(Agrégation interne 1998 -première épreuve de mathématiques)

L'objet du problème est l'étude des *réseaux* de $\mathbb{C}$ (sous-groupes additifs $\mathcal{R} \subset \mathbb{C}$, discrets, contenant une base de $\mathbb{C}$ sur $\mathbb{R}$) et de ceux d'entre eux qui sont de plus des sous-anneaux.

La qualité de la rédaction, plus que la quantité, tant sur la forme que sur le fond, sera un élément essentiel dans l'appréciation des copies.

I. Etude du groupe $GL(2,\mathbb{Z})$

On note $M_2(\mathbb{Z})$ l'ensemble des matrices carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers. C'est un sous-anneau de l'anneau $M_2(\mathbb{R})$ des matrices carrées d'ordre 2 à coefficients réels.

1. a) Déterminer les inverses dans $M_2(\mathbb{R})$ des matrices (inversibles) : $\begin{pmatrix}3 & 4\\ 2 & 3\end{pmatrix}$, $\begin{pmatrix}3 & 5\\ 2 & 3\end{pmatrix}$, $\begin{pmatrix}4 & 5\\ 2 & 3\end{pmatrix}$.

   b) Soit $A \in M_2(\mathbb{Z})$. A quelle condition nécessaire et suffisante portant sur $\det(A)$ la matrice A admet-elle une inverse A^{-1} dans $M_2(\mathbb{R})$? dans $M_2(\mathbb{Z})$?

   On note $GL(2,\mathbb{Z})$ (*resp.* $SL(2,\mathbb{Z})$) le groupe des matrices $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ de $M_2(\mathbb{Z})$ telles que $ad-bc = \pm 1$ (*resp.* $ad-bc=1$).

2. a) Déterminer l'ensemble des couples $(b,c) \in \mathbb{Z}^2$ tels que la matrice $\begin{pmatrix}3 & b\\ c & 3\end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$.

   b) On suppose (a,d) donné dans $\mathbb{Z}^2$ distinct des couples $(1,1)$ et $(-1,-1)$. L'ensemble des couples $(b,c) \in \mathbb{Z}^2$ tels que $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$ est-il non vide ? est-il infini ?

   c) Même question qu'en b) lorsque (a,d) est l'un des couples $(1,1)$, $(-1,-1)$.

3. a) Quel est l'ensemble des couples $(b,d) \in \mathbb{Z}^2$ tels que la matrice $\begin{pmatrix}3 & b\\ 2 & d\end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$? Dans $GL(2,\mathbb{Z})$?

   b) On suppose (a,c) donné dans $\mathbb{Z}^2$. A quelle condition l'ensemble des couples $(b,d) \in \mathbb{Z}^2$ tels que $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$ est-il non vide ? Décrire dans ce cas l'ensemble des couples (b,d) tels que $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL(2,\mathbb{Z})$.

II. Réseaux de $\mathbb{C}$

On rappelle que le corps $\mathbb{C}$ des nombres complexes est un plan vectoriel sur le corps $\mathbb{R}$ des nombres réels. Par *droite vectorielle*, on entendra sous $\mathbb{R}$-espace vectoriel de dimension 1 de $\mathbb{C}$. Pour $z \in \mathbb{C}^*$, on notera $\mathbb{R}z$ (*resp.* $\mathbb{Z}z$) la droite vectorielle (*resp.* le sous-groupe additif) des λz où λ décrit $\mathbb{R}$ (*resp.* λ décrit $\mathbb{Z}$).

Soient u, v deux nombres complexes indépendants sur $\mathbb{R}$ (c'est-à-dire non nuls de rapport non réel). On appelle *réseau de base* (u,v) le sous-groupe additif $\mathcal{R}(u,v)$ de $\mathbb{C}$ engendré par u et v :

$$\mathcal{R}(u,v) = \{z \in \mathbb{C};\ \exists (m,n) \in \mathbb{Z}^2;\ z = mu + nv\}.$$

1. Soient u, v deux nombres complexes indépendants sur $\mathbb{R}$. Notons $\mathcal{R} = \mathcal{R}(u,v)$ le réseau de base (u,v). Soient a, b, c, d des nombres réels. Posons $u' = au + cv,\ v' = bu + dv$.

a) A quelle condition nécessaire et suffisante portant sur les nombres réels a, b, c, d les nombres complexes u', v' sont-ils indépendants sur $\mathbb{R}$?

On supposera cette condition remplie dans la suite de la question II.1.

b) A quelle condition nécessaire et suffisante portant sur les nombres réels a, b, c, d le réseau $\mathcal{R}(u', v')$ est-il inclus dans le réseau $\mathcal{R}$?

c) A quelle condition nécessaire et suffisante portant sur les nombres réels a, b, c, d a-t-on l'égalité $\mathcal{R}(u', v') = \mathcal{R}$?

