Algèbre linéaire avancée II
printemps 2019

Série 12 - Corrigé

Exercice 1. 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 $G = U^\intercal U$.

Remarque: L'énoncé est vrai jusqu'à la dimension 7, mais en dimension 8 il existe un exemple où la décomposition n'est pas possible.

Solution. *On note que $a, c \geq 1$, car G est définie positive. De plus, par multiplication de la seconde colonne et la seconde ligne par -1, on peut supposer que $b \geq 0$. Nous affirmons que si $b \geq \min\{a, c\}$, alors il existe une matrice unimodulaire telle que pour la nouvelle matrice*

$$G' = U^\intercal G U = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix},$$

on a $0 \leq b' < b$. Comme b, b' sont entiers, cette procédure se termine avec $0 \leq b' < \min\{a', c'\}$.

De plus, comme $x^\intercal G' x = (x^\intercal U^\intercal) G (Ux) = x'^\intercal G x'$, G' est aussi définie positive et $a', c' > 0$.

Supposons $b \geq a$. En ajoutent la première colonne $\lambda \in \mathbb{Z}$ fois à la seconde colonne, et en faisant la même chose pour les lignes, (multiplication par une matrice unimodulaire U), nous obtenons

$$\begin{aligned} G' &= U^\intercal G U \\ &= \begin{pmatrix} a & b - \lambda a \\ b - \lambda a & c - 2\lambda b + \lambda^2 a \end{pmatrix} \\ &= \begin{pmatrix} a & b' \\ b' & c' \end{pmatrix}. \end{aligned}$$

Si on choisit $1 \leq \lambda = \lfloor \frac{b}{a} \rfloor$, on a $0 \leq b' < b$. Si on a $b \geq c$, nous ajoutons la seconde colonne λ' fois à la première colonne, respectivement ligne.

Nous obtenons une matrice G' congrue a G avec $0 \leq b < \min\{a, c\}$. Pour cette G', nous avons $\det(G') = a'c' - b'^2$. Si $b' \geq 1$, ceci est $\det(G') \geq (b'+1)^2 - b'^2 \geq 2b' + 1 > 1$, une contradiction. Donc, $b' = 0$, ce qui implique $a' = c' = 1$, et alors $G' = I_n$. Comme nous avons seulement effectué opérations élémentaires unimodulaires sur les lignes et les colonnes simultanément, il existe une matrcie unimodulaire telle que $G = U^\intercal I_n U = U^\intercal U$.

Exercice 2. Montrer qu'un réseau entier $\Lambda(A)$, pour une matrice $A \in \mathbb{Z}^{m\times n}$ de rang ligne plein est un groupe abelien.

Solution. *L'ensemble Z^n est un sous-ensemble d'une espace vectoriel (qui est une groupe abelien avec l'addition), et pour $u, v \in \mathbb{Z}^n$, le somme est définie par $(u+v)_i = u_i + v_i \in \mathbb{Z}$, et $o \in \mathbb{Z}^n$. Alors, Z^n est un (sous-)groupe. On a $\Lambda(A) = \{Az \mid z \in \mathbb{Z}^n\}$. Ce implique que $0 = A0 \in \Lambda$, car $0 \in \mathbb{Z}^n$. Comme $\Lambda(A) \subseteq \mathbb{R}^n$, on doit seulement montrer que $u + v \in \Lambda(A)$ pour $u, v \in \Lambda(A)$. Pour chaque $v \in \Lambda(A)$, on peut choisir $z_v \in \mathbb{Z}^n$ tel que $v = Az_v$.*

$$u + v = Az_u + Az_v = A \underbrace{(z_u + z_v)}_{\in \mathbb{Z}^n} \in \Lambda(A).$$

Exercice 3. Montrer que pour chaque n, il y a une matrice $A \in \mathbb{Z}^{n\times(n+1)}$ avec colonnes $A = (a_1, \dots, a_{n+1})$ tel que les assertions suivantes sont vraies:

i) Pour chaque $i \in \{1, \dots, n+1\}$, l'ensemble $R_i = \{a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}\}$ forme une base d'espace vectoriel $\mathbb{R}^n$.

ii) Aucune sous-matrice A_i, définie comme la matrice A sans la i-éme colonne, ne génère le même réseau entier que A, c.-à-d. $\forall A_i$: $\Lambda(A) \neq \Lambda(A_i)$, où

$$\Lambda(A) = \left\{ \sum_{j=1}^{n+1} a_j z_j \,\middle|\, z_j \in \mathbb{Z},\, j \in \{1, \dots, n+1\} \right\}$$
$$\Lambda(A_j) = \left\{ \sum_{j=1,\, j\neq i}^{n+1} a_j z_j \,\middle|\, z_j \in \mathbb{Z}, j \in \{1, \dots, n+1\} \setminus \{i\} \right\}.$$

