PROBLEME

Réseaux de $\mathbb{C}$ et similitudes.

On considère le corps des complexes $\mathbb{C}$ comme un espace vectoriel de dimension 2 sur $\mathbb{R}$. Une droite vectorielle de $\mathbb{C}$ sera donc, par définition, un sous-$\mathbb{R}$-espace vectoriel de dimension 1 de $\mathbb{C}$. Si $z \in \mathbb{C}^*$, on notera $\mathbb{R}z$ la droite vectorielle engendrée par z, et $\mathbb{Z}z$ le sous-groupe additif de $\mathbb{C}$ engendré par z. On a, bien entendu

$$\mathbb{R}z = \{\lambda z \,/\, \lambda \in \mathbb{R}\} \text{ et } \mathbb{Z}z = \{\lambda z \,/\, \lambda \in \mathbb{Z}\}.$$

Si u et v sont deux nombres complexes indépendants sur $\mathbb{R}$, le sous-groupe additif de $\mathbb{C}$ engendré par u et v est appelé réseau de base (u, v), et noté $\mathcal{R}(u, v)$. On a donc

$$\mathcal{R}(u, v) = \mathbb{Z}u + \mathbb{Z}v = \{nu + pv \,/\, n \in \mathbb{Z} \text{ et } p \in \mathbb{Z}\}.$$

Le but du problème est l'étude de certaines propriétés des réseaux de $\mathbb{C}$, et celle des similitudes de centre 0 laissant stable un réseau donné.

Partie I : Généralités

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

a) Trouver une condition nécessaire et suffisante portant sur les réels a, b, c, d pour que les vecteurs u' et v' soient linéairement indépendants. On supposera que cette condition est remplie dans toute la suite de la question 1.

b) Trouver une condition nécessaire et suffisante portant sur les réels a, b, c, d pour que le réseau $\mathcal{R}(u', v')$ soit inclus dans le réseau $\mathcal{R}$.

c) A quelle condition nécessaire et suffisante portant sur les réels a, b, c, d a-t-on l'égalité $\mathcal{R}(u', v') = \mathcal{R}$? Dans ce cas, on dit que (u', v') est une base du réseau $\mathcal{R}$.

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

a) Exprimer à quelle condition nécessaire et suffisante portant sur les entiers a et c le nombre $u' = au + cv$ est basique pour $\mathcal{R}$.

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

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

3) On dit qu'un sous-ensemble du plan $\mathbb{C}$ est discret si son intersection avec une partie bornée quelconque ne contient qu'un nombre fini de points. Le but de cette question est de montrer

[0] [unoc0003] v1.04 http://perso.wanadoo.fr/megamaths

qu'un sous-groupe additif de $\mathbb{C}$ non inclus dans une droite est discret si et seulement si c'est un réseau.

a) Soit $\mathcal{R}(u,v)$ un réseau de base (u,v). On note θ l'argument du quotient $\frac{v}{u}$ et l'on supposera que $\theta \in]0,\pi[$ sans nuire à la généralité du problème. Montrer que l'on a

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

pour tous les entiers a et b. En déduire que $\mathcal{R}(u,v)$ est discret.

b) Réciproquement, on considère un sous-groupe additif discret et non inclus dans une droite $\mathcal{R}$ de $\mathbb{C}$ et l'on choisit un élément u de $\mathcal{R}$ de module minimum parmi les éléments non nuls de $\mathcal{R}$, et un élément v de $\mathcal{R}$ de module minimum parmi les éléments de $\mathcal{R}$ non colinéaires à u. Les réels $|u|$ et $|v|$ sont appelés premier et second minimum du sous-groupe additif $\mathcal{R}$. Soit $\mathcal{R}'$ le réseau $\mathcal{R}(u,v)$ contenu dans $\mathcal{R}$.
Démontrer l'assertion suivante

$$\forall z \in \mathbb{C} \quad \exists z' \in \mathcal{R}' \quad \exists x,y \in \mathbb{R} \quad z - z' = xu + yv,\ |x| \leq \frac{1}{2} \text{ et } |y| \leq \frac{1}{2}.$$

En déduire l'inégalité $|z-z'| \leq |v|$. En envisageant plusieurs cas suivant la nullité de x et de y, démontrer que l'on a toujours $|z-z'| < |v|$, puis que cela implique l'égalité $\mathcal{R} = \mathcal{R}'$.

