Les exercices étoilés (*) s'adressent aux seuls étudiants inscrits à l'unité MO12

Corrigé de la feuille d'exercices 3

1 Le groupe modulaire

Exercice 1. *Soit $\mathcal{H} = \{z \in \mathbb{C},\ Im\ z > 0\}$, le demi-plan de Poincaré. A toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$, on associe la fonction homographique f_A définie pour tout $z \in \mathcal{H}$ par $f_A(z) = \frac{az+b}{cz+d}$*

(a) Montrez que l'application $f : A \mapsto f_A$ est un morphisme de groupes de $SL_2(\mathbb{Z})$ dans le groupe des permutations de $\mathcal{H}$. Déterminez $\operatorname{Ker} f$*. On note G l'image de f et on l'appelle le groupe modulaire*

(b) Pour $z \in \mathcal{H}$, on pose $I_z = \{Im\ g(z),\ g \in G\}$. Montrez que I_z est une partie de $\mathbb{R}_+^\times$ admettant un plus grand élément .

(c) On note G_0 le sous-groupe de G engendré par $S : z \mapsto -1/z$ et $T : z \mapsto z+1$. Pour $z \in \mathcal{H}$, montrez qu'il existe $g_0 \in G_0$ tel que si on pose $z_0 = g_0(z)$, on a pour tout $g \in G_0$, $Im\ g(z) \leqslant Im\ z_0$.

(d) Soit $D = \{z \in \mathcal{H}\ /\ |Re(z)| \leqslant 1/2,\ |z| \geqslant 1\}$, le domaine fondamental du groupe modulaire. Montrez que l'on peut choisir z_0 dans D.

(e) En déduire que $G_0 = G$.

Preuve : (a) On calculer aisément la partie imaginaire de $f_A(z) = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}$ soit

$$\operatorname{Im} f_A(z) = \frac{\operatorname{Im} z}{|cz+d|^2} > 0$$

de sorte que $f_A(\mathcal{H}) \subset \mathcal{H}$. De même on a

$$f_A(f_B(z)) = \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} = \frac{(aa'+bc')z + (ab'+bd')}{(ca'+dc')z + (cb'+dd')} = f_{AB}(z)$$

On en déduit alors comme $f_I = \mathrm{Id}_{\mathcal{H}}$, f_A est bijective d'inverse $f_{A^{-1}}$. L'application $f : A \mapsto f_A$ est donc un morphisme de groupes de $SL_2(\mathbb{Z})$ dans le groupe des permutations de $\mathcal{H}$. En outre $f_A(z) = z$ pour tout $z \in \mathcal{H}$ donne $az + b = cz^2 = dz$ soit $c = b = 0$ et $a = d$; l'égalité $ad - bc = 1$ donne alors $a = \pm 1$ et donc $\operatorname{Ker} f = \{\pm I\}$.

(b) Soit $\alpha > 0$, on va montrer que l'ensemble des $\operatorname{Im} g(z) > \alpha$ pour $g \in G$, est fini, ce qui implique trivialement le résultat. Or $\operatorname{Im} g(z) \geqslant \alpha$ équivaut à $|cz+d|^2 \geqslant \frac{\operatorname{Im} z}{\alpha}$; on écrit $z = x + iy$ avec $y > 0$. On a alors $c^2 y \leqslant |cz+d|^2 \leqslant \frac{\operatorname{Im} z}{\alpha}$ soit $c^2 \leqslant (\alpha \operatorname{Im} z)^{-1}$; de même on a $d^2 \leqslant |cz|^2 + |cz+d|^2 \leqslant c^2|z|^2 + \frac{\operatorname{Im} z}{\alpha}$, de sorte que l'ensemble des couples (c, d) est fini, éventuellement vide d'où le résultat. On notera que l'ensemble des $g \in G$ ayant pour deuxième ligne (c, d) n'est pas fini; a et b sont donnés par des coefficients de Bezout: $ad - bc = \pm 1$.

(c) La question se traite de manière identique à la précédente en remplaçant G par G_0.

(d) On écrit $Rez_0 = m + t$ avec $m \in \mathbb{Z}$ et $|t| \leqslant 1/2$ de sorte que $z_1 = T^{-m}(z_0)$ a t pour partie réelle et a la même partie imaginaire que z_0, et comme $T \in G_0$, on peut remplacer z_0 par z_1. En outre on a $\operatorname{Im} S(z_1) = \frac{\operatorname{Im} z_1}{|z_1|^2} \leqslant \operatorname{Im} z_1$ soit $|z_1| \geqslant 1$ soit $z_1 \in D$.

(e) On commence par montrer que deux points $z, z' \in D$ sont dans la même G-orbite alors z et z' appartiennent à la frontière de D soit $z' = g(z)$ avec quitte à échanger z et z' avec $z = g^{-1}(z')$, on peut supposer $\operatorname{Im} z \leqslant \operatorname{Im} z'$, soit en écrivant $z = x + iy$,

$$1 \geqslant (cx + d)^2 + c^2y^2 \geqslant c^2y^2 \geqslant \frac{3}{4}c^2$$

car $z \in D$. On en déduit alors $|c| \leqslant 2$ soit $c \in \{-1, 0, 1\}$. Comme il est loisible de changer les signes des coefficients de g, le cas $c = -1$ se ramène au cas $c = 1$.

Cas $c = 0$: on a alors $ad = 1$ soit $a = d = \pm 1$ et $g = T^n$ pour $n \in \mathbb{Z}$. Si $n = 0$, on a alors $g = I$ et $z = z'$ et sinon $n = \pm 1$ avec l'une des deux parties réelles Rez et Rez' est égale à $1/2$ l'autre étant égale à $-1/2$.

