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.

1 Étude du groupe $GL(2,\mathbb{Z})$

Soit l'ensemble $\mathcal{M}_2(\mathbb{Z})$ des matrices carrées d'ordre 2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients dans l'anneau $\mathbb{Z}$ des entiers.

1.1 Considérons $\mathcal{M}_2(\mathbb{Z})$ comme inclus dans l'ensemble $\mathcal{M}_2(\mathbb{R})$ des matrices carrées d'ordre 2 à coefficients réels.

a) Déterminer les inverses des matrices inversibles suivantes dans $\mathcal{M}_2(\mathbb{R})$:

$$\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$$

b) Soit $A \in \mathcal{M}_2(\mathbb{Z})$.
À quelle condition nécessaire et suffisante portant sur $\det(A)$ la matrice A admet-elle une inverse A^{-1}
- dans $\mathcal{M}_2(\mathbb{R})$?
- dans $\mathcal{M}_2(\mathbb{Z})$?

On note $GL(2,\mathbb{Z})$ (resp. $SL(2,\mathbb{Z})$) le groupe des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathcal{M}_2(\mathbb{Z})$ telles que $ad-bc = \pm 1$ (resp. $ad-bc = 1$).

1.2 a) Déterminer l'ensemble des couples $(b,c) \in \mathbb{Z} \times \mathbb{Z}$ 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 $\mathbb{Z} \times \mathbb{Z}$ distinct des couples $(1,1)$ et $(-1,-1)$. L'ensemble des couples $(b,c) \in \mathbb{Z} \times \mathbb{Z}$ 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 $(1,1)$, $(-1,-1)$.

1.3 a) Déterminer l'ensemble des couples $(b,d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice $\begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix}$ soit dans $SL(2,\mathbb{Z})$.
Même question en remplaçant $SL(2,\mathbb{Z})$ par $GL(2,\mathbb{Z})$.

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

2 Réseaux de $\mathbb{C}$

On rappelle que le corps $\mathbb{C}$ des nombres complexes est un plan vectoriel sur le corps $\mathbb{R}$ des 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 $\mathbb{Z}$).
Étant donné deux nombres complexes u, v indépendants sur $\mathbb{R}$ (c'est-à-dire non nuls de rapport non réel) on considère le sous-groupe additif $\mathcal{R}(u,v)$ de $\mathbb{C}$ engendré par u et v :

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

On dit que $\mathcal{R}(u,v)$ est *le réseau de base* (u,v).

2.1 On donne le réseau $\mathcal{R} = \mathcal{R}(u,v)$ de base (u,v). On considère des réels a, b, c, d et les nombres complexes $u' = au + cv$, $v' = bu + dv$.

a) À quelle condition nécessaire et suffisante portant sur les réels a, b, c, d les complexes u', v' sont-ils indépendants sur $\mathbb{R}$?
On supposera cette condition remplie dans la suite de la question 2.1.

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

c) À quelle condition nécessaire et suffisante portant sur les 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 $\mathcal{R}(u,v)$.

2.2 On se donne le réseau $\mathcal{R} = \mathcal{R}(u,v)$ de base (u,v).

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

Un complexe $u' \in \mathcal{R}$ est dit *basique* pour $\mathcal{R}$ s'il existe v' tel que $\mathcal{R} = \mathcal{R}(u',v')$.

b) À quelle condition nécessaire et suffisante portant sur les réels a, c le nombre $au+cv$ est-il basique pour $\mathcal{R}$? (utiliser le théorème de Bézout).

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

2.3 On dit qu'un sous-groupe additif de $\mathbb{C}$ est *discret* si toute partie bornée est finie. L'objet de cette question est de montrer que *tout réseau est un 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) Montrer 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) Déduire de a) et d'une autre inégalité analogue que $\mathcal{R}(u,v)$ est un sous-groupe discret de $\mathbb{C}$.

2.4 L'objet de cette question est d'établir une réciproque : *Si $\mathcal{R}$ est un sous-groupe additif discret de $\mathbb{C}$ dont les éléments non nuls n'ont pas tous même argument modulo π, alors $\mathcal{R}$ est un réseau* ; autrement dit, il eixste (u,v) tels que $\mathcal{R} = \mathcal{R}(u,v)$.

