Anneaux

Exercice 1. *Anneau de Boole*

Soit E un ensemble fini et $A = \mathcal{P}(E)$.

1) Montrer que $(A, \Delta, \cap)$ est un anneau commutatif. Est-il intègre ?

2) Soit I un idéal de A. Montrer que : $\begin{cases} \forall\, X \in I,\ \forall\, Y \subset X,\ \text{ on a } Y \in I \\ \forall\, X, Y \in I,\ \text{ on a } X \cup Y \in I. \end{cases}$

3) En déduire que $I = \mathcal{P}(E')$ avec $E' \subset E$.

4) Étudier la réciproque.

5) Si E est infini, montrer que $I = \{\text{parties finies de } E\}$ est un idéal qui n'est pas de la forme $\mathcal{P}(E')$.

Exercice 2. *Idéaux triviaux*

Soit A un anneau commutatif non nul dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps.

Exercice 3. *Idéaux premiers*

Un idéal I d'un anneau A est dit premier si : $\forall\, x, y \in A$, $xy \in I \Rightarrow x \in I$ ou $y \in I$.

1) Quels sont les idéaux premiers de $\mathbb{Z}$?

2) Montrer que si A est commutatif non nul et si tous les idéaux de A sont premiers alors A est un corps.

Exercice 4. *Thm de Gauss*

Soit A un anneau commutatif et $a, b \in A$. On dit que a *divise* b si $b \in aA$ et a *est premier à* b si $aA + bA = A$.

Montrer que si a est premier à b et a divise bc, alors a divise c.

Exercice 5. *Caractéristique*

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

1) Montrer que : $\forall\, x \in A$, $nx = 0$.

2) Si A est intègre non nul, montrer que n est un nombre premier.

3) Si A est intègre et commutatif, montrer que $x \mapsto x^n$ est un morphisme d'anneau.

Exercice 6. *Anneau de caractéristique 2*

Soit A un anneau non nul tel que : $\forall\, x \in A$, $x^2 = x$.

1) Exemple d'un tel anneau ?

2) Quels sont les éléments inversibles de A ?

3) Montrer que : $\forall\, x \in A,\ x + x = 0$. En déduire que A est commutatif.

4) Pour $x, y \in A$ on pose : $x \leqslant y \Leftrightarrow \exists\, a \in A$ tq $x = ay$. Montrer que c'est une relation d'ordre.

Exercice 7. *Eléments nilpotents*

Soit A un anneau commutatif, et $a \in A$. On dit que a est nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

1) Exemple : Déterminer les éléments nilpotents de $\mathbb{Z}/36\mathbb{Z}$.

2) Montrer que l'ensemble des éléments nilpotents est un idéal de A.

3) Soit a nilpotent. Montrer que $1 - a$ est inversible.

4) Soient a nilpotent et b inversible. Montrer que $a + b$ est inversible.

Exercice 8. $1 - ab$ *et* $1 - ba$

Soit A un anneau et $a, b \in A$. Montrer que $1 - ab \in A^* \Leftrightarrow 1 - ba \in A^*$.

Exercice 9. *Radical d'un idéal*

Soit A un anneau commutatif et I un idéal de A.

On note $\sqrt{I} = \{x \in A \text{ tq } \exists\, n \in \mathbb{N} \text{ tq } x^n \in I\}$ (radical de I).

1) Montrer que $\sqrt{I}$ est un idéal de A.

2) Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}$.

4) Exemple : $A = \mathbb{Z}$, $I = 3648\mathbb{Z}$. Trouver $\sqrt{I}$.

Exercice 10. *Produit de deux idéaux*

Soit A un anneau commutatif et I, J deux idéaux de A. On note $IJ = \{a_1b_1+\ldots+a_nb_n \text{ tq } a_i \in I, b_i \in J\}$.

1) Montrer que IJ est un idéal de A.

2) Montrer que $I(J+K) = IJ + IK$.

3) On suppose $I + J = A$. Montrer que $IJ = I \cap J$.

4) Pour $A = \mathbb{Z}$, $I = n\mathbb{Z}$, $J = p\mathbb{Z}$, qu'est-ce que IJ ?

Exercice 11. *Relation d'équivalence compatible avec les opérations d'anneau*

Soit A un anneau commutatif.

1) Soit $\mathcal{R}$ une relation d'équivalence compatible avec l'addition et la multiplication dans A. On note I la classe de 0. Montrer que I est un idéal de A.

