Université Lyon I
Département de Mathématiques

Année universitaire 2025-2026
L3 MGA
Anneaux et Corps

FEUILLE D'EXERCICES 1 : ANNEAUX ET IDÉAUX

Exercice 1

Soit $n \geq 2$ un entier et R un anneau commutatif. On considère les ensembles suivants de matrices $n \times n$ à coefficients dans R :

(1) $M_n(R)$, l'ensemble des matrices carrées.
(2) $T_n(R)$, l'ensemble des matrices triangulaires supérieures ($a_{ij} = 0$ pour $i > j$).
(3) $N_n(R)$, l'ensemble des matrices triangulaires supérieures strictes ($a_{ij} = 0$ pour $i \geq j$).

Déterminer si chacun de ces ensembles forme un anneau pour l'addition et la multiplication matricielles. S'il s'agit d'un anneau, est-il commutatif ? Est-il unitaire, c'est-à-dire admet-il un élément neutre pour la multiplication ?

Exercice 2

Lesquels de ces sous-ensembles de $\mathbb{C}$ sont des sous-anneaux ? Lesquels sont des corps ?

(1) $\bigcup_{n\in\mathbb{N}} 10^{-n}\mathbb{Z}$;
(2) $\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}^*, (m,n) = 1, p \mid n\}$ (p est un nombre premier fixé) ;
(3) $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i, \quad \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$;
(4) $\mathbb{Z} + \mathbb{Z}\sqrt[3]{2}$;
(5) $\mathbb{Q}[i] = \mathbb{Q} + \mathbb{Q}i, \quad \mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.

Exercice 3

Les éléments inversibles d'un anneau commutatif unitaire A forment le groupe multiplicatif $(A^\times, \cdot)$.

(1) Trouver le groupe $\mathbb{Z}[i]^\times$ en utilisant le module complexe.
(2) Montrer que le groupe $\mathbb{Z}[\sqrt{2}]^\times$ est infini.

Exercice 4

Un élément a d'un anneau A est dit nilpotent, s'il existe $k \in \mathbb{N}$ tel que $a^k = 0$.

(1) Trouver tous les éléments inversibles, les diviseurs de zéro, les nilpotents des anneaux suivants :
   (a) $\mathbb{Z}/12\mathbb{Z}$;
   (b) $\mathbb{Z}/n\mathbb{Z}$;
(2) Démontrer que, pour tout nilpotent x de A unitaire, l'élément $1 + x$ est inversible.
(3) Montrer que l'ensemble N des éléments nilpotents d'un anneau commutatif forme un idéal.

Exercice 5

Démontrer que tout morphisme non trivial d'un corps dans un anneau est injectif.

Exercice 6

Montrer que dans un anneau commutatif fini, tout idéal premier est maximal.

Exercice 7

Soient I et J deux idéaux de l'anneau commutatif A. Considérons la projection canonique $\pi_I : A \to A/I$ et l'image $\bar{J} = \pi_I(J)$ de l'idéal J.

(1) Montrer que $\bar{J}$ est un idéal de l'anneau quotient A/I.

(2) Démontrer qu'on a l'isomorphisme suivant : $(A/I)/\bar{J} \cong A/(I+J)$.

Exercice 8

Montrer que si M est un idéal maximal d'un anneau commutatif A, alors le seul idéal premier de A qui contient M^n est M.

Exercice 9

Deux idéaux I et J d'un anneau commutatif et unitaire A sont dits étrangers si $I + J = A$.

(1) Soit I et J deux idéaux étrangers d'un anneau A. Montrer que $I \cap J = (IJ)$. On rappelle que (IJ) est le groupe additif engendré par les produits.

(2) Trouver deux idéaux non étrangers d'un anneau A tels que $I \cap J \neq (IJ)$.

Exercice 10

Montrer que les ensembles suivants sont des idéaux non principaux :

(1) $I = \{f \in A : 5 \text{ divise } f(0)\}$ où $A = \mathbb{Z}[X]$.

(2) L'idéal (X, n) où $n \in \mathbb{Z}$, $n > 1$ de l'anneau $\mathbb{Z}[X]$.

(3) $I = \{f \in A : f(0) = 0\}$ où $A = C(\mathbb{R}, \mathbb{R})$ est l'anneau des applications continues de $\mathbb{R}$ dans $\mathbb{R}$.

Exercice 11

Démontrer que pour tout corps K, l'anneau des polynômes $K[x]$ a une infinité de polynômes unitaires irréductibles.