Partie II : Similitudes directes de centre 0 laissant un réseau stable

4) Soit $\mathcal{R} = \mathcal{R}(u,v)$ un réseau. On définit l'ensemble

$$Z(\mathcal{R}(u,v)) = \{z \in \mathbb{C} \,/\, z\mathcal{R}(u,v) \subset \mathcal{R}(u,v)\}.$$

a) Quel lien y-a-t-il entre $Z(\mathcal{R}(u,v))$ et l'ensemble des similitudes directes de centre 0 laissant $\mathcal{R}$ stable ? Quelles sont les homothéties de centre O qui laissent stable $\mathcal{R}$? Que peut-on en déduire pour $Z(\mathcal{R}(u,v)) \cap \mathbb{R}$?

b) Montrer que $Z(\mathcal{R}(u,v))$ est un anneau.

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

d) Démontrer l'égalité $Z(\mathcal{R}(u,v)) = Z(\mathcal{R}(1,w))$. Quelle relation d'inclusion a-t-on entre $Z(\mathcal{R}(1,w))$ et $\mathcal{R}(1,w)$?

5) Exhiber l'ensemble $Z(\mathcal{R}(1,w))$ dans les deux cas suivants :
a) lorsque $w = i\sqrt{2}$,
b) lorsque $w = i\sqrt[3]{2}$.

6) Montrer l'équivalence entre les affirmations suivantes :
i) L'ensemble $Z(\mathcal{R}(1,w))$ n'est pas réduit à $\mathbb{Z}$.
ii) w est une racine non réelle d'un polynôme du second degré $P(X) = \alpha X^2 + \beta X + \gamma$ non nul et à coefficients entiers.

7) Comparer les ensembles $Z(\mathcal{R}(1,w))$ et $\mathcal{R}(1,w)$ lorsque la propriété ii) est vérifiée avec $\alpha = 1$.

8) Dans cette question, $\mathcal{R}(u,v)$ désigne un un réseau tel que l'ensemble des similitudes directes de centre 0 et laissant stable $\mathcal{R}(u,v)$ n'est pas réduit à des homothéties. On rappelle que $Z(\mathcal{R}(u,v)) = Z(\mathcal{R}(1,w))$ où w est défini à la question 4).

a) Montrer que $Z(\mathcal{R}(1,w))$ est un réseau et qu'il admet une base de la forme $(1,\tau)$. On pourra utiliser la question 2.b) pour démontrer que 1 est un vecteur basique de $Z(\mathcal{R}(1,w))$.

b) En utilisant la question 4.b), montrer que τ est racine d'un polynôme X^2+pX+q où p et q sont des entiers relatifs avec $q>0$.

c) Montrer que l'on peut choisir τ de sorte que $p=0$ ou $p=1$.

Partie III : Rotations de centre 0 laissant $\mathcal{R}(1,\tau)$ stable

Soit τ la racine de partie imaginaire positive d'un polynôme X^2+pX+q où $p\in\{0,1\}$ et $q\in\mathbb{N}^*$. On note $\mathbb{Z}[\tau]=\mathcal{R}(1,\tau)$ l'anneau dont les éléments sont les complexes $a+b\tau$ avec $(a,b)\in\mathbb{Z}^2$.

9) On suppose $p=0$ et donc $\tau=i\sqrt{q}$.

a) Faire une figure représentant le réseau 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 laissant $\mathbb{Z}[\tau]$ stable.

10) On suppose $p=1$ et donc $\tau=\frac{1}{2}\left(-1+i\sqrt{4q-1}\right)$.

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

b) Quels sont les éléments non réels $a+b\tau$ de $\mathbb{Z}[\tau]$ de module minimum ?

c) Déterminer les rotations de centre 0 laissant $\mathbb{Z}[\tau]$ stable.

11) Application : Montrer que l'anneau $\mathbb{Z}[\tau]$ est principal dès que $\tau=i$ ou que $\tau=j$. On pourra considérer un idéal I de $\mathbb{Z}[\tau]$ non réduit à $\{0\}$, introduire un élément u de module minimum parmi les éléments non nuls de I, considérer le réseau $\mathcal{R}(u,\tau u)$ et utiliser la question 3.b).

Solution :

Ce problème est une adaptation personnelle des trois dernières parties de la première composition de l'Agrégation Interne 1998. La partie I qui proposait une étude du groupe $\mathrm{GL}(2,\mathbb{Z})$ a été ici complètement occultée, mais sous-tend des questions qui ont été rajoutées. L'adaptation et la solution proposée sont de Dany-Jack Mercier.

Partie I : Généralités

1.a) Les vecteurs u' et v' seront linéairement indépendants si et seulement si le déterminant de leurs coordonnées dans la base (u,v) n'est pas nul. Cela s'écrit par exemple $\begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$.

