Devoir Surveillé n° 1.
le 20 septembre.

Exercice 1

Un anneau A commutatif est dit principal lorsque tout idéal de A est engendré par un élément.

1. Donner deux exemples d'anneaux principaux.

Partie 1 : Anneaux $\mathbb{Z}[\sqrt{n}]$

Soit n un entier naturel qui n'est pas le carré d'un entier. On désigne par $\mathbb{Z}[\sqrt{n}]$ l'ensemble des réels de la forme $a + b\sqrt{n}$, où a et b sont des entiers relatifs quelconques.

2. Montrer que l'application de $\mathbb{Z}^2$ dans $\mathbb{Z}[\sqrt{n}]$ définie par $(a, b) \mapsto a + b\sqrt{n}$ est bijective.
On pourra utiliser sans démonstration que : $\sqrt{n} \notin \mathbb{Q}$.

3. Montrer que $\mathbb{Z}[\sqrt{n}]$ est un sous-anneau de $\mathbb{R}$.

4. L'anneau $\mathbb{Z}[\sqrt{n}]$ est-il intègre ?

5. Montrer que l'application φ de $\mathbb{Z}[\sqrt{n}]$ dans $\mathbb{Z}[\sqrt{n}]$ définie par : $a + b\sqrt{n} \mapsto a - b\sqrt{n}$ est un morphisme d'anneau involutif de $\mathbb{Z}[\sqrt{n}]$.
Rappel : un endomorphisme φ est dit involutif lorsque $\varphi \circ \varphi = \mathrm{id}$.

6. Pour tout élément x de $\mathbb{Z}[\sqrt{n}]$, on considère le produit $N(x) = x\varphi(x)$.

a) Montrer que : $\forall x \in \mathbb{Z}[\sqrt{n}], \quad N(x) = 0 \Leftrightarrow x = 0$.

b) Montrer que $\forall (x, y) \in \mathbb{Z}[\sqrt{n}]^2, \quad N(xy) = N(x)N(y)$.

7. Montrer qu'un élément x de $\mathbb{Z}[\sqrt{n}]$ est inversible dans $\mathbb{Z}[\sqrt{n}]$ si et seulement si $N(x) = \pm 1$.

Partie 2 : Anneau $\mathbb{Z}[\sqrt{5}]$

8. Donner quelques exemples d'éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{5}]$. Démontrer qu'il y en a une infinité.

9. **a)** Soit $\gamma, \delta \in \mathbb{Z}/4\mathbb{Z}$, montrer que $\gamma^2 - 5\delta^2 \in \{\bar{0}, \bar{1}, \bar{3}\}$.

b) En déduire qu'il n'existe pas d'entiers relatifs c et d tels que $c^2 - 5d^2 = \pm 2$.

c) En déduire que l'élément 2 est irréductible dans l'anneau $\mathbb{Z}[\sqrt{5}]$, c'est à dire : $\forall x, y \in \mathbb{Z}[\sqrt{5}]$

$$xy = 2 \Rightarrow x \in \left(\mathbb{Z}[\sqrt{5}]\right)^* \text{ ou } y \in \left(\mathbb{Z}[\sqrt{5}]\right)^*$$

10. Soit I l'ensemble des éléments $x = a + b\sqrt{5}$ de $\mathbb{Z}[\sqrt{5}]$ tels que les entiers a et b soient de même parité. Démontrer que I est un idéal de l'anneau $\mathbb{Z}[\sqrt{5}]$.

11. On suppose que l'idéal I est engendré par un élément x.

a) Montrer qu'il existe des éléments y et z de $\mathbb{Z}[\sqrt{5}]$ tels que $2 = xy$ et $1 + \sqrt{5} = xz$.

b) Trouver une contradiction.

c) Que peut-on dire de l'anneau $\mathbb{Z}[\sqrt{5}]$.

Exercice 2 :Matrices d'ordre 2 à coefficients entiers

Soit $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs. On note $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. Démontrer que l'ensemble $\mathcal{M}_2(\mathbb{Z})$ est un anneau.

