Université d'Angers **2025-26**
L3 Math à Distance **Module 8 : Anneaux**

Examen Session 1 : Mardi 12 Mai 2026, 14h-16h30.

Aucun document, aucun appareil électronique n'est autorisé (téléphone, calculatrice, ...).
Le nombre total de points est 20.

Exercice 1 : Noyau d'un morphisme d'anneaux Total de la partie 1 : 3 pts

Soit A un anneau commutatif non trivial. Soit $\mathbb{K}$ un corps commutatif. Soit $f : A \to \mathbb{K}$ un morphisme d'anneaux de A vers $\mathbb{K}$.

(a) (1 point) Montrer que le noyau de f, $\ker f$, est un idéal de A.

Solution: $f(0) = 0$. Donc $0 \in \ker f$. Soient x et $y \in \ker f$. Alors $f(x+y) = f(x) + f(y) = 0 + 0 = 0$. Donc $x + y \in \ker f$. Et $f(-x) = -f(x) = -0 = 0$. Donc $-x \in \ker f$. Nous avons donc montré que comme f est un morphisme de groupes, $\ker f$ est un sous-groupe de A.
Soient $a \in A$ et $x \in \ker f$. Alors $f(ax) = f(a)f(x) = f(a)0 = 0$. Donc $ax \in \ker f$.

(b) (1 point) Montrer que $\ker f$ est un idéal premier.

Solution: Soient a et b deux éléments de A tel que $ab \in \ker f$. Alors $f(ab) = f(a)f(b) = 0$. Comme $\mathbb{K}$ est un corps donc est intègre. Cela implique que $f(a) = 0$ (ou $f(b) = 0$), c'est à dire $a \in \ker f$.

(c) (1 point) Donner un exemple où $\ker f$ n'est pas un idéal maximal.

Solution: $\mathbb{Z}$ est un anneau intègre mais pas un corps donc (0) est un idéal premier mais pas un idéal maximal. Soit $f : \mathbb{Z} \to \mathbb{Q}$ l'inclusion des entiers dans les rationnels. Alors f est injectif donc $\ker f = \{0\}$. Si A est un anneau principal alors tout idéal premier non nul est maximal. Donc pour trouver un exemple d'idéal premier non nul et maximal, il faut considérer un anneau non principal, par exemple $\mathbb{Z}[X]$. Soit $ev : \mathbb{Z}[X] \to \mathbb{Q}$ l'application qui à tout polynôme P à coefficients entiers associe son terme constant $P(0)$. Alors ev est un morphisme d'anneaux d'image $\mathbb{Z}$ et de noyau (X), l'idéal principal engendré par le monôme X. Donc $\mathbb{Z}[X]/(X)$ est isomorphe à $\mathbb{Z}$. Comme $\mathbb{Z}$ est intègre, (X) est un idéal premier. Comme $\mathbb{Z}$ n'est pas un corps, (X) n'est pas un idéal maximal. Donc $\mathbb{Z}[X]$ n'est pas un anneau principal.

Exercice 2 : Polynômes minimaux de bas degré Total de la partie 2 : 4 pts

Soit $\mathbb{K}$ un corps commutatif de caractéristique différente de 2. Soit B une $\mathbb{K}$-algèbre non triviale. Alors B est muni d'un morphisme d'anneaux $f : \mathbb{K} \to B$. Comme $\mathbb{K}$ est un corps et B n'est pas trivial, alors f est injectif. On peut donc considérer que $\mathbb{K}$ est un sous-anneau de B. Soit α un élément de B. Soit $\mu_\alpha \in \mathbb{K}[X]$ son polynôme minimal.

(a) (1 point) Montrer que μ_α n'est pas de degré 0.

Solution: Supposons que μ_α est de degré 0. Alors $\mu_\alpha = 1_\mathbb{K}$. Donc $\mu_\alpha(\alpha) = 1_B = 0$. Donc B est l'anneau trivial !

(b) (1 point) Montrer que α appartient à $\mathbb{K}$ ssi μ_α est de degré 1.

Solution: Supposons que $\alpha \in \mathbb{K}$. Alors le polynôme de $\mathbb{K}[X]$, $X - \alpha$ annule α. D'après la question précédente, μ_α est degré ≥ 1. Donc $\mu_\alpha(X) = X - \alpha$.
Réciproquement, supposons que $\mu_\alpha(X) = X + a_0$. Alors $\mu_\alpha(\alpha) = \alpha + a_0 = 0$. Donc $\alpha = -a_0 \in \mathbb{K}$.

(c) (2 points) Supposons que $\mu_\alpha(X) = X^2 + bX + c$ où b et $c \in \mathbb{K}$. Soit $\beta = 2\alpha + b$. Soit μ_β le polynôme minimal de β. Montrer que $\mu_\beta(X) = X^2 - (b^2 - 4c)$.

Solution: Comme $\alpha^2 + b\alpha = -c$, $\beta^2 = 4\alpha^2 + 4b\alpha + b^2 = b^2 - 4c$. Donc $X^2 - (b^2 - 4c)$ est un polynome annulateur de β. Comme μ_α n'est pas de degre 1, $\alpha \notin \mathbb{K}$. Comme $\alpha = \frac{\beta - b}{2}$, $\beta \notin \mathbb{K}$. Donc μ_β n'est pas de degré 1, ni de degré 0. Donc $\mu_\beta(X) = X^2 - (b^2 - 4c)$.