1.b) Comme $\mathcal{R}(u',v')$ est le sous-groupe additif engendré par u' et v', on a

$$\mathcal{R}\left(u',v'\right) \subset \mathcal{R} \Leftrightarrow u' \in \mathcal{R} \text{ et } v' \in \mathcal{R} \Leftrightarrow u' = au + cv \in \mathcal{R} \text{ et } v' = bu + dv \in \mathcal{R} \Leftrightarrow a,b,c,d \in \mathbb{Z}.$$

1.c) On a

$$\mathcal{R}\left(u',v'\right) = \mathcal{R} \Leftrightarrow \left\{ \begin{array}{l} \mathcal{R}(u',v') \subset \mathcal{R} \\ \mathcal{R} \subset \mathcal{R}(u',v') \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a,b,c,d \in \mathbb{Z} \\ u,v \in \mathcal{R}(u',v') \end{array} \right. .$$

La matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ est inversible dans $M_2(\mathbb{R})$ et à coefficients dans $\mathbb{Z}$.
On aura $u,v \in \mathcal{R}(u',v')$ si et seulement si le système

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} u' \\ v' \end{pmatrix} \qquad (*)$$

se résout en

$$\begin{pmatrix} u \\ v \end{pmatrix} = A^{-1} \begin{pmatrix} u' \\ v' \end{pmatrix}$$

avec A^{-1} à coefficients dans $\mathbb{Z}$. Cela revient à dire que la matrice A est inversible dans $M_2(\mathbb{Z})$, et équivaut à $ad - bc = \pm 1$ d'après le Lemme ci-dessous.

Lemme : La matrice A à coefficients dans $\mathbb{Z}$ est inversible dans l'anneau $M_2(\mathbb{Z})$ si et seulement si $\det A = \pm 1$.

preuve du Lemme : Par hypothèse $A \in M_2(\mathbb{Z})$. Si A est inversible dans $M_2(\mathbb{Z})$, il existe une matrice $A' \in M_2(\mathbb{Z})$ telle que $AA' = A'A = I$, d'où $\det A \times \det A' = 1$. Comme $\det A$ et $\det A'$ sont des entiers, cela implique $\det A = \pm 1$. Réciproquement, si $\det A = \pm 1$, on sait que A est inversible dans $M_2(\mathbb{R})$ et que

$$A^{-1} = \frac{1}{\det A}\, {}^t(\mathrm{com}\, A).$$

On aura donc $A^{-1} = \pm\, {}^t(\mathrm{com}\, A) \in M_2(\mathbb{Z})$ et cela signifie bien que A est inversible dans $M_2(\mathbb{Z})$. ■

En conclusion

$$\mathcal{R}\left(u',v'\right)=\mathcal{R}\Leftrightarrow\left\{\begin{array}{l}a,b,c,d\in\mathbb{Z}\\ ad-bc=\pm1.\end{array}\right.$$

Autre solution : Soit $\delta=ad-bc$ le déterminant de A. Le système $(*)$ se résout en

$$\left(\begin{array}{c}u\\ v\end{array}\right)=\frac{1}{\delta}\left(\begin{array}{cc}d & -c\\ -b & a\end{array}\right)\left(\begin{array}{c}u'\\ v'\end{array}\right)$$

donc $u,v\in\mathcal{R}\left(u',v'\right)$ si et seulement si les quatre nombres $\frac{a}{\delta}$, $\frac{b}{\delta}$, $\frac{c}{\delta}$, $\frac{d}{\delta}$ sont des entiers relatifs. Dans ce cas

$$\frac{a}{\delta}\times\frac{d}{\delta}-\frac{b}{\delta}\times\frac{c}{\delta}\in\mathbb{Z}\Rightarrow\frac{1}{\delta}\in\mathbb{Z}\Rightarrow\delta=\pm1.$$

Comme la réciproque est triviale, on peut affirmer que $u,v\in\mathcal{R}\left(u',v'\right)$ si et seulement si $\delta=\pm1$.

2.a) Le vecteur u' sera basique si et seulement si il existe $(b,d)\in\mathbb{Z}^2$ tel que $ad-bc=\pm1$. Cela équivaut à dire que les entiers a et c sont premiers entre eux.