2. **a)** Démontrer que l'ensemble $GL_2(\mathbb{Z})$ des éléments de $\mathcal{M}_2(\mathbb{Z})$ inversibles dans $\mathcal{M}_2(\mathbb{Z})$ est un groupe pour la multiplication, il est appelé le groupe des unités de l'anneau $\mathcal{M}_2(\mathbb{Z})$ dans la suite de l'exercice.

b) Montrer l' équivalence : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ si et seulement si $|ad - bc| = 1$. On pourra utiliser la comatrice.

3. On pose $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) : ad - bc = 1 \right\}$.

a) Prouver que $SL_2(\mathbb{Z})$ est un groupe pour la multiplication des matrices.

b) Déterminer l'ensemble des couples $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ est dans $SL_2(\mathbb{Z})$.

c) Déterminer l'ensemble des couples $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice $\begin{pmatrix} 3 & 5 \\ c & d \end{pmatrix}$ est dans $GL_2(\mathbb{Z})$.

d) Quelle est la condition nécessaire et suffisante portant sur le couple (a, b) de $\mathbb{Z} \times \mathbb{Z}$ pour qu'il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartenant à $GL_2(\mathbb{Z})$?

4. On cherche les matrices A de $SL_2(\mathbb{Z})$ telles que $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

a) Soit A une telle matrice et $f : X \in \mathbb{R}^2 = \mathcal{M}_{2,1}(\mathbb{R}) \mapsto AX \in \mathbb{R}^2$ l'endomorphisme canoniquement associé à A. Quelle est la nature géométrique de f ? En déduire qu'il existe une base de $\mathbb{R}^2$ dans laquelle f admet une matrice diagonale B, en précisant les formes possibles de B. Quel lien y a-t-il entre A et B ?

b) En déduire l'ensemble des matrices solutions A.

Exercice 3 : Un algorithme de calcul de l'inverse

On s'intéresse à une méthode de calcul de l'inverse d'un élément a d'un groupe multiplicatif G de cardinal fini $N \in \mathbb{N}^*$. L'élément neutre de G est noté e.

1. Prouver que a^{N-1} est inverse de a dans G.

2. On considère la décomposition en base 2 de $N-1$:

$$N-1 = \sum_{i=0}^{k} x_i \times 2^i \text{ avec } k \in \mathbb{N}, x_i \in \{0,1\} \text{ pour } i \in [\![0,k]\!] \text{ et } x_k \neq 0$$

Soit alors les suites finies $(a_i)_{0 \leqslant i \leqslant k+1}$ et $(b_i)_{0 \leqslant i \leqslant k+1}$ définies par :

$$a_0 = e,\ b_0 = a \text{ et } \forall i \in [\![0,k]\!], a_{i+1} = a_i b_i^{x_i},\ b_{i+1} = b_i^2.$$

Démontrer que a_{k+1} est l'inverse de a dans G.

3. **[Informatique commune MP]**

a) Écrire une fonction Python `base2` d'argument N, qui détermine la liste $[x_0, \ldots, x_k]$ des chiffres en base 2 de $N-1$.

b) En déduire une fonction Python `inverse` de calcul de a^{-1} et d'arguments a et N. On suppose disposer d'une fonction `multi` qui prend en arguments deux éléments a et b de G et qui renvoie l'élément $a * b$ de G.

c) Préciser, en fonction de k, la complexité (c'est-à-dire le nombre de multiplications dans G) de la fonction `inverse` dans le pire des cas. On ne tiendra pas compte du coût du calcul des x_i, $0 \leqslant i \leqslant k$.

4. Dans cette question, G est le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$.

a) Déterminer le cardinal N de G.

b) Démontrer que $\overline{5}$ est un élément de G et trouver son inverse par la méthode de la question 2.

c) Déterminer par une autre méthode l'inverse de $\overline{5}$.