Exercice 12

Soit A un anneau intègre. Montrer que $A[X]$ est principal ssi A est un corps.

Exercice 13

(1) Soit $f(x) \in A[x]$ un polynôme sur un anneau commutatif A. Supposons que $(x-1) \mid f(x^n)$. Montrer que $(x^n - 1) \mid f(x^n)$.

(2) Pour $n, m \geq 2$, déterminer le reste de la division euclidienne du polynôme $(x-2)^m + (x-1)^n - 1$ par $(x-1)(x-2)$ dans $\mathbb{Z}[x]$.

Exercice 14

(1) Si K est un corps, montrer qu'un polynôme P de degré 2 et 3 dans $K[x]$ est irréductible si et seulement si il n'a pas de zéro dans K.

(2) Trouver tous les polynômes irréductibles de degré 2, 3 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

(3) Décrire tous les polynômes irréductibles de degré 4 et 5 sur $\mathbb{Z}/2\mathbb{Z}$.

Exercice 15

(1) Trouver tous les polynômes irréductibles de degré 2, 3 à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

(2) Décomposer les polynômes suivants en facteurs irréductibles dans $\mathbb{F}_3[x]$.
$$x^2+x+1, \qquad x^3+x+2, \qquad x^4+x^3+x+1\ .$$

Exercice 16

(1) En utilisant les réductions mod 2 ou mod 3 montrer que les polynômes
$$x^5-6x^3+2x^2-4x+5 \qquad \text{et} \qquad 7x^4+8x^3+11x^2-24x-455$$
sont irréductibles dans $\mathbb{Z}[x]$.

(2) En utilisant la partie précédente, montrer que les polynômes
$$5x^3+8x^2+3x+15 \qquad \text{et} \qquad x^5+2x^3+3x^2-6x-5$$
sont irréductibles dans $\mathbb{Z}[x]$.

Exercice 17

Soient
$$f(x)=(x-a_1)(x-a_2)\dots(x-a_n)-1, \quad g(x)=(x-a_1)^2(x-a_2)^2\dots(x-a_n)^2+1$$
où $a_1,\dots a_n\in\mathbb{Z}$ sont deux à deux distincts. Montrer que f et g sont irréductibles dans $\mathbb{Q}[x]$.

Exercice 18

Soient $f,g\in\mathbb{Q}[x]$. Supposons que f soit irréductible et qu'il existe $\alpha\in\mathbb{C}$ tel que $f(\alpha)=g(\alpha)=0$. Alors f divise g.

Exercice 19

Trouver le pgcd$(x^n-1,\ x^m-1)$ dans $\mathbb{Z}[x]$.

Exercice 20

Trouver le pgcd(f,g) dans $\mathbb{Z}_2[x]$ et sa représentation linéaire $fu+gv$ où $d,u,v\in\mathbb{Z}_2[x]$:

(1) $f=x^5+x^4+1, \qquad g=x^4+x^2+1;$

(2) $f=x^5+x^3+x+1, \qquad g=x^4+1.$

Exercice 21

Trouver le pgcd(f,g) dans $\mathbb{Z}_3[x]$ et $\mathbb{Z}_5[x]$ de $f=x^4+1$, $g=x^3+x+1$.

Exercice 22

Trouver le pgcd(f,g) dans $\mathbb{Z}[x]$ de $f=x^4+x^3-3x^2-4x-1$ et $g=x^3+x^2-x-1$.

Exercice 23

Soient $A=\mathbb{Z}[i\sqrt{3}]$ et K son corps de fractions.

(1) Montrer que x^2-x+1 n'est pas irréductible dans $K[x]$.

(2) Montrer que x^2-x+1 est irréductible dans $A[x]$.

(3) En déduire que $\mathbb{Z}[i\sqrt{3}]$ n'est pas euclidien (et même pas factoriel).

Exercice 24

Soit $P\in\mathbb{Z}[x]$.

(1) On suppose que $P(0)$ et $P(1)$ sont impairs. Montrer que P n'a pas de racine dans $\mathbb{Z}$.

(2) Soit $n\in\mathbb{N}$ tel qu'aucun des entiers $P(0),\dots,P(n-1)$ ne soit divisible par n. Montrer que P n'a pas de racine dans $\mathbb{Z}$.