Cas $c = 1$: on a $|z + d| \leqslant 1$ ce qui donne $d \in \{-1, 0, 1\}$. Pour $d = 0$, on obtient $b = -1$ et $z' = a - 1/z$. Si $Rez \neq \pm 1/2$, i.e. $z \neq j$ et $z \neq -j^2$ alors $a = 0$ et $z' = -\overline{z}$. Si $z = j$ (resp. $z = -j^2$), on peut avoir $a = 0$ ou -1 et $z' = -j^2$ ou $-j$ (resp. $z' = j$ ou $-j^2$); dans tous les cas on a $|z| = |z'| = 1$.

Si $d = 1$, on a $|z| = 1$ et $x = -1/2$ soit $z = j$; on a alors $a - b = 1$ et $z' = a + j$ ce qui implique $a = 0$ ou 1 et $z' = j$ ou $-j^2$. Si $d = -1$, on obtient de même $z = -j^2$ et $z' = j$ ou $-j^2$.

Montrons maintenant $G = G_0$; soit $g \in G$ et $z \in D$ un point intérieur. D'après (d), il existe $g_0 \in G_0$ tel que $g_0(g(z)) \in D$ ce qui implique $g_0 \circ g(z) = z$ soit $g = g_0^{-1} \in G_0$.

□

2 Réseaux

Exercice 1. *Soit G un $\mathbb{Z}$-module libre de rang n. Justifiez ou infirmez les affirmations suivantes:*

(i) de toute famille génératrice de G, on peut extraire une base;

(ii) toute famille libre de G de cardinal n est génératrice;

(iii) le théorème de la base incomplète est vérifié, i.e. on peut toujours compléter une famille libre en une base;

(iv) tout sous-groupe de G admet un supplémentaire.

Preuve: (i) c'est faux comme on peut le voir sur l'exemple: $(2, 3)$ est une fammille génératrice de $\mathbb{Z}$ dont on ne peut extraire aucune base;

(ii) c'est à nouveau faux: par exemple $2\mathbb{Z} \subset \mathbb{Z}$;

(iii) c'est encore faux: par exemple $G = \mathbb{Z}^2$ et soit $v = (2, 0)$ alors quelque soit $w = (a, b)$ tel que (v, w) soit libre, le point $(1, 0)$ ne sera jamais atteint;

(iv) c'est toujours faux: en effet $2\mathbb{Z} \subset \mathbb{Z}$ n'admet pas de supplémentaire.

□

Exercice 2. *Montrez l'équivalence entre les trois points suivants:*

(i) $(n_1, \cdots, n_r) = 1$*;*

(ii) il existe une matrice A *de* $SL_r(\mathbb{Z})$ *tel que* $A \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$*;*

(iii) $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ *peut être complété en une base de* $\mathbb{Z}^r$*.*

Exemple: complétez $(10, 6, 7, 11)$ *en une base de* $\mathbb{Z}^4$*.*

Preuve: (i) implique (ii): le résultat se démontre par récurrence; la première étape du calcul est la suivante:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \cdots & u & v \\ 0 & \cdots & -n_r/(n_r, n_{r-1}) & n_{r-1}/(n_r, n_{r-1}) \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ (n_r, n_{r-1}) \\ 0 \end{pmatrix}$$

où u et v sont les coefficients de Bezout entre n_{r-1} et n_r: $un_{r-1} + vn_r = (n_r, n_{r-1})$. On peut aussi utiliser le résultat (**??**) du cours, dont la preuve repose sur un calcul du genre de celui exposé ci-dessus: on considère $f : \mathbb{Z}^r \longrightarrow \mathbb{Z}$ défini par $f(a_1, \cdots, a_r) = a_1 n_1 + \cdots + a_r n_r$. Le théorème fondamental du cours dit de la base adpatée, nous assure l'existence d'une base $(e_1, \cdots, e_n)$ de $\mathbb{Z}^n$ tel que $\operatorname{Ker} \phi = \mathbb{Z}a_1 e_1 \oplus \cdots \oplus \mathbb{Z}a_r e_r$ avec $a_i | a_{i+1}$ dans $\mathbb{Z}$ que l'on appelle les facteurs invariants de $\mathbb{Z}^n / \operatorname{Ker} \phi$; d'après l'exercice 1 on a en outre que les a_i sont tous égaux à 1 pour $1 \leqslant i < r$ et $a_r = 0$ (par un argument de dimension). Ainsi si on note A transposée de la matrice de passage de la base $(e_r, e_{r-1}, \cdots, e_1)$ dans la base canonique, on a $A \in SL_r(\mathbb{Z})$ et $A \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

(ii) implique (iii): il est évident que la famille $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, A^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots, A^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ forme une base de $\mathbb{Z}^n$.

(iii) implique (i): soit $e_2, \cdots, e_r$ une famille qui complète $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ en une base et on note A la matrice de passage de cette base dans la base canonique; on calcule le déterminant de A en le développant par rapport à la première colonne de sorte que celui-ci est divisible par le pgcd des n_i qui est donc égal à 1 car $\det A = \pm 1$.

