

Objectif du problème

Cette introduction est destinée à expliquer le type des résultats obtenus dans le problème. Ce dernier ne commence qu'à partir du I.

Dans la démonstration en 1994 du « dernier théorème » de Fermat par Andrew Wiles, les « courbes elliptiques » jouent un rôle central par le biais de l'action du groupe $SL_2(\mathbb{Z})$ sur le demi-plan ouvert $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$.

En effet, il se trouve que l'ensemble des courbes elliptiques sur le corps \mathbb{C} est en bijection (à un \mathbb{C} -isomorphisme près) avec l'ensemble des réseaux de \mathbb{C} (à une similitude près), lui-même en bijection avec l'ensemble des orbites du demi-plan \mathcal{H} sous l'action de $SL_2(\mathbb{Z})$. Ce sont quelques propriétés de ces deux derniers ensembles que nous proposons d'étudier dans ce problème.

Partie I - Matrices carrées d'ordre 2 à coefficients entiers

Soit $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau \mathbb{Z} des entiers relatifs.

Dans les parties I, II, III, les lettres a, b, c, d désignent des éléments de \mathbb{Z} . On pose :

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

I.A - Démontrer que l'ensemble $\mathcal{M}_2(\mathbb{Z})$ est un anneau.

I.B -

I.B.1) Démontrer que l'ensemble $GL_2(\mathbb{Z})$ des éléments de $\mathcal{M}_2(\mathbb{Z})$ inversibles dans $\mathcal{M}_2(\mathbb{Z})$ est un groupe pour la multiplication, appelé le groupe des unités de l'anneau $\mathcal{M}_2(\mathbb{Z})$.

I.B.2) Montrer que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) \text{ si et seulement si } |ad - bc| = 1.$$

I.C - On pose

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{Z}) : ad - bc = 1 \right\} ;$$

I.C.1) Montrer que $SL_2(\mathbb{Z})$ est un groupe pour la multiplication des matrices.

I.C.2) Déterminer l'ensemble des couples $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice

$$\begin{bmatrix} 3 & 5 \\ c & d \end{bmatrix} \text{ appartienne à } SL_2(\mathbb{Z}).$$

I.C.3) Déterminer l'ensemble des couples $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice

$$\begin{bmatrix} 3 & 5 \\ c & d \end{bmatrix} \text{ appartienne à } GL_2(\mathbb{Z}).$$

I.C.4) Quelle est la condition nécessaire et suffisante portant sur le couple (a,b) de $\mathbb{Z} \times \mathbb{Z}$ pour qu'il existe une matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ appartenant à } GL_2(\mathbb{Z}) ?$$

I.D - Soient S et T les éléments de $SL_2(\mathbb{Z})$ définis par

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ et } T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} .$$

Pour chacune des trois matrices T , S et TS , répondre aux questions suivantes :

I.D.1) La matrice est-elle diagonalisable, ou à défaut trigonalisable, dans $\mathcal{M}_2(\mathbb{C})$? Donner une forme réduite éventuelle ainsi qu'une matrice de passage.

I.D.2) La matrice est-elle diagonalisable, ou à défaut trigonalisable, dans $\mathcal{M}_2(\mathbb{R})$? Donner une forme réduite éventuelle ainsi qu'une matrice de passage.

I.E - On cherche les matrices A de $SL_2(\mathbb{Z})$ telles que

$$A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2 .$$

- I.E.1) Soit A une telle matrice. Montrer que A est diagonalisable dans $\mathcal{M}_2(\mathbb{R})$ et préciser les formes réduites diagonales possibles de A .
- I.E.2) En déduire l'ensemble des matrices solutions A .

I.F -

On cherche les matrices A de $SL_2(\mathbb{Z})$ telles que

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- I.F.1) Soit A une telle matrice. Montrer que A est diagonalisable dans $\mathcal{M}_2(\mathbb{C})$ et calculer la trace $Tr(A)$ de A .
- I.F.2) Donner la forme générale des matrices solutions A en fonction des trois paramètres a, b, c et d'une relation liant ces trois paramètres.

