

Feuille de TD n°7

Anneaux, corps

Exercice 1

On note $A = \mathbb{Z}/20\mathbb{Z}$.

- Calculer $\varphi(20)$.
- Déterminer A^* , le groupe des inversibles de A . Pour chaque élément $a \in A^*$, on déterminera l'ordre de a et son inverse.
- Déterminer les diviseurs de 0 de A .

Exercice 2

Sur l'ensemble \mathbb{R}^2 , on définit la loi \star par : $\forall (x, y), (x', y') \in \mathbb{R}^2, (x, y) \star (x', y') = (xx', x'y + xy')$.

- Montrer que $A = (\mathbb{R}^2, +, \star)$ est un anneau commutatif.
 - Expliciter les diviseurs de zéros dans A .
- On note f l'application
$$\begin{cases} \mathbb{R}[X] & \longrightarrow & A \\ P & \longmapsto & (P(0), P'(0)) \end{cases} .$$
 - Montrer que f est un morphisme d'anneaux.
 - Le morphisme f est-il surjectif? Donner son noyau.

Exercice 3

- Soit $n \in \mathbb{N}^*$, déterminer les inversibles de $\mathcal{M}_n(\mathbb{Z})$.
- On note $\mathcal{A} = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}, (a, b) \in \mathbb{Z}^2 \right\}$. Montrer que $(\mathcal{A}, +, \cdot)$ est un sous-anneau de $\mathcal{M}_2(\mathbb{Z})$. Déterminer \mathcal{A}^* et les diviseurs de 0 dans \mathcal{A} .
- On note $\mathcal{B} = \mathbb{Z} \times \mathbb{Z}$. Pour $(a, b), (a', b') \in \mathcal{B}$, on pose $(a, b) \star (a', b') = (aa', ab' + a'b)$. Montrer que $(\mathcal{B}, +, \star)$ est un anneau.
- Soit $f : \begin{cases} \mathcal{A} & \longrightarrow & \mathcal{B} \\ (a, b) & \longmapsto & \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \end{cases}$. Montrer que f est un isomorphisme d'anneaux.
- Déterminer \mathcal{B}^* et les diviseurs de 0 dans \mathcal{B} .

Exercice 4

On considère les matrices $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On définit l'ensemble $\mathcal{K} = \{aI + bJ, a, b \in \mathbb{R}\}$. Montrer que $(\mathcal{K}, +, \cdot)$ est un corps.

Exercice 5

Soient K un corps, A un anneau et $\varphi : K \longrightarrow A$ un morphisme d'anneaux. Montrer que φ est injectif.

Exercice 6

Soit B un anneau (unitaire) dont tout élément est idempotent, c'est-à-dire $\forall x \in B, x^2 = x$.

- Quels sont les inversibles de B ?
- Montrer que pour tout $x \in B, x + x = 0$.
 - En déduire que B est commutatif.

Exercice 7

Soient A un anneau (unitaire), $a \in A$ nilpotent et $x \in A$ inversible tels que a et x commutent. Montrer que $x - a$ est inversible et donner son inverse.

Exercice 8

Soit p un nombre premier. On pose, pour tout $\alpha \in \mathbb{N}, S_\alpha := \sum_{k=1}^{p-1} k^\alpha \in \mathbb{Z}/p\mathbb{Z}$.

- Montrer que pour tout $u \in (\mathbb{Z}/p\mathbb{Z})^*, S_\alpha = u^\alpha S_\alpha$.
- Calculer S_α lorsque $p - 1$ divise α .
- On suppose $0 < \alpha < p - 1$. En considérant le polynôme $X^\alpha - 1$ sur le corps $\mathbb{Z}/p\mathbb{Z}$, montrer qu'il existe $u \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $u^\alpha \neq 1$. En déduire la valeur de S_α .
- Calculer S_α lorsque $p - 1$ ne divise pas α .

Exercice 9

Soient $m, n \in \mathbb{Z}$ tels que m divise n . Soit $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ le morphisme surjectif canonique.

1. Montrer que π induit un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$.
2. En déduire que les anneaux $(\mathbb{Z}/n\mathbb{Z}) / (m\mathbb{Z}/n\mathbb{Z})$ et $\mathbb{Z}/m\mathbb{Z}$ sont isomorphes.

Exercice 10

Résoudre pour $n \in \mathbb{Z}$ le système de congruences $\begin{cases} n \equiv 4 & [19] \\ n \equiv 6 & [7] \end{cases}$.

Exercice 11

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se le partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Exercice 12 indicatrice d'Euler.

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.

1. Montrer que si $m, n \in \mathbb{N}^*$ sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
2. Soient p un nombre premier et k un entier naturel satisfaisant $k < p^\alpha$ où $\alpha \in \mathbb{N}^*$. Montrer que k n'est pas premier avec p^α si et seulement si k est un multiple de p . En déduire la valeur de $\varphi(p^\alpha)$.
3. Calculer $\varphi(n)$ pour tout $n \in \mathbb{N}^*$.

Exercice 13

Soit $n \in \mathbb{N}, n \geq 2$. Trouver le nombre de solutions de l'équation $x^2 = x$ dans $\mathbb{Z}/n\mathbb{Z}$

1. lorsque n premier ;
2. lorsque n est puissance d'un nombre premier ;
3. dans le cas général.

Exercice 14

Soient A un anneau et $a \in A - A^*$ non nul. On dit que a est *irréductible dans A* si

$$\forall b, c \in A, a = bc \implies b \in A^* \text{ ou } c \in A^*.$$

Préciser les éléments irréductibles des anneaux suivants :

1. \mathbb{Z} ,
2. $\mathbb{C}[X]$,
3. $\mathbb{R}[X]$.

Exercice 15

On définit l'ensemble $\mathbb{Z}[i] := \{a + ib \in \mathbb{C}, a, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} . On l'appelle l'anneau des *entiers de Gauss*.
2. On pose $N(a + ib) := a^2 + b^2$. Montrer que $z \in \mathbb{Z}[i]^*$ si et seulement si $N(z) = 1$. Calculer le groupe $\mathbb{Z}[i]^*$ et montrer qu'il est cyclique.
3. L'entier 2 est-il irréductible dans l'anneau $\mathbb{Z}[i]$? Même question pour 3.

Exercice 16

Soit A un anneau (unitaire). On appelle *caractéristique* de A l'ordre de 1 dans le groupe additif $(A, +)$. On suppose A de caractéristique finie n .

1. Montrer que tout élément x de A vérifie $nx = 0$.
2. Si A est intègre, montrer que n est un nombre premier.
3. Si A est intègre, montrer que $x \longmapsto x^n$ est un morphisme d'anneaux.

Exercice 17

Décrire les idéaux des anneaux suivants, on précisera ceux qui sont premiers, maximaux : a. \mathbb{Z} , b. \mathbb{R} , c. $\mathbb{R}[X]$.

Exercice 18

On considère l'application $f : \begin{cases} \mathbb{R}[X, Y] & \longrightarrow & \mathbb{R}[X] \\ P & \longmapsto & P(X, 0) \end{cases}$.

1. Montrer que f est un morphisme d'anneaux. Est-il surjectif ?
2. Calculer le noyau de f . Cet idéal est-il premier ? maximal ?