Exemples: le premier cas est simple car on a la relation $7 - 6 = 1$ de sorte que la matrice suivante est de déterminant -11

$$\begin{pmatrix} 10 & 6 & 7 & 11 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

de sorte que les 4 vecteurs colonnes de la transposée de la patrice ci-dessus constituent une base de $\mathbb{Z}^4$.
Dans le deuxième exemple on a la relation de Bezout: $1 = 6.6 - 2.10 - 15$. On cherche donc 6 coefficients a, b, c, d, e, f tels que $cf - de = 6$, $af - be = 2$ et $ad - bc = -1$. Par exemple la matrice suivante convient

$$\begin{pmatrix} 6 & 1 & 0 \\ 10 & 0 & -1 \\ 15 & 6 & 2 \end{pmatrix}$$

□

Exercice 3. *Diverses propriétés des réseaux (voir chap 5 §2 du cours) dans la suite K est l'un des corps $\mathbb{Q}$ ou $\mathbb{R}$ et V est un K-espace vectoriel de dimension finie $n > 0$. Une partie Γ de V est un sous-réseau s'il existe une famille libre $\mathbf{e} = (e_1, \cdots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$. On dit que $\mathbf{e}$ est une $\mathbb{Z}$-base de Γ et r est son rang. On dit que Γ est un réseau si $r = n$.*

(i) *$\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un sous-réseau de $\mathbb{R}$?*

(ii) *Soit Γ un réseau de V, $\mathbf{e}$ une $\mathbb{Z}$-base de Γ et $\mathbf{v}$ une base de V. Montrez que $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ si et seulement si la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ appartient à $GL_n(\mathbb{Z})$.*

(iii) *Soient Γ un réseau de V et $\Lambda \subset \Gamma$ un sous-groupe. Montrez que Λ est un sous-réseau de V et qu'il existe une $\mathbb{Z}$-base $(e_1, \cdots, e_n)$ de Γ, $1 \leqslant s \leqslant n$ et $a_1, \cdots, a_s \in \mathbb{Z}^\times$ vérifiant:*

- *$(a_1e_1, \cdots, a_se_s)$ est une $\mathbb{Z}$-base de Λ,*
- *pour $1 \leqslant i < s$, a_i divise a_{i+1}*

En déduire une CNS pour que Γ/Λ soit fini et calculez son cardinal en fonction des a_i.

(iv) *On suppose ici $K = \mathbb{Q}$. Soient Γ, Λ des réseaux de V. Montrez que*

- *il existe $d \in \mathbb{N}\backslash\{0\}$ tel que $d\Gamma \subset \Lambda$,*
- *$\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont des réseaux de V.*

(v) *On suppose ici $K = \mathbb{R}$ et on munit V de sa topologie canonique. Montrez que tout sous-groupe discret[1] Γ de V en est un sous-réseau.*

Indication: soit $(e_1, \cdots, e_r)$ une famille libre maximale de Γ et $\mathcal{K} = \{\lambda_1e_1 + \cdots + \lambda_re_r; \lambda_i \in [0, 1]\}$. En utilisant le fait que $\mathcal{K} \cap \Gamma$ est fini et en considérant pour $j \in \mathbb{Z}$ et $x = \lambda_1e_1 + \cdots + \lambda_re_r \in \Gamma$, les $x_j = jx - ([j\lambda_1]e_1 + \cdots + [j\lambda_r]e_r)$[2], montrez que $\lambda_i \in \mathbb{Q}$ et conclure.

A quelles conditions est-ce un réseau?

[1] i.e. tel que pour tout compact $\mathcal{K}$ de V, $\mathcal{K} \cap \Gamma$ est fini
[2] $[\lambda]$ désigne la partie entière de λ

Preuve: (i) $\sqrt{2}$ n'appartenant pas à $\mathbb{Q}$, $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense dans $\mathbb{R}$; si G était un réseau on aurait $G = \alpha\mathbb{Z}$ et serait discret, ce qui n'est pas.

(ii) Si $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ, la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ et celle de $\mathbf{v}$ à $\mathbf{e}$ sont à coefficients dans $\mathbb{Z}$ et sont inverses l'une de l'autre, d'où le résultat. Réciproquement soit P (resp. P^{-1}) la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ (reps. de $\mathbf{v}$ à $\mathbf{e}$). Comme P est à coefficients dans $\mathbb{Z}$, le réseau engendré par $\mathbf{e}$ est inclus dans celui engendré par $\mathbf{v}$; l'inclusion inverse découle de même du fait que P^{-1} est à coefficients dans $\mathbb{Z}$.

(iii) C'est le théorème de la base adaptée, sur les modules de type fini sur un anneau principal. Le quotient Γ/Λ est fini si et seulement si les deux réseaux ont le même rang et alors le cardinal est égal à la valeur absolue du produit des a_i, $1 \leqslant i \leqslant n$.

(iv) - Soient $\mathbf{e}$ et $\mathbf{f}$ des $\mathbb{Z}$-bases de respectivement Γ et Λ. On note $P = (p_{i,j})_{1\leqslant i,j\leqslant n} \in GL_n(\mathbb{Q})$ la matrice de passage de $\mathbf{f}$ à $\mathbf{e}$ et soit d le ppcm des dénominateurs des $p_{i,j}$, $1 \leqslant i, j \leqslant n$, écrits sous formes irréductibles. Il est alors clair que l'on a $d\Gamma \subset \Lambda$.

- Soit d comme ci-dessus. On a alors

$$d\Gamma \subset \Gamma \cap \Lambda \subset \Gamma$$

$$\Gamma \subset \Gamma + \Lambda \subset d^{-1}\Lambda$$

L'inclusion $\Gamma \cap \Lambda \subset \Gamma$ (resp. $\Gamma + \Lambda \subset d^{-1}\Lambda$) prouve d'après (iii) que $\Gamma \cap \Lambda$ (resp. $\Gamma + \Lambda$) est un sous-réseau de Γ (resp. $d^{-1}\Lambda$). Les autres inclusions montrent que $\Gamma + \Lambda$ et $\Gamma \cap \Lambda$ sont de rang n.