I.G -

- I.G.1) Démontrer que si deux matrices U et V de $\mathcal{M}_2(\mathbb{R})$ sont semblables en tant que matrices de $\mathcal{M}_2(\mathbb{C})$, alors elles sont semblables dans $\mathcal{M}_2(\mathbb{R})$.
- I.G.2) En déduire que les matrices A de $SL_2(\mathbb{Z})$ solutions de l'équation :

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \text{ sont semblables dans } \mathcal{M}_2(\mathbb{R}) \text{ à la matrice } S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Partie II - Réseaux de \mathbb{C}

On note \mathcal{H} le demi-plan ouvert défini par $\mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$.

$\mathcal{B} = (\alpha, \beta)$ étant une base de \mathbb{C} considéré comme plan vectoriel réel, on appelle réseau engendré par \mathcal{B} l'ensemble $\Lambda_{\mathcal{B}} = \mathbb{Z}\alpha + \mathbb{Z}\beta = \{u\alpha + v\beta; (u, v) \in \mathbb{Z}^2\}$.

Pour simplifier les notations, un réseau sera généralement désigné par la lettre Λ , sans préciser quelle base \mathcal{B} de \mathbb{C} l'engendre.

II.A -

- II.A.1) De quelle structure algébrique est doté un réseau Λ ?
- II.A.2) Démontrer que tout réseau Λ peut être engendré par une base

$$\mathcal{B} = (\alpha, \beta) \text{ de } \mathbb{C} \text{ telle que } \frac{\alpha}{\beta} \in \mathcal{H}.$$

- II.A.3) Démontrer que pour tout quadruplet $(a, b, c, d) \in \mathbb{Z}^4$ et pour tout $z \in \mathbb{C}$ tel que $cz + d \neq 0$, on a

$$\text{Im}\left(\frac{az + b}{cz + d}\right) = \frac{ad - bc}{|cz + d|^2} \text{Im}(z).$$

II.B -

II.B.1) Démontrer que si deux bases $\mathcal{B} = (\omega_1, \omega_2)$ et $\mathcal{B}' = (\omega'_1, \omega'_2)$ de \mathbb{C} telles que

$$\frac{\omega_1}{\omega_2} \in \mathcal{H} \text{ et } \frac{\omega'_1}{\omega'_2} \in \mathcal{H}$$

engendrent le même réseau Λ , alors il existe une matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ telle que } \begin{bmatrix} \omega'_1 \\ \omega'_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

II.B.2) Étudier la réciproque.

II.C - On considère un réseau Λ engendré par une base $\mathcal{B} = (\omega_1, \omega_2)$ de \mathbb{C} telle que

$$\frac{\omega_1}{\omega_2} \in \mathcal{H}$$

Déterminer l'ensemble des couples $(c, d) \in \mathbb{Z}^2$ tels que $\mathcal{B}' = (\omega'_1, \omega'_2)$ avec $\omega'_1 = 3\omega_1 + 5\omega_2$ et $\omega'_2 = c\omega_1 + d\omega_2$ soit une base de \mathbb{C} engendrant également le réseau Λ .

II.D - Pour tout complexe $\tau \in \mathbb{C} \setminus \mathbb{R}$ on note Λ_τ le réseau engendré par la base $(\tau, 1)$ de \mathbb{C} . On suppose que $\tau \in \mathcal{H}$. Trouver la condition nécessaire et suffisante pour qu'un élément $\tau' \in \mathcal{H}$ vérifie $\Lambda_{\tau'} = \Lambda_\tau$.

Partie III - Similitudes directes de centre 0 laissant stable un réseau

Si Λ est un réseau et z un nombre complexe, on pose $z\Lambda = \{z\rho; (\rho \in \Lambda)\}$.

On dit que deux réseaux Λ et Λ' sont semblables s'il existe $\lambda \in \mathbb{C}^*$ tel que $\Lambda' = \lambda\Lambda$.

III.A -

III.A.1) Démontrer que tout réseau Λ est semblable à un réseau Λ_τ où $\tau \in \mathcal{H}$.

