Algèbre linéaire avancée II
printemps 2019

Série 11 - Corrigé

Exercice 1. Soient $a, b, \lambda \in \mathbb{Z}$, et $a \neq 0$. Montrer que

$$g \mid a \text{ et } g \mid b \qquad \Leftrightarrow \qquad g \mid b \text{ et } g \mid (a - \lambda b).$$

Conclure que $\gcd(a, b) = \gcd(b, a - \lambda b)$.

Solution. $[g \mid a \text{ et } g \mid b] \Rightarrow [g \mid (a - \lambda b)]$.
$[g \mid b \text{ et } g \mid (a - \lambda b)] \Rightarrow [g \mid ((a - \lambda b) + \lambda b)]$.

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

ii) *Comme* $U \in \mathbb{Z}^n$, $Uz \in \mathbb{Z}^n$ *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. Avec partie a), 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 5.4),

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

Solution. *Par le cours, il existe des matrices* $E_1, \cdots E_m$ *telles que* $U \cdot E_1 E_2 \cdots E_m = H$, *où* H *est la fome normale d'Hermite. Comme* $\det(U) \in \{\pm 1\}$, *on a* $H_{ii} = 1$ *pour tous* i. *Ca implique que* $H_{i,j} = 0$ *quand* $i \neq j$, *et donc* $H = I_n$.

On remplace U *par* $U' := U^{-1}$ *et 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 4. Utiliser l'algorithme d'Euclide étendu pour calculer p, q avec

$$\gcd(1463, 1235) = 1463p + 1235q.$$

Solution. *On a la récurrence* $a_{i-1} = q_i a_i + a_{i+1} \Leftrightarrow a_{i+1} = a_{i-1} - q_i a_i$, *et nous obtenons le tableau*

i	a_i	$q_i = \left\lfloor \frac{a_{i-1}}{a_i} \right\rfloor$
0	1463	$--$
1	1235	1
2	228	5
3	95	2
4	38	2
5	19	2
6	0	$--$

.

Donc, $a_5 = \gcd(a_5, a_6) = 1 \cdot 19 = 1 \cdot a_5$. *Avec l'exercice 1, on a* $\gcd(a_0, a_1) = \gcd(a_5, a_6)$ *et on peut résoudre*

$$\begin{aligned} \gcd(a_0, a_1) &= \gcd(a_5, a_6) \\ &= 1 \cdot a_5 \\ &= 1 \cdot (a_3 - q_4 a_4) = a_3 - 2a_4 \\ &= a_3 - 2(a_2 - q_3 a_3) = -2a_2 + 5a_3 \\ &= -2a_2 + 5(a_1 - q_2 a_2) = 5a_1 - 27a_2 \\ &= 5a_1 - 27(a_0 - q_1 a_1) = -27a_0 + 32a_1 \\ &= -27 \cdot 1463 + 32 \cdot 1235. \end{aligned}$$

Exercice 5. Soient $n \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}$ pas tous égaux à zéro. On définit

$$\gcd(a_1, \ldots, a_n) := \max\{z \in \mathbb{Z} : \ z \mid a_1, \ z \mid a_2, \ldots, z \mid a_n\}$$

comme le plus grand diviseur commun de $a_1, \ldots, a_n$. Montrer:

i) $\gcd(a_1, \ldots, a_n) = \min\{x_1 a_1 + \cdots + x_n a_n : \ x_1 a_1 + \cdots + x_n a_n \geq 1, \ x_i \in \mathbb{Z}, \ i = 1, \ldots, n\}$.

ii) $\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n)$ pour $n \geq 3$.

Solution. *Soit* $z := \min\{x_1a_1 + \cdots + x_na_n : x_1a_1 + \cdots + x_na_n \geq 1,\ x_i \in \mathbb{Z},\ i = 1, \ldots, n\}$.

i) Si $z' \mid a_i\ \forall i$, *alors* $z' \mid z$. *Supposons qu'il y a un* k *tel que* $z \nmid a_k$, *et soit* $z = \sum_{i=1}^{n} x_i a_i$. *Avec* $r = \gcd(z, a_k) = (pz + qa_k) < z$, *on obtient que*

$$1 \leq r = pz + qa_k = \sum_{i=1, i\neq k}^{n} (px_i)a_i + (px_k + q)a_k < z,$$

c'est absurde.

ii) Soient

$$g = \gcd(a_1, \ldots, a_n)$$
$$g' = \gcd(\gcd(a_1, a_2), a_3 \ldots, a_n).$$

Comme $g \mid a_1$ *et* $g \mid a_2$, *aussi* $g \mid \gcd(a_1, a_2)$ *par Corollaire 5.2. Donc,* $g \mid g'$ *par Corollaire 5.2.*

Comme $g' \mid \gcd(a_1, a_2)$, *on a* $g' \mid a_1$ *et* $g' \mid a_2$. *Mais ca implique que* $g' \mid \gcd(a_1, \ldots, a_n) = g$ *par Corollaire 5.2*

Nous obtenons $g = g'$.

Exercice 6. 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 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 un 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 *le colonne dernier (n-ième colonne) de* U. *Alors,* $Au_n = 0$, *et* $u_n \in \mathbb{Z}^n$ *car* $U \in \mathbb{Z}^{n\times n}$.

Exercice 7. Parmi les matrices suivantes, lesquelles génèrent le même réseau?

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

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

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

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

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