2) Réciproquement, soit J un idéal de A. On pose $x \sim y \Leftrightarrow x - y \in J$. Montrer que $\sim$ est une relation d'équivalence compatible avec $+$ et $\times$.

Exercice 12. *Étude de l'anneau $\mathbb{Z}^2$*

1) Soit $d \in \mathbb{N}$. On pose $A_d = \{(x,y) \in \mathbb{Z}^2 \text{ tq } x \equiv y \pmod d\}$ ($x = y$ pour $d = 0$). Montrer que A_d est un sous-anneau de $\mathbb{Z}^2$.

2) Montrer que l'on obtient ainsi tous les sous-anneaux de $\mathbb{Z}^2$.

3) Soit I un idéal de $\mathbb{Z}^2$. On note : $I_1 = \{x \in \mathbb{Z} \text{ tq } (x,0) \in I\}$ et $I_2 = \{y \in \mathbb{Z} \text{ tq } (0,y) \in I\}$. Montrer que I_1 et I_2 sont des idéaux de $\mathbb{Z}$, et que $I = I_1 \times I_2$.

4) En déduire que I est un idéal monogène.

Exercice 13. *Idéaux de $\mathbb{K}^E$*

Soit $\mathbb{K}$ un corps, E un ensemble fini, et $A = K^E$. Pour $e \in E$, on pose :

$$I_e = \{f \in A \text{ tq } f(e) = 0\}, \qquad \chi_e \ : \ x \mapsto \begin{cases} 1 & \text{si } x = e \\ 0 & \text{si } x \neq e. \end{cases}$$

1) Montrer que I_e est un idéal monogène de A.

2) Soit $f \in A$. Vérifier que $f = \sum_{e \in E} f(e)\chi_e$.

3) Soit I un idéal quelconque de A, et $F = \{e \in E \text{ tq } \exists\, f \in I \text{ tq } f(e) \neq 0\}$. Montrer que I est un idéal monogène engendré par $\sum_{e\in F} \chi_e$.

Exercice 14. *Fonctions trigonométriques*

Soit $A = \{f \ : \ \mathbb{R} \to \mathbb{R} \text{ de la forme } f(x) = a_0 + \sum_{k=1}^{n} a_k \cos(kx),\ n \in \mathbb{N},\ a_i \in \mathbb{R}\}$.

1) Montrer que A est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.

2) Soit $f \in A$. Calculer $\int_{t=0}^{2\pi} f(t)\cos(nt)\,dt$ en fonction des a_k.

3) En déduire que A est intègre.

4) Soit Φ : $\begin{cases} \mathbb{R}[X] & \longrightarrow & A \\ P & \longmapsto & x \mapsto P(\cos x). \end{cases}$ Montrer que Φ est un isomorphisme d'anneaux. En déduire que A est principal.

Exercice 15. *Suites croissantes d'idéaux*

Soit A un anneau commutatif et (I_n) une suite croissante d'idéaux de A. On pose $I = \cup_{n\in\mathbb{N}} I_n$.

1) Montrer que I est un idéal de A.

2) On suppose que A est principal. Montrer qu'il existe $p \in \mathbb{N}$ tel que $I = I_p$.

3) Application : soit A principal et $a \in A \setminus \{0\}$. Montrer que a est produit d'éléments irréductibles (on raisonnera par l'absurde).

Exercice 16. *Endomorphismes d'un groupe commutatif*

Soit G un groupe additif et $A = \{\text{morphismes } G \to G\}$.

1) Montrer que $(A, +, \circ)$ est un anneau.

2) On prend $G = \mathbb{Z}/n\mathbb{Z}$, $n \geqslant 2$. Montrer que A est l'ensemble des applications $x \mapsto kx$ avec $k \in G$, et que A est isomorphe à l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exercice 17. *Entiers 2-adiques*

Soit $A = \{m/n \in \mathbb{Q} \text{ tq } n \text{ est impair}\}$.

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

2) Chercher les éléments inversibles dans A.

3) Montrer que les idéaux non nuls de A sont tous monogènes engendrés par les nombres de la forme 2^k, $k \in \mathbb{N}$.

Exercice 18. *Morphismes $\mathbb{Z}^n \to \mathbb{Z}$*

Chercher les morphismes d'anneaux : $\mathbb{Z}^n \to \mathbb{Z}$.

Exercice 19. *Suites stationnaires*

Soit $A = \{\text{suites d'entiers relatifs stationnaires}\}$ muni des opérations usuelles.

