Devoir surveillé 1

Vendredi 21 septembre 2018
L'usage des calculatrices n'est pas autorisé

Vous attacherez la plus grande importance à la clarté, à la précision et à la concision de la rédaction, même si tout résultat qui n'est pas explicitement dans le cours de MPSI ou de MP doit être démontré. Si vous repèrez ce qui semble être une erreur d'énoncé, signalez le sur votre copie et poursuivez votre composition en expliquant les raisons des initiatives que vous avez été amené à prendre.

Consignes à respecter sous peine d'être pénalisé :

- Utiliser des copies doubles.
- Changer de feuille/copie à chaque exercice ou partie d'un problème.
- Faire clairement apparaître le numéro (et le cas échéant la partie) de la question traitée.
- Faire apparaître toutes les étapes **importantes** d'un calcul et la propriété/définition/caractérisation utilisée pour passer à la ligne suivante.
- Souligner les résultats intermédiaires dans une démonstration à tiroirs.

- Faire une phrase de conclusion répondant clairement à la/les question(s) posées, et encadrer le résultat.

Exercice - Questions de cours

1. Parmi les couples suivants, identifier puis relever sur votre copie ceux qui sont des groupes :
$(\mathbb{R},+)$, $(\mathbb{R}+^*,\times)$, $(\mathbb{R}_-^*,\times)$, $(\mathbb{C},\times)$, $(\mathbb{U}_n,+)$, $(\mathcal{M}_n(\mathbb{R}),+)$, $(\mathcal{M}_n(\mathbb{R}),\times)$, $(GL_n(\mathbb{R}),+)$, $GL_n(\mathbb{R}),\cdot)$.

2. Recopier et compléter les points de suspension de sorte que les applications suivantes soient des morphismes de groupes :
$det : (\dots,\dots) \to (\dots,\dots).$, $tr : (\dots,\dots) \to (\dots,\dots).$, $\exp : (\mathbb{C},\dots) \to (\dots,\dots)$

3. **En déduire** que $SL_n(\mathbb{C}) = \{M \in M_n(\mathbb{C}) | det(M) = 1\}$ est un groupe pour la loi de multiplication des matrices.

4. Montrer que si I est un idéal de $\mathbb{K}[X]$, alors il existe $P \in \mathbb{K}[X]$ tel que P engendre I.

5. Quels sont les polynômes irréductibles de $\mathbb{R}[X]$? de $\mathbb{C}[X]$?

6. Rappeler la définition de l'indicatrice d'Euler d'un entier $n \in \mathbb{N}^*$, puis démontrer que pour x et n premiers entre eux, $x^{\varphi(n)} \equiv 1[n]$.

7. Résoudre le système de congruences :

$$\begin{cases} x \equiv 2[4] \\ x \equiv 1[5] \\ x \equiv 9[17] \end{cases}$$

Exercice : Polynômes de Tchebychev

1. Soit $n \in \mathbb{N}$. Après avoir justifié que $\cos(n\theta)$ est la partie réelle de $(\cos\theta + i\sin\theta)^n$, démontrer l'existence d'un polynôme T_n tel que

$$\forall \theta \in \mathbb{R}, T_n(\cos\theta) = \cos(n\theta).$$

2. Démontrer l'unicité d'un tel polynôme.

3. On suppose $n \in \mathbb{N}^*$. Démontrer l'existence et l'unicité d'un polynôme U_n tel que

$$\forall \theta \in \mathbb{R}, (\sin\theta)U_n(\cos\theta) = \sin(n\theta).$$

4. Justifier, si ce n'est pas déjà fait, que $\forall n \in \mathbb{N}^*$, $U_n = \dfrac{1}{n}T'_n$.

5. En transformant $2\cos\theta\cos((n+1)\theta)$, déterminer une formule de récurrence permettant de calculer T_{n+2} en fonction de T_{n+1} et T_n.

6. En déduire soigneusement le terme de plus haut degré de T_n par une récurrence double, puis en utilisant l'expression de T_n trouvée dans **1.**, démontrer que $\displaystyle\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = 2^{n-1}$.

Problème

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

Soit $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs. Dans tout le problème, les lettres a, b, c, d désignent des éléments de $\mathbb{Z}$ et on note : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. Démontrer que $(\mathcal{M}_2(\mathbb{Z}), +, \times)$ est un anneau.

