(Agrégation interne 1998 -première épreuve de mathématiques)

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

1. a) Rappelons que si $ad-bc\neq 0$, on a $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On trouve

$$\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -3 & 5 \\ 2 & -3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}^{-1} = \frac{1}{2}\begin{pmatrix} 3 & -5 \\ -2 & 4 \end{pmatrix}.$$

   b) La matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ admet un inverse dans $M_2(\mathbb{R})$ si et seulement si $\det(A)\neq 0$.
   Si A admet un inverse dans $M_2(\mathbb{Z})$, on a $\det A \in \mathbb{Z}$ et $\det A^{-1}\in\mathbb{Z}$, donc $1 = \det A \det A^{-1}$. Cela implique que $\det A = \pm 1$.
   Inversement, si $\det A = \pm 1$, alors $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbb{Z})$.

2. a) On a $\begin{pmatrix} 3 & b \\ c & 3 \end{pmatrix} \in SL(2,\mathbb{Z})) \iff bc = 8$, soit

$$(b,c)\in\{(1,8),(-1,-8),(2,4),(-2,-4),(4,2),(-4,-2),(8,1),(-8,-1)\}.$$

   b) On a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ si et seulement si $bc = ad-1$. Si (a,d) n'est pas égal à l'un des couples $(1,1)$, $(-1,-1)$, alors $ad\neq 1$, donc l'ensemble des solutions est l'ensemble fini non vide des couples de la forme $(\delta, \dfrac{ad-1}{\delta})$, où δ parcourt l'ensemble fini, non vide des diviseurs de $ad-1$.

   c) Lorsque (a,d) est l'un des couples $(1,1)$, $(-1,-1)$, l'ensemble des solutions est $\{(0,n);\ n\in\mathbb{Z}\}\cup\{(n,0);\ n\in\mathbb{Z}\}$; il est infini.

3. a) Pour $(b,d)\in\mathbb{Z}^2$, on a $3d-2b=1$, si et seulement si $3d-2b=3-2$, soit, $3(d-1)=2(b-1)$. Dans ce cas, $3(d-1)$ est pair, donc $d-1$ est pair. Il existe donc $k\in\mathbb{Z}$ tel que $d=2k+1$. L'équation devient $3k=b-1$. Donc l'ensemble des $(b,d)\in\mathbb{Z}^2$, tels que $3d-2b=1$ est $\{(3k+1,2k+1);\ k\in\mathbb{Z}\}$.
   Pour $(b,d)\in\mathbb{Z}^2$, on a $\begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix}\in GL(2,\mathbb{Z})$ si et seulement si $\begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix}\in SL(2,\mathbb{Z})$ ou $\begin{pmatrix} 3 & -b \\ 2 & -d \end{pmatrix}\in SL(2,\mathbb{Z})$, *i.e.* si et seulement si $(b,d)\in\{(\varepsilon(3k+1),\varepsilon(2k+1));\ \varepsilon\in\{-1,1\};\ k\in\mathbb{Z}\}$.

   b) Soit $(a,c)\in\mathbb{Z}^2$. D'après le théorème de Bézout, il existe $(b,d)\in\mathbb{Z}^2$ tel que $ad-bc=1$ si et seulement si a et c sont premiers entre eux. Dans ce cas, soit (b_0,d_0) une solution. Alors pour tout $k\in\mathbb{Z}$, le couple (b_0+ka, d_0+kc) est aussi solution : donc l'ensemble des solutions est vide si a et c ne sont pas premiers entre eux et infini si a et c sont premiers entre eux.

II. Réseaux de $\mathbb{C}$

1. a) Posons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Les nombres complexes $u' = au+cv,\ v' = bu+dv$ sont indépendants sur $\mathbb{R}$ si et seulement si leurs composantes dans la base (u,v) ne sont pas proportionnelles, *i.e.* si $\det A = ad-bc$ n'est pas nul.

   b) Si $\mathcal{R}(u',v')\subset\mathcal{R}$, alors $u'\in\mathcal{R}$ et $v'\in\mathcal{R}$, donc leurs composantes dans la base u,v sont entières, *i.e.* $A\in M_2(\mathbb{Z})$. Inversement, si $A\in M_2(\mathbb{Z})$, alors $u'\in\mathcal{R}$ et $v'\in\mathcal{R}$, et comme $\mathcal{R}$ est un sous-groupe de $\mathbb{C}$, il contient le sous-groupe $\mathcal{R}(u',v')$ de $\mathbb{C}$ engendré par u',v'.

c) La matrice de passage de la base (u', v') à (u, v) est A^{-1}. Par (a), on a $\mathcal{R}(u, v) \subset \mathcal{R}(u', v')$ si et seulement si $A^{-1} \in M_2(\mathbb{Z})$. Donc $\mathcal{R}(u, v) = \mathcal{R}(u', v')$ si et seulement si $A \in M_2(\mathbb{Z})$ et $A^{-1} \in M_2(\mathbb{Z})$, ce qui est équivalent d'après I.1.b), à $A \in GL(2, \mathbb{Z})$.