(v) On procède comme suggéré dans l'indication; $\mathcal{K}$ étant compact, $\mathcal{K} \cap \Gamma$ est fini; on note $y_1, \cdots, y_s$ ses éléments . Soit $x = \sum_{i=1}^r \lambda_i e_i \in \Gamma$, $\lambda_i \in \mathbb{R}$. On considère pour $j \in \mathbb{Z}$, $x_j = jx - \sum_{i=1}^r [j\lambda_i]e_i$; $x_j \in \Gamma \cap \mathcal{K}$ de sorte qu'il existe $j \neq k$ tels que $x_j = x_k$, soit $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ pour $1 \leqslant i \leqslant r$ et donc $\lambda_i \in \mathbb{Q}$. Pour $1 \leqslant i \leqslant s$, on écrit $y_i = \sum_{k=1}^r \lambda_k^i e_k$ avec $\lambda_k^i \in \mathbb{Q}$ et soit d le ppcm des dénominateurs des λ_k^i écrits sous forme irréductible. De l'égalité $x = x_1 + \sum_{i=1}^r [\lambda_i]e_i$, on en déduit $dx \in \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$ soit $d\Gamma \subset \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$, soit $\Gamma \subset \mathbb{Z}d^{-1}e_1 + \cdots + \mathbb{Z}d^{-1}e_r = \Lambda$ et ainsi Γ est un sous-groupe du sous-réseau Λ de V et donc Γ est un sous-réseau de V. En outre Γ est un réseau de V si et seulement si Γ est discret et V/Γ est compact.

□

Exercice 4. *(*) On reprend les notations de l'exercice précédent avec $K = \mathbb{R}$. On note μ la mesure de Lebesgue de $\mathbb{R}^n$, $(\epsilon_1, \cdots, \epsilon_n)$ sa base canonique et $(.|.)$ le produit scalaire associé $(\epsilon_i|\epsilon_j) = \delta_{i,j}$. Pour Γ un réseau de $\mathbb{R}^n$ et $\mathbf{e} = (e_1, \cdots, e_n)$ une $\mathbb{Z}$-base de Γ, on pose*

- $P_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1]\}$,
- $D_{\mathbf{e},\Gamma} = \{\sum_{i=1}^n \lambda_i e_i;\ \lambda_1, \cdots, \lambda_n \in [0,1[\}$,

On note $S_{\mathbf{e},\Gamma}$ (resp. $T_{\mathbf{e},\Gamma}$) la matrice de terme général $(e_i|e_j)$ (resp. $(\epsilon_i|e_j)$).

(a) Montrez que $S_{\mathbf{e},\Gamma} = {}^tT_{\mathbf{e},\Gamma}T_{\mathbf{e},\Gamma}$. En utilisant la formule du jacobien pour le changement de variables dans les intégrales multiples, en déduire l'égalité $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$. Montrez ensuite que $\mu(P_{\mathbf{e},\Gamma})$ ne dépend que de Γ et non de $\mathbf{e}$; on dit que c'est la mesure du réseau et on la note $\mu(\mathbb{R}^n/\Gamma)$.

(b) Une partie $\mathcal{D}$ de $\mathbb{R}^n$ est un domaine fondamental de Γ, si $\mathcal{D}$ est μ-mesurable et si ses translatés par les vecteurs de Γ forment une partition de $\mathbb{R}^n$. Montrez que $D_{\mathbf{e},\Gamma}$ est un domaine fondamental et que $\mu(\mathcal{D}) = \mu(\mathbb{R}^n/\Gamma)$ pour tout domaine fondamental $\mathcal{D}$ de Γ.

(c) En utilisant le théorème de la base adaptée, montrez que si $\Lambda \subset \Gamma$ *sont des réseaux alors* Γ/Λ *est fini et*

$$\mu(\mathbb{R}^n/\Lambda) = \mathrm{card}(\Gamma/\Lambda)\mu(\mathbb{R}^n/\Gamma)$$

(d) (i) Soit $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\Gamma$ *la surjection canonique associé au réseau* Γ *et soit* F *une partie de* $\mathbb{R}^n$*,* μ*-mesurable vérifiant* $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$*. Montrez que la restriction de* φ *à* F *n'est pas injective.*

(ii) Déduire de (i), le théorème de Minkowski: soient Γ *un réseau de* $\mathbb{R}^n$ *et* A *une partie* μ*-mesurable, convexe, symétrique par rapport à* O *et vérifiant* $\mu(A) > 2^n\mu(\mathbb{R}^n/\Gamma)$*, alors* $A \cap \Gamma \neq \{O\}$*.*

(iii) Montrez que si C *est un convexe compact de* $\mathbb{R}^n$*, symétrique par rapport à* O *tel que* $\mu(C) \geqslant 2^n\mu(\mathbb{R}^n/\Gamma)$ *alors* $C \cap \Gamma \neq \{O\}$*.*

(iv) Soit v_n *le volume de la boule unité fermée de* $\mathbb{R}^n$*. Montrez qu'il existe* $\gamma \in \Gamma$ *différent de* O *et de norme inférieure ou égale à deux fois la racine* n*-ième de* $v_n^{-1}\mu(\mathbb{R}^n/\Gamma)$*.*

