PROBLÈME 1

Partie I : Groupe de Heisenberg d'un anneau

Soit $(A, +, \times)$ un anneau. On note $\mathcal{M}_3(A)$ l'ensemble des matrices $M = (m_{i,j})_{1\leq i,j\leq 3}$ avec $\forall (i,j) \in [\![1,3]\!]^2, m_{i,j} \in A$. On munit $\mathcal{M}_3(A)$ de l'addition et la multiplication des matrices, si $M = (m_{i,j})_{1\leq i,j\leq 3}$ et $M' = (m'_{i,j})_{1\leq i,j\leq 3}$ alors $M + M' = (m_{i,j} + m'_{i,j})_{1\leq i,j\leq 3}$ et $M \times M' = (c_{i,j})_{1\leq i,j\leq 3}$ avec $c_{i,j} = \sum_{k=1}^{3} m_{i,k} \times m'_{k,j}$. On admet que $(\mathcal{M}_3(A), +, \times)$ est un anneau et on note $\mathbf{GL}_3(A)$ son groupe des inversibles. On définit :

$$\mathcal{H}_3(A) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} / (a,b,c) \in A^3 \right\}.$$

1. Démontrer que $\mathcal{H}_3(A)$ est un sous-groupe de $\mathbf{GL}_3(A)$. On l'appelle le groupe de **Heisenberg** de l'anneau A.
2. On munit A^3 de la loi de composition interne $\star$ tel que pour tout $X = (x,y,z)$ et tout $Y = (a,b,c)$ éléments de A^3, on a $X \star Y = (x+a, y+b, z+c+xb)$.
   - a. Démontrer que $(A^3, \star)$ est un groupe isomorphe à $(\mathcal{H}_3(A), \times)$.
   - b. Préciser l'élément neutre e de $(A^3, \star)$
   - c. Si $X = (x,y,z)$ et X^{-1} le symétrique de X dans $(A^3, \star)$ exprimer X^{-1} en fonction de x, y et z.
   - d. Si $X = (x,y,z) \in A^3$, exprimer $X^n = \underbrace{X \star \cdots \star X}_{n \text{ fois}}$ en fonction de x, y, z et n pour tout $n \in \mathbb{N}^*$.
   - e. Soit $X = (x,y,z)$ et $Y = (a,b,c)$ deux éléments de A^3. Calculer $[X,Y] = X \star Y \star X^{-1} \star Y^{-1}$.
3. On notre $Z(\mathcal{H}_3(A)) = \{M \in \mathcal{H}_3(A) / \forall X \in \mathcal{H}_3(A), M \times X = X \times M\}$. Démontrer que $Z(\mathcal{H}_3(A))$ est un sous-groupe de $\mathcal{H}_3(A)$ et que les groupes $(Z(\mathcal{H}_3(A)), \times)$ et $(A, +)$ sont isomorphes.

Le groupe de Heisenberg de $\mathbb{Z}/2\mathbb{Z}$

1. Démontrer que :
   - a. Tout groupe de cardinal p avec p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$
   - b. Tout groupe de cardinal 2 est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
   - c. Tout groupe de cardinal 4 est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit à $(\mathbb{Z}/2\mathbb{Z})^2$.
2. Démontrer que les groupes additifs $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ et $\mathbb{Z}/2Z \times \mathbb{Z}/4\mathbb{Z}$ sont deux à deux non isomorphes.
3. On note $G = \mathcal{H}_3(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} \overline{1} & a & b \\ \overline{0} & \overline{1} & c \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} / a,b,c \in \mathbb{Z}/2\mathbb{Z} \right\}$, le groupe de **Heisenberg** de $\mathbb{Z}/2\mathbb{Z}$.
   - a. Que vaut $\operatorname{card}(\mathcal{M}_3(\mathbb{Z}/2\mathbb{Z}))$?
   - b. Démontrer $\operatorname{card}(G) = 8$ et que $(G, \times)$ n'est pas commutatif.
   - c. Dites si les assertions suivantes sont vraies ou fausses et bien justifier votre réponse :
     - i. Tout élément de G est d'ordre fini.
     - ii. Le groupe G est cyclique.
     - iii. Le groupe G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$
     - iv. Le groupe G est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
   - d. Démontrer que si H est un sous-groupe H de G tel que $H \neq G$ alors H est commutatif.

4 On rappelle que $\mathscr{S}(\mathbb{C})$ ensemble des bijections de $\mathbb{C}$ vers $\mathbb{C}$ muni de la composition des applications est un groupe. On notre φ et ψ les applications de $\mathbb{C}$ vers $\mathbb{C}$ définies par $\forall z \in \mathbb{C}, \quad \begin{cases} \varphi(z) = \overline{z} \\ \psi(z) = iz \end{cases}$ et on note Γ le sous-groupe de $\mathscr{S}(\mathbb{C})$ engendré par φ et ψ, c'est-à-dire $\Gamma = \langle \varphi, \psi \rangle$.

- **a** Démontrer que $H = \langle \varphi \rangle$ et $K = \langle \psi \rangle$ sont deux sous-groupes cycliques de Γ et préciser $\text{card}(H)$ et $\text{card}(K)$.
- **b** On définit $HK = \{f \circ g / f \in H, g \in K\}$. Démontrer que $HK = KH = \Gamma$.
- **c** En déduire $\text{card}(\Gamma)$ et la forme générale d'un élément de Γ.