2. On note $GL_2(\mathbb{Z})$ l'ensemble des éléments de $\mathcal{M}_2(\mathbb{Z})$ inversibles dans $\mathcal{M}_2(\mathbb{Z})$.

a. Rappeler la définition d'un élement inversible dans un anneau.

b. 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 $\mathcal{M}_2(\mathbb{Z})$.

c. Montrer que

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

3. On pose

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) \middle| ad - bc = 1 \right\}.$$

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

b. Trouver un couple d'**entiers** $(c_0, d_0) \in \mathbb{Z}^2$ tels que $3c_0 - 5d_0 = 1$.

c. En déduire que l'ensemble des couples d'**entiers** $(c, d) \in \mathbb{Z}^2$ tels que $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ appartienne à $SL_2(\mathbb{Z})$ sont exactement les couples d'entiers (c, d) tels que $c = c_0 + 5k$ et $d = d_0 + 3k$ pour $k \in \mathbb{Z}$.

d. Déterminer l'ensemble des couples $(c, d) \in \mathbb{Z}^2$ tels que $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ appartienne à $GL_2(\mathbb{Z})$.

e. Quelle est la condition nécessaire et suffisante portant sur le couple (a, b) de $\mathbb{Z}^2$ pour qu'il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartenant à $GL_2(\mathbb{Z})$?

Partie II - Réseaux de $\mathbb{C}$

Dans cette partie, pour tout complexe z, on note $\operatorname{Re}(z)$ (resp. $\operatorname{Im}(z)$) sa partie réelle (resp. sa partie imaginaire).

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

Soient α et β deux nombres complexes tels que $\mathcal{B} = (\alpha, \beta)$ soit une base de $\mathbb{C}$ considéré comme plan vectoriel réel. On appelle réseau engendré par $\mathcal{B}$ l'ensemble $\Lambda_{\mathcal{B}} = \mathbb{Z}\alpha + \mathbb{Z}\beta = \left\{u\alpha + v\beta; (u, v) \in \mathbb{Z}^2\right\}$.

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

1. a. Montrer que $(\Lambda, +)$ est un groupe.

b. Justifier que le triplet $(\Lambda, +, \times)$ n'est pas toujours un anneau.

c. Démontrer que tout réseau Λ peut être engendré par une base $\mathcal{B} = (\alpha, \beta)$ de $\mathbb{C}$ telle que $\dfrac{\alpha}{\beta} \in \mathcal{H}$.

d. 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

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

2. a. 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 (de passage) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$.

b. Étudier la réciproque.

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

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.

4. Pour tout complexe $\tau \in \mathcal{H}$ on note Λ_τ le réseau engendré par la base $(\tau, 1)$ de $\mathbb{C}$.

Trouver la condition nécessaire et suffisante pour qu'un élément $\tau' \in \mathcal{H}$ vérifie $\Lambda_{\tau'} = \Lambda_\tau$.

Tourner la page S.V.P.

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

À toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$ on associe l'application $g : \mathcal{H} \to \mathbb{C}$ définie par :

$$\forall \tau \in \mathcal{H}, g(\tau) = \frac{a\tau + b}{c\tau + d}.$$

1. a. 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

$$\Phi : SL_2(\mathbb{Z}) \to \Gamma \text{ telle que } \Phi : A \mapsto g$$

b. 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.

c. Pour tout $A \in SL_2(\mathbb{Z})$, montrer que $\Phi(A)$ est une bijection de $\mathcal{H}$ sur $\mathcal{H}$ et que

$$[\Phi(A)]^{-1} = \Phi\left(A^{-1}\right).$$

En déduire que $(\Gamma, \circ)$ est un groupe.

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

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

ii. En utilisant les matrices S et T définies par $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, vérifier que le groupe $(\Gamma, \circ)$ n'est pas commutatif.

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

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

À quelle condition nécessaire et suffisante (portant sur ω et R) ce cercle est-il inclus dans $\mathcal{H}$?

b. On appelle s l'application de $\mathcal{H}$ vers $\mathcal{H}$ associée à la matrice $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, 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 $\mathcal{H}$.

