6

Agrégation interne 1998, épreuve 1

– I – Les groupes $GL(2,\mathbb{Z})$ et $SL(2,\mathbb{Z})$

On note respectivement : $\mathcal{M}_2(\mathbb{Z})$ [resp. $\mathcal{M}_2(\mathbb{R})$] l'anneau des matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$ [resp. dans $\mathbb{R}$], $GL(2,\mathbb{Z})$ le groupe des matrices $A \in \mathcal{M}_2(\mathbb{Z})$ telles que $\det(A) = \pm 1$ et $SL(2,\mathbb{Z})$ le groupe des matrices $A \in \mathcal{M}_2(\mathbb{Z})$ telles que $\det(A) = 1$.

1. À quelle condition nécessaire et suffisante, portant sur $\det(A)$, la matrice A est-elle inversible dans $\mathcal{M}_2(\mathbb{Z})$?
2. Déterminer l'ensemble des couples (b,c) d'entiers relatifs tels que la matrice $A = \begin{pmatrix} 3 & b \\ c & 3 \end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$.
3. Soit (a,d) dans $\mathbb{Z}^2$.
   (a) On suppose que (a,d) est distinct de $(1,1)$ et $(-1,-1)$. Déterminer l'ensemble des couples (b,c) d'entiers relatifs tels que la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$.
   (b) Étudier les cas $(a,d) = (1,1)$ et $(a,d) = (-1,-1)$.
4. Déterminer l'ensemble des couples (b,d) d'entiers relatifs tels que la matrice $A = \begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$ [resp. dans $GL(2,\mathbb{Z})$].
5. Soit (a,c) dans $\mathbb{Z}^2$. Déterminer l'ensemble des couples (b,d) d'entiers relatifs tels que la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$.

– II – Réseaux de $\mathbb{C}$

Si u, v sont deux nombres complexes indépendants sur $\mathbb{R}$, on note :

$$\mathcal{R}(u,v) = \left\{ au + bv \mid (a,b) \in \mathbb{Z}^2 \right\}$$

le sous-groupe additif de $\mathbb{C}$ engendré par u et v. On dit que $\mathcal{R}(u,v)$ est le réseau de base (u,v).

1. Soient $\mathcal{R} = \mathcal{R}(u,v)$ un réseau de base (u,v) et $u' = au + cv$, $v' = bu + dv$ deux nombres complexes indépendants sur $\mathbb{R}$, où a, b, c, d sont des réels.
   (a) À quelle condition nécessaire et suffisante, portant sur les réels a, b, c, d, a-t-on $\mathcal{R}(u',v') \subset \mathcal{R}$?

(b) À quelle condition nécessaire et suffisante, portant sur les réels a, b, c, d, a-t-on $\mathcal{R}(u', v') = \mathcal{R}$? On dit alors que (u', v') est une base de $\mathcal{R}$.

(c) On suppose que $u' = 3u + 2v$. Déterminer les vecteurs v' tels que (u', v') soit une base de $\mathcal{R}$.

On dit qu'un nombre complexe $u' \in \mathcal{R}$ est basique pour $\mathcal{R}$ s'il existe $v' \in \mathbb{C}$ tel que $\mathcal{R} = \mathcal{R}(u', v')$.

(d) À quelle condition nécessaire et suffisante, portant sur les entiers a, c, le nombre complexe $u' = au + cv$ est basique pour $\mathcal{R}$?

(e) Soit Δ une $\mathbb{R}$-droite vectorielle de $\mathbb{C}$ telle que $\Delta \cap \mathcal{R}$ ne soit pas réduit à $\{0\}$.

i. Montrer que Δ contient vecteur basique δ.

ii. Comparer $\Delta \cap \mathcal{R}$ et $\delta\mathbb{Z}$.

(f) Deux éléments basiques non colinéaires forment-ils toujours une base de $\mathcal{R}$?

On dit qu'un sous-ensemble X de $\mathbb{C}$ est discret si son intersection avec toute partie bornée de $\mathbb{C}$ est finie.

2. Soit $\mathcal{R} = \mathcal{R}(u, v)$ un réseau de base (u, v). On note θ un argument de $\dfrac{v}{u}$ et on suppose que θ est dans $]0, \pi[$.

(a) Montrer que pour tout $(a, b) \in \mathbb{Z}^2$, on a :

$$|au + bv|^2 = (a|u| + b|v|\cos(\theta))^2 + b^2|v|^2\sin^2(\theta).$$

(b) En déduire que $\mathcal{R}$ est discret.

3. Soit $\mathcal{R}$ un sous-groupe additif de $\mathbb{C}$ discret non inclus dans une $\mathbb{R}$-droite vectorielle de $\mathbb{C}$. On choisit dans $\mathcal{R} \setminus \{0\}$ un élément u de module minimum et dans $\mathcal{R} \setminus \mathbb{R}u$ (l'ensemble des éléments de $\mathcal{R}$ non $\mathbb{R}$-colinéaires à u) un élément v de module minimum. On note $\mathcal{R}' = \mathcal{R}(u, v)$.