5 **a** Démontrer que les groupe $(G, \times)$ et $(\Gamma, \circ)$ sont isomorphes.

- **b** En déduire que $G = G_1 G_2$ avec G_1 et G_2 deux groupes cycliques isomorphes respectivement à $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

Une représentation dans $\mathbf{GL}_2(\mathbb{R})$ et dans $\mathscr{S}_4$

On considère les matrices carrées de $\mathbf{GL}_2(\mathbb{R})$ suivantes : $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et soit $\mathcal{G} = \langle R, S \rangle$ le sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ engendré par $\{R, S\}$ et $\mathcal{H} = \langle R \rangle$ le sous-groupe engendré par R.

1 Démontrer que $\langle R \rangle$ est cyclique de cardinal 4 et que tout élément de $\mathcal{G}$ est de la forme $\prod_{k=1}^{m} M_k$ avec $m \in \mathbb{N}^*$ et pour tout $k \in [\![1, m]\!]$, $M_k \in \{R, R^3, S\}$

2 Démontrer que $\forall p \in \mathbb{Z}, \exists q \in \mathbb{Z}, R^p S = S R^q$. En déduire que $\text{card}(\mathcal{G}) = 8$ et préciser les éléments de $\mathcal{G}$.

3 Démontrer que $(\mathcal{G}, \times)$ et $(G, \times)$ sont isomorphes et en déduire les ordres possibles des éléments de G en citant les éléments respectifs ayant un ordre donné.

4 Dans le groupe symétrique $\mathscr{S}_4$, on considère le cycle $s = (1, 2, 3, 4)$ et la permutation $t = (1, 2) \circ (3, 4)$ produit des transpositions $(1, 2)$ et $(3, 4)$. Démontrer que $G \simeq \langle s, t \rangle$.

PROBLÈME 2

Dans tout le problème θ est un nombre réel tel qu'il existe un polynôme non nul P de $\mathbb{Q}[X]$ tel que $P(\theta) = 0$.

1 **a** Démontrer qu'il existe un et un seul polynôme M_θ unitaire et irréductible dans $\mathbb{Q}[X]$ tel que $M_\theta(\theta) = 0$.

- **b** Exprimer M_θ dans chacun des cas particuliers suivants :
  - **i** Si on suppose que $\theta \in \mathbb{Q}$.
  - **ii** Si on suppose que $\theta = \sqrt{2}$.

2 Soit $M \in \mathbb{Q}[X]$ un polynôme irréductible.

- **a** Démontrer que pour tout polynôme $P \in \mathbb{Q}[X]$ on a $P \wedge M_\theta = 1 \Leftrightarrow P(\theta) \neq 0$
- **b** En déduire que si $P(\theta) \neq 0$ alors il existe un polynôme $Q \in \mathbb{Q}[X]$ tel que $\frac{1}{P(\theta)} = Q(\theta)$.

3 On note $\mathbb{Q}(\theta) = \{P(\theta) / P \in \mathbb{Q}[X]\}$.

- **a** Démontrer que $\mathbb{Q}(\theta)$ est un sous-corps de $\mathbb{R}$.
- **b** Montrer que l'on peut considérer $\mathbb{R}$ comme un espace vectoriel sur $\mathbb{Q}$ et que $\mathbb{Q}(\theta)$ est un sous-espace vectoriel de dimension finie du $\mathbb{Q}-$espace vectoriel $\mathbb{R}$.
- **c** On suppose que $\deg(M_\theta) = d$. Justifier que $d \geq 1$ et que $\mathbb{Q}(\theta) = \text{Vect}(1, \theta, \ldots, \theta^{d-1})$.
- **d** Donner alors une relation simple entre $\dim(\mathbb{Q}(\theta))$ est $d = \deg(M_\theta)$.

4 Dans cette question, on suppose que $\theta = \sqrt{2} + \sqrt{3}$ et on note $M(X) = X^4 - 10X^2 + 1$.

- **a** Démontrer que $M(X)$ n'a aucune racine rationnelle.
- **b** On suppose que $M(X) = (X^2 + aX + b)(X^2 + cX + d)$ avec $a, b, c, d \in \mathbb{Q}$.
  - **i** Démontrer que les polynômes $X^2 + aX + b$ et $X^2 + cX + d$ sont irréductibles.
  - **ii** Démontrer que $M(X) = (X^2 - aX + b)(X^2 - cX + d)$.
  - **iii** En déduire que $a = c = 0$ ou $M = (X^2 + aX + b)(X^2 - aX + b)$
- **c** Déduire de ce qui précède que M est irréductible et que $M_\theta = X^4 - 10X + 1$.
- **d** Démontrer que les familles $\Theta = (1, \theta, \theta^2, \theta^3)$ et $\mathscr{C} = (1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ sont des bases du $\mathbb{Q}-$espace vectoriel $\mathbb{Q}(\theta)$ et determiner U la matrice de passage de Θ à $\mathscr{C}$ ainsi que U^{-1}.