Preuve: (a) L'égalité $S_{\mathbf{e},\Gamma} = {}^tT_{\mathbf{e},\Gamma}T_{\mathbf{e},\Gamma}$ découle directement des formules classiques du cours d'algèbre bilinéaire en remarquant par exemple que $T_{\mathbf{e},\Gamma}$ est la matrice de passage de la base $\mathbf{e}$ à la base canonique; ainsi on a $\det S_{\mathbf{e},\Gamma} = (\det T_{\mathbf{e},\Gamma})^2 \geqslant 0$. En outre, par la formule du changement de variable dans une intégrale multiple via le jacobien, on a $\mu(P_{\mathbf{e},\Gamma} = \int_{P_{\mathbf{e},\Gamma}} d\mu = \int_0^1 \cdots \int_0^1 |\det T_{\mathbf{e},\Gamma}| dx_1.\cdots.dx_n$, soit $\mu(P_{\mathbf{e},\Gamma}) = \sqrt{\det S_{\mathbf{e},\Gamma}}$.

Si $\mathbf{f}$ est une autre $\mathbb{Z}$-base de Γ, on ntoe Q la matrice de passage de $\mathbf{e}$ à $\mathbf{f}$; $Q \in GL_n(\mathbb{Z})$ et $S_{\mathbf{f},\Gamma} = {}^tQS_{\mathbf{e},\Gamma}Q$, soit $\det S_{\mathbf{f},\Gamma} = \det S_{\mathbf{e},\Gamma}(\det Q)^2$; or comme $Q \in GL_n(\mathbb{Z})$, on a $\det Q \in \mathbb{Z}^\times$, soit $\det Q = \pm 1$, d'où le résultat.

(b) $D_{\mathbf{e},\Gamma}$ est évidemment un domaine fondamental. Soient alors $\mathcal{D}_1$ et $\mathcal{D}_2$ des domaines fondamentaux quelconques. En considérant $\mathcal{D}_2$ comme un domaine fondamental, on écrit

$$\mathcal{D}_1 = \coprod_{v\in\Gamma} \mathcal{D}_1 \cap (v + \mathcal{D}_2),$$

Γ étant dénombrable et μ étant invariante par translation, on a

$$\begin{array}{rl} \mu(\mathcal{D}_1) & = \sum_{v\in\Gamma} \mu(\mathcal{D}_1 \cap (v + \mathcal{D}_2)) \\ & = \sum_{v\in\Gamma} \mu((-v + \mathcal{D}_1) \cap \mathcal{D}_2) \end{array}$$

Or comme $-\Gamma = \Gamma$, on en déduit $\mu(\mathcal{D}_1) = \sum_{v\in\Gamma} \mu(\mathcal{D}_2 \cap (v + \mathcal{D}_1)) = \mu(\mathcal{D}_2)$, la dernière égalité découlant du fait que $\mathcal{D}_1$ est un domaine fondamental.

(c) D'après le théorème de la base adaptée, il existe une $\mathbb{Z}$-base $\mathbf{v} = (v_1, \cdots, v_n)$ de Γ et des entiers $a_1|a_2|\cdots|a_n$ tels que $\mathbf{w} = (a_1v_1, \cdots, a_nv_n)$ est une $\mathbb{Z}$-base de Λ. Ainsi on obtient $\mathrm{card}(\Gamma/\Lambda) = \prod_{i=1}^n a_i$ et $S_{\mathbf{w},\Lambda} = {}^tDS_{\mathbf{v},\Gamma}D$ avec $D = \mathrm{diag}(a_1, \cdots, a_n)$, d'où le résultat.

(d) (i) Soit $\mathcal{D}$ un domaine fondamental:

$$\mu(F) = \sum_{\gamma\in\Gamma} \mu(F \cap (\gamma + \mathcal{D})) = \sum_{\gamma\in\Gamma} \mu((F - \gamma) \cap \mathcal{D}) > \mu(D)$$

d'où il en résulte que les $(F - \gamma) \cap \mathcal{D}$ pour $\gamma \in \Gamma$ ne sont pas deux à deux disjoints. Soient donc $x, y \in F$ et $\alpha \neq \beta \in \Gamma$ vérifiant $x - \alpha = y - \beta$ soit $x - y = \alpha - \beta \in \Gamma\backslash\{O\}$ et donc φ non injective.

(ii) Soit $F = \frac{1}{2}A$; on a donc $\mu(F) > \mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, il existe donc $x, y \in F$ tels que $x - y \in \Gamma\backslash\{O\}$. En outre $2x$ et $-2y$ appartiennent à A d'après la propriété de symétrie de A par rapport à O, et donc $x - y = \frac{(2x-2y)}{2}$ appartient à A d'après la propriété de convexité de A, d'où le résultat.

(iii) Soit $C_r = (1+1/r)C$ pour $r \geqslant 1$; $C = \cap_{r\geqslant 1} C_r$ et $\mu(C_r) > 2^n\mu(\mathbb{R}^n/\Gamma)$. D'après la question précédente, soit $x_r \in C_r \cap (\Gamma\backslash\{O\}) \subset K := 2C \cap (\Gamma\backslash\{O\})$; K étant fini, on peut extraire de la suite $(x_r)_{r\geqslant 1}$ une sous-suite convergente, donc stationnaire, d'où le résultat.

