Algèbre linéaire avancée II
printemps 2019

Série 13 - Corrigé

Exercice 1.

i) Montrer que $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

ii) Montrer que $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

iii) Soient $m, n \in \mathbb{N}_{>0}$ tel que $m \mid n$. Montrer qu'il existe un surjective homomorphisme des groupes

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

Solution.

i) *Soit* $\varphi(x) : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *définie par* $x \mapsto (x \mod 2, x \mod 3)$. *Partie iii) va impliquer que* φ *est une homomorphisme des groupes. De plus, on a*

$x \in \mathbb{Z}/6\mathbb{Z}$	0	1	2	3	4	5
$\varphi(x)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$

alors φ *est bijective, et un isomorphisme.*

ii) *Regarder* $1 \in \mathbb{Z}/4\mathbb{Z}$. *On a* $1 + 1 \neq 0$, *mais pour tout* $a \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, *on a* $a + a = 0$. *Alors, il ný a pas de isomorphisme.*

iii) *Soit* $n = km$. *Définir* $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *par* $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$. *Nous voulons montrer que* φ *est bien définie. Soit* $a' \in a + n\mathbb{Z}$. *Alors,* $\varphi(a + n\mathbb{Z}) = a + m\mathbb{Z}$ *et* $\varphi(a' + n\mathbb{Z}) = a' + m\mathbb{Z}$. *Comme* $a' \in a + n\mathbb{Z} = a + km\mathbb{Z} \subseteq a + m\mathbb{Z}$, *on a que* $\varphi(a + n\mathbb{Z}) = \varphi(a' + n\mathbb{Z})$, *donc* φ *est bien définie.*

On va montrer que φ *est une homomorphisme des groupes. On a* $\varphi(0) = 0$. *De plus, on a*

$$\varphi(a+b+n\mathbb{Z}) = \varphi(a+b+(km)\mathbb{Z}) = a+b+m\mathbb{Z} = a+m\mathbb{Z}+b+m\mathbb{Z} = \varphi(a+n\mathbb{Z})+\varphi(b+n\mathbb{Z}).$$

Il faut montrer que pour tout ℓ *il y a un* x *tel que* $\varphi(x) = \ell$. *Comme* $a = a \mod m$ *pour* $a < m$, *c'est vrai.*

Exercice 2. Si H est un sous-groupe normale de G, $H \lhd G$, et $|H| = 2$, montrer que $H \subseteq Z(G)$, où

$$Z(G) = \{z \in G \mid zg = gz \ \forall\, g \in G\}.$$

Solution. *$H \lhd G \Rightarrow H = \{1, a\}$ avec $a^2 = 1$. On a $1 \in Z(G)$ trivialement, alors on fait montrer que $a \in Z(G)$. On a $ga \in \{1g, ag\}$, car $gH = Hg$. Si $ga = 1g = g$, alors $a = gg^{-1}a = gg^{-1}g = 1$, un contradiciton. $ga = ag$ suit.*

Exercice 3. Soient $A \in \mathbb{Z}^{m\times n}$ et $A' \in \mathbb{Z}^{m\times n'}$ deux matrices de rang ligne plein.
Montrer que si $\Lambda = \Lambda(A) \subseteq \Lambda(A') = \Lambda'$, alors $\det(\Lambda') \mid \det(\Lambda)$.

Solution. *Soit B une base de Λ avec des colonnes $B = (b_1, \ldots, b_m)$, et B' une base de Λ' avec des colonnes $B' = (b'_1, \ldots, b'_m)$ (par instance, les formes normales d'Hermite). Comme $\Lambda \subseteq \Lambda'$, en particulaire $b_i \in \Lambda'$ pour tous $i = 1, \ldots, m$. Donc, il y a vecteurs $z_i \in \mathbb{Z}^m$ tels que $b_i = B'z_i$. Alors, on a $B = B'Z$, où $Z \in \mathbb{Z}^{m\times m}$. Comme B et B' ont le méme rang, Z est inversible. Comme $\det(Z) \in \mathbb{Z}$, la formule $\det(\Lambda) = |\det(B)| = |\det(B')\det(Z)|$ implique que $\det(B') \mid \det(B)$.*

