Feuille de TD n°7

Anneaux, corps

Exercice 1

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

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

Exercice 2

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

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

Exercice 3

1. Soit $n \in \mathbb{N}^*$, déterminer les inversibles de $\mathcal{M}_n(\mathbb{Z})$.
2. 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 $\mathcal{A}$.
3. 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.
4. 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.
5. 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 $\forall x \in B,\ x^2 = x$.

1. Quels sont les inversibles de B ?
2. a) Montrer que pour tout $x \in B$, $x + x = 0$.
   b) 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 $\alpha \in \mathbb{N}$, $S_\alpha := \sum_{k=1}^{p-1} \bar{k}^\alpha \in \mathbb{Z}/p\mathbb{Z}$.

1. Montrer que pour tout $u \in (\mathbb{Z}/p\mathbb{Z})^*$, $S_\alpha = u^\alpha S_\alpha$.
2. Calculer S_α lorsque $p-1$ divise α.

3. 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.
4. 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 $\left\{ \begin{array}{rcll} n & \equiv & 4 & [19] \\ n & \equiv & 6 & [7] \end{array} \right.$.

Exercice 11

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les 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

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

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

Préciser les éléments irréductibles des anneaux suivants : $\mathbb{Z}$, $\mathbb{C}[X]$, $\mathbb{R}[X]$.

Exercice 13

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 14

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 (appelé *morphisme de Frobenius*).

Exercice 15

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

Exercice 16

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

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

Exercice 17

1. Donner la liste des polynômes irréductibles de $\mathbb{Z}/2\mathbb{Z}[X]$ de degrés 1, 2, 3, 4.
2. Même question pour $\mathbb{Z}/3\mathbb{Z}[X]$.

Exercice 18

1. Montrer que $P(X) = X^2 + X + 1$ est irréductible dans $A = \mathbb{Z}/2\mathbb{Z}[X]$.
2. En déduire des propriétés de (P) et de $A/(P)$.
3. Dresser les tables d'addition et de multiplication de $A/(P)$.

Exercice 19

1. Soient $P(X) = X^2 + X + 1$ et $Q(X) = X^2 + 1$. Sont-ils irréductibles dans $A = \mathbb{Z}/3\mathbb{Z}[X]$? En déduire une construction d'un corps à 9 éléments K.
2. Quel est l'ordre de $\alpha = X + 1 \mod Q$ dans K^* ? En déduire que K^* est cyclique.

Exercice 20

1. Soit $P(X) = X^4 + X + 1$. Montrer que P est irréductible dans $A = \mathbb{Z}/2\mathbb{Z}[X]$.
2. Montrer que $A/(P)$ est un corps. Combien compte-t-il d'éléments ?
3. Montrer que $\alpha = X \mod P$ est d'ordre 15 dans le groupe multiplicatif K^*. En déduire que K^* est cyclique.