Soit $\mathcal{R}$ un tel sous-groupe additif, u un élément de module minimum parmi les éléments non nuls de $\mathcal{R}$, v un élément de module minimum parmi les éléments de $\mathcal{R}$ non colinéaires à u, $\mathcal{R}'$ le réseau $\mathcal{R}(u,v)$ contenu dans $\mathcal{R}$.

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

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

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

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

e) Conclure que $\mathcal{R} = \mathcal{R}'$.

2.1 Similitudes de centre 0 laissant stable un réseau

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

2.1 Soit $\mathcal{R} = \mathcal{R}(u,v)$ un réseau.

a) Indiquer sans démonstration quel lien existe entre le sous-ensemble de $\mathbb{C}$
$$Z(\mathcal{R}(u,v)) = \{z \in \mathbb{C} \mid z\mathcal{R}(u,v) \subset \mathcal{R}(u,v)\}$$
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 $Z(\mathcal{R}(u,v)) \cap \mathbb{R}$?

c) De quelle structure algébrique est doté le sous-ensemble $Z(\mathcal{R}(u,v))$ de $\mathbb{C}$?

d) Montrer que pour tout réseau $\mathcal{R}(u,v)$, il existe $w \notin \mathbb{R}$ et une similitude directe de centre 0 transformant $\mathcal{R}(u,v)$ en $\mathcal{R}(1,w)$.

e) Comparer les sous-anneaux de $\mathbb{C}$
$$Z(\mathcal{R}(u,v)) \text{ et } Z(\mathcal{R}(1,w)).$$
Quelle relation d'inclusion a-t-on entre $Z(\mathcal{R}(1,w))$ et $\mathcal{R}(1,w)$? (remarquer que $1 \in \mathcal{R}(1,w)$).

f) Indiquer sans démonstration quel est l'ensemble $Z(\mathcal{R}(1,w))$ dans les deux cas suivants :

- f1) $w = (\sqrt{2})i$,
- f2) $w = \left(\sqrt[3]{2}\right) i$.

Désormais, $\mathcal{R}$ est le réseau de base $(1,w)$ où w est un nombre réel donné.

Les questions posées dans la suite de cette partie 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* $z\mathcal{R} \subset \mathcal{R}$ *?*

2.2 On suppose dans cette question que $Z(\mathcal{R})$ n'est pas réduit à $\mathbb{Z}$.

Montrer que w est racine d'un polynôme du deuxième degré à coefficients dans $\mathbb{Z}$. (On pourra utiliser l'existence d'un élément non réel dans $Z(\mathcal{R})$ et utiliser 3.1 e)

2.3 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) Montrer 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) Montrer que $Z(\mathcal{R})$ est un réseau et qu'il admet une base de la forme $(1,\tau)$ (on pourra utiliser 2.2 c pour montrer que 1 est basique).

d) Montrer que τ est racine d'un polynôme $X^2 + pX + q$ où p et q sont des entiers de $\mathbb{Z}$ (utiliser 3.1 c). Quels sont les signes de $p^2 - 4q$ et de q ?

e) Montrer qu'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*

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

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.

3 Rotations de centre 0 laissant stable un réseau

Soit τ la racine de partie imaginaire positive d'une 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.

3.1 On suppose $p = 0$, donc $\tau = i\sqrt{q}$. Dans cette question, on demande les résultats sans démonstration.

a) Faire une figure représentant le réseau $\mathbb{Z}[\tau]$ dans les cas $\tau \neq i$ et $\tau = i$.

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

c) Quelles sont les rotations de centre 0 qui laissent $\mathbb{Z}[\tau]$ stable ?

3.2 On suppose $p = 1$, donc $\tau = \dfrac{1}{2}\left(-1 + i\sqrt{4q-1}\right)$.

a) Faire une figure représentant le réseau $\mathbb{Z}[\tau]$ lorsque $q = 1$ et $q = 2$.

b) Parmi les éléments $z = a + b\tau$ non réels de $\mathbb{Z}[\tau]$, quels sont ceux de module minimum ?

c) 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 ?

3.3 Déduire de tout ce qui précède que si τ est i (racine carrée de -1) ou j (racine cubique de 1 distincte de 1), l'anneau $\mathbb{Z}[\tau]$ est principal (en considérant un idéal I et un élément u de module minimum parmi les éléments non nuls de I, considérer le réseau $I' = \mathcal{R}(u, \tau u)$ et utiliser 2.4).