DM n°8

Deuxième page facultative.

Quelques indications au dos.

Exercice 1. Déterminant dans $\mathcal{M}_2(\mathbb{C})$, et étude du groupe $GL_2(\mathbb{Z})$.

1) Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$. Montrer que

$$A^2 - (a+d)A + (ad-bc)I_2 = O_2.$$

On rappelle qu'une matrice $A \in \mathcal{M}_2(\mathbb{C})$ est dite inversible s'il existe une matrice $B \in \mathcal{M}_2(\mathbb{C})$ telle que $AB = BA = I_2$.

2) En déduire que A est inversible si et seulement si $ad - bc \neq 0$.
Si A est inversible, justifier que

$$A^{-1} = \frac{1}{ad-bc}\big((a+d)I_2 - A\big).$$

Pour $A \in \mathcal{M}_2(\mathbb{C})$, on note $\det A = ad - bc$, appelé déterminant de la matrice A. D'après la question précédente, A est inversible si et seulement si $\det A \neq 0$.

3) Montrer que

$$\forall A, B \in \mathcal{M}_2(\mathbb{C}), \quad \det(AB) = \det A \det B.$$

4) Pour A inversible, montrer que $\det(A^{-1}) = \frac{1}{\det A}$.

5) Soit $A \in M_2(\mathbb{Z})$. Montrer que A est inversible et $A^{-1} \in \mathcal{M}_2(\mathbb{Z})$ si et seulement si $\det A = \pm 1$.

6) On note $GL_2(\mathbb{Z})$ l'ensemble des matrices 2-2 inversibles à coefficients entiers dont l'inverse est à coefficients entiers.
Justifier que $GL_2(\mathbb{Z})$ forme un groupe pour la multiplication matricielle.

7) On note $A\mathbb{Z}^2 = \big\{AX,\ X \in \mathbb{Z}^2\big\} = \big\{A\begin{pmatrix} x \\ y \end{pmatrix},\ x, y \in \mathbb{Z}\big\}$.

a) Montrer que $A\mathbb{Z}^2 \subset \mathbb{Z}^2$ si et seulement si $A \in \mathcal{M}_2(\mathbb{Z})$.

b) Montrer que $A\mathbb{Z}^2 = \mathbb{Z}^2$ si et seulement si $A \in GL_2(\mathbb{Z})$.

Exercice 2. Structure des solutions de l'équation de Pell-Fermat.

I. Préliminaires

Soit d un entier naturel non nul. ★ Montrer que si d n'est pas un carré alors $\sqrt{d} \notin \mathbb{Q}$.

Dans la suite, d désigne un entier naturel tel que $\sqrt{d}$ soit irrationnel. On considère l'équation de Pell-Fermat :

$$(E) : \quad x^2 - dy^2 = 1,$$

d'inconnues $x, y \in \mathbb{Z}$. On note $\mathcal{S}$ l'ensemble des solutions de (E).

II. Structure de l'ensemble des solutions.

On note $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d},\ x, y \in \mathbb{Z}\}$.

1) a) Montrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $\mathbb{R}$.

b) Soit $z \in \mathbb{Z}[\sqrt{d}]$. Montrer qu'il existe un unique couple $(x, y) \in \mathbb{Z}^2$ tel que $z = x + y\sqrt{d}$.

c) Soient $x, y \in \mathbb{Z}$ et $z = x + y\sqrt{d}$. On pose $\overline{z} = x - y\sqrt{d}$ et $N(z) = z\overline{z} = x^2 - dy^2$. Montrer que

$$\forall z, z' \in \mathbb{Z}[\sqrt{d}], \quad \overline{zz'} = \overline{z}\,\overline{z'} \text{ et } N(zz') = N(z)N(z').$$

d) Soit $z \in \mathbb{Z}[\sqrt{d}]$. Montrer que z est inversible dans l'anneau $\mathbb{Z}[\sqrt{d}]$ si et seulement si $N(z) = \pm 1$.

2) a) Justifier que l'ensemble $U = \{z \in \mathbb{Z}[\sqrt{d}] \mid N(z) = 1\}$ des éléments de norme 1 forme un groupe et que $\mathcal{S}$ est en bijection canonique avec ce groupe U (il s'agit d'expliciter une bijection naturelle).
Pour $z = x + y\sqrt{d} \in U$, à quelles solutions de (E) correspondent les nombres $1/z$, $-z$ et $-1/z$?

b) Soit $z = x + y\sqrt{d} \in U$. Montrer que $z > 1$ si et seulement si $x \geqslant 1$ et $y \geqslant 1$.