••• FIN •••

Devoir surveillé 1

Vendredi 21 septembre 2018
Élements de correction

Exercice - Questions de cours

1. $(\mathbb{R}, +)$, $(\mathbb{R}+^*, \times)$, $(\mathcal{M}_n(\mathbb{R}), +)$, $GL_n(\mathbb{R}), \cdot)$ sont des groupes.
2. $det : (GL_n(\mathbb{K}), \cdot) \to (\mathbb{K}^*, \cdot)$, $tr : (\mathcal{M}_n(\mathbb{K}), +) \to (\mathbb{K}, +)$, $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$ sont des morphismes de groupes.
3. $SL_n(\mathbb{C}) = \{M \in M_n(\mathbb{C}) | det(M) = 1\}$ est le noyau du morphisme det, donc un sous groupe de $(GL_n(\mathbb{C}), \cdot)$, donc un groupe.
4. On montre grâce à la division euclidienne que tout idéal de $\mathbb{K}[X]$ est monogène (voir démo dans le cours).
5. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et de degré 2 dépourvus de racine réelle (à discriminant négatif).

   Ceux de $\mathbb{C}[X]$ sont les polynômes de degré 1.
6. Ll'indicatrice d'Euler d'un entier $n \in \mathbb{N}^*$ est égale au cardinal des élements inversibles ou réguliers de $\mathbb{Z}/n\mathbb{Z}$. C'est le nombre d'éléments de $[1, n-1]$ qui sont premiers avec n.

   Si x et n sont premiers entre eux, par le théorème de Lagrange, l'ordre de x divise l'ordre de $\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$. Donc $x^{\varphi(n)} \equiv 1[n]$ (1 est le neutre multiplicatif de $\mathbb{Z}/n\mathbb{Z}^*$).
7. On trouve 26 mod 340.

Exercice : Polynômes de Tchebychev

1. Soit $n \in \mathbb{N}$. $\cos(n\theta) = Re(e^{in\theta}) = Re((\cos\theta + i\sin\theta)^n)$. D'après le binôme de Newton, et après avoir pris la partie réelle et utilisé que $(\sin\theta)^{2k} = (1-\cos^2\theta)^k$,

$$\cos(n\theta) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{2k} X^{n-2k}(1-X^2)^k = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} X^{n-2k}(X^2-1)^k$$

2. Deux éventuels polynômes P_1 et P_2 convenables coïncideraient sur $[-1, 1]$. Donc leur différence $P_1 - P_2$ serait nulle sur $[-1, 1]$. Ayant une infinité de racines, $P_1 - P_2$ serait le polynôme nul, donc $P_1 = P_2$.
3. On suppose $n \in \mathbb{N}^*$. Il serait possible de procéder de même que dans la question **1.**, mais on doit lire le sujet en entier ! La question suivante suggère de dériver la relation $T_n(\cos\theta) = \cos n\theta$, ce qui donne $-\sin\theta \cdot T_n'(\cos\theta) = -n\sin(n\theta)$ et donc $U_n = \dfrac{T_n'}{n}$ convient. L'unicité se démontre comme à la question **2.** (deux tels polynômes coïncident sur $]-1, 1[$).
4. On l'a déjà fait...
5. $2\cos\theta\cos((n+1)\theta) = \cos(n\theta) + \cos((n+2)\theta)$, donc $T_{n+2} = 2XT_{n+1} - T_n$.

6. On peut calculer les premiers polynômes $T_0 = 1$, $T_1 = X$, $T_2 = 2X^2 - 1$, $T_3 = 4X^3 - 3X$... on conjecture que "le terme de plus haut degré de T_n est $2^{n-1}X^n$".

La propriété est initialisée aux rangs 0 et 1.

Soit $n \in \mathbb{N}$ tel que la propriété soit vraie aux rangs n et $n+1$. Alors $T_{n+2} = 2XT_{n+1} - T_n = 2X(2^n X^{n+1} + P_1) - P_2$ où $deg(P_1) \leq n$ et $deg(P_2) \leq n$. On en déduit que $T_{n+2} = 2^{n+1}X^{n+2} + P$ avec $deg(P) \leq n+1$.

La propriété est initialisée et héréditaire, donc vraie pour tout entier.

