* $\det(f)$ *est inversible dans A.*
(2) *f est injectif ssi* $\det(f)$ *est non diviseur de zéro dans A.*

De plus, dans le cas injectif,

(3) *Si $A = \mathbb{Z}$, le conoyau de f est fini de cardinal* $|\det(f)|$.
(4) *Si $A = k[X]$, le conoyau de f est un k-espace vectoriel de dimension finie égale à* $\deg(\det(f))$.

Rappelons que le *conoyau* est le quotient de l'ensemble but par l'image, i.e. $\mathrm{coker}(f) = A^n/f(A^n)$. Le conoyau est une mesure du défaut de surjectivité de la même façon que le noyau est une mesure du défaut d'injectivité. Ainsi, f est surjectif si et seulement si $\mathrm{coker}(f) = 0$.

Démonstration : On notera $e_1, \dots, e_n$ la base canonique de A^n.

(1) Si f est surjectif, pour tout i il existe un vecteur ϵ_i tel que $f(\epsilon_i) = e_i$. Si l'on pose $g(e_i) = \epsilon_i$ pour tout i, on définit un unique morphisme $g : A^n \to A^n$. De plus, on a $f \circ g = \mathrm{Id}$ car ceci est vrai pour tous les e_i, qui forment une partie génératrice. On en déduit que $\det(f)\det(g) = 1$ et donc $\det(f)$ est inversible. Alors, la formule de la comatrice :

$$M{}^t\tilde{M} = {}^t\tilde{M}M = \det(M)\,\mathrm{Id}$$

montre que f est bijectif. Comme enfin bijectif implique surjectif, on a tout démontré.

(2) Posons $d = \det(f)$. Si d est non diviseur de zéro, supposons que $f(x) = 0$. Matriciellement, on a $Mx = 0$ et en appliquant la transposée de la comatrice, on trouve $dx = 0$. En regardant les coordonnées de x, l'hypothèse sur d implique que $x = 0$ donc f est injectif.

Réciproquement, si d est diviseur de zéro, on va montrer que f n'est pas injectif. Soit $u \in A$ non nul tel que $ud = 0$.

Si pour tout mineur μ de M on a $u\mu = 0$, alors en particulier ceci est vrai pour les mineurs de taille 1, i.e. les coefficients de la matrice M. On a donc $f(ue_1) = 0$, or $ue_1 \neq 0$, donc f n'est pas injectif.

Sinon, il existe une matrice extraite N de M telle que $u\det(N) \neq 0$. Choisissons une telle matrice de taille r maximale ; on a $r < n$ puisque $ud = 0$. Quitte à réordonner les vecteurs de base à la source et au but, c'est-à-dire à multiplier M à gauche et à droite par des matrices de permutation, on peut supposer que N est la matrice de taille r située en haut à gauche. Maintenant, pour chaque $i \in \{1, \dots, n\}$, bordons les r premières lignes de M inférieurement avec la i-ème ligne, et appelons P_i la matrice de taille $r+1$ située à gauche :

$$P_i = \begin{pmatrix} m_{1,1} & \dots & m_{1,r+1} \\ \vdots & & \vdots \\ m_{r,1} & \dots & m_{r,r+1} \\ m_{i,1} & \dots & m_{i,r+1} \end{pmatrix}.$$

Pour $i \leq r$ la matrice P_i a deux lignes égales donc son déterminant est nul, et pour $i \geq r+1$ c'est une matrice extraite de M de taille $r+1$, donc son déterminant est annulé par u compte tenu de l'hypothèse sur r. Dans les deux cas $u\det(P_i) = 0$, et si on développe par rapport à la dernière ligne, on trouve $u\sum_{j=1}^{r+1}(-1)^j m_{i,j}\mu_j = 0$ où μ_j est le mineur du coefficient de position $(r+1, j)$. Pour i variant, ces égalités disent exactement que $M(ux) = 0$ où x est le vecteur de coordonnées $(-\mu_1, \dots, (-1)^{r+1}\mu_{r+1}, 0, \dots, 0)$. Comme $u\mu_{r+1} = u\det(N) \neq 0$, on a $ux \neq 0$, donc f n'est pas injectif.

(3) D'après les résultats sur les classes de congruence de matrices à coefficients dans un anneau principal, il existe des matrices R, S inversibles à coefficients dans $\mathbb{Z}$ telles que $D := RMS$ est diagonale d'éléments diagonaux égaux aux facteurs invariants $d_1, \dots, d_n$ tels que $d_i | d_{i+1}$ pour tout i. On en déduit que

$$\mathrm{coker}(f) \simeq \mathbb{Z}^n / D(\mathbb{Z}^n) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$$

de sorte que $|\,\mathrm{coker}(f)| = d_1 \dots d_n = |\det(f)|$.

(4) Le raisonnement est le même : il existe des matrices R, S inversibles à coefficients dans $k[X]$ telles que $D := RMS$ est diagonale d'éléments diagonaux égaux aux facteurs invariants $P_1, \dots, P_n$ tels que $P_i | P_{i+1}$ pour tout i. On en déduit que

$$\mathrm{coker}(f) \simeq \frac{k[X]}{(P_1)} \times \dots \times \frac{k[X]}{(P_n)}$$

puis $\dim_k(\mathrm{coker}(f)) = \deg(P_1) + \dots + \deg(P_n) = \deg(P_1 \dots P_n) = \deg(\det(f))$. $\square$