2. a) Par (a), le couple $(3u + 2v, bu + dv)$ est une base du réseau $\mathcal{R}(u, v)$ si et seulement si $\begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix} \in GL(2, \mathbb{Z})$, *i.e.* $(b, d) \in \{(\varepsilon(3k + 1), \varepsilon(2k + 1));\ \varepsilon \in \{-1, 1\};\ k \in \mathbb{Z}\}$ (d'après I.3.a)).

b) Le nombre $au + cv$ est basique pour $\mathcal{R}$ si et seulement s'il existe b, d tel que $ad - bc = \pm 1$ ce qui a lieu si et seulement si a et c sont premiers entre eux (théorème de Bézout).

c) Soit $u' = au + cv$ un élément non nul de $\Delta \cap \mathcal{R} \neq \{0\}$. Écrivons $a = a'd$ et $c = c'd$ avec $d = PGCD(a, c)$ et a' et c' premiers entre eux. Posons $\delta = a'u + c'v$. C'est un élément basique de $\mathcal{R}$ d'après (c) et $\delta = \dfrac{u'}{d} \in \Delta$. Puisque δ est basique, il existe $v' \in \mathcal{R}$ tel que $\mathcal{R} = \mathcal{R}(\delta, v') = \{m\delta + nv';\ (m, n) \in \mathbb{Z}^2\}$; or, puisque $\mathcal{R} \not\subset \Delta$ on a $v' \notin \Delta$, donc $m\delta + nv' \in \Delta \iff n = 0$, soit $\Delta \cap \mathcal{R} = \mathbb{Z}\delta$.

d) Les éléments u et $u + 2v$ sont basiques mais comme $\det \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = 2$, $(u, u + 2v)$ n'est pas une base de $\mathcal{R}$.

3. a) Ecrivons $\dfrac{v}{u} = re^{i\theta}$ (avec $r = \dfrac{|v|}{|u|}$). On a

$$\begin{aligned} |au + bv|^2 &= |u|^2(a + bre^{i\theta})^2 = |u|^2\big((a + br\cos\theta)^2 + b^2r^2\sin^2\theta\big) \\ &= (a|u| + b|v|\cos\theta)^2 + b^2|v|^2\sin^2\theta \\ &\geqslant b^2|v|^2\sin^2\theta. \end{aligned}$$

b) On trouve de même $|au+bv|^2 = (a|u|\cos\theta+b|v|)^2+a^2|u|^2\sin^2\theta \geqslant a^2|u|^2\sin^2\theta$. Soit $M \in \mathbb{R}_+^*$. Si $|au+bv| \leqslant M$, il vient $b^2 \leqslant \dfrac{M^2}{|v|^2\sin^2\theta}$ et donc $|b| \leqslant \dfrac{M}{|v|\sin\theta}$ et $|a| \leqslant \dfrac{M}{|u|\sin\theta}$. Donc dans la boule de centre 0 et de rayon M il y a au plus $\left(2E\left(\dfrac{M}{|v|\sin\theta}\right) + 1\right)\left(2E\left(\dfrac{M}{|u|\sin\theta}\right) + 1\right)$ éléments de $\mathcal{R}$.

4. a) Soit u_0 un élément non nul de Γ. Comme Γ est discret, l'ensemble $\{u \in \Gamma \setminus \{0\};\ |u| \leqslant |u_0|\}$ est fini et non vide, donc il existe un élément u de module minimum dans cet ensemble. On aura bien $|u| \leqslant |w|$ pour tout $w \in \Gamma \setminus \{0\}$. De même, soit $v_0 \in \Gamma \setminus \mathbb{R}u$; l'ensemble $\{v \in \Gamma \setminus \mathbb{R}u;\ |v| \leqslant |v_0|\}$ est fini et non vide, donc il existe un élément v de module minimum dans cet ensemble. Puisque Γ est un sous-groupe de $\mathbb{C}$ contenant u et v, il contient le sous-groupe $\mathcal{R}(u, v)$ qu'ils engendrent.

