Université de Rennes 1 | Master M1 de mathématiques
Année 2006-2007 | H04. Théorie algébrique des nombres

Feuille de TD 3

Exercice 1

1. Soit $\mathbf{K}$ un corps, $m \geqslant 1$ et $n \geqslant 1$ des entiers et $\mathcal{M}_{m,n}(\mathbf{K})$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans $\mathbf{K}$. Deux matrices M et N de $\mathcal{M}_{m,n}(\mathbf{K})$ sont dites *L-équivalentes* si on peut passer de M à N par des opérations élémentaires sur les lignes. Vérifier que la L-équivalence est une relation d'équivalence sur $\mathcal{M}_{m,n}(\mathbf{K})$, et que deux matrices L-équivalentes ont le même rang.
2. Soit $M \in \mathcal{M}_{m,n}(\mathbf{K})$. On dit que M est *sous forme normale échelonnée selon les lignes* s'il existe un entier r tel que $0 \leqslant r \leqslant m$ et les propriétés suivantes sont vérifiées :
   (a) les r premières lignes de M sont non nulles et les $m - r$ dernières lignes de M sont nulles ; pour tout i vérifiant $1 \leqslant i \leqslant r$, on note $p(i)$ le plus petit indice tel que $m_{i,p(i)}$ soit non nul ;
   (b) la suite $(p(i))_{1 \leqslant i \leqslant r}$ est strictement croissante (la suite $(p(i))_{1 \leqslant i \leqslant r}$ est appelée *suite des pivots* de la matrice M) ;
   (c) pour tout $1 \leqslant i \leqslant r$ on a $m_{i,p(i)} = 1$;
   (d) pour tout $1 \leqslant i \leqslant r$ et tout $j < i$, le coefficient $m_{j,p(i)}$ est nul.

   Vérifier que pour une telle matrice M, r est le rang de M. Montrer que toute matrice de $\mathcal{M}_{m,n}(\mathbf{K})$ est L-équivalente à une matrice sous forme normale échelonnée selon les lignes. Montrer que toute matrice de $\mathrm{GL}_m(\mathbf{K})$ est L-équivalente à la matrice identité ; en déduire que deux matrices M et N de $\mathcal{M}_{m,n}(\mathbf{K})$ sont L-équivalentes si et seulement s'il existe un élément U de $\mathrm{GL}_m(\mathbf{K})$ tel que $M = U\,N$.
3. Soit M une matrice de $\mathcal{M}_{m,n}(\mathbf{K})$. Par des opérations élémentaires sur les lignes de M, on transforme M en une matrice sous forme normale échelonnée selon les lignes. On effectue les mêmes opérations élémentaires sur les lignes de la matrice identité de taille m. Qu'obtient-on ?
4. Soit E et F des $\mathbf{K}$-espace vectoriels de dimension finie m et n respectivement. Soit $\mathcal{B} = (e_j)_{1 \leqslant j \leqslant n}$ une base de E. Pour $0 \leqslant j \leqslant n$, soit E_j le sous-espace de E engendré par les $(e_k)_{1 \leqslant k \leqslant j}$. Soit u une application linéaire de E vers F. Pour $0 \leqslant j \leqslant n$, on pose $d_j^{\mathcal{B}}(u) = \dim(\mathrm{Ker}(u) \cap E_j)$. Les

$\mathcal{B}$-*paliers* de u sont les entiers j vérifiant $1 \leqslant j \leqslant n$ et $d_j^{\mathcal{B}}(u) = d_{j-1}^{\mathcal{B}}(u)$. Vérifier que le nombre de $\mathcal{B}$-paliers de u est égal au rang de u. Soit $\mathcal{B}'$ une base de F et $M = \mathrm{Mat}(u, \mathcal{B}, \mathcal{B}')$. On suppose que M est sous forme normale échelonnée selon les lignes. Montrer que la suite des $\mathcal{B}$-paliers de u est la suite des pivots de M.

5. Soit M et N deux matrices de $\mathcal{M}_{m,n}(\mathbf{K})$ qui sont sous forme normale échelonnée selon les lignes et L-équivalentes. Déduire du 4. que $M = N$. Ainsi toute matrice M de $M_{n,m}(\mathbf{K})$ est L-équivalente à une unique matrice sous forme normale échelonnée selon les lignes. On appelle cette matrice la *forme normale échelonnée selon les lignes* de M.
6. Énoncer les versions «tranposées» des résultats précédents (C-équivalence, forme normale échelonnée selon les colonnes...)