On dit alors que (u', v') est une base du réseau $\mathcal{R}(u, v)$.

2. On donne le réseau $\mathcal{R} = \mathcal{R}(u, v)$ de base (u, v). On dit qu'un élément $u' \in \mathcal{R}$ est *basique* (pour $\mathcal{R}$) s'il existe $v' \in \mathcal{R}$ tel que (u', v') soit une base de $\mathcal{R}$.

a) Posons $u' = 3u+2v$. Déterminer l'ensemble des couples (b, d) de $\mathbb{Z}^2$ tels que $(3u+2v, bu+dv)$ soit une base du réseau $\mathcal{R}$.

b) A quelle condition nécessaire et suffisante portant sur les entiers a, c le nombre $au + cv$ est-il basique pour $\mathcal{R}$?

c) Soit Δ une $\mathbb{R}$-droite vectorielle de $\mathbb{C}$ telle que $\Delta \cap \mathcal{R}$ ne soit pas réduit à $\{0\}$. Démontrer que Δ contient un vecteur basique δ. Comparer $\Delta \cap \mathcal{R}$ et $\mathbb{Z}\delta$.

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

3. On dit qu'un sous-groupe additif Γ de $\mathbb{C}$ est *discret* si toute partie bornée de Γ est finie. L'objet de cette question est de démontrer que tout réseau est un sous-groupe discret.

Soit $\mathcal{R}(u, v)$ le réseau de base (u, v) ; on suppose qu'un argument θ de $\dfrac{v}{u}$ est dans $]0, \pi[$.

a) Démontrer que, pour a, b entiers, $|au + bv|^2 = (a|u| + b|v|\cos\theta)^2 + b^2|v|^2\sin^2\theta \geqslant b^2|v|^2\sin^2\theta$.

b) Démontrer que $\mathcal{R}(u, v)$ est un sous-groupe discret de $\mathbb{C}$.

4. L'objet de cette question est d'établir une réciproque : si Γ est un sous-groupe additif discret de $\mathbb{C}$ qui n'est pas contenu dans une droite vectorielle, alors Γ est un réseau ; autrement dit, il existe (u, v) tels que $\Gamma = \mathcal{R}(u, v)$.
Soit Γ un tel sous-groupe additif.

a) Démontrer qu'il existe un élément u de module minimum parmi les éléments non nuls de Γ, et un élément v de module minimum parmi les éléments de Γ non colinéaires à u. Démontrer que $\mathcal{R}(u, v)$ est contenu dans Γ.

On fixe u et v satisfaisant ces conditions et on pose $\mathcal{R} = \mathcal{R}(u, v)$.

b) Démontrer que pour tout $z \in \mathbb{C}$, il existe $z' \in \mathcal{R}$ et des nombres réels x, y tels que $|x| \leqslant \dfrac{1}{2}$, $|y| \leqslant \dfrac{1}{2}$ et $z - z' = xu + yv$.

c) En déduire que $|z - z'| \leqslant |v|$.

d) Rappeler sans démonstration à quelle condition deux nombres complexes z_1, z_2 vérifient l'inégalité stricte $|z_1 + z_2| < |z_1| + |z_2|$.

e) Établir l'inégalité stricte $|z - z'| < |v|$ (*on pourra distinguer plusieurs cas selon que x et y sont nuls ou non*).

f) Conclure que $\Gamma = \mathcal{R}$.

III. Similitudes de centre 0 laissant stable un réseau

On rappelle que $\mathbb{C}$ est doté d'une structure de plan euclidien orienté.

1. Soit $\mathcal{R} = \mathcal{R}(u, v)$ un réseau. On pose $Z(\mathcal{R}) = \{z \in \mathbb{C};\ z\mathcal{R} \subset \mathcal{R}\}$

a) Quel lien existe-il entre le sous-ensemble $Z(\mathcal{R})$ de $\mathbb{C}$ et l'ensemble des similitudes directes de centre 0 laissant $\mathcal{R}$ stable ?

b) Quel est l'ensemble des homothéties de centre 0 laissant $\mathcal{R}$ stable ? Comment cela se traduit-il pour $Z(\mathcal{R}) \cap \mathbb{R}$?

c) Démontrer que $Z(\mathcal{R})$ est un sous-anneau de $\mathbb{C}$.

d) Démontrer qu'il existe $w \in \mathbb{C} \setminus \mathbb{R}$ et une similitude directe de centre 0 transformant $\mathcal{R}$ en $\mathcal{R}(1, w)$. Comparer les sous-anneaux $Z(\mathcal{R})$ et $Z(\mathcal{R}(1, w))$ de $\mathbb{C}$.

e) Démonter que $Z(\mathcal{R}(1, w)) \subset \mathcal{R}(1, w)$?

f) Indiquer sans démonstration quel est l'ensemble $Z(\mathcal{R}(1, w))$ dans les deux cas suivants :
- $w = (\sqrt{2})i$,
- $w = (\sqrt[3]{2})i$.