2.b) Par hypothèse il existe $u'=au+cv$ appartenant à $\Delta\cap\mathcal{R}\backslash\{0\}$. Soit $t=\mathrm{pgcd}\left(a,c\right)$ et notons $a=a't$ et $c=c't$. On aura $u'=t\delta$ où $\delta=a'u+c'v\in\Delta\cap\mathcal{R}$. Alors δ sera un vecteur basique de Δ puisque $\mathrm{pgcd}\left(a',c'\right)=1$.
On a évidemment $\mathbb{Z}\delta\subset\Delta\cap\mathcal{R}$. Réciproquement, si $u'=au+cv\in\Delta\cap\mathcal{R}$, et comme $\Delta=\mathbb{R}\delta$, il existe $\lambda\in\mathbb{R}$ tel que

$$u'=au+cv=\lambda\delta=\lambda\left(a'u+c'v\right).$$

Par conséquent $a=\lambda a'$ et $c=\lambda c'$. Il s'agit de montrer que $\lambda\in\mathbb{Z}$ pour pouvoir conclure à $u'\in\mathbb{Z}\delta$. On a $\lambda\in\mathbb{Q}$ et l'on peut poser $\lambda=\frac{p}{q}$ où $p\in\mathbb{Z}$, $q\in\mathbb{N}^*$ et $\mathrm{pgcd}\left(p,q\right)=1$. On aura $aq=pa'$ et $cq=pc'$. Le Théorème de Gauss montre que q divise à la fois a' et c', et donc que q divise $\mathrm{pgcd}\left(a',c'\right)=1$. Cela entraîne $q=1$ et $\lambda\in\mathbb{Z}$. En conclusion $\mathbb{Z}\delta=\Delta\cap\mathcal{R}$.

2.c) Bien sûr que non : les complexes u et $u+2v$ sont des vecteurs basiques mais ne forment pas une base de $\mathcal{R}$ puisque $u+v$ ne peut pas s'écrire comme combinaison linéaire entière de u et $u+2v$. En effet,

$$u+v=au+b\left(u+2v\right)$$

entraîne $1=2b$, ce qui est impossible si b est un entier.

3.a) Comme $v=\frac{|v|}{|u|}e^{i\theta}u$, on peut écrire $u\overline{v}=\frac{|v|}{|u|}e^{-i\theta}\left|u\right|^2=\left|u\right|\left|v\right|e^{-i\theta}$ et

$$\begin{array}{rcl}\left|au+bv\right|^2 & = & a^2\left|u\right|^2+b^2\left|v\right|^2+2\,\mathrm{Re}\left(abu\overline{v}\right)=a^2\left|u\right|^2+b^2\left|v\right|^2+2ab\left|u\right|\left|v\right|\cos\theta\\ & = & \left(a\left|u\right|+b\left|v\right|\cos\theta\right)^2+b^2\left|v\right|^2-b^2\left|v\right|^2\cos^2\theta\\ & = & \left(a\left|u\right|+b\left|v\right|\cos\theta\right)^2+b^2\left|v\right|^2\sin^2\theta.\end{array}$$

Notons B la boule de centre 0 et de rayon M. Si $z=au+bv\in\mathcal{R}\left(u,v\right)\cap B$, alors $\left|au+bv\right|^2\leq M^2$ et l'égalité ci-dessus entraîne simultanément

$$b^2\left|v\right|^2\sin^2\theta\leq M^2\text{ et }\left(a\left|u\right|+b\left|v\right|\cos\theta\right)^2\leq M^2$$

donc

$$|b| \leq \frac{M}{|v|\,|\sin\theta|} \text{ et } |au| \leq M + b\,|v|\,|\cos\theta|$$

Cela entraîne

$$|b| \leq \frac{M}{|v|\,|\sin\theta|} \text{ et } |a| \leq \frac{M}{|u|}\left(1 + \frac{|\cos\theta|}{|\sin\theta|}\right)$$

et ces deux inégalités montrent que les entiers a et b ne peuvent prendre qu'un nombre fini de valeurs. Cela montre que $\mathcal{R}(u,v)$ est discret.

3.b) Notons $z = au + bv$ avec $a, b \in \mathbb{R}$, et $[a]$ la partie entière de a. Pour tout réel a on peut écrire $[a] \leq a < [a] + 1$, et deux cas seulement sont possibles. Ou bien $[a] \leq a \leq [a] + \frac{1}{2}$ et l'on pose $e_a = [a]$, ou bien $[a] + \frac{1}{2} < a < [a] + 1$ et l'on pose $e_a = [a] + 1$. Dans tous les cas, on a trouvé un entier e_a et un réel x tels que

$$a = e_a + x \text{ et } |x| \leq \frac{1}{2}.$$

On aura donc $z = (e_a + x)\,u + (e_b + y)\,v$ avec $|x| \leq \frac{1}{2}$ et $|y| \leq \frac{1}{2}$. En notant $z' = e_a u + e_b v \in \mathcal{R}'$, on obtient bien

$$\forall z \in \mathbb{C} \quad \exists z' \in \mathcal{R}' \quad \exists x, y \in \mathbb{R} \quad z - z' = xu + yv,\ |x| \leq \frac{1}{2} \text{ et } |y| \leq \frac{1}{2}. \qquad (1)$$