3) ★ En utilisant l'alternative sur les sous-groupes de $(\mathbb{R}, +)$, montrer que tout sous-groupe multiplicatif G de $(\mathbb{R}_+^*, \times)$ est soit dense dans $\mathbb{R}_+^*$, soit monogène, c'est-à-dire qu'il existe $\delta > 0$ tel que $G = \{\delta^n,\ n \in \mathbb{Z}\}$.

4) On suppose, jusqu'à la fin de cette partie que (E) possède une solution non triviale, c'est-à-dire différente de $(\pm 1, 0)$. On pose $H = U \cap]1, +\infty[$.

a) Montrer que H est non vide.

b) Montrer qu'il existe $\delta > 1$ tel que $H = \{\delta^n,\ n \in \mathbb{N}^*\}$.

c) Soit $x_0 \geqslant 1$ et $y_0 \geqslant 1$ tels que $\delta = x_0 + y_0\sqrt{d}$. Montrer que (x_0, y_0) est une solution de (E), appelée solution fondamentale, et exprimer les autres solutions en fonction de x_0 et y_0.

5) Déterminer la solution fondamentale lorsque $d = 2$.

III. Existence de solutions non triviales.

1) Soit $\alpha \geqslant 0$.

a) Montrer que pour tout $n \in \mathbb{N}^*$, il existe $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$ tels que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$ et $q \leqslant n$.

On pourra considérer les éléments $0, \alpha - E(\alpha), 2\alpha - E(2\alpha), \ldots, (n-1)\alpha - E((n-1)\alpha), n\alpha - E(n\alpha)$ de $[0,1[$.

b) En déduire qu'il existe une infinité de couples $(p,q) \in \mathbb{N} \times \mathbb{N}^*$ pour lesquels $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

L'algorithme de décomposition en fraction continue permet de déterminer de tels couples.

2) **a)** Soit $(p,q) \in \mathbb{N} \times \mathbb{N}^*$ tels que $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$. Montrer que $|p^2 - dq^2| < 1 + 2\sqrt{d}$.

b) En déduire qu'il existe $k \in \mathbb{Z}^* \cap \left]-(1+2\sqrt{d}),1+2\sqrt{d}\right[$ tel que l'équation $x^2 - dy^2 = k$ possède une infinité de solutions.

3) **a)** Soit $k \in \mathbb{Z}^*$, $z_1 = x_1 + y_1\sqrt{2}$ et $z_2 = x_2 + y_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. On note $z_1 \equiv z_2[k]$ s'il existe $u \in \mathbb{Z}[\sqrt{d}]$ tel que $z_1 = z_2 + ku$. À quelles conditions sur x_i, y_i a-t-on $z_1 \equiv z_2[k]$? Combien y a-t-il sur $\mathbb{Z}[\sqrt{d}]$ de classes de congruence modulo k ?

b) Montrer qu'il existe $k \in \mathbb{Z}^*$ et $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ tels que $N(z_1) = N(z_2) = k$, $z_1 \equiv z_2[k]$ et $z_1 \neq \pm z_2$. Montrer que si l'on pose $z_1\overline{z_2} = x + y\sqrt{d}$ alors $x \equiv 1[k]$ et $y \equiv 0[k]$.

En considérant $u = \frac{1}{k}z_1\overline{z_2}$, établir l'existence d'une solution non triviale de (E).

Exercice 3. ★ Soit $A \subset \mathbb{R}_+$ stable par addition. Montrer l'alternative

(i) $\exists a \geqslant 0,\ A \subset a\mathbb{N}$.

(ii) $\forall \varepsilon > 0, \exists M > 0, \forall x \geqslant M,\ A \cap [x-\varepsilon, x+\varepsilon] \neq \varnothing$.

Indications Exercice 1.

5) Pour une implication, utiliser la question 2, et pour l'autre la question 4.

6) On montre que c'est un sous-groupe de l'ensemble des matrices inversibles.

Indications Exercice 2.

I. Considérer la décomposition en facteurs premiers de d. À quelle condition d n'est-il pas un carré ?

Indications Exercice 3. Pourquoi n'est-il, par exemple, pas possible que A contienne 1 et π ?