Exercice 25

Montrer que f est irréductible dans $\mathbb{Q}[x]$ dans chacun des cas suivants :

(1) $f = x^4 - 8x^3 + 12x^2 - 6x + 2$;
(2) $f = x^5 - 12x^3 + 36x - 12$;
(3) $f = x^4 - x^3 + 2x + 1$;

Exercice 26

(1) Soit $P \in \mathbb{Z}[x]$. Soit $\dfrac{a}{b}$ une racine rationnelle : $P(\dfrac{a}{b}) = 0$, $\mathrm{pgcd}(a, b) = 1$.
  (a) Montrer que $\forall\, k \in \mathbb{Z}\;\; (a - bk)$ divise $P(k)$.
  (b) Montrer que b divise le coefficient dominant de P.
(2) Quelles racines rationnelles ont les polynômes $f(x) = x^3 - 6x^2 + 15x - 14$ et $g(x) = 2x^3 + 3x^2 + 6x - 4$?

Exercice 27

(1) Soient $P \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, $m = P(n)$. On suppose $m \neq 0$. Montrer que $\forall\, k \in \mathbb{Z}\quad m \mid P(n+km)$.
(2) En déduire qu'il n'existe aucun polynôme $P \in \mathbb{Z}[x]$, non constant, tel que, pour tout $n \in \mathbb{Z}$, $P(n)$ soit un nombre premier.

Exercice 28

Soit $(x^3 - x + 2)$ l'idéal principal engendré par $x^3 - x + 2$ dans l'anneau $\mathbb{Q}[x]$.

(1) Montrer que l'anneau quotient $\mathbb{Q}[x]/(x^3 - x + 2)$ est un corps.
(2) Soit y l'image de x dans $\mathbb{Q}[x]/(x^3 - x + 2)$ par la surjection canonique. Calculer son inverse.
(3) Montrer que $1 + y + y^2$ est non nul et calculer son inverse.

Exercice 29

Les polynômes suivants sont-ils irréductibles ?

(1) $X^5 + 121X^4 + 1221X^3 + 12221X^2 + 122221X + 222222$ dans $\mathbb{Q}[X]$.
(2) $f(X, Y) = X^2Y^3 + X^2Y^2 + Y^3 - 2XY^2 + Y^2 + X - 1$ dans $\mathbb{C}[X, Y]$ et $\mathbb{F}_2[X, Y]$.
(3) $f(X, Y) = Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2Y^2 - 5Y + X^2 + X + 1$ dans $\mathbb{Q}[X, Y]$.

Exercice 30

L'idéal principal $(x^2 + y^2 + 1)$ est-il maximal dans les anneaux $\mathbb{C}[x, y]$, $\mathbb{R}[x, y]$, $\mathbb{Q}[x, y]$, $\mathbb{Z}[x, y]$, $\mathbb{Z}_2[x, y]$?

Exercice 31

Vrai ou faux ?

(1) $\mathbb{R}[X, Y]$ est un anneau euclidien.
(2) $\mathbb{Z}[X]$ est un anneau principal.
(3) $\mathbb{Z}[X, Y]$ est un anneau factoriel.
(4) Un anneau factoriel est principal.
(5) Un anneau euclidien est principal.
(6) Un anneau euclidien est factoriel.

Exercice 32

Soit $d \in \mathbb{Z}$ sans facteur carré.

(1) Trouver le nombre d'éléments de l'anneau quotient $\mathbb{Z}[\sqrt{d}]/(m)$ où $m \in \mathbb{Z}$ et $m \neq 0$.

(2) L'idéal principal engendré par 2 est-il premier dans l'anneau $\mathbb{Z}[\sqrt{d}]$?

Exercice 33

(1) Soit A un anneau principal, I un idéal de A. Montrer que tous les idéaux de l'anneau quotient A/I sont principaux.

(2) Trouver tous les idéaux des anneaux suivants : $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}[x]/(f)$ où (f) est l'idéal principal engendré par un polynôme f.

(3) Trouver les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ et de $\mathbb{Q}[x]/(f)$.

Exercice 34

(1) Les idéaux $(5, x^2+3)$, $(x^2+1, x+2)$, (x^3-1, x^4-1) sont-ils principaux dans $\mathbb{Z}[x]$?

(2) Les idéaux $(x, x+1)$, $(5, x^2+4)$ et $(x^2+1, x+2)$ sont-ils premiers ou maximaux dans $\mathbb{Z}[x]$?

Exercice 35

Soient A un anneau intègre et K son corps de fractions. On dit qu'un élément x de K est *entier* sur A s'il vérifie une équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \qquad \text{avec } a_i \in A.$$

On dit que A est *intégralement clos* si pour tout $x \in K$ qui est entier sur A on a $x \in A$.