Solution. *Soit*

$$A = \begin{pmatrix} 2 & 3 & 0 & & 0 \\ 0 & 2 & 3 & \ddots & \\ & \ddots & \ddots & \ddots & 0 \\ 0 & & 0 & 2 & 3 \end{pmatrix} \in \mathbb{Z}^{n\times(n+1)}.$$

Pour chaque $i \in \{1, \dots, n\}$, $\Lambda(A)$ contient un v_i tel que $(v_i)_i$ est impaire. Le réseau entier $\Lambda(A_{i+1})$ ne contient pas v_i. Le réseau entier $\Lambda(A_1)$ ne contient pas a_1. La suppression de la k-ième colonne de la matrice A donne une matrice block-diagonale

$$A' = \begin{pmatrix} M_1 & \\ & M_2 \end{pmatrix},$$

où $M_1 \in \mathbb{Z}^{(k-1)\times(k-1)}$ est une matrice triangulaire supérieure avec entrées non-nulles, et $M_2 \in \mathbb{Z}^{(n-k+1)\times(n-k+1)}$ est une matrice triangulaire infèrieure avec entrées non-nulles. Donc A' est de rang plein et chaque A_k est une base de $\mathbb{R}^n$.

Exercice 4. Montrer que d dans le lemme 5.6 est le gcd de la première ligne de A. En d'autres mots, montrer le lemme suivant.

<u>*Lemme.*</u> 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 unimoduilaires. 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* $a_k' = a_k + \lambda a_j$ *pour quelqu'une* $\lambda \in \mathbb{Z}$. *Par exercices* 1 *et* 5.*ii*) *dans fiche* 11, *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* $\gcd(d, 0, \ldots, 0) = d$, *nous avons gagné.*

Exercice 5. Calculer la forme normale de Smith pour

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

(Vous pouvez utiliser le fichier python sur la page web du cours.)

Solution. *Le forme normale d'Hermite.*

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

Échange les lignes 1 *et* 3, *Hermite encore.*

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

On soustrait 9*-fois la ligne* 1 *à la ligne* 3.

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

Échanger les lignes 3 *et* 4, *et les colonnes* 3 *et* 4, *la forme normale de Smith est*

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

Et pour la matrice B:

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

Ajouter la 3-ième ligne dans la première ligne, Hermite encore.

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

On soustrait 10-fois la ligne 1 à la ligne 3.

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

Échanger les lignes 3 et 4, et les colonnes 3 et 4, la forme normale de Smith est

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

Exercice 6. Soit G un groupe. Le centre de G est définie par $Z(G) = \{z \in G \mid zg = gz \ \forall\, g \in G\}$.

i) Montrer que $Z(G)$ est un sous-groupe de G.

ii) Montrer que si G est abelien, alors $Z(G) = G$.

Solution.

1. *Soit $z_1, z_2 \in Z(G)$. Donc pour tout $g \in G$:*
$$g(z_1 z_2^{-1}) = z_1 z_2^{-1} z_2 g z_2^{-1} = (z_1 z_2^{-1}) g z_2 z_2^{-1} = (z_1 z_2^{-1}) g,$$
alors $(z_1 z_2^{-1}) \in Z(G)$.

2. *Si G est abelien, alors $gz = zg$ pour tout $z, g \in G$. Donc, $G = Z(G)$.*

Exercice 7. Soit H un sous-groupe de G, tel que pour chaque $a \in G$, il y a un $b \in G$ avec $aH = Hb$. Montrer que H est un sous-groupe normal de G, $H \lhd G$.

Solution. *On doit montrer que $aH = Ha$ pour tout $a \in G$. Pour $a \in G$, il existe des éléments $h, h' \in H$, $b \in G$ tels que*

$$\begin{aligned} && ah &= h'b \\ \Rightarrow && b &= h'^{-1} a h \\ \Rightarrow && aH &= aHh^{-1} \\ && &= Hbh^{-1} \\ && &= Hh'^{-1} a h h^{-1} \\ && &= Ha. \end{aligned}$$

Exercice 8. Soit $N \lhd G$ et $K \lhd G$. Montrer que $N \cap K \lhd G$.

Solution. *$a(N \cap K)a^{-1} \subseteq aNa^{-1} = N$ et $a(N \cap K)a^{-1} \subseteq aKa^{-1} = K$. Donc $a(N \cap K)a^{-1} \subseteq N \cap K$ pour tout $a \in G$, et $N \cap K \lhd G$.*