TD3. Structures algébriques. Anneau $\mathbb{Z}/n\mathbb{Z}$

Exercice 1. On considère l'ensemble $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} / a, b \in \mathbb{Z}\}$. Cet ensemble, muni de l'addition et la multiplication des nombres complexes, est un sous-anneau de $\mathbb{C}$.

1. Montrer que la conjugaison est un morphisme d'anneaux de $\mathbb{Z}[i]$ dans lui-même, puis que c'est un isomorphisme d'anneaux (c'est-à-dire un morphisme bijectif).

2. Soit φ un morphisme d'anneaux de $\mathbb{Z}[i]$ dans lui-même. Montrer que $\varphi(i) = \pm i$. En déduire que les seuls morphismes d'anneaux de $\mathbb{Z}[i]$ dans lui-même sont l'identité et la conjugaison.

3. L'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a + bi) = a^2 + b^2$ est appelée la *norme*.

a. Montrer que la norme est multiplicative, c'est-à-dire que pour tous $z, z' \in \mathbb{Z}[i]$, on a $N(zz') = N(z)N(z')$.

b. Déterminer tous les éléments du groupe $\mathbb{Z}[i]^*$.

c. Montrer que $2 + 3i$ est un irréductible de $\mathbb{Z}[i]$, c'est-à-dire que si $z, z' \in \mathbb{Z}[i]$ sont tels que $zz' = 2 + 3i$, alors z ou z' est inversible.

Exercice 2. On note $\mathcal{M}_2(\mathbb{R})$ l'anneau des matrices 2×2 à coefficients réels.

1. Montrer que $\mathcal{M}_2(\mathbb{R})$ n'est pas commutatif.

2. L'anneau $\mathcal{M}_2(\mathbb{R})$ est-il intègre ?
On rappelle qu'un anneau A est dit intègre lorsque pour tous $x, y \in A$, $xy = 0 \Rightarrow (x = 0$ ou $y = 0)$.

3. On considère l'ensemble

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} / a, b \in \mathbb{R} \text{ et } a^2 + b^2 = 1 \right\}$$

a. Montrer que G, muni de la multiplication des matrices, est un groupe.
Remarque : une matrice M est dans G si et seulement s'il existe $\theta \in \mathbb{R}$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$. La matrice M est alors la matrice de la rotation d'angle $\theta \mod 2\pi$ dans le plan muni d'un repère orthonormé.

b. G est-il un groupe commutatif ?

c. Pourquoi G n'est-il pas un sous-anneau de $\mathcal{M}_2(\mathbb{R})$?

4. On considère l'ensemble

$$H = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} / \lambda \in \mathbb{R} \right\}$$

Montrer que H, muni de la multiplication des matrices, est un groupe.

5. Quel est le groupe des inversibles de $\mathcal{M}_2(\mathbb{R})$?

Exercice 3. On considère l'ensemble $\mathbb{Q}(i) = \{a + bi \in \mathbb{C} / a, b \in \mathbb{Q}\}$.

1. Montrer que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$.

2. Montrer que $\mathbb{Q}(i)$ est un corps.

Exercice 4. Danger d'un anneau non intègre...
Montrer que $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.
On considère l'ensemble des fonctions polynomiales de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.
Etant donnée une fonction polynomiale f de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$, on appelle *racine* de f tout $a \in \mathbb{Z}/6\mathbb{Z}$ tel que $f(a) = 0$. Montrer que la fonction polynomiale f définie par $f(x) = (x - 2)(x - 3)$ a (au moins) quatre racines dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 5. Soient m, n des entiers naturels supérieurs à 2. Montrer qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n, et que dans ce cas, ce morphisme est unique.

Exercice 6. Isomorphisme réciproque dans le lemme des restes chinois
On dit que deux anneaux sont *isomorphes* s'il existe un morphisme d'anneau bijectif entre ces deux anneaux.
Pour tout $n \geqslant 2$, notons π_n le morphisme canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
Le lemme des restes chinois affirme que

$$f : \left\{ \begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ \pi_6(x) & \mapsto & (\pi_2(x), \pi_3(x)) \end{array} \right.$$

est un isomorphisme d'anneaux.
Etant donnés $a, b \in \mathbb{Z}$, on cherche dans cet exercice l'image de $(\pi_2(a), \pi_3(b))$ par l'isomorphisme réciproque.

1. Donner une relation de Bézout entre 2 et 3.

2. En déduire un entier k tel que $\left\{ \begin{array}{rcl} k & \equiv & 1 \mod 2 \\ k & \equiv & 0 \mod 3 \end{array} \right.$ et un entier ℓ tel que $\left\{ \begin{array}{rcl} \ell & \equiv & 0 \mod 2 \\ \ell & \equiv & 1 \mod 3 \end{array} \right.$

3. Pour tous entiers relatifs a et b, en déduire un entier x qui soit solution de

$$\left\{ \begin{array}{rcl} x & \equiv & a \mod 2 \\ x & \equiv & b \mod 3 \end{array} \right.$$

4. Conclure.

5. Prolongement : déterminer l'isomorphisme réciproque du morphisme du lemme des restes chinois

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

dans le cas général où p, q sont des entiers premiers entre eux et $p, q \geqslant 2$.

Exercice 7.

1. Montrer que les anneaux $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes, bien qu'ils aient le même nombre d'éléments.

2. Combien y a-t-il de morphismes d'anneaux de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? Pour chacun d'entre eux, donner leur noyau.

3. Montrer qu'il n'y a pas de morphisme d'anneaux de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$.

4. Démontrer que les anneaux $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sont isomorphes.

5. Expliciter l'isomorphisme d'anneaux entre les deux.

Exercice 8. Indicatrice d'Euler
Pour tout entier naturel $n \geqslant 2$, on note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$, c'est-à-dire le nombre d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. La fonction φ ainsi définie s'appelle *l'indicatrice d'Euler*.

1. Soit $p \geqslant 2$ un nombre premier. Que vaut $\varphi(p)$?

2. Montrer que pour tout entier naturel $k \geqslant 2$ et tout nombre premier $p \geqslant 2$, on a $\varphi(p^k) = p^{k-1}(p-1)$.

3. Montrer que si $m, n \geqslant 2$ sont des entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
On dit que l'indicatrice d'Euler est une fonction multiplicative.

4. Soit $n = 3 \times 5^3 \times 7^2 \times 11$. Calculer le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.

Exercice 9. Un petit corps fini
L'anneau $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ est un corps ayant deux éléments $\bar{0}$ et $\bar{1}$. On ajoute à ce corps un élément α vérifiant $\alpha^2 + \alpha + \bar{1} = \bar{0}$, et on considère l'ensemble $\mathbb{F}_4 = \{a + b\alpha / a, b \in \mathbb{F}_2\}$.

1. Montrer que $\alpha \neq \bar{0}$ et $\alpha \neq \bar{1}$.

2. Vérifier que $\mathbb{F}_4$ est un anneau commutatif ayant quatre éléments.

3. Pour tous $a, b \in \mathbb{F}_2$, calculer $(a\alpha + b)(a(\alpha + 1) + b)$.

4. En déduire que $\mathbb{F}_4$ est un corps.