III.A.2) Démontrer que deux réseaux Λ_τ et $\Lambda_{\tau'}$, où $(\tau, \tau') \in \mathcal{H} \times \mathcal{H}$, sont semblables si et seulement si il existe une matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ telle que } \tau' = \frac{a\tau + b}{c\tau + d}.$$

La fin de la partie III montre qu'il existe des similitudes directes de centre O , autres que des homothéties, laissant stable un réseau donné Λ .

III.B - Soit Λ un réseau.

III.B.1) Indiquer, sans faire de démonstration, le lien existant entre l'ensemble $S(\Lambda) = \{z \in \mathbb{C} ; z\Lambda \subset \Lambda\}$ et l'ensemble des similitudes directes σ de centre O laissant stable le réseau Λ , c'est-à-dire telles que $\sigma(\Lambda) \subset \Lambda$.

III.B.2) Quel est l'ensemble des homothéties de centre O laissant stable le réseau Λ ? En déduire l'ensemble $S(\Lambda) \cap \mathbb{R}$.

III.B.3) De quelle structure algébrique est doté l'ensemble $S(\Lambda)$?

III.B.4) $\mathcal{B} = (\omega_1, \omega_2)$ étant une base de \mathbb{C} , on pose

$$\tau = \frac{\omega_1}{\omega_2}. \text{ Comparer les ensembles } S(\Lambda_{\mathcal{B}}) \text{ et } S(\Lambda_{\tau}).$$

III.B.5) Quelle relation d'inclusion existe-t-il entre les ensembles $S(\Lambda_{\tau})$ et Λ_{τ} ?

III.C - τ étant un complexe de $\mathbb{C} \setminus \mathbb{R}$, on considère le réseau Λ_{τ} engendré par la base $(\tau, 1)$ de \mathbb{C} .

III.C.1) On suppose que l'ensemble $S(\Lambda_{\tau})$ n'est pas réduit à \mathbb{Z} . Montrer que τ est alors racine d'un polynôme du second degré à coefficients dans \mathbb{Z} .

III.C.2) Réciproquement, on suppose que τ est racine non réelle d'un polynôme $P(X) = uX^2 + vX + w$ du second degré à coefficients u, v, w dans \mathbb{Z} .

a) Montrer que $S(\Lambda_{\tau})$ n'est pas contenu dans \mathbb{R} .

b) Que dire des ensembles $S(\Lambda_{\tau})$ et Λ_{τ} si $u = 1$?

Partie IV - Action du groupe Γ des homographies associées à $SL_2(\mathbb{Z})$ sur l'ensemble \mathcal{H}

Dans cette dernière partie, on étudie l'action de ce groupe Γ sur l'ensemble \mathcal{H} . On introduit au IV.D un sous-ensemble fondamental \mathcal{F} de \mathcal{H} . On montre aux questions IV.E et IV.F que Γ est engendré par les homographies s et t associées aux matrices S et T introduites au I.D et qu'un système de représentants des orbites de Γ est constitué par les points de \mathcal{F} .

À toute matrice

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

de $SL_2(\mathbb{Z})$ on associe l'application $g : \mathcal{H} \rightarrow \mathbb{C}$ définie par : $\forall \tau \in \mathcal{H}, g(\tau) = \frac{a\tau + b}{c\tau + d}$.

IV.A -

IV.A.1) Montrer que l'on a $g(\mathcal{H}) \subset \mathcal{H}$. On identifie dorénavant g avec l'application de \mathcal{H} vers \mathcal{H} qu'elle induit. Lorsque la matrice A parcourt $SL_2(\mathbb{Z})$, l'application correspondante g de \mathcal{H} vers \mathcal{H} décrit un ensemble noté Γ . Dans la suite de cette question on s'intéresse aux propriétés de la surjection

$$\Phi: \begin{cases} SL_2(\mathbb{Z}) \rightarrow \Gamma \\ A \mapsto g \end{cases}$$

IV.A.2) Montrer que $\Phi(A) \circ \Phi(A') = \Phi(AA')$. En déduire que la loi \circ de composition des applications est une loi interne sur Γ .

