

6. Anneaux et polynômes (I)

Exercice 6.1 On définit deux lois de composition $+$ et \cdot sur $\mathbb{Z} \times \mathbb{Z}$ par :

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b) \cdot (a', b') = (aa', bb' + ab' + ba').$$

Montrer que $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ est un anneau unitaire commutatif. Cet anneau est-il intègre ?

Exercice 6.2 On appelle *entier de Gauss* tout nombre complexe $z = x + iy$ dont la partie réelle x et la partie imaginaire y sont des entiers relatifs. Montrer que l'ensemble des entiers de Gauss muni des lois d'addition et de multiplication usuelles est un anneau unitaire commutatif intègre. Cet anneau est-il un corps ?

Exercice 6.3 Soit $(A, +, \cdot)$ un anneau unitaire idempotent (c'est-à-dire tout élément $a \in A$ satisfait $a \cdot a = a$).

1. Montrer $1 = -1$ dans A et que A est commutatif.
2. Montrer que $xy(x + y) = 0$ pour tout $x, y \in A$.
3. Montrer que si A n'a pas de diviseur de 0 et n'est pas réduit à $\{0\}$, alors A est le corps à deux éléments.

Exercice 6.4 Soit F un corps commutatif. On suppose qu'il existe un élément non nul $x \in F$ tel que $x + x = 0$. Montrer que, pour tout $y, z \in F$, on a :

$$(y + z)^2 = y^2 + z^2.$$

Exercice 6.5 Déterminer tous les morphismes d'anneaux de \mathbb{Z} dans \mathbb{Z} , puis de \mathbb{Q} dans \mathbb{Z} , et finalement de \mathbb{R} dans \mathbb{Q} .

Exercice 6.6 Soit $(A, +, \cdot)$ un anneau commutatif non nul. Soit P une partie non-vide de A . On pose :

$$E(P) = \{a \in A \text{ tels que } xa = 0 \text{ pour tout } x \in P\}.$$

1. Montrer que $E(P)$ est un idéal de A .
2. Soit α un idempotent de A et soit I l'idéal de A engendré par α . On note $J = E(I)$. Montrer que :
 - (a) $I \cap J = \{0\}$
 - (b) Tout élément de A est la somme d'un élément de I et d'un élément de J .

Exercice 6.7 Soit p un nombre premier. Déterminer tous les diviseurs de zéro de l'anneau $\mathbb{Z}/p^2\mathbb{Z}$.

Exercice 6.8 Soit A un anneau unitaire. Un élément $a \in A$ est *nilpotent* s'il existe un entier $n > 0$ tel que $a^n = 0$.

1. Soient a et b deux éléments d'un anneau A tels que ab soit nilpotent. Montrer que ba est aussi nilpotent.
2. Montrer que si a et b sont nilpotents et de plus $ab = ba$, alors ab et $a + b$ sont aussi nilpotents.

3. Soit a un élément d'un anneau A tel que $1 - a$ est nilpotent. Montrer que a est inversible, et que si b est l'inverse de a , alors $1 - b$ est aussi nilpotent.

Exercice 6.9 Soient A un anneau commutatif et I un idéal de A . On appelle radical de I l'ensemble

$$\sqrt{I} = \{x \in A \text{ tels qu'il existe } n \geq 1 \text{ avec } x^n \in I\}.$$

1. Montrer que \sqrt{I} est un idéal de A contenant I .
2. Soit J un idéal de A contenant I . Montrer que $\sqrt{I} \subset \sqrt{J}$.
3. En déduire que $\sqrt{\sqrt{I}} = \sqrt{I}$.

Exercice 6.10 (Idéaux bilatères de $\mathcal{M}_n(\mathbb{R})$) Soit J un idéal bilatère de $\mathcal{M}_n(\mathbb{R})$. On suppose que $J \neq \{0\}$.

1. Montrer que si J contient une matrice inversible alors $J = \mathcal{M}_n(\mathbb{R})$.
2. Soit A une matrice de $\mathcal{M}_n(\mathbb{R})$ de rang $r \geq 1$. Montrer que J contient la matrice

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$
3. Montrer l'existence de $n - r + 1$ matrices A_1, \dots, A_{n-r+1} toutes équivalentes à A dont la somme est une matrice inversible.
4. Conclure que $J = \mathcal{M}_n(\mathbb{R})$.
(On dit qu'un anneau est simple lorsque qu'il n'admet que deux idéaux bilatères qui sont $\{0\}$ et lui-même. On vient ainsi de montrer que $\mathcal{M}_n(\mathbb{R})$ est simple.)

Exercice 6.11 Soit A un anneau commutatif, on définit :

$$\text{Nil}(A) = \{a \in A \text{ tels qu'il existe } n \geq 1 \text{ avec } a^n = 0\}.$$

1. Montrer que $\text{Nil}(A)$ est un idéal de A .
2. Montrer que si P est idéal premier de A , alors $\text{Nil}(A) \subset P$.
3. Montrer que le seul élément nilpotent de $A/\text{Nil}(A)$ est 0.

Exercice 6.12 (Les nombres p -adiques) Soit p un nombre premier. Pour $a \in \mathbb{Z}$, a non nul, on appelle *valuation p -adique* de a , noté $v_p(a)$, le plus grand entier $i \geq 0$ tel que p^i divise a . Par convention, on pose $v_p(0) = \infty$.

1. Montrer que, pour tout $a, b \in \mathbb{Z}$, on a :

$$v_p(ab) = v_p(a) + v_p(b).$$

2. Soit $r \in \mathbb{Q}$. On écrit $r = a/b$ avec $a, b \in \mathbb{Z}$ et on pose

$$v_p(r) = v_p(a) - v_p(b).$$

Montrer que cette valeur ne dépend que de r et permet d'étendre la valuation p -adique à \mathbb{Q} .

On définit :

$$A_p = \{x \in \mathbb{Q} \text{ tels que } v_p(x) \geq 0\}.$$

3. Montrer que A_p est un sous-anneau unitaire de \mathbb{Q} et déterminer ses éléments inversibles.
4. Montrer que A_p est principal et que le seul idéal maximal est (p) .
5. Montrer que $A_p/(p)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.