En utilisant l'expression de T_n trouvée dans **1.**, on trouve que le coefficient dominant de T_n est égal à $\displaystyle\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}$. On en déduit que cette somme vaut 2^{n-1}.

Problème

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

Soit $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs. Dans tout le problème, les lettres a, b, c, d désignent des éléments de $\mathbb{Z}$ et on note : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. $\mathcal{M}_2(\mathbb{Z})$ est un anneau car il contient I_2 et est stable pour $+$ et $\times$.

2. On note $GL_2(\mathbb{Z})$ l'ensemble des éléments de $\mathcal{M}_2(\mathbb{Z})$ inversibles dans $\mathcal{M}_2(\mathbb{Z})$.

a. Un élément a est inversible ssi il existe b tel que $ab = 1$.

b. On a montré en cours que dans un anneau, l'ensemble des éléments inversibles est toujours un groupe multiplicatif.

c. Si A et $A^{-1} \in \mathcal{M}_2(\mathbb{Z})$, $\det(A).\det(A^{-1}) = 1$ donc $D = \det(A)$ divise 1 et $|D| = 1$; la réciproque se voit par la formule $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \dfrac{1}{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

3. a. $SL_2(\mathbb{Z})$ est un groupe car il contient I_2 et $\left(A, B \in SL_2(\mathbb{Z}) \Rightarrow AB^{-1} \in SL_2(\mathbb{Z})\right)$.

b. $(c_0, d_0) = (2, 1)$ convient.

c. $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \Leftrightarrow \begin{cases} 3d - 5c = 1 \\ 3.2 - 5.1 = 1 \end{cases} \Leftrightarrow 3(d-2) = 5(c-1) \Leftrightarrow \exists k \in \mathbb{Z} \ / \begin{cases} c = 1 + 3k \\ d = 2 + 5k \end{cases}$

$\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) \backslash SL_2(\mathbb{Z}) \Leftrightarrow \begin{cases} 3d - 5c = -1 \\ 3.3 - 5.2 = -1 \end{cases} \Leftrightarrow 3(d-3) = 5(c-2) \Leftrightarrow \exists k \in \mathbb{Z} \ / \begin{cases} c = 2 + 3k \\ d = 3 + 5k \end{cases}$

d. Réponse au dessus...

e. $\exists (c, d) \in \mathbb{Z}^2 \ / \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) \Leftrightarrow PGCD(a, b) = 1$: c'est exactement le théorème de Bézout.

Partie II - Réseaux de $\mathbb{C}$

1. a. Λ contient 0 et est stable par soustraction : c'est donc un groupe additif.

b. Pour $\alpha = 1$ et $\beta = i\pi$, Λ n'est pas un anneau (en effet π^2 ne peut s'écrire $u + v\pi$ avec u et v entier car π n'est pas algébrique).

c. Remarquons déjà que $Im\left(\dfrac{\alpha}{\beta}\right) \neq 0$ car sinon (α, β) serait $\mathbb{R}$-liée. Si $Im\left(\dfrac{\alpha}{\beta}\right) < 0$, on change β en $-\beta$: le réseau engendré est identique : on peut donc toujours supposer $\dfrac{\alpha}{\beta} \in \mathcal{H}$.

d. $Im\left(\dfrac{az+b}{cz+d}\right) = \dfrac{1}{2i}\left(\dfrac{az+b}{cz+d} - \dfrac{a\overline{z}+b}{c\overline{z}+d}\right) = \dfrac{1}{2i}\left(\dfrac{(ad-bc)(z-\overline{z})}{|cz+d|^2}\right) = \dfrac{ad-bc}{|cz+d|^2} Im(z)$.