L'inégalité (1) entraîne

$$\left|z - z'\right| = |xu + yv| \leq |xu| + |yv| \leq \frac{1}{2}\left(|u| + |v|\right) \leq |v| \qquad (2)$$

d'après les définitions de u et v. Supposons par l'absurde que $|z - z'| = |v|$. Les inégalités (2) entraînent alors $|xu + yv| = |xu| + |yv|$, et cela signifie que les vecteurs xu et yv sont colinéaires et de même sens (égalité dans Minkowski), autrement dit qu'il existe $\lambda \in \mathbb{R}$ tel que $xu = \lambda yv$ ou $yv = 0$. Comme v n'est pas nul, cela équivaut à

$$xu = \lambda yv \text{ ou } y = 0.$$

Si $y \neq 0$, alors $xu = \lambda yv$. Comme u et v ne sont pas colinéaires, on obtient $x = \lambda = 0$. Dans ce cas, les égalités (2) entraînent $|yv| = |v|$ d'où $|y| = 1$, ce qui contredit (1). Si $y = 0$, les égalités (2) donnent encore

$$|xu| = |v|$$

d'où $|v| = |xu| \leq \frac{1}{2}|u|$. Cela contredit l'inégalité $|u| \leq |v|$ provenant du choix de $|u|$. Finalement

$$\left|z - z'\right| < |v|. \qquad (3)$$

Montrons maintenant que $\mathcal{R} = \mathcal{R}'$. Soit $z \in \mathcal{R}$. On a $z - z' \in \mathcal{R}$. L'inégalité stricte (3) montre que $z - z'$ est colinéaire à u (sinon il y a contradiction avec la définition du deuxième minimum $|v|$ de $\mathcal{R}$). Donc $y = 0$ et $z - z' = xu$. Si $x \neq 0$, la définition de u entraîne $|u| \leq |z - z'| = |xu|$ d'où $1 \leq |x|$, en contradiction avec $|x| \leq \frac{1}{2}$. Finalement $x = y = 0$ et $z = z' \in \mathcal{R}'$.

Partie II : Similitudes directes de centre 0 laissant un réseau stable

4.a) L'ensemble S des similitudes directes de centre 0 laissant $\mathcal{R}$ stable est en bijection avec $Z(\mathcal{R}(u,v))$. La bijection est l'application qui à la similitude directe f d'écriture complexe $f(z)=az$ associe le complexe $a\in Z(\mathcal{R}(u,v))$.
Une homothétie $h(z)=\lambda z$ (où $\lambda\in\mathbb{R}$) laisse stable $\mathcal{R}(u,v)$ si et seulement si $\lambda au+\lambda bv$ appartient à $\mathcal{R}(u,v)$ pour tout $(a,b)\in\mathbb{Z}^2$, i.e. si $(\lambda a,\lambda b)\in\mathbb{Z}^2$ dès que $(a,b)\in\mathbb{Z}^2$, et cela équivaut à $\lambda\in\mathbb{Z}$. Par conséquent $Z(\mathcal{R}(u,v))\cap\mathbb{R}=\mathbb{Z}$.

4.b) L'ensemble $Z(\mathcal{R}(u,v))$ est un sous-anneau de $\mathbb{C}$ puisqu'il n'est pas vide ($1\in Z(\mathcal{R}(u,v))$), puisque $z-z'\in Z(\mathcal{R}(u,v))$ dès que z et z' appartiennent à $Z(\mathcal{R}(u,v))$, et puisque zz' appartient à $Z(\mathcal{R}(u,v))$ dès que z et z' appartiennent à $Z(\mathcal{R}(u,v))$. Ces vérifications sont triviales :

$$\begin{aligned}\left(z-z'\right)(\mathcal{R}(u,v)) &\subset z(\mathcal{R}(u,v))-z'(\mathcal{R}(u,v))\subset\mathcal{R}(u,v),\\ zz'(\mathcal{R}(u,v)) &\subset z(\mathcal{R}(u,v))\subset\mathcal{R}(u,v).\end{aligned}$$

4.c) Soient $a=\frac{1}{u}$ et $w=av$. La similitude directe $z\mapsto az$ transforme alors u et v respectivement en 1 et w. Bien entendu $w=\frac{v}{u}\notin\mathbb{R}$ puisque (u,v) est une base de $\mathbb{C}$.