(a) Montrer que pour tout nombre complexe z, il existe z' dans $\mathcal{R}'$ et x, y dans $\left[-\dfrac{1}{2}, \dfrac{1}{2}\right]$ tels que $z - z' = xu + yv$.

(b) En déduire, avec les notations précédentes, que $|z - z'| < |v|$.

(c) Montrer que $\mathcal{R} = \mathcal{R}'$, c'est-à-dire que $\mathcal{R}$ est un réseau.

On a donc ainsi montré qu'un sous-groupe additif de $\mathbb{C}$ non inclus dans une $\mathbb{R}$-droite vectorielle de $\mathbb{C}$ est discret si, et seulement si, c'est un réseau.

– III – Similitudes directes de centre 0 laissant stable un réseau

Si $\mathcal{R} = \mathcal{R}(u, v)$ est un réseau, on note :

$$Z(\mathcal{R}) = \{\alpha \in \mathbb{C} \mid \alpha\mathcal{R} \subset \mathcal{R}\}.$$

1. Quel lien a-t-on entre $Z(\mathcal{R})$ et l'ensemble des similitudes directes de centre 0 laissant $\mathcal{R}$ stable ?

2. Quelles sont les homothéties de centre 0 qui laissent stable $\mathcal{R}$? Comment cela se traduit-il pour $Z(\mathcal{R}) \cap \mathbb{R}$?

3. Montrer que $Z(\mathcal{R})$ est un anneau.
4.
   (a) Montrer qu'il existe $w \in \mathbb{C} \setminus \mathbb{R}$ et une similitude directe de centre 0 qui transforme $\mathcal{R}$ en $\mathcal{R}(1, w)$.
   (b) Comparer $Z(\mathcal{R})$ et $Z(\mathcal{R}(1, w))$.
   (c) Quelle relation a-t-on entre $Z(\mathcal{R}(1, w))$ et $\mathcal{R}(1, w)$?
5. Déterminer $Z(\mathcal{R}(1, w))$ pour $w = i\sqrt{2}$ et $w = i\sqrt[3]{2}$.
   On suppose, pour la suite de cette partie, que $\mathcal{R} = \mathcal{R}(1, w)$ avec $w \in \mathbb{C} \setminus \mathbb{R}$.
6. Montrer l'équivalence entre les deux assertions :
   (i) $Z(\mathcal{R})$ n'est pas réduit à $\mathbb{Z}$;
   (ii) w est racine non réelle d'un polynôme de degré 2, $P(X) = \alpha X^2 + \beta X + \gamma$ à coefficients entiers.
7. Comparer $Z(\mathcal{R})$ et $\mathcal{R}$ lorsque la propriété (ii) est vérifiée avec $\alpha = 1$.
8. On suppose que w est racine non réelle d'un polynôme non nul $P(X) = \alpha X^2 + \beta X + \gamma$ à coefficients entiers relatifs.
   (a) Montrer que $Z(\mathcal{R})$ est un réseau et qu'il admet une base de la forme $(1, \tau)$ avec $\tau \in \mathbb{C} \setminus \mathbb{R}$.
   (b) Montrer que τ est racine d'un polynôme $P(X) = X^2 + pX + q$, où p, q sont des entiers relatifs avec $q > 0$.
   (c) Montrer qu'on peut choisir τ de sorte que $p = 0$ ou $p = 1$.

– IV – Rotations de centre 0 laissant stable un réseau

Soit τ la racine de partie imaginaire positive d'un polynôme $P(X) = X^2 + pX + q$, où $p \in \{0, 1\}$ et q est un entier naturel non nul.
L'anneau $\mathcal{R}(1, \tau) = \{a + b\tau \mid (a, b) \in \mathbb{Z}^2\}$ est noté $\mathbb{Z}[\tau]$.

1. On suppose que $p = 0$.
   (a) Faire une figure représentant $\mathbb{Z}[\tau]$ dans les cas $\tau = i$ et $\tau \neq i$.
   (b) Quels sont les éléments non réels de $\mathbb{Z}[\tau]$ de module minimum ?
   (c) Déterminer les rotations de centre 0 qui laissent $\mathbb{Z}[\tau]$ stable.
2. On suppose que $p = 1$.
   (a) Faire une figure représentant $\mathbb{Z}[\tau]$ dans les cas $q = 1$ et $q = 2$.
   (b) Quels sont les éléments non réels de $\mathbb{Z}[\tau]$ de module minimum ?
   (c) Déterminer les rotations de centre 0 qui laissent $\mathbb{Z}[\tau]$ stable.
3. Montrer que l'anneau $\mathbb{Z}[\tau]$ est principal pour $\tau = i$ et pour $\tau = j$ (racine cubique de 1 distincte de 1).