Algèbre linéaire avancée II
printemps 2022

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 $A \in \mathbb{C}^{n\times n}$. Montrer qu'il existe un polynôme $m_A(x) \in \mathbb{C}[x] \setminus \{0\}$ de degré minimal et dont le coefficient du monôme dominant est 1 tel que $m_A(A) = 0$. De plus, montrer que $m_A(x)$ est unique. Le polynôme $m_A(x)$ est appelé le *polynôme minimal de A*.

Solution. *Comme $p_A(A) = 0$ pour le polynôme caractéristique, on obtient l'existence.*

Soit $p(x) = \sum_{i=0}^{\deg(m_A)} \alpha_i x^i$ un autre polynôme tel que $p(A) = 0$, $\deg(p) = \deg(m_A)$ et le coefficient du monôme dominant de p est 1. Alors on peut écrire $p(x) = q(x)m_A(x) + r(x)$, où $r(x)$ est un autre polynôme avec $\deg(r) < \deg(m_A)$ et $q(x) \in \mathbb{C}[x]$. Comme $p(A) = m_A(A) = 0$, on doit avoir $r(A) = 0$. Comme m_A est choisi de degré minimal, on doit avoir $r = 0$.

Ainsi, $p(x) = q(x)m_A(x)$. Comme $p(x)$ et $m_A(x)$ ont le même degré, $q(x)$ est constant et comme $p(x)$ et $m_A(x)$ ont le même coefficient dominant, $p(x) = m_A(x)$. Ceci conclut la preuve de l'unicité.

Exercice 2. 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 sur $\mathbb{Z}^n$.

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 $\det(U) \in \{\pm 1\}$, $U^{-1} \in \mathbb{Z}^{n\times n}$. De plus, $\det(U)\det(U^{-1}) = 1$ implique que $\det(U^{-1}) \in \{\pm 1\}$.*

ii) Comme $U \in \mathbb{Z}^n$, $Uz \in \mathbb{Z}^n$ 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 alors $g(U^{-1}z) = z$. Donc, g est aussi surjective.

Exercice 3. 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, $i \in \{1, \ldots, m\}$ tels que

i) chaque E_i représente une opération élémentaire unimodulaire (cf. définition 6.4),

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

Solution. *Par le Corollaire 6.7 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

$$\begin{aligned} & U' \cdot E_1E_2 \cdots E_m = I_n \\ \Rightarrow \quad & UU' \cdot E_1E_2 \cdots E_m = U \\ \Rightarrow \quad & E_1E_2 \cdots E_m = U. \end{aligned}$$

Exercice 4. 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 6.8 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 5. Trouver toutes les solutions entières de

$$Ax = b_1, \text{ où } A = \begin{pmatrix} 5 & 1 & 3 \\ 4 & 10 & 2 \end{pmatrix}, \; x \in \mathbb{Z}^3 \text{ et } b_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \tag{1}$$

et de

$$Bx = b_2, \text{ où } B = \begin{pmatrix} 8 & -7 & -10 \\ -6 & 15 & 12 \end{pmatrix}, \; x \in \mathbb{Z}^3 \text{ et } b_2 = \begin{pmatrix} 4 \\ 6 \end{pmatrix}. \tag{2}$$

Solution. *On va trouver la forme normale de Hermite des matrices A et B afin de résoudre ces systèmes.*

On a que la forme normale de Hermite de A est

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

avec matrice de passage unimodulaire $U_A = \begin{pmatrix} -1 & 3 & -14 \\ 0 & 0 & 1 \\ 2 & -5 & 23 \end{pmatrix}$. *Ainsi, on a :*

$$AU_A = H_A.$$

On trouve d'abord les solutions de $H_A y = b_1$ qui sont

$$Y_A = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mid z \in \mathbb{Z} \right\}.$$

On a donc que les solutions entières de (1) *sont*

$$\{U_A y \mid y \in Y_A\} = \left\{ \begin{pmatrix} 2 \\ 0 \\ -3 \end{pmatrix} + z \begin{pmatrix} -14 \\ 1 \\ 23 \end{pmatrix} \mid z \in \mathbb{Z} \right\}.$$

De la même manière on a que la forme normale de Hermite de B est

$$H_B = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 6 & 0 \end{pmatrix}$$

avec matrice de passage unimodulaire $U_B = \begin{pmatrix} 3 & -2 & 11 \\ -1 & 2 & -6 \\ 3 & -3 & 13 \end{pmatrix}$. *Ainsi, on a :*

$$BU_B = H_B.$$

On trouve d'abord les solutions de $H_B y = b_2$ qui sont

$$Y_B = \left\{ \begin{pmatrix} 4 \\ -1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mid z \in \mathbb{Z} \right\}.$$

On a donc que les solutions entières de (2) *sont*

$$\{U_B y \mid y \in Y_B\} = \left\{ \begin{pmatrix} 14 \\ -6 \\ 15 \end{pmatrix} + z \begin{pmatrix} 11 \\ -6 \\ 13 \end{pmatrix} \mid z \in \mathbb{Z} \right\}.$$

Exercice 6. Montrer que d dans le lemme 6.6 est le gcd de la première ligne de A. En d'autres mots, montrer le lemme suivant.

Lemme. Soit $A \in Z^{m \times n}$ une matrice en nombres entiers de plein ligne rang, 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 *dans une autre colonne* k, $j \neq k$, *change* a_k *en* $a'_k = a_k + \lambda a_j$. *On a*

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

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

Exercice 7. (*) Soit $G = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ un matrice symétrique, unimodulaire, et définie positive. Montrer qu'il existe une matrice unimodulaire U telle que $G = U^\intercal U$.

Indication: Regarder ac. Si $ac \geq 2$, est-ce qu'il y a une matrice unimodulaire U t.q. $U^\intercal G U = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$ avec $0 \leq b' < b$?

Solution.