4.d) On a

$$\begin{aligned}[z\in Z(\mathcal{R}(u,v))] &\Leftrightarrow z\mathcal{R}(u,v)\subset\mathcal{R}(u,v)\Leftrightarrow za\mathcal{R}(u,v)\subset a\mathcal{R}(u,v)\\ &\Leftrightarrow z\mathcal{R}(1,w)\subset\mathcal{R}(1,w)\Leftrightarrow z\in Z(\mathcal{R}(1,w))\end{aligned}$$

donc $Z(\mathcal{R}(u,v))=Z(\mathcal{R}(1,w))$. Par ailleurs si $z\in Z(\mathcal{R}(1,w))$, alors $1\in\mathcal{R}(1,w)$ entraîne $z\times 1\in\mathcal{R}(1,w)$, et cela prouve l'inclusion $Z(\mathcal{R}(1,w))\subset\mathcal{R}(1,w)$.

5.a) Ici $w^2=-2$ et

$$\begin{aligned}[z=a+bw\in Z(\mathcal{R}(1,w))] &\Leftrightarrow \begin{cases} z\times 1\in\mathcal{R}(1,w)\\ z\times w\in\mathcal{R}(1,w)\end{cases}\Leftrightarrow\begin{cases}(a,b)\in\mathbb{Z}^2\\ aw-2b\in\mathcal{R}(1,w)\end{cases}\\ &\Leftrightarrow (a,b)\in\mathbb{Z}^2.\end{aligned}$$

Donc $Z(\mathcal{R}(1,w))=\mathcal{R}(1,w)$.

5.b) Ici $w^2=-2^{\frac{2}{3}}$ et

$$\begin{aligned}[z=a+bw\in Z(\mathcal{R}(1,w))] &\Leftrightarrow \begin{cases} z\times 1\in\mathcal{R}(1,w)\\ z\times w\in\mathcal{R}(1,w)\end{cases}\Leftrightarrow\begin{cases}(a,b)\in\mathbb{Z}^2\\ aw-2^{\frac{2}{3}}b\in\mathcal{R}(1,w)\end{cases}\\ &\Leftrightarrow \left(a,b,2^{\frac{2}{3}}b\right)\in\mathbb{Z}^2.\end{aligned}$$

Si $b\neq 0$, alors $2^{\frac{2}{3}}b\in\mathbb{Z}$ montre que $2^{\frac{2}{3}}\in\mathbb{Q}$, ce qui est impossible. Donc $b=0$ et $Z(\mathcal{R}(1,w))=\mathbb{Z}$.

6) i) $\Rightarrow$ ii) : Soit $z=a+bw\in Z(\mathcal{R}(1,w))\setminus\mathbb{Z}$. On a

$$[z\in Z(\mathcal{R}(1,w))]\Leftrightarrow\begin{cases} z\times 1\in\mathcal{R}(1,w)\\ z\times w\in\mathcal{R}(1,w)\end{cases}\Leftrightarrow\begin{cases}a,b\in\mathbb{Z}\\ aw+bw^2\in\mathcal{R}(1,w).\end{cases}$$

.

Il existe donc $a, b, c, d \in \mathbb{Z}$ tels que $aw + bw^2 = c + dw$, d'où

$$bw^2 + (a-d)\, w - c = 0.$$

On a bien $P(w) = 0$ avec $P(X) = bX^2 + (a-d)\, X - c \in \mathbb{Z}[X]$ et $b \neq 0$.

ii) $\Rightarrow$ i) : Si w est une racine non réelle de $P(X) = \alpha X^2 + \beta X + \gamma \in \mathbb{Z}[X]$, alors

$$w(\alpha w + \beta) = -\gamma \in \mathcal{R}(1, w)$$

montre que $z = \alpha w + \beta \in Z(\mathcal{R}(1, w))$. Le complexe z n'est pas dans $\mathbb{R}$ sinon $\alpha w + \beta = \delta \in \mathbb{R}$ entraînerait $w = \frac{\delta - \beta}{\alpha} \in \mathbb{R}$, ce qui est contraire à l'hypothèse.

7) Ici $w^2 = -\beta w - \gamma \in \mathcal{R}(1, w)$ donc

$$\begin{aligned}[z = a + bw \in Z(\mathcal{R}(1, w))] &\Leftrightarrow \left\{ \begin{array}{l} z \times 1 \in \mathcal{R}(1, w) \\ z \times w \in \mathcal{R}(1, w) \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a, b \in \mathbb{Z} \\ aw + b(-\beta w - \gamma) \in \mathcal{R}(1, w) \end{array} \right. \\ &\Leftrightarrow a, b \in \mathbb{Z} \Leftrightarrow z \in \mathcal{R}(1, w).\end{aligned}$$

En conclusion $Z(\mathcal{R}(1, w)) = \mathcal{R}(1, w)$.