b) Soit $z \in \mathbb{C}$. Notons $(s, t) \in \mathbb{R}^2$ les composantes de z dans la $\mathbb{R}$-base (u, v) de $\mathbb{C}$, de sorte que $z = su + tv$. Posons $m = E(s + 1/2)$ et $n = E(t + 1/2)$, de sorte que $-1/2 \leqslant s - m < 1/2$ et $-1/2 \leqslant t-n < 1/2$, soit $|s-m| \leqslant 1/2$ et $|t-n| \leqslant 1/2$. Alors $z' = mu+nv \in \mathcal{R}$ et $z-z' = xu+yv$ avec $x = s - m$ et $y = t - m$; on a bien $|x| \leqslant \dfrac{1}{2}$, $|y| \leqslant \dfrac{1}{2}$.

c) Comme $|u|$ est minimum, il vient $|u| \leqslant |v|$. On a $|z - z'| \leqslant |x||u| + |y||v| \leqslant (|x| + |y|)|v| \leqslant |v|$.

d) Si z_1 et z_2 ne sont pas dans une même demi-droite vectorielle on a l'inégalité stricte $|z_1 + z_2| < |z_1| + |z_2|$.

e) Si x et y sont tous deux non nuls, xu et yv ne sont pas dans une même (demi-)droite vectorielle, donc l'inégalité $|z - z'| \leqslant |x||u| + |y||v|$ est stricte. Si x ou y est nul, l'inégalité $(|x| + |y|)|v| \leqslant |v|$ est stricte. Dans tous les cas, l'inégalité $|z - z'| \leqslant |v|$ est stricte.

f) Supposons $z \in \Gamma$ et soit $z' \in \mathcal{R}$ tel que $z - z' = xu + yv$ avec $|x| \leqslant 1/2$ et $|y| \leqslant 1/2$. Alors $z - z' \in \Gamma$ et $|z - z'| < |v|$; par minimalité de $|v|$, il vient $z - z' \in \mathbb{R}u$, soit $z - z' = xu$ donc $|z - z'| < |u|$. Par minimalité de $|u|$, il vient $z = z'$. Cela prouve que $\Gamma \subset \mathcal{R}$, d'où l'égalité.

III. Similitudes de centre 0 laissant stable un réseau

1. a) Les similitudes directes de centre 0 sont les applications de la forme $w \mapsto zw$ (ou $z \in \mathbb{C}^*$). Donc les similitudes directes de centre 0 laissant $\mathcal{R}$ stable sont les applications $w \mapsto zw$ avec $z \in Z(\mathcal{R}) \setminus \{0\}$.

   b) Si $w \in \mathcal{R}$ et $k \in \mathbb{Z}^*$, il vient $kw \in \mathcal{R}$ donc l'homothétie de centre 0 et rapport k stabilise $\mathcal{R}$. Inversement si l'homothétie de rapport $k \in \mathbb{R}^*$ laisse $\mathcal{R}$ stable, on a $ku = au+bv$ avec $(a,b) \in \mathbb{Z}^2$; comme (u,v) est libre (sur $\mathbb{R}$) cela implique $k \in \mathbb{Z}$. On a donc $Z(\mathcal{R}) \cap \mathbb{R} = \mathbb{Z}$.

   c) On a vu que $\mathbb{Z} \subset Z(\mathcal{R})$, donc $0 \in Z(\mathcal{R})$ et $1 \in Z(\mathcal{R})$. Si $x, y \in Z(\mathcal{R})$, pour tout $w \in \mathcal{R}$ on a $xw \in \mathcal{R}$ et $yw \in \mathcal{R}$, donc $(x-y)w \in \mathcal{R}$ (car $\mathcal{R}$ est un sous-groupe additif de $\mathbb{C}$). On en déduit que $x - y \in Z(\mathcal{R})$, donc $Z(\mathcal{R})$ est un sous-groupe additif de $\mathbb{C}$. Enfin, puisque $yw \in \mathcal{R}$ et $x \in Z(\mathcal{R})$, il vient $xyw \in \mathcal{R}$. Comme cela est vrai pour tout $w \in \mathcal{R}$, on trouve $xy \in Z(\mathcal{R})$. Donc $Z(\mathcal{R})$ est un sous-anneau de $\mathbb{C}$.