(iv) Une boule $\overline{B}(O, r)$ vérifie $\overline{B}(O, r) \cap (\Gamma\backslash\{O\}) \neq$ dès que $v_n r^n \geqslant \mu(\mathbb{R}^n/\Gamma)$, d'où le résultat. □

Exercice 5. *(*) Quelques applications arithmétiques (utiliser le point (iii) ci-dessus)*

(a) Soient $\epsilon > 0$ et $(\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n\backslash\mathbb{Q}^n$; montrez qu'il existe $p_1, \cdots, p_n \in \mathbb{Z}$ et $q \in \mathbb{N}$ non nul tels que pour tout $1 \leqslant i \leqslant n$, on ait $|\alpha_i - \frac{p_i}{q}| < \frac{\epsilon}{q}$.

Indication: considérez le groupe Γ engendré par les vecteurs de la base canonique et le vecteur $(\alpha_1, \cdots, \alpha_n)$ et remarquez que Γ n'est pas un réseau et n'est donc pas discret.

(b) Montrez que si $p \equiv 1 \bmod 4$, p premier, alors p est somme de deux carrés.

Indication: (-1) étant un carré modulo p, soit $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0 \bmod p$ et soit $\Gamma = \{(a, b) \in \mathbb{Z}^2 \ / \ a \equiv ub \bmod p\}$. Soit $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = \overline{a - ub}$. Montrez que Γ est un réseau de mesure p et utilisez le point (d) (iv) de l'exercice précédent.

(c) Montrez que tout nombre premier p est somme de quatre carrés.

ndication: montrez l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \bmod p$. On fixe un tel couple et soit $\Gamma = \{(a, b, c, d) \in \mathbb{Z}^4 \ / \ ua + vb \equiv c \bmod p$ et $ub - va \equiv d \bmod p\}$. Soit $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2$ défini par $\psi(a, b, c, d) = (\overline{c - ua - vb}, \overline{d + va - ub})$. Montrez que Γ est un réseau de $\mathbb{R}^4$ de mesure p^2 et utilisez le point (d) (iv) de l'exercice précédent.

Preuve: (a) Soit Γ le groupe engendré par $(e_1, \cdots, e_n, e_0)$ où $e_1, \cdots, e_n$ sont les vecteurs de la base canonique de $\mathbb{R}^n$ et $e_0 = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. Si Γ était discret, il serait un réseau; soit $\mathbf{f}$ une $\mathbb{Z}$-base de Γ et P la matrice de passage de $(e_1, \cdots, e_n)$ à $\mathbf{f}$, $P \in M_n(\mathbb{Z})$ et $P^{-1} \in M_n(\mathbb{Q})$ de sorte que e_0 est une combinaison linéaire à coefficients dans $\mathbb{Q}$ des e_i, ce qui n'est pas. Ainsi Γ n'est pas discret et admet un point d'accumulation P. Soit alors $\epsilon > 0$ avec $\overline{B}(O, \epsilon) \cap \Lambda = \{O\}$, où Λ est le réseau $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$; il existe alors des entiers comme dans l'énoncé tels que $(qe_0 + p_1e_1 + \cdots + p_ne_n) - (q'e_0 + p'_1e_1 + \cdots + p'_ne_n)$ soit de norme inférieure à ϵ avec $q - q' \neq 0$, d'où le résultat.

car $\gamma \notin \Lambda$, d'où le résultat.

(b) Soit x un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; on a $x^{p-1} = 1$ et $u = x^{p-1/4}$ est d'ordre 4, soit u^2 d'ordre 2; or dans un corps commutatif de caractéristique différent de 2, il y a exactement un élément d'ordre 2, i.e. -1; en effet l'équation $X^2 - 1$ y a au plus deux solutions. Soit alors $\Gamma = \{(a, b) \in \mathbb{Z}^2 \ / \ a \equiv ub \bmod p\}$ et $\psi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ défini par $\psi(a, b) = a - ub$; ψ est clairement surjective et son noyau est Γ de sorte que ψ induit un isomorphisme $\mathbb{Z}^2/\Gamma \simeq \mathbb{Z}/p\mathbb{Z}$. On en déduit donc que Γ est un réseau de mesure p car $\mu(\mathbb{R}^2/\mathbb{Z}^2) = 1$. D'après l'exercice précédent question (d) (iv), il existe donc $\gamma = ae_1 + be_2 \neq O \in \Gamma$ de module inférieur ou égal à

$2\sqrt{\frac{p}{\pi}}$, soit $0 < a^2 + b^2 \leqslant 4p/\pi < 2p$; or comme $\gamma \in \Gamma$, on a $a^2 + b^2 \equiv b^2(u^2 + 1) \equiv 0 \bmod p$, d'où $a^2 + b^2 = p$.

(c) Le cas $p = 2 = 1^2+1^2+0^2+0^2$ est vite traité, soit donc $p \geqslant 3$ premier. Soit $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ défini par $\phi(x) = x^2$; $\mathbb{Z}/p\mathbb{Z}$ étant un corps, $\operatorname{Ker}\phi = \{1, -1\}$ de sorte que $\mathbb{I}\phi$ est de cardinal $(p-1)/2$. En remarquant que 0 est un carré, on en déduit que $\{u^2 \ / \ u \in \mathbb{Z}/p\mathbb{Z}\}$ est de cardinal $(p+1)/2$ et qu'il en est de même pour $\{1 - v^2 \ / \ v \in \mathbb{Z}/p\mathbb{Z}\}$; comme $2(p+1)/2 > p$ on en déduit que $\{u^2 \ / \ u \in \mathbb{Z}/p\mathbb{Z}\} \cap \{1 - v^2 \ / \ v \in \mathbb{Z}/p\mathbb{Z}\}$ est non vide, et on fixe u, v tels que $u^2 + v^2 + 1 \equiv 0 \bmod p$. Avec les notations de l'énoncé, ψ est clairement surjective et son noyau est le groupe Γ; ψ induit donc un isomorphisme $\mathbb{Z}^4/\Gamma \simeq (\mathbb{Z}/p\mathbb{Z})^2$. On en déduit donc que Γ est un réseau de mesure p^2. D'après le point (d) (iv) de l'exercice précédent, soit $\gamma = (a, b, c, d) =\in \Gamma\backslash\{O\}$ de norme au carré inférieure ou égale à $4\sqrt{2}p/\pi < 2p$. Or comme $\gamma \in \Gamma$, on a $a^2 + b^2 + c^2 + d^2 \equiv (a^2 + b^2)(u^2 + v^2 + 1) \equiv 0 \bmod p$, soit $p = a^2 + b^2 + c^2 + d^2$.
Remarque: En utilisant l'identité remarquable[3]