1) Montrer que A est un anneau.

2) Chercher les morphismes d'anneaux : $A \to \mathbb{Z}$.

3) Soit $I = \{\text{suites presque nulles}\}$. Montrer que c'est un idéal non monogène.

Exercice 20. *Entiers de Gauss*

Soit $A = \{a + bi \text{ tq } a, b \in \mathbb{Z}\}$.

1) Montrer que A est un sous-anneau de $\mathbb{C}$. Quels sont les éléments inversibles ?

2) Soient $u, v \in A$ avec $v \neq 0$. Montrer qu'il existe $q, r \in A$ tels que $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?

3) Montrer que A est principal.

Exercice 21. *Anneau intègre fini*

Soit A un anneau non nul, commutatif et intègre.

1) Montrer que si A est fini, alors c'est un corps.

2) Montrer que si A n'a qu'un nombre fini d'idéaux, alors c'est un corps (considérer les idéaux $I_n = x^n A$ pour $x \in A$ non nul).

Exercice 22. *Corps $\mathbb{F}_4$*

Chercher les structures de corps à quatre éléments.

Exercice 23. *Groupe multiplicatif d'un corps fini*

Soit $\mathbb{K}$ un corps fini. Pour $x \in \mathbb{K}^*$ on note $O(x)$ l'ordre multiplicatif de x et n le ppcm des ordres des éléments de $\mathbb{K}^*$.

1) Soient $a, b \in \mathbb{N}^*$. Montrer qu'il existe $a', b' \in \mathbb{N}^*$ tels que $a'|a$, $b'|b$, $a' \wedge b' = 1$ et $a'b' = a \vee b$.

2) Soient $x, y \in \mathbb{K}^*$ d'ordres a et b. Montrer qu'il existe u, v entiers tels que $O(x^u y^v) = a \vee b$. En déduire qu'il existe $z \in \mathbb{K}^*$ d'ordre n.

3) Montrer que $n = \mathrm{card}(\mathbb{K}^*)$ (ceci prouve que $\mathbb{K}^*$ est cyclique).

Exercice 24. *Groupe multiplicatif d'un corps fini*

Soit $\mathbb{K}$ un corps fini de cardinal n. Si $a, b \in \mathbb{N}$ sont tels que $ab = n - 1$, on considère l'application

$$f_a : \begin{cases} \mathbb{K}^* & \longrightarrow & \mathbb{K}^* \\ x & \longmapsto & x^a \end{cases}$$

(remarquer que f_a est un morphisme de groupe). On note $N_a = \mathrm{card}(\mathrm{Ker}\, f_a)$.

1) Expliquer pourquoi $N_a \leqslant a$.

2) Montrer que $\mathrm{Im}(f_a) \subset \mathrm{Ker}\, f_b$. En déduire que $N_a = a$ et $N_b = b$.

3) Soit φ l'indicateur d'Euler. Montrer par récurrence sur a, diviseur de $n-1$, que le nombre d'éléments de $\mathbb{K}^*$ d'ordre a est égal à $\varphi(a)$ (ceci prouve que $\mathbb{K}^*$ est cyclique).

Exercice 25. *Théorème de Wedderburn*

On dit qu'un anneau A est un *anneau à division* si $A^* = A \setminus \{0\}$. L'objet de l'exercice est de démontrer le théorème de Wedderburn : *tout anneau à division fini est commutatif* (c'est donc un corps fini).

1) *Polynômes cyclotomiques*

Pour $n \in \mathbb{N}^*$, soit $\mathcal{P}_n$ l'ensemble des racines primitives n-èmes de l'unité dans $\mathbb{C}$ et $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n}(X - \zeta)$ ($\mathcal{P}_1 = \{1\}$, $\Phi_1(X) = X - 1$)

a) Démontrer : $X^n - 1 = \prod_{d|n} \Phi_d(X)$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Montrer que si m divise n et $m < n$ alors $\Phi_n(X)$ divise $(X^n - 1)/(X^m - 1)$ dans $\mathbb{Z}[X]$.

c) Justifier : $\forall\, p \in \mathbb{N}^*$, $|\Phi_n(p)| \geqslant (p-1)^{\mathrm{card}(\mathcal{P}_n)}$ avec égalité si et seulement si $n = 1$.