   d) La multiplication par $1/u$ est une similitude directe qui transforme le réseau $\mathcal{R}(u,v)$, en $\mathcal{R}(1,w)$ où $w = v/u \in \mathbb{C} \setminus \mathbb{R}$.
   Soient $z \in Z(\mathcal{R}(1,w))$ et $x \in \mathcal{R}(u,v)$. On a $x/u \in \mathcal{R}(1,w)$, donc $z(x/u) \in \mathcal{R}(1,w)$, soit $zx \in \mathcal{R}(u,v)$. Cela prouve que $z \in Z(\mathcal{R}(u,v))$.
   Soient $z \in Z(\mathcal{R}(u,v))$ et $x \in \mathcal{R}(1,w)$. On a $xu \in \mathcal{R}(u,v)$, donc $z(xu) \in \mathcal{R}(u,v)$, soit $zx \in \mathcal{R}(1,w)$. Cela prouve que $z \in Z(\mathcal{R}(1,w))$.
   Donc $Z(\mathcal{R}(1,w)) = Z(\mathcal{R}(u,v))$.

   e) Puisque $1 \in \mathcal{R}(1,w)$, si $z \in \mathcal{R}(1,w)$, alors $z = z1 \in \mathcal{R}(1,w)$. On a donc $Z(\mathcal{R}(1,w)) \subset \mathcal{R}(1,w)$.

   f) On a $Z(\mathcal{R}(1,(\sqrt{2})i)) = \mathcal{R}(1,(\sqrt{2})i)$ et $Z(\mathcal{R}(1,(\sqrt[3]{2})i)) = \mathbb{Z}$.

2. Soit $z \in Z(\mathcal{R}) \setminus \mathbb{Z}$. Comme $Z(\mathcal{R}) \subset \mathcal{R}$, il existe $a, b \in \mathbb{Z}$ tels que $z = a + bw$. Comme $z \notin \mathbb{Z}$ on a $b \neq 0$. Enfin, puisque $z \in Z(\mathcal{R})$, il bien $wz \in \mathcal{R}$, donc il existe $c, d \in \mathbb{Z}$ tels que $wz = c + dw$. On a donc $aw + bw^2 = c + dw$, soit $bw^2 + (a-c)w - d = 0$.

3. a) Si $\alpha w^2+\beta w+\gamma = 0$, pour tout $a, b \in \mathbb{Z}^2$, on a $(\alpha w)(a+bw) = \alpha aw+\alpha bw^2 = \alpha aw-b(\beta w+\gamma) \in \mathcal{R}$. Donc $\alpha w \in Z(\mathcal{R})$.

   b) Si $\alpha = 1$, on a $w \in Z(\mathcal{R})$. Puisque $Z(\mathcal{R})$ est un sous groupe de $\mathbb{C}$ contenant 1 et w, il contient $\mathcal{R}$, donc $Z(\mathcal{R}) = \mathcal{R}$.

   c) Puisque $Z(\mathcal{R})$ est contenu dans $\mathcal{R}$ il est discret. Comme $Z(\mathcal{R})$ contient $\mathbb{Z}$ et n'est pas contenu dans $\mathbb{R}$, c'est un réseau d'après II.4. Enfin, il existe un élément basique $\delta \in Z(\mathcal{R}) \cap \mathbb{R} = \mathbb{Z}$ (d'après II.2.b) et l'on a $\delta\mathbb{Z} = \mathbb{Z}$ (d'après II.2.c), donc $\delta = \pm 1$. Cela prouve que 1 est basique. Autrement dit, le réseau $Z(\mathcal{R})$ admet une base de la forme $(1, \tau)$.

   d) D'après III.1.c), $\tau^2 \in Z(\mathcal{R})$, donc il existe $a, b \in \mathbb{Z}$ tels que $\tau^2 = a+b\tau$. Autrement dit, τ est racine du polynôme $X^2 + pX + q$ où $p = -b$ et $q = -a$ sont des entiers. Le trinôme $X^2 + pX + q$ admet une racine non réelle (τ) donc son discriminant est strictement négatif. On a donc $p^2 - 4q < 0$ et $4q = p^2 - (p^2 - 4q) > 0$, donc $q > 0$.

   e) Ecrivons $p = 2k+p'$ avec $p' = 0$ ou $p' = 1$. Posons $\tau' = \tau+k$. Puisque $(1, \tau)$ est une base de $Z(\mathcal{R})$, il en va de même pour $(1, \tau')$. Or τ' est racine du trinôme $(X-k)^2+p(X-k)+q = X^2+p'X+q'$ avec et $q' = k^2 - pk + q$.