8.a) $Z(\mathcal{R}(1, w))$ est un sous-groupe additif de $\mathcal{R}(1, w)$, n'est pas inclus dans une droite par hypothèse, et sera à fortiori discret (puisque inclus dans le réseau $\mathcal{R}(1, w)$ qui est discret). La question 3) permet d'affirmer que $Z(\mathcal{R}(1, w))$ est un réseau.
La droite $\mathbb{R}$ coupe le réseau $Z(\mathcal{R}(1, w))$ suivant $\mathbb{Z}$, de sorte que la question 2.b) nous montre l'existence d'un vecteur basique δ dans $\mathbb{Z}$. Cette même question montre aussi que

$$Z(\mathcal{R}(1, w)) \cap \mathbb{R} = \mathbb{Z} = \delta\mathbb{Z},$$

et donc que $\delta = \pm 1$. Cela prouve que 1 (et aussi -1) sont basiques pour $Z(\mathcal{R}(1, w))$. Cela signifie l'existence d'un complexe τ tel que $Z(\mathcal{R}(1, w)) = \mathcal{R}(1, \tau)$.

8.b) La question 4.b) montre que $Z(\mathcal{R}(1, w)) = \mathcal{R}(1, \tau)$ est un anneau, et donc que

$$(1 + \tau, \tau) \in \mathcal{R}(1, \tau) \times \mathcal{R}(1, \tau) \Rightarrow (1 + \tau)\, \tau \in \mathcal{R}(1, \tau).$$

Il existe donc deux entiers a, b, tels que $\tau^2 + \tau = a + b\tau$. Ainsi τ sera bien racine d'un polynôme $X^2 + pX + q$ où p et q sont des entiers relatifs. Comme $\mathcal{R}(1, \tau)$ n'est pas inclus dans $\mathbb{R}$, τ ne sera pas réel et le discriminant $p^2 - 4q$ sera strictement négatif. Cela implique $q > 0$.

8.c) Il s'agit de troquer τ pour un nombre z qui vérifie

P1. $z = a + b\tau$ avec $a, b \in \mathbb{Z}$,
P2. z est racine de $X^2 + X + \gamma$ ou de $X^2 + \gamma$ où $\gamma \in \mathbb{Z}$,
P3. $(1, z)$ est une base du réseau $\mathcal{R}(1, \tau)$.

La condition P3 signifie que la matrice $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ est inversible dans $M_2(\mathbb{Z})$, i.e. $b = \pm 1$. Prenons $b = 1$, par exemple. On a $z = a + \tau$. L'égalité $\tau^2 + p\tau + q = 0$ devient

$$(z - a)^2 + p(z - a) + q = 0$$

soit

$$z^2 + (p - 2a)\, z + a^2 - pa + q = 0.$$

Il suffit de choisir a tel que $p = 2a + 1$ (si p impair) ou $p = 2a$ (si p pair) pour conclure.

Partie III : Rotations de centre 0 laissant $\mathcal{R}(1,\tau)$ stable

9.a) (...)

9.b) Pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$,

$$|a+b\tau|^2 = a^2 + b^2 q \geq b^2 q \geq q$$

et l'égalité a lieu si et seulement si $b = \pm 1$ et $a = 0$. Les éléments de module minimum cherchés sont donc $\pm\tau = \pm i\sqrt{q}$.

9.c) Une rotation r transformera 1 en un point du réseau situé à la distance 1 de son centre 0. Si $q \neq 1$, la question précédente montre que tout $z \in \mathcal{R}(1,\tau) \setminus \mathbb{R}$ vérifie $|z| \geq \sqrt{q} > 1$, et donc les seuls éléments z de $\mathcal{R}(1,\tau)$ de module 1 seront ± 1. On aura $r(1) \in \{\pm 1\}$ et r sera l'identité ou la symétrie de centre 0. La réciproque est triviale.
Si $q = 1$, alors $\tau = i$. La question précédente montre que tout $z \in \mathcal{R}(1,\tau) \setminus \mathbb{R}$ vérifie $|z| \geq \sqrt{q} = 1$ et que l'égalité n'a lieu que si $z \in \{\pm 1, \pm i\}$. Ainsi $r(1) \in \{\pm 1, \pm i\}$ et r sera une rotation de centre 0 et d'angles $k\frac{\pi}{2}$ avec $k = 0, ..., 3$. La réciproque est triviale.

Autre solution : Les rotations r cherchées sont les similitudes dont l'expression complexe $s(t) = zt$ vérifie $|z| = 1$ et $z \in Z(\mathcal{R}(1,\tau))$. Ici $Z(\mathcal{R}(1,\tau)) = \mathcal{R}(1,\tau)$ (Question 7) et si l'on pose $z = a + b\tau$, on est ramené à résoudre

$$|a+b\tau| = \sqrt{a^2 + b^2 q} = 1.$$

On retrouve les résultats précédents.

10.a) (...)

