

Examen d'Algèbre - Semestre N°1  
Section : M.P.1

Durée : 2 Heures

Date : 18 Décembre 2024

## Problème 1 (10 points)

## Partie I

On se donne deux groupes  $(G, \star)$  et  $(G', \cdot)$  d'éléments neutres respectifs  $e$  et  $e'$ .  
Soit  $\varphi : G \rightarrow G'$  une application vérifiant

$$\forall x, y \in G, \varphi(x \star y) = \varphi(x) \cdot \varphi(y).$$

$\varphi$  est dite un morphisme de groupes.

1. (a) En écrivant  $e \star e = e$ , montrer que  $\varphi(e) = e'$ .  
(b) Dédire que pour tout  $x \in G$ ,  $\varphi(x^{-1}) = \varphi(x)^{-1}$ .  
(c) i. Montrer que  $(\mathbb{R}_+^*, \times)$  est un groupe.  
ii. Vérifier que l'application  $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$  est un morphisme de groupes.
2. On note  $\ker(\varphi) = \varphi^{-1}(\{e'\})$ .  
(a) Montrer que  $\ker(\varphi)$  est un sous groupe de  $G$ .  
(b) Dédire que  $\varphi$  est injective si et seulement si,  $\ker(\varphi) = \{e\}$ .
3. On rappelle l'espace  $M_2(\mathbb{R})$ , l'ensemble des matrices carrées de taille 2.  
Pour toute matrice  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , on note  $\det(M) = ad - bc$ .  
(a) Montrer que pour tout  $M, N \in M_2(\mathbb{R})$ ,  $\det(MN) = \det(M) \det(N)$ .  
(b) Montrer que si  $M$  est inversible alors  $\det(M) \neq 0$  et donner  $\det(M^{-1})$  en fonction de  $\det(M)$ .  
(c) Montrer que si  $rg(M) < 2$  alors  $\det(M) = 0$ , où  $rg$  désigne le rang de la matrice  $M$ .  
(d) Dédire que  $M$  est inversible si et seulement si,  $\det(M) \neq 0$ .  
(e)  $(GL_2(\mathbb{R}), \times)$  désigne le groupe des matrices inversibles de taille 2.  
i. Montrer que l'application  $\det : (GL_2(\mathbb{R}), \times) \rightarrow (\mathbb{R}^*, \times)$  est un morphisme de groupes.  
ii. Montrer que le morphisme  $\det$  est surjectif et non injectif.

## Partie II

Dans cette partie  $M_2(\mathbb{Z}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ tel que } a, b, c, d \in \mathbb{Z} \right\}$ , et  
 $GL_2(\mathbb{Z}) = \{ M \in M_2(\mathbb{Z}) \text{ telle que } M \text{ est inversible et } M^{-1} \in M_2(\mathbb{Z}) \}$ .

1. (a) Soit  $M = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ .
  - i. Montrer que  $M$  est inversible
  - ii. Calculer  $M^{-1}$  par la méthode de pivot de Gauss et en déduire que  $M^{-1} \notin M_2(\mathbb{Z})$ .
2. Soit  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$  et soit  $A^{-1} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ .
  - (a) En évaluant  $AA^{-1}$  et  $A^{-1}A$ , montrer que  $a \wedge b = a \wedge c = 1$  et  $d \wedge b = d \wedge c = 1$
  - (b) Montrer qu'il existe  $\alpha \in \mathbb{Z}$  tel que  $A^{-1} = \begin{pmatrix} d\alpha & -b\alpha \\ -c\alpha & a\alpha \end{pmatrix}$  et  $\alpha \det(A) = 1$ .  
(Indication : On distinguera les trois cas  $a = 0$ ,  $c = 0$  et  $ac \neq 0$ .)
  - (c) Déduire que  $A^{-1} = \det(A) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$  et que  $\det(A) \in \{-1, 1\}$ .
  - (d)
    - i. Montrer que pour tout  $A \in M_2(\mathbb{Z})$ ,  $A^{-1} \in M_2(\mathbb{Z})$  si et seulement si  $\det(A) \in \{-1, 1\}$ .
    - ii. Déduire que  $GL_2(\mathbb{Z})$  est un sous groupe de  $(GL_2(\mathbb{R}), \times)$ .
3. (a) Montrer que  $\{-1, 1\}$  est un sous groupe de  $(\mathbb{R}^*, \times)$ 
 (b) Déduire que l'application  $\det : (GL_2(\mathbb{Z}), \times) \rightarrow (\{-1, 1\}, \times)$  est un morphisme de groupes surjectif et non injectif.
 (c) Montrer que  $SL_2(\mathbb{Z}) = \{A \in GL_2(\mathbb{Z}) \text{ tel que } \det(A) = 1\}$  est un sous groupe de  $(GL_2(\mathbb{Z}), \times)$ .
4. On note  $O_2(\mathbb{Z}) = \{M \in M_2(\mathbb{Z}) \mid ({}^t A)A = I_2\}$  où  ${}^t A$  désigne la matrice transposée de  $A$  et  $I_2$  est la matrice unité de  $M_2(\mathbb{R})$ .
  - (a) Montrer que pour tout  $A \in O_2(\mathbb{Z})$ ,  $A$  est inversible et donner  $A^{-1}$
  - (b) Déduire que  $O_2(\mathbb{Z})$  est un sous groupe de  $(GL_2(\mathbb{Z}), \times)$ .
  - (c) Montrer que pour tout  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2(\mathbb{Z})$  on a  $a = d = 0$  ou  $b = c = 0$ .
  - (d) Déduire que  $O_2(\mathbb{Z})$  est fini et donner ses éléments.

