• *Les calculatrices ne sont pas autorisées.*
• *Je vous conseille de bien lire chaque énoncé entièrement avant de vous lancer, de souligner ou de surligner les points ou notations importants.*
• *Les trois exercices peuvent être traités dans l'ordre que vous souhaitez, mais vous devez l'indiquer clairement sur votre copie.*
• *La présentation, la lisibilité et la qualité de la rédaction des copies font l'objet d'une appréciation spécifique. En particulier, les résultats doivent être encadrés à la règle.*
• *Si vous repérez une erreur d'énoncé, vous l'indiquez sur votre copie et expliquez les raisons des initiatives que vous prenez.*

Exercice 1 - Groupe de Heisenberg

On considère un corps $\mathbb{K}$ et l'ensemble des matrices carrées $\mathcal{M}_3(\mathbb{K})$ de taille 3 sur le corps $\mathbb{K}$. Pour tout triplet $(x,y,z)\in\mathbb{K}^3$, on note

$$h(x,y,z)=\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}$$

On note de plus

$$\mathcal{H}_3(\mathbb{K})=\left\{h(x,y,z)\,|\,(x,y,z)\in\mathbb{K}^3\right\}$$

1. Montrer que
$$\forall(x,y,z,x',y',z')\in\mathbb{K}^6,\quad h(x,y,z)h(x',y',z')=h(x+x',y+y',z+z'+xy')$$
2. Montrer que pour tout triplet (x,y,z) dans $\mathbb{K}^3$, la matrice $h(x,y,z)$ est inversible et que son inverse est donné par
$$h(x,y,z)^{-1}=h(-x,-y,-z+xy)$$
3. En déduire que $\mathcal{H}_3(\mathbb{K})$ est un sous-groupe de $\mathrm{GL}_3(\mathbb{K})$, le groupe linéaire d'ordre 3 sur le corps $\mathbb{K}$.
4. Montrer que
$$\forall n\in\mathbb{N},\forall(x,y,z)\in\mathbb{K}^3,\quad h(x,y,z)^n=h\left(nx,ny,nz+\frac{n(n-1)}{2}xy\right)$$
5. Le groupe $\mathcal{H}_3(\mathbb{K})$ est-il commutatif ?
6. On munit $\mathbb{K}^2$ de sa structure additive de groupe produit, i.e
$$\forall(x,y,x',y')\in\mathbb{K}^4,\quad (x,y)+(x',y')=(x+x',y+y').$$
On introduit l'application
$$\begin{array}{rccc} f & : & \mathcal{H}_3(\mathbb{K}) & \to & \mathbb{K}^2\\ & & h(x,y,z) & \mapsto & (x,y)\end{array}$$
Montrer que l'application f est un morphisme de groupes.
7. Quel est le noyau de l'application f ? En particulier, f est-elle injective ?
8. On munit à présent $\mathbb{K}^3$ de sa structure additive de groupe produit, i.e
$$\forall(x,y,z,x',y',z')\in\mathbb{K}^6,\quad (x,y,z)+(x',y',z')=(x+x',y+y',z+z')$$
Montrer que l'application
$$\begin{array}{rccc} g & : & \mathcal{H}_3(\mathbb{K}) & \to & \mathbb{K}^3\\ & & h(x,y,z) & \mapsto & (x,y,z)\end{array}$$
n'est pas un morphisme de groupes.

Exercice 2 - Les entiers de Gauss

On se place dans l'anneau $\mathbb{C}$ (qui se trouve être un corps). On note

$$\mathbb{Z}[\mathrm{i}] = \left\{ a + b\mathrm{i} \,|\, (a,b) \in \mathbb{Z}^2 \right\}$$

Les éléments de l'ensemble $\mathbb{Z}[\mathrm{i}]$ sont appelés des entiers de Gauss.