(1) Montrer qu'un anneau factoriel est intégralement clos.

(2) Soit d un entier sans facteur carré. Posons $A = \mathbb{Z}[X]/(X^2-d)$ et δ la classe de X dans A. Montrer que si $d \equiv 1 \mod 4$, alors A n'est pas intégralement clos.

Exercice 36

On dit qu'un nombre algébrique (sur $\mathbb{Q}$) est un *entier algébrique* s'il est racine d'un polynôme unitaire à coefficients entiers.

(1) Montrer qu'un nombre algébrique est un entier algébrique si et seulement si son polynôme minimal sur $\mathbb{Q}$ est à coefficients entiers.

(2) Montrer qu'un nombre rationnel est un entier algébrique si et seulement s'il est entier.

(3) On suppose que α est un nombre algébrique et racine d'un polynôme irréductible

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \qquad \text{avec } a_n \neq 0,\ a_i \in \mathbb{Z}.$$

Montrer que $a_n\alpha$ est un entier algébrique.

(4) Les nombres algébriques suivants sont-ils des entiers algébriques : i, $\frac{i}{2}$, $\frac{1}{2}(1+\sqrt{2})$, $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$?
Dans la suite, on fixe un entier $d \in \mathbb{Z}$ sans facteur carré, une de ses racines carrées $\delta \in \mathbb{C}$ et le corps $\mathbb{Q}(\delta)$.

(5) Montrer que le polynôme $X^2 - 2aX + a^2 - db^2$ annule $a + b\delta$. Montrer que $a + b\delta$ pour $a, b \in \mathbb{Q}$ est un entier algébrique si et seulement si $a^2 - db^2$ et $2a$ sont des entiers.

(6) Déterminer les entiers algébriques du corps $\mathbb{Q}(i)$.

(7) Montrer que les entiers algébriques de $\mathbb{Q}(\sqrt{2})$ sont les $a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$.

(8) Est-il vrai que les entiers algébriques de $\mathbb{Q}(i\sqrt{3})$ sont les $a + ib\sqrt{3}$ avec $a, b \in \mathbb{Z}$?

Exercice 37

Théorème des zéros de Hilbert.

(1) Soit E un espace vectoriel et $\mathcal{B} = (e_i)_{i\in\mathbb{N}}$ une base dénombrable de E.
Soit $\mathcal{C}$ une famille libre de E. Montrer que
$$\mathcal{C} = \bigcup_{n\in\mathbb{N}} \mathcal{C} \cap \mathrm{Vect}(e_0, \dots, e_n).$$
En déduire que $\mathcal{C}$ est au plus dénombrable.

Justifier que l'on peut donc parler d'espace vectoriel de dimension dénombrable.

(2) Montrer que $\mathbb{C}[X_1, \dots, X_n]$ est un espace vectoriel de dimension dénombrable.

(3) Montrer que $\mathbb{C}(X)$ n'est pas un espace vectoriel de dimension dénombrable.

(4) Soit $(a_1, \dots, a_n) \in \mathbb{C}^n$. Montrer que l'idéal $I = (X_1 - a_1, \dots, X_n - a_n)$ de $\mathbb{C}[X_1, \dots, X_n]$ est maximal.

Réciproquement, soit I un idéal maximal de $\mathbb{C}[X_1, \dots, X_n]$.

(5) Montrer que si $n = 1$, il existe $a_1 \in \mathbb{C}$ tel que $I = (X_1 - a_1)$.

(6) Pour $i = 1, \dots, n$, soit
$$\varphi_i : \mathbb{C}[X_i] \longrightarrow \mathbb{C}[X_1, \dots, X_n]/I.$$
Montrer que φ_i n'est pas injective.

(7) Montrer qu'il existe a_i tel que $\mathrm{Ker}\,\varphi_i = (X_i - a_i)$.

(8) En déduire que $I = (X_1 - a_1, \dots, X_n - a_n)$.

(9) Soit $P_1, \dots, P_m$ dans $\mathbb{C}[X_1, \dots, X_n]$ tels que
$$P_1(x) = \cdots = P_m(x)$$
n'a pas de solution dans $\mathbb{C}^n$.
Montrer qu'il existe $Q_1, \dots, Q_m$ dans $\mathbb{C}[X_1, \dots, X_n]$ tels que
$$1 = P_1Q_1 + \cdots + P_mQ_m.$$