IV.A.3) Pour tout $A \in SL_2(\mathbb{Z})$, montrer que $\Phi(A)$ est une bijection de \mathcal{H} sur \mathcal{H} et que l'on a $[\Phi(A)]^{-1} = \Phi(A^{-1})$. En déduire que (Γ, \circ) est un groupe.

IV.A.4) Montrer que $[\Phi(A) = id_{\mathcal{H}}] \Leftrightarrow [A = \pm I_2]$.

IV.A.5)

a) Résoudre l'équation $\Phi(A') = \Phi(A)$.

b) En utilisant les matrices S et T définies en I.D, vérifier que le groupe (Γ, \circ) n'est pas commutatif.

IV.B -

IV.B.1) Montrer que le cercle $\mathcal{C}(\omega, R)$ de centre $\omega \in \mathbb{C}$ et de rayon $R > 0$ a pour équation

$$|z|^2 - (\omega\bar{z} + \bar{\omega}z) + |\omega|^2 = R^2.$$

À quelle condition nécessaire et suffisante ce cercle est-il inclus dans \mathcal{H} ?

IV.B.2) On appelle s l'application de \mathcal{H} vers \mathcal{H} associée à la matrice

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

définie au I.D, c'est-à-dire l'élément $s = \Phi(S)$ de Γ . Déterminer l'image par s d'un cercle $\mathcal{C}(\omega, R)$ inclus dans \mathcal{H} .

IV.C -

IV.C.1) Trouver l'image par s d'une droite \mathcal{D} incluse dans \mathcal{H} , c'est-à-dire d'une droite \mathcal{D} d'équation $y = \beta$, avec $\beta > 0$.

IV.C.2) Trouver l'image par s d'une demi-droite \mathcal{D}_+ d'équation

$$\begin{cases} x = \alpha \\ y > 0 \end{cases}, \text{ où } \alpha \in \mathbb{R}, \text{ incluse dans } \mathcal{H}.$$

IV.D - On introduit le sous-ensemble \mathcal{F} de \mathcal{H} , défini par

$$\mathcal{F} = \left\{ \tau \in \mathcal{H} : |\tau| \geq 1, |Re(\tau)| \leq \frac{1}{2} \right\}.$$

On appelle t l'application de \mathcal{H} vers \mathcal{H} associée à la matrice

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

définie au I.D, c'est-à-dire l'élément $t = \Phi(T)$ de Γ . Représenter graphiquement l'ensemble \mathcal{F} et ses images $t(\mathcal{F})$ et $t^{-1}(\mathcal{F})$ par les applications t et t^{-1} .

IV.E - On note G le sous-groupe de Γ engendré par l'ensemble $\{s, t\}$. Soit τ un élément de \mathcal{H} .

IV.E.1) Montrer qu'il existe un élément $g_0 \in G$ tel que

$$(\forall g \in G) Im(g(\tau)) \leq Im(g_0(\tau)).$$

IV.E.2) On pose alors $\tau' = g_0(\tau)$. Démontrer qu'il existe un entier $m \in \mathbb{Z}$ tel que

$$|Re(t^m(\tau'))| \leq \frac{1}{2}.$$

IV.E.3) Vérifier que $|t^m(\tau')| \geq 1$ et en conclure que $t^m(\tau') \in \mathcal{F}$.

IV.F - On peut démontrer le résultat suivant, que l'on admettra ici : si $\tau \in \mathcal{F}$ et si pour un élément $g \in \Gamma$, avec $g \neq id_{\mathcal{H}}$, on a $g(\tau) \in \mathcal{F}$ alors τ est un point frontière de \mathcal{F} , autrement dit on a

$$Re(\tau) = \pm \frac{1}{2} \text{ ou } |\tau| = 1.$$

En utilisant ce résultat ainsi que ceux de la section IV.E, démontrer que $G = \Gamma$.

Indication : on pourra considérer un point τ intérieur à F (c'est-à-dire $\tau \in \overset{\circ}{F}$) et son image $g(\tau)$ par $g \in \Gamma$.

••• FIN •••