Exercice 4. Soient $\mathbb{C}^\star = \mathbb{C} \setminus \{0\}$, $\mathbb{R}_+ = \{r \in \mathbb{C} \mid \Re(r) > 0, \Im(r) = 0\}$ et $S = \{c \in \mathbb{C} \mid |c| = 1\}$.

i) Montrer que $(\mathbb{R}_+, \cdot)$ est un sous-groupe de $(\mathbb{C}^\star, \cdot)$.

ii) Montrer que $(S, \cdot)$ est un sous-groupe de $(\mathbb{C}^\star, \cdot)$.

iii) Montrer que $\mathbb{C}^\star/\mathbb{R}_+ \simeq S$.

Solution.

i) *Associativité et commutativité sont hérités par $\mathbb{C}$. Si $a, b \in \mathbb{R}$, alors $ab \in \mathbb{R}$.*

ii) *Encore, seulement il faut que S est fermé sous $\cdot$. Pour nombres complexes sur le cercle unitaire, on peut écrire $a = e^{i\varphi(a)} \in S$ et $b = e^{i\varphi(b)} \in S$. Donc, $ab = e^{i\varphi(a)+i\varphi(b)} = e^{i\varphi(ab)} \in S$.*

iii) *Soit $\psi : \mathbb{C}^\star/\mathbb{R}_+ \to S$ définie par $ae^{i\varphi}\mathbb{R}_+ \mapsto e^{\varphi}$. Ceci est bien défini car pour $a = re^{i\varphi}$ et $r' \in \mathbb{R}_+$, on a $\psi(a) = e^{i\varphi}$ et $\psi(r'a) = e^{i\varphi}$. De plus,*

$$\begin{aligned}\psi\left(r_1e^{i\varphi_1}\mathbb{R}_+ \cdot r_2e^{i\varphi_2}\mathbb{R}_+\right) &= \psi(e^{i(\varphi_1+\varphi_2)}\mathbb{R}_+) = e^{i(\varphi_1+\varphi_2)} = e^{i\varphi_1}e^{i\varphi_2} \\ &= \psi(r_1e^{i\varphi_1}\mathbb{R}_+)\psi(r_2e^{i\varphi_2}\mathbb{R}_+).\end{aligned}$$

Exercice 5. Soit $\Lambda(B) \subseteq \mathbb{Z}^n$ un réseau entier pour une matrice inversible $B \in \mathbb{Z}^{n\times n}$, $d = |\det(B)|$, et $\langle\cdot,\cdot\rangle$ le produit scalaire standard. Soit $D = d(B^{-1})^\intercal$.

i) Soient $x \in \Lambda(B)$, $y \in \Lambda(D)$. Montrer que $\langle x, y\rangle \in d\mathbb{Z}$.

ii) Soit $z \in \mathbb{R}^n$, et $\langle x, z\rangle \in d\mathbb{Z}$ pour tout $x \in \Lambda(B)$. Montrer que $z \in \Lambda(D)$.

Solution.

i) Comme on multiplié B^{-1} par $|\det(B)|$ pour obtenir $D^\intercal$, on sait que $D^\intercal \in \mathbb{Z}^{n\times n}$ (cf. preuve de lemme 5.4). Donc, $\langle x, y\rangle$ est le somme de deux nombres entiers.

ii) Comme B est inversible, on peut écrire $z = Dy$ pour un certain $y \in \mathbb{R}^n$. Comme la condition est vraie pour tout $x \in \Lambda$, nous obtenons pour toute colonne b_i de B la reformulation

$$\langle z, b_i\rangle = y^\intercal D^\intercal B e_i = dy^\intercal e_i = dy_i.$$

Ca implique que y est un vecteur entier, donc $z \in \Lambda(D)$.