2. **a.** Λ est engendré par $\mathcal{B} = (\omega_1, \omega_2)$ et par $\mathcal{B}' = (\omega_1', \omega_2')$ avec $\dfrac{\omega_1}{\omega_2}$ et $\dfrac{\omega_1'}{\omega_2'} \in \mathcal{H}$. il existe donc 8 entiers a, b, c, d, e, f, g, h tels que $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ et $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$; mais $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $\begin{pmatrix} e & g \\ f & h \end{pmatrix}$ sont les matrices de passage respectives de $\mathcal{B}$ à $\mathcal{B}'$ et de $\mathcal{B}'$ à $\mathcal{B}$, donc sont inverses l'une de l'autre; $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient donc à $GL_2(\mathbb{Z})$; de plus $Im\left(\dfrac{\omega_1'}{\omega_2'}\right) = \dfrac{ad-bc}{\left|c\dfrac{\omega_1}{\omega_2}+d\right|^2} Im\left(\dfrac{\omega_1}{\omega_2}\right)$, donc $ad - bc > 0$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient à $SL_2(\mathbb{Z})$.

b. On montre la réciproque en prouvant que les réseaux engendrés par $\mathcal{B}$ et $\mathcal{B}'$ sont inclus l'un dans l'autre.

3. C'est le même problème que **I. 3. c**

4. Si $\Lambda_\tau = \Lambda_{\tau'}$, il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $\begin{cases} \tau' = a\tau + b \\ 1 = c\tau + d \end{cases}$, or τ est non réel donc $c = 0$ et $d = 1$; de $ad - bc = 1$ on tire $a = 1$: donc $\tau' = \tau + b$; réciproquement, on montre facilement que pour tout b entier $\Lambda_\tau = \Lambda_{\tau+b}$.

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

À toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$ on associe l'application $g : \mathcal{H} \to \mathbb{C}$ définie par :

$$\forall \tau \in \mathcal{H}, g(\tau) = \frac{a\tau + b}{c\tau + d}.$$

1. **a.** $Im(g(z)) = \dfrac{1}{|cz+d|^2} Im(z)$, donc $Im(z) > 0 \Rightarrow Im(g(z)) > 0$ et $g(\mathcal{H}) \subset \mathcal{H}$.

b. On montre par le calcul que $(\Phi(A) \circ \Phi(A'))(z) = \Phi(AA')(z)$. Γ est donc stable pour la loi $\circ$.

c. $\Phi(A) \circ \Phi(A^{-1}) = \Phi(I_2) = id_{\mathcal{H}}$ donc $\Phi(A)$ est bijective et $(\Phi(A))^{-1} = \Phi(A^{-1})$. Φ est donc un morphisme du groupe $SL_2(\mathbb{Z})$ dans le groupe de bijections de $\mathcal{H}$, et son image Γ est donc un groupe.

d.

$$\begin{aligned} \Phi(A) &= id_{\mathcal{H}} \Leftrightarrow \forall z \in \mathcal{H} \quad z = \frac{az+b}{cz+d} \Leftrightarrow \forall z \in \mathcal{H} \quad cz^2 + dz = az + b \Leftrightarrow \begin{cases} c = 0 \\ d = a \\ b = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} b = c = 0 \\ a = d = \pm 1 \end{cases} \Leftrightarrow A = \pm I_2 \end{aligned}$$

e. i. $\Phi(A) = \Phi(A') \Leftrightarrow \Phi(AA'^{-1}) = id_{\mathcal{H}} \Leftrightarrow AA'^{-1} = \pm I_2 \Leftrightarrow \boxed{A' = \pm A}$.

ii. $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ donc $ST \neq \pm TS$ d'où $\Phi(S) \circ \Phi(T) \neq \Phi(T) \circ \Phi(S)$ et Γ n'est pas commutatif.

2. a. L'équation demandée est une traduction de $|z-\omega|^2 = R^2$; $\mathcal{C}(\omega, R) \subset H \Leftrightarrow R < Im\omega$.

b. On a $s(z) = s^{-1}(z) = -\dfrac{1}{z}$; donc

$$z \in s(\mathcal{C}(\omega, R)) \Leftrightarrow -\frac{1}{z} \in \mathcal{C}(\omega, R) \Leftrightarrow |z|^2 + \frac{\overline{\omega z} + \omega z}{|\omega|^2 - R^2} + \frac{|\omega|^2}{\left(|\omega|^2 - R^2\right)^2} = \frac{R^2}{\left(|\omega|^2 - R^2\right)^2}$$

donc $s(\mathcal{C}(\omega, R)) = \mathcal{C}\left(-\dfrac{\overline{\omega}}{|\omega|^2 - R^2}, \dfrac{R}{|\omega|^2 - R^2}\right)$

••• FIN •••