10.b)

$$|a+b\tau|^2 = \frac{1}{4}\left|2a - b + ib\sqrt{4q-1}\right|^2 = \frac{1}{4}\left[(2a-b)^2 + b^2(4q-1)\right] = a^2 - ab + b^2 q.$$

Posons $\varphi(a,b) = a^2 - ab + b^2 q$. Pour chaque b fixé, le minimum de la parabole

$$a \mapsto \varphi(a,b) = a^2 - ab + b^2 q$$

est atteint pour $a = \frac{b}{2}$. D'où la discussion :

⋆ Pour tout b pair, on a

$$\varphi(a,b) \geq \varphi\left(\frac{b}{2}, b\right) = b^2\left(q - \frac{1}{4}\right) \geq \varphi(1,2) = 4q - 1.$$

⋆ Pour tout b impair, on a

$$\varphi(a,b) \geq \text{Min}\left(\varphi\left(\frac{b-1}{2}, b\right), \varphi\left(\frac{b+1}{2}, b\right)\right) = \varphi\left(\frac{b+1}{2}, b\right) = b^2\left(q - \frac{1}{4}\right) + \frac{1}{4} \geq \varphi(1,1) = q. \ (*)$$

En conclusion

$$\text{Min}\{\varphi(a,b) \ / \ (a,b) \in \mathbb{Z} \times \mathbb{Z}^*\} = \varphi(1,1) = q.$$

Les inégalités $(*)$ montrent que le minimum des $\varphi(a,b)$ pour $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ est atteint en (a,b) si et seulement si

$$b = \pm 1 \text{ et } a = \frac{b \pm 1}{2},$$

d'où les solutions

a	0	1	-1	0
b	1	1	-1	-1
$a+b\tau$	τ	$1+\tau$	$-1-\tau$	$-\tau$

.

Le module minimum sera $|1+\tau| = |\tau| = \sqrt{q}$.

10.c) Si r est une rotation de centre 0 qui laisse stable $\mathbb{Z}[\tau]$, la conservation des distances impose d'avoir $|r(1)| = 1$.

Si $q \neq 1$, alors $\sqrt{q} \neq 1$ et les seules possibilités sont $r(1) \in \{-1, 1\}$.

Si $q = 1$, alors $|1+\tau| = |\tau| = \sqrt{q} = 1$ et $\tau = j$. Les 6 complexes 1, $1+j$, j, -1, j^2, $1+j^2$ sont les seuls éléments de module 1 de $\mathbb{Z}[j]$ d'après 10.b, et les seules images possibles de 1 par r. La rotation r sera donc d'angle 0, π, $\pm\frac{2\pi}{3}$ ou $\pm\frac{4\pi}{3}$. La réciproque est triviale si l'on prend la représentation complexe de r. Par exemple, si r est la rotation de centre O et d'angle $\frac{2\pi}{3}$, sa représentation complexe est $r(z) = jz$ et

$$r(a+bj) = b(-1-j) + aj = -b + (a-b)j \in \mathbb{Z}[j]$$

pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, i.e. $\mathbb{Z}[j]$ est stable par r.

Autre solution : Comme en 9.b) on est ramené à poser $z = a + b\tau$ et à résoudre l'équation $|a+b\tau| = 1$. On a

$$|a+b\tau| = 1 \Leftrightarrow \frac{1}{4}\left[(2a-b)^2 + b^2(4q-1)\right] = 1 \Leftrightarrow (2a-b)^2 + b^2(4q-1) = 4.$$

Il suffit de résoudre cette dernière équation en nombres entiers pour retrouver les résultats précédents.

11) Soit I un idéal de $\mathbb{Z}[\tau]$ non réduit à $\{0\}$. Soit u de module minimum parmi les éléments non nuls de I. L'idéal I est un sous-groupe de $\mathbb{Z}[\tau]$, est discret (puisque inclus dans un ensemble), et n'est pas inclus dans une droite (en effet $\tau = i$ ou j, donc τu appartient à I sans être colinéaire à u).

La question 3.b) montre que I est un réseau. Cette question prouve aussi que $\mathcal{R}(u, \tau u) = I$ puisque u est de module minimum parmi les éléments non nuls de I, et que τu (dont le module est $|\tau u| = |u|$) est encore de module minimum parmi les éléments de I non colinéaires à u. Finalement $I = \mathcal{R}(u, \tau u) = u\,\mathbb{Z}[\tau]$ est l'idéal de $\mathbb{Z}[\tau]$ engendré par u.

Tout idéal de $\mathbb{Z}[\tau]$ est donc engendré par un seul élément, et cela signifie que l'anneau $\mathbb{Z}[\tau]$ est principal.