Exercice 2

1. Soient $m \geqslant 1$ et $n \geqslant 1$ des entiers et $\mathcal{M}_{m,n}(\mathbf{Z})$ l'ensemble des matrices à m lignes et n colonnes. Deux matrices M et N de $\mathcal{M}_{m,n}(\mathbf{Z})$ sont dites dites ***Z**-L-équivalentes* si on peut passer de M à N par des $\mathbf{Z}$-opérations élémentaires sur les lignes. Montrer que la $\mathbf{Z}$-L-équivalence est une relation d'équivalence sur $\mathcal{M}_{m,n}(\mathbf{Z})$.
2. Soit $M \in \mathcal{M}_{m,n}(\mathbf{Z})$. On dit que M est *sous forme normale de Hermite selon les lignes* s'il existe un entier r tel que $0 \leqslant r \leqslant m$ et les propriétés suivantes sont vérifiées :

   (a) les r premières lignes de M sont non nulles et les $m - r$ dernières lignes de M sont nulles ;

   (b) pour tout i vérifiant $1 \leqslant i \leqslant r$, soit $p(i)$ le plus petit indice tel que $m_{i,p(i)}$ soit non nul ; la suite $(p(i))_{1 \leqslant i \leqslant r}$ est strictement croissante et pour tout $1 \leqslant i \leqslant r$ on a $m_{i,p(i)} > 0$;

   (c) pour tout $1 \leqslant i \leqslant r$ et tout $j < i$, on a $0 \leqslant m_{j,p(i)} < m_{i,p(i)}$.

   Montrer que toute matrice de $\mathcal{M}_{m,n}(\mathbf{Z})$ est $\mathbf{Z}$-L-équivalente à une matrice sous forme normale de Hermite selon les lignes. Montrer que toute matrice de $\mathrm{GL}_m(\mathbf{Z})$ est $\mathbf{Z}$-L-équivalente à la matrice identité ; en déduire que deux matrices M et N de $\mathcal{M}_{m,n}(\mathbf{Z})$ sont L-équivalentes si et seulement s'il existe un élément U de $\mathrm{GL}_m(\mathbf{Z})$ tel que $M = U\,N$.
3. Comment s'obtient la forme normale échelonnée selon les lignes d'une matrice sous forme normale de Hermite selon les lignes ?
4. Soit M une matrice de $\mathcal{M}_{m,n}(\mathbf{Z})$. Par des $\mathbf{Z}$-opérations élémentaires sur les lignes de M, on transforme M en une matrice sous forme normale

de Hermite selon les lignes. On effectue les mêmes **Z**-opérations élémentaires sur les lignes de la matrice identité de taille m. Qu'obtient-on ?

5. Soit M et N deux matrices de $\mathcal{M}_{m,n}(\mathbf{Z})$ qui sont sous forme normale de Hermite selon les lignes et **Z**-L-équivalentes. Montrer que $M = N$. Ainsi toute matrice M de $M_{n,m}(\mathbf{Z})$ est **Z**-L-équivalente à une unique matrice sous forme normale de Hermite selon les lignes. On appelle cette matrice la *forme normale de Hermite selon les lignes* de M.
6. Énoncer les résultats «transposés» des résultats précédents.

Exercice 3

1. Deux matrices M et N de $\mathcal{M}_{m,n}(\mathbf{Z})$ sont dites **Z**-équivalentes s'il existe des éléments U de $\mathrm{GL}_m(\mathbf{Z})$ et V de $\mathrm{GL}_n(\mathbf{Z})$ tels que $M = U\,N\,V$. Vérifier que la **Z**-équivalence est une relation d'équivalence sur $\mathcal{M}_{m,n}(\mathbf{Z})$ (ouf...) et que deux matrices de $\mathcal{M}_{m,n}(\mathbf{Z})$ sont **Z**-équivalentes si et seulement si l'une se déduit de l'autre par des **Z**-opérations élémentaires sur les lignes et les colonnes.
2. Soit $M \in \mathcal{M}_{m,n}(\mathbf{Z})$. On dit que M est *sous forme normale de Smith* si elle est diagonale à coefficients diagonaux positifs et pour tout i vérifiant $1 \leqslant i \leqslant \mathrm{Min}(m,n) - 1$, $m_{i,i}$ divise $m_{i+1,i+1}$. Montrer que toute matrice M de $\mathcal{M}_{m,n}(\mathbf{Z})$ est **Z**-équivalente à une matrice sous forme normale de Smith.
3. Soit $M \in \mathcal{M}_{m,n}(\mathbf{Z})$. Pour tout i vérifiant $1 \leqslant i \leqslant \mathrm{Min}(m,n)$, soit $\Delta_i(M)$ le pgcd des mineurs d'ordre i de la matrice M. Montrer que si N s'obtient à partir de M par des **Z**-opérations élementaires sur les lignes, on a $\Delta_i(N) = \Delta_i(M)$ pour tout i. Calculer les $\Delta_i(M)$ si M est sous forme normale de Smith.
4. Déduire de la question précédente que toute matrice $M \in \mathcal{M}_{m,n}(\mathbf{Z})$ est **Z**-équivalente à une unique matrice sous forme de Smith ; on appelle cette matrice la *forme normale de Smith* de M.
5. Soit M une matrice de $\mathcal{M}_{m,n}(\mathbf{Z})$. Par des **Z**-opérations élémentaires sur les lignes et les colonnes de M, on transforme M en une matrice sous forme normale de Smith. On effectue les mêmes **Z**-opérations élémentaires sur les lignes (respectivement sur les colonnes) de la matrice identité de taille m (respectivement de taille n). Qu'obtient-on ?
6. (Théorème de la base adaptée) Soit E un **Z**-module libre de rang fini m, $f_1, \ldots, f_n$ des éléments de E et F le sous-module de E engendré par les f_i. Soit $\mathcal{B}$ une base de E et M la matrice à m lignes et n colonnes dont la i-ème colonne est le vecteur des coordonnées de f_i dans la base $\mathcal{B}$.

