Algèbre linéaire avancée II
printemps 2024

Série 13 – Corrigé

L'exercice marqué d'un (+) sert d'introduction à la série, tandis que celui marqué d'une (*) est plus difficile. Tous les exercices sauf celui marqué d'une (*) seront corrigés. La correction sera postée sur Moodle 2 semaines après. Les solutions des exercices (*) et (+) seront discutées dans les séances d'exercices du mardi d'après et d'avant respectivement. Un des exercices (*) sera une question ouverte de l'examen final.

Exercice 1. (+) Soit $A \in \mathbb{Z}^{m\times n}$ une matrice de rang ligne plein et $n > m$. Montrer qu'il existe $b_1, \ldots, b_k \in \mathbb{Z}^n$ linéairements indépendants sur $\mathbb{R}$ tels que

$$\ker_{\mathbb{Z}}(A) = \left\{ \sum_{i=1}^{k} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

Le noyau $\ker_{\mathbb{Z}}$ est défini par $\{x \in \mathbb{Z}^n \mid Ax = 0\}$.

Solution. *Soit $U \in \mathbb{Z}^{n\times n}$ unimodulaire telle que $AU = [H \mid 0]$ est en forme normale d'Hermite.*

$$\begin{aligned} Ax = 0 &\Leftrightarrow AU\underbrace{(U^{-1}x)}_{=:z} = 0 \\ &\Leftrightarrow [H|0]z = 0 \\ &\Leftrightarrow \forall i \in \{1,\ldots,m\} : z_i = 0. \end{aligned}$$

Donc, comme $x = Uz$ on observe que $\ker(A) = \operatorname{span}\{u_{m+1}, \ldots, u_n\}$ *où u_i est la i-ème colonne de U.*

Exercice 2. Soit $A \in \mathbb{Z}^{m\times n}$ et $d \in \mathbb{Z}$ un nombre entier qui divise chaque composante de A. Montrer que si $U \in \mathbb{Z}^{m\times m}$ et $V \in \mathbb{Z}^{n\times n}$ sont des matrices unimodulaires, alors d divise chaque composante de UAV.

Solution. *Si d divise toutes les composantes de A, alors le* gcd *de chaque ligne (resp. colonne) est un multiple de d. Comme les opérations unimodulaires ne change pas le* gcd *d'une ligne (resp. colonne), d va diviser le* gcd *de toutes les lignes (resp. colonnes) de UAV et donc chaque composante de UAV.*

Exercice 3. Calculer la forme normale de Smith pour

$$A = \begin{pmatrix} 3 & 12 & 9 & 0 & -3 \\ 4 & 1 & 0 & 1 & 1 \\ 7 & 3 & 21 & 0 & 8 \\ 7 & 6 & 4 & 5 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 12 & 9 & 0 & -3 \\ 4 & 1 & 0 & 1 & 1 \\ 5 & -5 & 15 & 0 & 10 \\ 7 & 6 & 4 & 5 & 2 \end{pmatrix}.$$

Solution. *La forme normale d'Hermite de A est donnée par :*

$$A_1 = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

On échange les lignes 1 *et* 3 *de A_1. La forme normale d'Hermite de cette nouvelle matrice est donnée par :*

$$A_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 9 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

On soustrait 9*-fois la ligne* 1 *de A_2 à la ligne* 3 *de A_2. On obtient :*

$$A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

On échange les lignes 3 *et* 4 *et les colonnes* 3 *et* 4 *de A_3. On obtient alors la forme normale de Smith :*

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 15 & 0 \end{pmatrix}.$$

La forme normale d'Hermite de B est donnée par :

$$B_1 = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

On ajoute la 3*-ième ligne de B_1 à la première ligne de B_1. La forme normale d'Hermite de cette nouvelle matrice est donnée par :*

$$B_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 10 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

