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

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 $G_0 = G$.

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.

Exercice 2. *(*) Donnez une base adpatée du sous-$\mathbb{Z}$-module Λ de $\mathbb{Z}^3$ engendré par les vecteurs $(2,3,6)$, $(4,6,3)$, $(10,6,9)$ et $(12,4,2)$. Précisez alors les facteurs invariants ainsi que la décomposition en modules indécomposables de $\mathbb{Z}^3/\Lambda$.*

Exercice 3. *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* $\mathbb{Z}^4$.

Exercice 4. *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?

Exercice 5. *(*) 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*

[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

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

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 $v_n^{-1}\mu(\mathbb{R}^n/\Gamma)$.*

Exercice 6. *(*) 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 $\Gamma = \{(a,b,c,d) \in \mathbb{Z}^4 \ /\ ua + vb \equiv c \bmod p \text{ et } ub - va \equiv d \bmod p\}$. 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.

3 Invariants de similitude

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

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

Exercice 2. *(*) 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 les invariants de similitudes et précisez les polynômes minimaux et les déterminants des matrices suivantes, écrites par blocs:*

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

(b) $A_2 = \mathrm{diag}(I_3, I_2 + J_2, I_2 + J_2, I_3 + J_3, I_3 + J_3, 2I_2, 2I_3 + J_3, 3I_2, 3I_1 + J_1)$;

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

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.

4 Groupes de pavages

(voir chap2 §2 du cours)
Définition des groupes de paveurs: soit E un plan euclidien et P un compact connexe de E d'intérieur $\dot{P}$ non vide. Un groupe G sera dit un groupe de paveur de P si G est un sous-groupe du groupe des isométries directes $Is^+(E)$ de E vérifiant les deux propriétés suivantes:
(i) GP1: $\bigcup_{g\in G} g(P) = E$
(ii) GP2: $g(\dot{P}) \cap h(\dot{P}) \neq \emptyset \Rightarrow g(P) = h(P)$.
Remarque: Un pavé P sera dit fondamental s'il vérifie la version plus forte de GP2: $g(\dot{P}) \cap h(\dot{P}) \neq \emptyset \Rightarrow g = h$.

(1) Montrer que $Is^+(E)$ est le produit semi-direct du sous-groupe des translations $T(E)$ de E par le groupe $O^+(\vec{E})$, où $\vec{E}$ est l'espace vectoriel sous-jacent à l'espace affine E.

(2) (i) Montrer que tout compact de P ne contient qu'un nombre fini de pavés $g(P)$ distincts.

(ii) Pour $g_0 \in G$, on pose $G_{g_0(P)} = \{g \in G : g(g_0(P)) = g_0(P)\}$. Montrer qu'il existe $a \in E$ tel que $G_{g_0(P)} \subset G_a = \{g \in G! g(a) = a\}$ et en déduire que $G_{g_0(P)}$ est fini.

(iii) Montrer que G opère discrètement dans E, i.e. pour tout $e \in E$ l'orbite $G(e)$ de e sous G est constituée de points isolés ($\forall a \in G(e) \exists \epsilon > 0$ tel que le disque $D(a, \epsilon)$ a une intersection avec $G(e)$ réduite à b).

(3) Soit $\Gamma := G \cap T(E)$.

(i) Supposons que Γ est trivial, i.e. réduit à l'élément identité. En considérant des commutateurs montrer que G est commutatif et que cela est en contradiction avec GP1.

(ii) Supposons que toutes les directions des éléments de Γ soient parallèles. Montrer à nouveau que cela contredit GP1.

(iii) Soit alors $\vec{u}$ un vecteur de norme minimale (non nulle) tel qu'il existe une translation de Γ de vecteur $\vec{u}$ et soit $\vec{v} \notin \mathbb{R}\vec{u}$ de plus petite norme tel qu'il existe une translation de Γ de vecteur $\vec{v}$. Pour un point $e \in E$ quelconque on considère le parallélogramme $Q = \{e + t\vec{u} + s\vec{v} : \ t, s \in [0, 1]\}$. En utilisant le fait que les $g(Q)$ pour $g \in \Gamma$, remplissent E, montrer que $\Gamma = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$.

(4) Soit $g \in G' = G \backslash \Gamma$ que l'on supposera non vide. Montrer que g est d'ordre fini n_g.

(i) Traiter le cas où tous les n_g sont égaux à 2.

(ii) Supposons qu'il existe g tel que $n_g \geqslant 3$. Montrer que l'on peut supposer que g est une rotation de centre a et d'angle $2\pi/\alpha$ avec $\alpha = n_g$. Soit alors b un centre de rotation d'un élément de G' tel que la distance $d(a, b)$ soit minimale et soit $g_1 \in G'$ une rotation de centre b et d'angle $2\pi/\beta$ pour $\beta = n_{g_1} \geqslant 3$ et soit $h = (gg_1)^{-1}$ de sorte que $gg_1h = Id$. Montrer que h est un rotation d'angle $2\pi/\gamma$ avec $\gamma = n_h$.

(iii) En utilisant le fait que le centre c de h est tel que le triangle abc ait des angles moitié de ceux de g, g_1, h, en déduire l'égalité $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} = 1$

(iv) En utilisant $\alpha, \beta \geqslant 3$ et $\gamma \geqslant 2$ donner tous les triplets (α, β, γ) vérifiant l'égalité de (iii) et déterminer les groupes de paveurs ainsi que les pavages correspondants.

Remarque: On peut étudier le même problème pour le groupe $Is(E)$ ce qui donne 12 groupes supplémentaires.