Montrer en utilisant la forme normale de Smith de M qu'il existe un unique entier $0 \leqslant r \leqslant m$ et une unique suite $d_1, \dots, d_r$ d'entiers strictement positifs vérifiant les propriétés suivantes :

(a) pour tout $1 \leqslant i \leqslant r-1$, d_i divise d_{i+1} ;

(b) il existe une base $(e_1, \dots, e_m)$ de E telle que $(d_1\, e_1, \dots, d_r\, e_r)$ est une base de F.

Exercice 4

1. Soit A le vecteur colonne $\begin{pmatrix} 6 \\ 15 \\ 10 \end{pmatrix}$ et H la forme normale de Hermite selon les lignes de A. Calculer H et une matrice $U \in \mathrm{GL}_3(\mathbf{Z})$ telle que $U\, A = H$. En déduire que l'on peut compléter le vecteur $\begin{pmatrix} 6 \\ 15 \\ 10 \end{pmatrix}$ en une base de $\mathbf{Z}^3$, et donner une telle base. Quelle est la forme normale de Hermite selon les colonnes de A ?
2. À quelle condition nécessaire et suffisante peut-on compléter une famille de vecteurs de $\mathbf{Z}^n$ en une base de $\mathbf{Z}^n$?

Exercice 5

1. Soit A la matrice $\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}$. Soit S la forme de Smith de M. Calculer S et deux matrices U et V de $\mathrm{GL}_2(\mathbf{Z})$ telles que $S = U\, A\, V$.
2. Soit M le sous $\mathbf{Z}$-module de $\mathbf{Z}^2$ engendré par $(2, 4)$ et $(4, 11)$. Déduire du calcul précédent une base de $\mathbf{Z}^2$ adaptée à M.

Exercice 6

1. Soit A la matrice $\begin{pmatrix} 2 & 4 & 3 \\ 4 & 5 & 7 \end{pmatrix}$ et B la matrice $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$.
2. Soit H_1 la forme normale de Hermite selon les lignes de la matrice A Déterminer H_1 ainsi qu'une matrice $U \in \mathrm{GL}_2(\mathbf{Z})$ telle que $U\, A = H_1$.
3. Soit H_2 la forme normale de Hermite selon les colonnes de la matrice A. Déterminer H_2 ainsi qu'une matrice $V \in \mathrm{GL}_3(\mathbf{Z})$ telle que $A\, V = H_2$.
4. Résoudre le système d'équations diophantiennes linéaires

$$A\, X = B, \quad X \in \mathbf{Z}^3.$$

Exercice 7

Résoudre l'équation

$$2\,x + 3\,y + 5\,z = 1, \quad (x, y, z) \in \mathbf{Z}^3.$$

Exercice 8

Résoudre dans $\mathbf{Q}^4$ puis dans $\mathbf{Z}^4$

$$\left\{ \begin{array}{rcrcrcrcl} 4\,x_1 & - & 17\,x_2 & - & 22\,x_3 & - & 9\,x_4 & = & a \\ & - & 30\,x_2 & + & 45\,x_3 & - & 18\,x_4 & = & b \\ 20\,x_1 & - & 75\,x_2 & + & 95\,x_3 & - & 39\,x_4 & = & c \\ 7\,x_1 & - & 25\,x_2 & + & 33\,x_3 & - & 14\,x_4 & = & d \end{array} \right.$$

(discuter suivant les valeurs de a, b, c et d).