On soustrait 10*-fois la ligne* 1 *de B_2 à la ligne* 3 *de B_2. On obtient :*

$$B_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

On échange les lignes 3 *et* 4 *et les colonnes* 3 *et* 4 *de B_3. On obtient alors la forme normale de Smith :*

$$B_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 15 & 0 \end{pmatrix}.$$

Exercice 4. Soit $A \in \mathbb{Z}^{m\times n}$ et $\operatorname{rang}(A) = m$. L'ensemble $\Lambda(A) := \{Ax \mid x \in \mathbb{Z}^n\}$ est un réseau entier généré par A. Parmi les matrices suivantes, lesquelles génèrent le même réseau?

$$A_1 = \begin{pmatrix} 4 & 2 & 2 & 0 \\ -4 & -1 & 0 & 1 \\ 0 & 2 & 1 & 2 \\ 5 & 0 & -3 & -2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 3 & 0 & -6 & 0 \\ 1 & -1 & 1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & -3 & 2 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 & 2 & 6 & 0 \\ 0 & 0 & -3 & 1 \\ 4 & 1 & 3 & 2 \\ -2 & -3 & 0 & -2 \end{pmatrix}.$$

Solution. *Pour quelques matrices unimodulaires U_1, U_2, U_3, on a*

$$A_1U_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = A_3U_3, \qquad A_2U_2 = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

Comme la forme normale d'Hermite est unique et une matrice unimodulaire est un automorphisme sur $\mathbb{Z}^n$ on observe que les matrices A_1 et A_2 génèrent le même réseau, mais A_3 génère un autre réseau.

Exercice 5. Soit $U \in \mathbb{Z}^{n\times n}$ une matrice unimodulaire.

i) Montrer que U^{-1} est aussi unimodulaire.

ii) Montrer que $\mathbb{Z}^n = \{Uz \mid z \in \mathbb{Z}^n\}$, c'est-à-dire que U est un automorphisme de $\mathbb{Z}^n$.

Solution.

i) *On sait que $U^{-1} = \frac{\mathrm{ad}(U)}{\det(U)}$ où $\mathrm{ad}(U)$ est la matrice adjointe de U. On se rappelle que $(\mathrm{ad}(U))_{ij} = (-1)^{i+j}\det(U_{ji})$ où $U_{ji} \in \mathbb{Z}^{(n-1)\times(n-1)}$ est la matrice qu'on obtient de U en supprimant la j-ème ligne et i-ème colonne. Comme $\det(U) \in \{\pm 1\}$ on observe que $U^{-1} \in \mathbb{Z}^{n\times n}$. De plus, $\det(U)\det(U^{-1}) = 1$ implique que $\det(U^{-1}) \in \{\pm 1\}$.*

ii) *Comme $U \in \mathbb{Z}^n$ on voit que $Uz \in \mathbb{Z}^n$ si $z \in \mathbb{Z}^n$ et on peut définir l'endomorphisme $g : \mathbb{Z}^n \to \mathbb{Z}^n : z \mapsto Uz$. Comme U est de rang plein, g est injective. Par la partie i), pour $z \in Z^n$, on a aussi $U^{-1}z \in \mathbb{Z}^n$, et ainsi $g(U^{-1}z) = z$. Donc g est aussi surjective.*

Exercice 6. Soit $U \in \mathbb{Z}^{n\times n}$ une matrice unimodulaire. Montrer qu'il existe un $m \in \mathbb{N}_{\geq 0}$ et des matrices E_i pour $i \in \{1, \ldots, m\}$ tels que

i) chaque E_i représente une opération élémentaire unimodulaire (cf. définition 8.4.),

ii) on a $U = E_1 \cdot E_2 \cdots E_m$.