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = (a\alpha - b\beta - c\gamma - d\delta)^2 + (a\beta + b\alpha + c\delta - d\gamma)^2 +$$

$$+(a\gamma + c\alpha + d\beta - b\delta)^2 + (a\delta + b\gamma + d\alpha - c\beta)^2$$

on en déduit que tout entier est somme de quatre carrés.

□

3 Invariants de similitude

Exercice 1. *Donnez les facteurs invariants du $\mathbb{Z}$-module*

$$\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

Preuve : On cherche donc $a_r|a_{r-1}|\cdots|a_1$; évidemment a_1 est l'ordre maximal d'un élément soit donc le ppcm des nombres qui apparaissent, soit $a_1 = 2^2 3^2 5$ et le lemme chinois nous donne $G = \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. On recommence alors le procédé, soit $a_2 = 2^2 3^2$, et $G = \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$; soit $a_3 = 23^2$ et $a_4 = 2$.
Une façon d'automatiser le procédé est de faire à tableau à double entrée; à la position (i, j) on mets le nombre de fois que p_i^j apparait où p_i est le i-ième facteur premier qui apparait. On élimine étape par étape les termes les plus à droite du tableau, un par ligne (bref on calcule le ppcm), jusqu'à épuiser les entrées.

□

Exercice 2. *(*) Pour $n > 1$, on note $J_n \in \mathbb{M}_n(\mathbb{C})$ la matrice nilpotente dont tous les coefficients sont nuls, sauf de la première sur-diagonal $j_{i,i+1}$ pour $1 \leqslant i < n$ qui sont égaux à 1. Donnez*

(i) les invariants de similitudes;

(ii) les polynômes minimaux et caractéristiques;

(iii) la suite des dimensions des noyaux $\operatorname{Ker}(A_i - \alpha)^k$ où α est une valeur propre

des matrices suivantes, écrites par blocs:

[3] cf. le corps des quaternions

(a) $A_1 = \mathrm{diag}(aI_3, bI_2, cI_1)$*;*

(b) $A_2 = \mathrm{diag}(I_3, I_2 + J_2, I_2 + J_2, I_3 + J_3, I_3 + J_3, 2I_2, 2I_3 + J_3, 3I_2, 3I_2 + J_2)$*;*

(c) $A_3 = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & \cdots & 0 & 0 & a_n \end{pmatrix}$

Preuve: On note $V = \mathbb{C}^n$ l'espace vectoriel en question, que l'on munit de la structure de $A = \mathbb{C}[X]$-module définie par la matrice à étudier; on notera $a_r(X)|\cdots|a_1(X)$, ses invariants de similitude. Le polynôme minimal est alors $a_1(X)$ et le polynôme caractéristique est le produit des invariants de similitude. Pour tout valeur propre $\alpha \in \mathbb{C}$, on notera $K_\alpha^i = \mathrm{Ker}(u - \alpha\mathrm{Id})^i$ où u est l'endomorphisme associé à la matrice en question dans la base canonique; on note aussi r_α l'indice i tel que $K_\alpha^{i-1} \neq K_\alpha^i = K_\alpha^j$ pour tout $j \geqslant i$; $K_\alpha^{r_\alpha}$ est appelé le sous-espace caractéristique associé à α. L'entier r_α est la multiplicité de α dans $a_1(X)$ tandis que sa dimension est la multiplicité de α dans le produit des a_i. On note $\delta_\alpha^i = \dim K_\alpha^i - \dim K_\alpha^{i-1}$; partant de la forme de Jordan il est aisé de voir que δ_α^i est égal au nombre de a_k divisible par $(X - \alpha)^i$. On remarque ainsi que le nombre r d'invariants de similitude est égal au maximum des dimensions des sous-espaces propres.

(a) Le A-module V est clairement isomorphe à $(A/(X-a))^3 \times (A/(X-b))^2 \times A/(X-c)$; on calcule alors les invariants de similitude via le théorème chinois comme dans la feuille précédente ce qui donne: $(X-a)$, $(X-a)(X-b)$ et $(X-a)(X-b)(X-c)$. La matrice étant diagonalisable, les sous-espaces propres sont les sous-espaces caractéristiques, i.e. tous les δ_α^i sont nuls.