1. L'anneau $\mathbb{Z}[\mathrm{i}]$.
   (a) Montrer que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$.
   (b) Montrer que $\mathbb{Z}[\mathrm{i}]$ un anneau commutatif, puis qu'il est intègre.
   (c) On introduit l'application
   $$\begin{array}{rccc} \mathrm{N} & : & \mathbb{Z}[\mathrm{i}] & \to & \mathbb{N} \\ & & a+b\mathrm{i} & \mapsto & a^2+b^2 \end{array}$$
   Montrer que
   $$\forall (z,z') \in \mathbb{Z}[\mathrm{i}]^2, \quad \mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$$
   (d) Soit $z \in \mathbb{Z}[\mathrm{i}]$. Montrer que z est inversible dans $\mathbb{Z}[\mathrm{i}]$ si et seulement si $\mathrm{N}(z) = 1$.
   (e) En déduire la liste des éléments inversibles de $\mathbb{Z}[\mathrm{i}]$.
2. L'anneau euclidien $\mathbb{Z}[\mathrm{i}]$.
   (a) Soit $(z,w) \in \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]^*$. Montrer qu'il existe un couple (q,r) dans $(\mathbb{Z}[\mathrm{i}])^2$ tel que
   $$z = qw + r \quad \text{et} \quad 0 \leq \mathrm{N}(r) < \mathrm{N}(w)$$
   Indication : on pourra placer le complexe z/w dans un quadrillage de $\mathbb{C}$
   (b) Déterminer un tel couple (q,r) pour $z = 7 + 2\mathrm{i}$ et $w = 2 + 3\mathrm{i}$.
3. On dit qu'un élément z de $\mathbb{Z}[\mathrm{i}]$ est irréductible lorsque z est non nul, non inversible et
   $$\forall (s,t) \in \mathbb{Z}[\mathrm{i}]^2, z = st \Rightarrow s \text{ ou } t \text{ est inversible}$$
   (a) Montrer que 3 est irréductible dans $\mathbb{Z}[\mathrm{i}]$, mais que 2 ne l'est pas.
   (b) Soit (w,a,b) un triplet de $\mathbb{Z}[\mathrm{i}]$. On suppose que w est irréductible, puis que w divise ab, i.e qu'il existe un entier de Gauss v tel que $vw = ab$. Montrer qu'alors w divise a ou b.
   Indication : Raisonner par l'absurde, et prendre un triplet absurde avec b tel que $\mathrm{N}(b)$ est minimal.
   (c) Soit p un entier premier dans $\mathbb{Z}$. On suppose qu'il existe deux entiers naturels a et b tels que $p = a^2 + b^2$. Montrer que $w = a + \mathrm{i}b$ et $\overline{w} = a - \mathrm{i}b$ sont irréductibles dans $\mathbb{Z}[\mathrm{i}]$.
   (d) Avec les mêmes hypothèses et notations qu'en question précédente, montrer que
   $$\forall z \in \mathbb{Z}[\mathrm{i}], \mathrm{N}(z) = p \Rightarrow \exists u \in \{1,-1,\mathrm{i},-\mathrm{i}\}, z = u(a+\mathrm{i}b) \text{ ou } z = u(a-\mathrm{i}b)$$
   (e) On considère q un entier premier dans $\mathbb{Z}$. On suppose qu'il ne s'écrit pas comme somme de deux carrés d'entiers naturels. Montrer qu'alors q est irréductible dans $\mathbb{Z}[\mathrm{i}]$.

Exercice 3 - Une extension quadratique

1. (a) Soit $\mathbb{K}$ un sous-corps de $(\mathbb{C}, +, \times)$. Montrer que $\mathbb{K}$ contient $\mathbb{Q}$.
   Indication : on pourra commencer par montrer par récurrence que $\mathbb{K}$ contient $\mathbb{N}$.

   (b) Soit A une partie de $\mathbb{C}$. On note

$$\mathbb{Q}(A) = \bigcap_{\substack{\mathbb{K} \text{ sous-corps de } \mathbb{C} \\ A \subset \mathbb{K}}} \mathbb{K}$$

   l'intersection de tous les sous-corps de $\mathbb{C}$ qui contiennent A. Montrer que $\mathbb{Q}(A)$ est un sous-corps de $\mathbb{C}$, et que c'est le plus petit qui contient A.

   (c) Dans le cas particulier où $A = \left\{\sqrt{2}\right\}$, démontrer que $\mathbb{Q}\left(\left\{\sqrt{2}\right\}\right) = \left\{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\right\}$.

   Indication : on pourra commencer par montrer que $\left\{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\right\}$ est un sous-corps de $\mathbb{C}$.

   On le note plus légèrement $\mathbb{Q}\left(\sqrt{2}\right)$ dans ce qui suit.

2. On considère f un morphisme de corps de $\mathbb{Q}\left(\sqrt{2}\right)$ dans $\mathbb{Q}\left(\sqrt{2}\right)$.

   (a) Montrer que $\forall x \in \mathbb{Q}$, $f(x) = x$.

   (b) Montrer que $f\left(\sqrt{2}\right) = \sqrt{2}$ ou $f\left(\sqrt{2}\right) = -\sqrt{2}$.

   (c) En déduire la liste des automorphismes de corps de $\mathbb{Q}\left(\sqrt{2}\right)$, i.e des morphismes bijectifs de $\mathbb{Q}\left(\sqrt{2}\right)$ dans lui-même. On montrera en particulier qu'il n'y en a que deux.

3. (a) Soit $(a,b) \in \mathbb{Q}^2$ et $z = a + b\sqrt{2}$. Montrer qu'il existe un polynôme non nul unitaire $P \in \mathbb{Q}[X]$ (donc à coefficients dans $\mathbb{Q}$) tel que $P(z) = 0$. Parmi ces polynômes, déterminer celui de plus petit degré (on ne demande pas de démontrer son unicité).

   (b) On suppose que $2a \in \mathbb{Z}$, et que $a^2 - 2b^2 \in \mathbb{Z}$. En écrivant b sous forme irréductible $b = r/s$, montrer par l'absurde que $a \in \mathbb{Z}$. En déduire que $b \in \mathbb{Z}$.