### Problème 2(10 points)

Dans tout le problème, on note  $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \text{ tel que } a, b \in \mathbb{Z}\}$ . On appelle cet ensemble, l'anneau des entiers de Gauss. On peut donc écrire :  $z \in \mathbb{Z}[i] \Leftrightarrow \exists a, b \in \mathbb{Z} \text{ tels que } z = a + ib$ . Pour tout  $z \in \mathbb{Z}[i]$ , on note  $N(z) = z\bar{z} = |z|^2 \in \mathbb{N}$

#### Partie I

1. Montrer que  $\mathbb{Z}[i]$  est un sous anneau de  $(\mathbb{C}, +, \times)$ .
2. Vérifier que  $\forall z, z' \in \mathbb{Z}, N(zz') = N(z)N(z')$ .
3. On note  $\mathcal{U} = \{z \in \mathbb{Z}[i] \text{ tel qu'il existe } z' \in \mathbb{Z}[i] \text{ avec } zz' = 1\}$  l'ensemble des éléments inversibles de l'anneau  $\mathbb{Z}[i]$ .
  - (a) Montrer que  $\mathcal{U} = \{z \in \mathbb{Z}[i] \text{ tel que } N(z) = 1\}$ .
  - (b) Déduire que  $\mathcal{U} = \{-1, 1, -i, i\}$ .

**N.B :** Dans la suite les parties II et III sont indépendantes.

## Partie II

D'une façon analogue à la divisibilité dans  $\mathbb{Z}$ , pour tous entiers de Gauss  $u, v \in \mathbb{Z}[i]$ , on dit que  $v$  divise  $u$  s'il existe  $q \in \mathbb{Z}[i]$  tel que  $u = vq$ . On dit que  $p \in \mathbb{Z}[i]$  est irréductible si :  
 $p$  n'est pas inversible dans  $\mathbb{Z}[i]$  et pour tout  $a, b \in \mathbb{Z}[i]$ ,  $p = ab$ , alors  $a \in \mathcal{U}$  ou  $b \in \mathcal{U}$ .

1. Soit  $p \in \mathbb{Z}[i]$  un entier de Gauss irréductible. Donner l'ensemble des diviseurs de  $p$ .
2. Montrer que si  $\forall p \in \mathbb{Z}[i]$ , si  $N(p)$  est premier dans  $\mathbb{Z}$  alors  $p$  est nécessairement irréductible.
3. Vérifier que 3 est irréductible dans  $\mathbb{Z}[i]$ , en déduire que la réciproque de la propriété précédente est fausse.
4. L'entier 5 est-il irréductible dans  $\mathbb{Z}[i]$  ?

## Partie III

Dans cette partie, nous allons définir une sorte de division euclidienne sur  $\mathbb{Z}[i]$ . Soit  $u, v \in \mathbb{Z}[i]$  tels que  $v \neq 0$ , et soit  $\frac{u}{v} = x + iy \in \mathbb{C}$ ,  $x, y \in \mathbb{R}$  ( $\frac{u}{v}$  n'est pas forcément entier de Gauss).

1. On désigne par  $n$  et  $m$  les parties entières respectives de  $x$  et de  $y$ . On note  $z_0 = n + im$ ,  $z_1 = n + i(m+1)$ ,  $z_2 = (n+1) + im$  et  $z_3 = (n+1) + i(m+1)$ . Montrer qu'il existe  $k \in \{0, 1, 2, 3\}$  tel que  $|z_k - \frac{u}{v}| \leq \frac{\sqrt{2}}{2}$  (faites une figure).
2. Soit  $q \in \{z_0, z_1, z_2, z_3\}$  tel que  $|\frac{u}{v} - q|$  soit minimale. Montrer que  $N(u - qv) < N(v)$ .
3. En déduire qu'il existe  $r \in \mathbb{Z}[i]$  tel que  $u = vq + r$  avec  $N(r) < N(v)$ . (Dite la division euclidienne de  $u$  par  $v$ )
4. Effectuer la division euclidienne de  $5 + 3i$  par  $1 + i$ .