(b) De même on a

$$V \simeq (A/(X-1))^3 \times (A/(X-1)^2)^2 \times (A/(X-1)^3)^2 \times \\ (A/(X-2))^2 \times A/(X-2)^3 \times (A/(X-3))^2 \times A/(X-3)^2$$

les invariants de similitude donnés comme d'habitude par application du théorème chinois sont alors

$$(X-1)^3(X-2)^3(X-3)^2, \quad (X-1)^3(X-2)(X-3), \quad (X-1)^2(X-2)(X-3), \\ (X-1)^2, \quad (X-1), \quad (X-1), \quad (X-1).$$

Avec les notations introduites ci-dessus, on a $\delta_1^1 = 7$ (resp. $\delta_2^1 = 3$, resp. $\delta_3^1 = 3$), puis $\delta_1^2 = 4$ (resp. $\delta_2^2 = 1$, resp. $\delta_3^2 = 1$), et $\delta_1^3 = 2$ (resp. $\delta_2^3 = 1$, resp. $\delta_3^3 = 0$) tous les δ_i^k étant nuls pour $k > 3$. On obtient alors $\dim K_1^1 = 7$ (resp. $\dim K_2^1 = 3$, resp. $\dim K_3^1 = 3$), $\dim K_1^2 = 11$ (resp. $\dim K_2^2 = 4$, resp. $\dim K_3^2 = 4$) et $\dim K_1^3 = 13$ (resp. $\dim K_2^3 = 5$, resp. $\dim K_3^3 = 4$) avec $r_1 = 3$ (resp. $r_2 = 3$, resp. $r_3 = 2$).

(c) Le sous-espace propre associé à la valeur propre 0 (resp. 1) est de dimension supérieure ou égale à 1 (resp. $n-2$); dans $\mathbb{C}$, la dernière valeur propre est déterminée via la trace de la matrice dont on sait qu'elle est égale à la somme des valeurs propres comptées avec multiplicité (en effet toute matrice complexe est trigonalisable); ainsi on a $1.0 + (n-2).1 + x = n - 2 + a_n$ de sorte que la dernière valeur propre est a_n. Si $a_n \neq 0, 1$ alors la somme des dimensions des sous-espaces

propres associés aux valeurs propres $0, 1, a_n$ est n de sorte que la matrice est diagonalisable et donc

$$V \simeq A/(X) \times A/(X - a_n) \times (A/(X-1))^{n-2}$$

et les invariants de similitude sont

$$a_1(X) = (X-1)X(X-a_n), \quad a_2(X) = X-1, \quad \cdots \quad a_{n-2}(X) = X-1.$$

Si $a_n = a_1 = 0$, on est dans la même situation, car le noyau de la matrice est alors de dimension 2 car son rang est de manière évidente $n-2$; les invariants de similitude sont alors

$$a_1(X) = X(X-1), \quad a_2(X) = X(X-1), \quad a_3(X) = \cdots = a_{n-2}(X) = X-1.$$

Dans le cas où $a_n = 0$ et a_1 non nul, on a alors $r_0 = 2$ avec $\dim K_0^1 = 1$ de sorte que

$$V \simeq A/(X^2) \times (A/(X-1))^{n-2}$$

soit

$$a_1(X) = X^2(X-1), \quad a_2(X) = \cdots = a_{n-2}(X) = (X-1).$$

□

Exercice 3. *(*) Ecrivez sous la forme de Jordan les matrices dont les invariants de similitudes sont:*

(a) $\mu_1(X) = X$*;*

(b) $\mu_1(X) = X(X-1)$*;*

(c) $\mu_1(X) = X$ *et* $\mu_2(X) = X^2$*;*

(d) $\mu_1(X) = X$ *et* $\mu_2(X) = X(X-1)$*;*

(e) $\mu_1(X) = X^2(X-1)$, $\mu_2(X) = X^2(X-1)(X-2)$, $\mu_3(X) = X^3(X-1)^2(X-2)$ *et* $\mu_4(X) = X^4(X-1)^3(X-2)^4$*;*

Précisez en outre les dimensions des noyaux itérés pour les différentes valeurs propres.

Preuve: on reprend les notations des exercices précédents. On rappelle que la dimension n de l'espace vectoriel en question est la somme des degrés des invariants de similitude.

(a) Ici $n = 1$ et l'endomorphisme en question est l'identité.

(b) On a $n = 2$ et un espace cyclique avec deux valeurs propres distinctes; u est donc diagonalisable et sa matrice dans une base diagonalisante est la matrice diagonale $\mathrm{diag}(0, 1)$.

(c) $n = 3$ et 0 est la seule valeur propre avec $\delta_0^1 = 2$ et $\delta_0^2 = 1$ soit $\dim K_0^1 = 2$ et $\dim K_0^2 = 3$ et la matrice de Jordan associée est $\mathrm{diag}(0, J_2)$.

(d) $n = 3$ et $0, 1$ sont les valeurs propres de u avec $\delta_0^1 = 2$ (resp. $\delta_1^1 = 1$) et $\delta_1^i = \delta_0^i = 0$ pour $i > 1$. On obtient alors $\dim K_0^1 = 2$ et $\dim K_1^1 = 1$, l'endomorphisme est donc diagonalisable.

(e) $n = 24$, les valeurs propres étant $0, 1, 2$; la suite δ_0^i (resp. δ_1^i, resp. δ_2^i) est $(4, 4, 2, 1, 0, \cdots)$ (resp. $(4, 2, 1, 0, \cdots)$, resp. $(3, 1, 1, 1, 0, \cdots)$) de sorte que la suite des dimensions des K_0^i (resp K_1^i, resp. K_2^i) est $(4, 8, 10, 11, \cdots)$ (reps. $(4, 6, 7, \cdots)$, resp. $(3, 4, 5, 6, \cdots)$). La forme de Jordan est la matrice diagonale par blocs

$$\mathrm{diag}(J_2, J_2, J_3, J_4, I_1, I_1, I_2, I_3, 2I_2, 2I_4 + J_4).$$

□