IV. Rotations de centre 0 laissant stable un réseau

1. Un élément non réel de $\mathbb{Z}[\tau]$ s'écrit $a + b\tau$ avec $b \neq 0$.

   a) Lorsque $\tau = i\sqrt{q}$, on a $|a + b\tau|^2 = a^2 + qb^2$. Le module sera minimum si $|a|$ et $|b|$ sont les plus petits possibles soit $a = 0$ et $b = \pm 1$.

b) Si $\tau = \frac{1}{2}(-1+i\sqrt{4q-1})$, on a $4|a+b\tau|^2 = (2a-b)^2+(4q-1)b^2$. En particulier $|\tau|^2 = q$. Puisque $|b| \geqslant 1$, on ne peut avoir $(2a-b)^2 + (4q-1)b^2 \leqslant 4q$ à moins que $|b| = 1$ et $|2a-b| \leqslant 1$. Cela donne les 4 points suivants : τ, $-\tau$, $\tau+1$ et $-\tau-1$.

2. Les rotations de centre 0 qui laissent $\mathbb{Z}[\tau]$ invariant sont des similitudes de module 1 qui laissent $\mathbb{Z}[\tau]$ invariant. Ce sont donc des multiplications par des éléments de module 1 de $\mathbb{Z}[\tau]$. Le module d'un élément non réel de $\mathbb{Z}[\tau]$ est $\geqslant \sqrt{q}$ d'après la question précédente.
   * Si $q \neq 1$ les seules rotations possibles sont la multiplication par ± 1.
   * Si $q = 1$ et $p = 0$ ($\tau = i$) on obtient les multiplications par ± 1 et $\pm i$ soit les rotations d'angle $k\pi/2$.
   * Si $q = 1$ et $p = 1$ ($\tau = j$) on obtient les multiplications par ± 1, $\pm\tau$ et $\pm\tau + 1$ soit les rotations d'angle $k\pi/3$.

3. a) Soit $u_0 \in I$. Comme I est contenu dans $\mathcal{R}$ qui est discret, l'ensemble $\{u \in I \setminus \{0\};\ |u| \leqslant |u_0|\}$ est fini, donc il existe un élément u de module minimum dans cet ensemble. On aura bien $|u| \leqslant |w|$ pour tout $w \in I \setminus \{0\}$.

   b) Posons $v = \tau u$. Comme I est un idéal, on a bien $v \in I$; comme $|v| = |u|$, on a bien $|v| = \min\{w;\ w \in I \setminus \mathbb{R}u\}$. Par II.4. le réseau I est égal à $\mathcal{R}(u, v)$.

   c) On a démontré que tout idéal non nul de I est de la forme $\mathcal{R}(u, \tau u) = u\mathbb{Z}[\tau]$. Donc l'anneau $\mathbb{Z}[\tau]$ est principal.

4. Soit I un idéal non nul de $\mathbb{Z}[\tau]$. Soit $u \in I$ un élément non nul de module minimum. Comme $\tau u \in I$, I n'est pas contenu dans $\mathbb{R}u$. Soit $v \in I$ un élément non colinéaire à u de module minimum. D'après II.4, on a $I = \mathcal{R}(u, v)$.

   Posons $q = \frac{v}{u}$. Comme $|u| \leqslant |v|$ on a $|q| \geqslant 1$. Comme $|v \pm u| \geqslant |v|$, il vient $|q \pm 1| \geqslant |q|$ et comme q et $q \pm 1$ ont même partie imaginaire, il vient $|(\operatorname{Re} q) \pm 1| \geqslant |\operatorname{Re} q|$ ce qui donne $|\operatorname{Re} q| \leqslant \frac{1}{2}$. Enfin, puisque $|q| \geqslant 1$, il vient $(\operatorname{Im} q)^2 \geqslant 1 - \frac{1}{4}$, soit $|\operatorname{Im} q| \geqslant \frac{\sqrt{3}}{2}$.

   Puisque $\tau u \in I = \mathcal{R}(u, v)$, il existe $a, b \in \mathbb{Z}$ tels que $\tau u = au + bv$, soit $\tau = a + bq$. On a donc $\operatorname{Im}\tau = b\operatorname{Im} q$. Comme $\operatorname{Im}\tau < \sqrt{3}$ cela impose $b = \pm 1$, donc $I = \mathcal{R}(u, v) = \mathcal{R}(u, \tau u) = u\mathbb{Z}[\tau]$ donc $\mathbb{Z}[\tau]$ est principal.