2) *Cardinal d'un anneau à division*

Soient A un anneau fini à division et B un sous-anneau de A. On note α, β les cardinaux de A, B.

a) Montrer que B est aussi un anneau à division.

b) Pour $x \in A$, on note $Bx = \{bx \text{ tq } b \in B\}$ et on considère une famille $(x_1, \ldots, x_n)$ de cardinal minimal telle que $A = Bx_1 + \ldots + Bx_n$. Justifier l'existence d'une telle famille et montrer que l'application

$$\Phi : \begin{cases} Bx_1 \times \ldots \times Bx_n & \longrightarrow \quad A \\ \quad (y_1, \ldots, y_n) & \longmapsto \quad y_1 + \ldots + y_n \end{cases}$$

est une bijection.

c) En déduire que α est une puissance de β.

3) *Théorème de Wedderburn*

Soit A un anneau à division, B son centre et α, β les cardinaux de A, B. Pour $a \in A^*$, on note $\mathcal{C}_a$ le commutant de a et $\mathcal{O}_a = \{xax^{-1} \text{ tq } x \in A^*\}$.

a) Montrer que $\mathcal{C}_a$ est un anneau à division et qu'il existe des entiers m, n tels que : $\alpha = \beta^n$, $\mathrm{card}(\mathcal{C}_a) = \beta^m$ et m divise n.

b) Montrer que $\mathrm{card}(\mathcal{O}_a) = \mathrm{card}(A^*)/\,\mathrm{card}(\mathcal{C}_a^*)$. En déduire que si $a \notin B$ alors $\Phi_n(\beta)$ divise $\mathrm{card}(\mathcal{O}_a)$.

c) Pour $a, b \in A$, montrer que $\mathcal{O}_a$ et $\mathcal{O}_b$ sont soit disjoints, soit égaux. En déduire qu'il existe une partition de A^* de la forme $A^* = \mathcal{O}_{a_1} \sqcup \ldots \sqcup \mathcal{O}_{a_k}$.

d) Montrer que $\Phi_n(\beta)$ divise $\mathrm{card}(B^*) = \beta - 1$ puis que $n = 1$ (et donc $A = B$, ce qui prouve la commutativité de A).

solutions

Exercice 3.

2) A est intègre car $\{0\}$ est premier et si $a \in A \setminus \{0\}$ alors $a \times a \in (a^2)$ qui est premier donc a^2 divise a d'où a est inversible.

Exercice 6.

2) 1.

3) $x + y = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx \Rightarrow xy + yx = 0$.
Pour $y = 1$: $x + x = 0 \Rightarrow 1 = -1$.
Pour y quelconque : $xy = -yx = yx$.

4) Antisymétrie : si $x = ay$, alors $xy = ay^2 = ay = x$. Donc $(x \leqslant y)$ et $(y \leqslant x) \Rightarrow xy = x = y$.

Exercice 8.

Si $(1 - ab)c = 1 = c(1 - ab)$ alors $abc = c - 1 = cab$ donc $babca = bca - ba = bcaba$,
soit $ba(1 + bca) = bca = (1 + bca)ba$ et $1 + bca$ est inverse de $1 - ba$.

Exercice 9.

3) Réciproque fausse : $A = \mathbb{Z}[X]$, $I = (X)$, $J = (X + 4)$.

4) $114\mathbb{Z}$.

Exercice 14.

2) πa_n.

3) Si $f(x) = \sum_{k=0}^{n} a_k \cos(kx)$ et $g(x) = \sum_{k=0}^{p} b_k \cos(kx)$ avec $a_n \neq 0$ et $b_p \neq 0$ alors,
$2 \int_{t=0}^{2\pi} f(t)g(t)\cos(nt)\,\mathrm{d}t = \pi a_n b_p \neq 0$ donc $fg \neq 0$.

Exercice 18.

$f(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n$.
f est multiplicative sur la base canonique $\Rightarrow a_ia_j = 0$ pour $i \neq j$.
$f(1, \dots, 1) = 1 \Rightarrow$ un des a_i vaut 1, et les autres 0.
conclusion : $f =$ fct coordonnée.

Exercice 19.

2) idem **18** : les projections + la valeur de stationnement.

Exercice 20.

1) $\pm 1, \pm i$.

2) Non : $1 + i = 0 \times 2 + (1 + i) = 1 \times 2 + (i - 1)$.

Exercice 22.

$\mathbb{K} = \{0, 1, a, b\}$ et $\{1, a, b\}$ est un groupe multiplicatif d'où $b = a^2$, $a^3 = 1$.

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

$\times$	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a