Désormais, $\mathcal{R}$ est le réseau de base $(1, w)$ où w est un nombre non réel donné. Les questions proposées dans la suite de cette parties sont :
- Existe-t-il des similitudes directes de centre 0, autres que des homothéties, laissant $\mathcal{R}$ stable ?
- Si oui, que peut-on dire de l'anneau $Z(\mathcal{R})$ des $z \in \mathbb{C}$ tels que $z\mathcal{R} \subset \mathcal{R}$?

2. On suppose dans cette question que $Z(\mathcal{R})$ n'est pas réduit à $\mathbb{Z}$. Démontrer que w est racine d'un polynôme du deuxième degré à coefficients dans $\mathbb{Z}$ (*utiliser III.1.e*).

3. On suppose inversement que w est racine non réelle d'un polynôme non nul $P(X) = \alpha X^2 + \beta X + \gamma$ à coefficients α, β, γ dans $\mathbb{Z}$.

a) Démontrer que $Z(\mathcal{R})$ n'est pas contenu dans $\mathbb{R}$.

b) Que peut-on dire des ensembles $Z(\mathcal{R})$ et $\mathcal{R}$ lorsque $\alpha = 1$?

c) Démontrer que $Z(\mathcal{R})$ est un réseau et qu'il admet une base de la forme $(1, \tau)$.

d) Démontrer que τ est racine d'un polynôme $X^2 + pX + q$ où p et q sont des éléments de $\mathbb{Z}$ (*utiliser III.1.c*). Quels sont les signes de $p^2 - 4q$ et de q ?

e) Démontrer que l'on peut choisir τ de sorte que $p = 0$ ou $p = 1$ (*on pourra considérer* $\tau' = \tau + k$ *où* $k \in \mathbb{Z}$ *est un entier convenable*).

L'anneau $Z(\mathcal{R}) = \mathcal{R}(1, \tau)$ sera noté $\mathbb{Z}[\tau]$.

Conclusion.

Si l'ensemble des similitudes directes de centre 0 laissant le réseau $\mathcal{R}$ stable n'est pas réduit à des homothéties, l'anneau $Z(\mathcal{R}) = \{z \in \mathbb{C};\ z\mathcal{R} \subset \mathcal{R}\}$ est un réseau de $\mathbb{C}$: c'est l'ensemble $\mathbb{Z}[\tau]$ des $z = a + b\tau$ où a, b sont dans $\mathbb{Z}$ et où τ est racine d'un polynôme d'une des deux formes suivantes : $X^2 + q$, $X^2 + X + q$ où, dans les deux cas, q est un entier positif.

IV. Rotations de centre 0 laissant stable un réseau

Soit τ la racine de partie imaginaire positive d'un polynôme de la forme $X^2 + pX + q$ où $p \in \{0, 1\}$ et $q > 0$ entier. On cherche s'il existe des rotations de centre 0 laissant $\mathbb{Z}[\tau]$ stable.

1. Parmi les éléments non réels de $\mathbb{Z}[\tau]$, quels sont ceux de module minimum

a) lorsque $p = 0$, donc $\tau = i\sqrt{q}$?

b) lorsque $p = 1$, donc $\tau = \dfrac{1}{2}(-1 + i\sqrt{4q - 1})$?

2. Quelle valeur doit avoir q pour que l'ensemble des rotations de centre 0 conservant $\mathbb{Z}[\tau]$ ne soit pas réduit à l'identité et à la symétrie centrale de centre 0 ? Quel est alors cet ensemble de rotations ?

3. On suppose que $\tau = i$ ou $\tau = j$.

a) Soit I un idéal non nul de l'anneau $\mathbb{Z}[\tau]$. Démontrer qu'il existe un élément $u \in I$ non nul de module minimum.

b) Posons $v = \tau u$. Démontrer que $I = \mathcal{R}(u, v)$ (*utiliser II.4*).

c) En déduire que l'anneau $\mathbb{Z}[\tau]$ est principal.

4. *Facultatif.* On suppose que $\mathrm{Im}(\tau) < \sqrt{3}$. Démontrer que $\mathbb{Z}[\tau]$ est principal.