Exercice 6. Soit $\Lambda(B) \subseteq \mathbb{Z}^n$ un réseau entier pour une matrice inversible $B \in \mathbb{Z}^{n\times n}$ et $\langle\cdot,\cdot\rangle$ le produit scalaire standard de $\mathbb{R}^n$. Soit $a \in \mathbb{R}^n$ un vecteur tel que $\langle a, x\rangle \in \mathbb{Z}$ pour tout $x \in \Lambda(B)$. Soit

$$\Lambda' := \{x \in \Lambda \mid \langle a, x\rangle = 0\}.$$

Montrer que Λ' est un sous-groupe de $\Lambda(B)$.

Solution. *Par le classe, on sait qu'il y a une base V avec colonnes $v_1, \dots, v_{n-1} \in \mathbb{Z}^{n-1}$ de $\ker_{\mathbb{Z}}(a^\intercal)$. Comme B est entier, $\Lambda(B), \ker_{\mathbb{Z}}(a^\intercal)$ sont sous-groupes abelien de $\mathbb{Z}^n$. Mais $\Lambda' = \Lambda(B) \cap \ker_{\mathbb{Z}}(a^\intercal)$ est l'intersection de deux groupes abelien, alors un sous-groupe abelien pour chaque.*

Exercice 7. Soit G un groupe abelien généré a g_1, g_2, g_3, tel que

$$\begin{aligned} -25g_1 + 7g_2 + 11g_3 &= 0,\\ 18g_1 - 4g_2 - 8g_3 &= 0,\\ -10g_1 + 2g_2 + 4g_3 &= 0. \end{aligned}$$

Utilizer la forme normale de Smith pour trouver générateurs $h_1, \dots, h_m$ et nombres entiers $k_i \in \mathbb{Z}_{\geq 1}$ tel que G est le groupe avec conditionnes $k_i h_i = 0$.

Indication:

$$\begin{pmatrix} -5 & 4 & -2\\ 3 & -1 & 1\\ 3 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} -3 & 2 & -2\\ -2 & 2 & -1\\ 2 & -1 & 1 \end{pmatrix}.$$

Solution. *Regarder l'homomorphisme des groupes*

$$\varphi :\ \mathbb{Z}^3 \to G, \quad \begin{pmatrix} x_1\\ x_2\\ x_3 \end{pmatrix} \mapsto x_1 g_1 + x_2 g_2 + x_3 g_3.$$

Le noyau d'homomorphisme est

$$\ker(\varphi) = \{Az \mid z \in \mathbb{Z}^3\} \quad \textit{avec la matrice} \quad A = \begin{bmatrix} -25 & 18 & -10\\ 7 & -4 & 2\\ 11 & -8 & 4 \end{bmatrix}.$$

Avec python, nous avons le forme normale de Smith

$$A = USV = \begin{bmatrix} -5 & 4 & -2 \\ 3 & -1 & 1 \\ 3 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix} \begin{bmatrix} -3 & 2 & -2 \\ -2 & 2 & -1 \\ 2 & -1 & 1 \end{bmatrix}.$$

De plus,

$$\ker(\varphi) = \{USVz \mid z \in \mathbb{Z}^3\} = \{USz \mid z \in \mathbb{Z}^3\}.$$

Alors, les colonnes de U donnent les vecteurs désirés,

$$\begin{aligned} h_1 &= -5g_1 + 3g_2 + 3g_3, \\ h_2 &= 4g_1 - g_2 - 2g_3, \\ h_3 &= -2g_1 + g_2 + g_3. \end{aligned}$$

Les k_i sont les elements diagonale de S, c.-à-d. $k_1 = 1$ (qui implique que G es genere $parh_2, h_3$ seulement), $k_2 = 2$, et $k_3 = 6$.

Exercice 8. Soit $A \in \mathbb{Z}^{m\times n}$ et $d \in \mathbb{Z}$ un nombre entier qui divise chaque composante de A. 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 $U \cdot A \cdot V$.

Solution. *Si d divise toutes les composantes de A, alors le* gcd *de chaque ligne (colonne) est un multiple de d. Comme operations unimodulaire ne change pas le* gcd *d'une ligne (colonne), (Montrer avec série* 11*, exercice* 1*!!), d va diviser le* gcd *de toutes colonnes (lignes) de UAV, alors chaque composante de UAV.*