Solution. *Par le Corollaire 8.7. du cours, il existe des matrices $E_1, \cdots E_m$ telles que $U \cdot E_1E_2 \cdots E_m = L$, où L est triangulaire inférieure. On montre que quitte à multiplier L à droite par d'autres opérations élémentaires unimodulaires, on peut supposer $L = I_n$. En effet, comme $\det(U) \in \{\pm 1\}$, on a $L_{i,i} \in \{\pm 1\}$ pour tout i. Quitte à multiplier certaines colonnes par -1, on peut supposer que $L_{i,i} = 1$. En additionnant $-L_{2,1}$ fois la 2-ème colonne de L à la 1-ère colonne de L, on peut supposer $L_{2,1} = 0$. En additionnant, $-L_{3,1}$ fois la 3-ème colonne de L à la 1-ère*

colonne de L, on peut supposer $L_{3,1} = 0$. En continuant ainsi pour les colonnes $j = 4, 5, ..., n$, on peut supposer $L = I_n$.

On remplace U par $U' := U^{-1}$. En appliquant le résultat ci-dessus à U', on obtient

$$\begin{aligned} & U' \cdot E_1 E_2 \cdots E_m = I_n \\ \Rightarrow \quad & UU' \cdot E_1 E_2 \cdots E_m = U \\ \Rightarrow \quad & E_1 E_2 \cdots E_m = U. \end{aligned}$$

Exercice 7. Montrer que le système $Ax = 0$ a une solution $0 \neq z^\star \in \mathbb{Z}^n$ pour chaque matrice $A \in \mathbb{Z}^{m \times n}$ avec $m < n$.

Solution. *Par le théorème 7.8. du cours, on sait qu'il existe une matrice U unimodulaire tel que $AU = [H \mid 0]$ est la forme normale d'Hermite. Comme $m < n$, il y a au moins une colonne dans la partie 0 à droite. Alors, $AUe_n = 0$, où $e_n = (0, \ldots, 0, 1)^\intercal \in \mathbb{Z}^n$. Soit u_n la dernière colonne (i.e. la n-ième colonne) de U. Comme $U \in \mathbb{Z}^{n \times n}$, on a $u_n \in \mathbb{Z}^n$ et comme U est inversible, on a $u_n \neq 0$. De plus, $0 = AUe_n = Au_n$.*

Exercice 8. Montrer que d dans le lemme 8.6. est le gcd de la première ligne de A. En d'autres mots, montrer le lemme suivant:

Soit $A \in Z^{m \times n}$ une matrice de plein rang ligne, alors il existe une matrice unimodulaire $U \in \mathbb{Z}^{n \times n}$, tel que la première ligne de AU est de la forme $(d, 0, \ldots, 0)$ où $d = \gcd(a_{1,1}, a_{1,2}, \ldots, a_{1,n})$.

Solution. *Nous allons montrer que $\gcd(a_{1,1}, \ldots, a_{1,n})$ est invariant sous opérations élémentaires unimodulaires. L'échange de deux colonnes ne change pas le* gcd. *Ajouter $\lambda \in \mathbb{Z}$ fois une colonne j à une autre colonne k pour $j \neq k$, change a_k en $a'_k = a_k + \lambda a_j$. On a*

$$\begin{aligned} \gcd(a_{1,1}, a_{1,2}, \ldots, a_{1,n}) &= \gcd(\gcd(a_k, a_j), a_{1,1}, a_{1,2}, \ldots, a_{1,n}) \\ &= \gcd(\gcd(a_k + \lambda a_j, a_j), a_{1,1}, a_{1,2}, \ldots, a_{1,n}) \\ &= \gcd(a_{1,1}, a_{1,2}, \ldots, a'_k, \ldots, a_{1,n}). \end{aligned}$$

Ainsi les opérations élémentaires unimodulaires ne changent pas le gcd *d'une ligne. Comme $\gcd(d, 0, \ldots, 0) = d$, on conclut.*

Exercice 9. (*) Soit $G = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$ une matrice symétrique, unimodulaire et définie positive. Montrer qu'il existe une matrice unimodulaire U telle que $G = U^\intercal U$.

Solution.