Exercice 3 : Anneaux de cardinal 9 Total de la partie 3 : 7 pts

(a) (1 point) Montrer que le polynôme $X^2 + 1$ est un élément irréductible de $\mathbb{F}_3[X]$.

Solution: 0, 1 et 2 ne sont pas racines de X^2+1. Donc d'après la proposition **??** $X^2 + 1$ est irréductible.

(b) (2 points) Montrer que les anneaux $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{F}_3[X]/(X^2+1)$ et $\mathbb{F}_3[X]/(X^2)$ ne sont pas isomorphes.

Solution: Vidéo du regroupement Jeudi 10 Avril 2026, partie 4.
Posons $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$. Comme $X^2 + 1$ est irréductible, $\mathbb{F}_9$ est un corps. Comme $\mathbb{F}_9$ est le seul corps, il n'est pas isomorphe aux autres anneaux. $\mathbb{Z}/9\mathbb{Z}$ est le seul anneau de caractéristique 9. Pour tout $x \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $x^2 = (a, b)^2 = (a^2, b^2) = 0$ implique $x = (a, b) = (0, 0)$. Donc aucun élément de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ non nul n'est de carré nul. Dans $\mathbb{F}_3[X]/(X^2)$, il y a un élément ($\overline{X}$!) non nul dont le carré est nul.

(c) (2 points) Montrer que si B est un anneau de cardinal p^2 où p est un nombre premier différent de 2, alors B est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à un quotient de l'anneau

des polynômes $\mathbb{F}_p[X]$ par l'idéal principal $(X^2 - D)$, engendré par un polynôme de la forme $X^2 - D$ où $D \in \mathbb{F}_p$. Indication : utiliser l'exercice sur les polynômes minimaux de bas degré.

Solution: La caractéristique de B divise p^2. Si la caractéristique de B est p^2 alors B est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Supposons que la caractéristique de B est p. Alors B est un $\mathbb{F}_p$-algèbre de dimension 2. Soit $\alpha \in B$ et pas dans $\mathbb{F}_p$. Alors la famille 1_B, α est libre donc génératrice du $\mathbb{F}_p$-espace vectoriel B de dimension 2. Donc B est égal à $\mathbb{F}_p[\alpha]$, la $\mathbb{F}_p$-algèbre engendré par α. En particulier B est commutative.

Plus précisément, la proposition **??** montre que α admet un polynôme minimal μ_α de degré inférieur ou égal à 2. Ce polynôme n'est pas de degré 1 car $\alpha \notin \mathbb{F}_p$. Donc $\mu_\alpha(X) = X^2 + bX + c$ et $\mathbb{F}_p[X]/(\mu_\alpha)$ est isomorphe à B. D'après l'exercice sur les polynômes minimaux de bas degré, $\beta = 2\alpha + b$ a pour polynôme minimal $\mu_\beta(X) = X^2 - D$ où $D = b^2 - 4c$ et donc en remplaçant α par β, $\mathbb{F}_p[X]/(\mu_\beta)$ est isomorphe à B.

(d) (2 points) Montrer que si B est un anneau de cardinal 9 alors B est isomorphe à $\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{F}_3[X]/(X^2 + 1)$ ou $\mathbb{F}_3[X]/(X^2)$.

Solution: D'après la question précédente, si caract B=9 alors B est isomorphe à $\mathbb{Z}/9\mathbb{Z}$. Sinon la caractéristique de B est 3. Et B est isomorphe à $\mathbb{F}_3[X]/(X^2-D)$ où $D \in \mathbb{F}_3$. Il y a 3 polynômes de ce type modulo 3.

-$X^2 + 1$ irréductible qui donne le corps $\mathbb{F}_9$.

-$X^2 + 2 = (X - 1)(X - 2)$. D'après le théorème des restes chinois, comme $X - 1$ et $X - 2$ sont premiers entre eux, $\mathbb{F}_3[X]/((X - 1)(X - 2))$ est isomorphe à $\mathbb{F}_3[X]/(X - 1) \times \mathbb{F}_3[X]/(X - 2)$. Or $\mathbb{F}_3[X]/(X - a) = \mathbb{F}_3$. Donc B est isomorphe à $\mathbb{F}_3 \times \mathbb{F}_3$.

-$X^2 + 0$. Donc B est isomorphe à $\mathbb{F}_3[X]/(X^2)$.

Exercice 4 : Décomposition en somme de carrés Total de la partie 4 : 6 pts

(a) (1 point) $9409 = 97^2$ s'écrit comme la somme des deux carrés d'entiers : $9409 = 97^2 + 0^2$. Trouver l'autre décomposition de 9409 en somme de deux carrés d'entiers.

Solution: 97 est un nombre premier impaire et $97 \equiv 1 \pmod 4$. Donc 97 s'écrit comme somme de deux carres. On trouve $97 = 9^2 + 4^2 = (9 + 4i)(9 - 4i)$. Donc $97^2 = (9 + 4i)^2(9 - 4i)^2$ est le carré du module de $(9 + 4i)^2 = 81 + 72i + 16i^2 = 65 + 72i$. Donc $97^2 = 65^2 + 72^2$.

(b) (1 point) Expliquer à l'aide des théorèmes du cours pourquoi $49725 = 3^2 \times 5^2 \times 13 \times 17$ se décompose en somme de carrés d'entiers.

Solution: $3 \equiv 3 \pmod 4$. Mais sa puissance 2 est pair. 5, 13 et 17 sont des nombres premiers congrus à 1 modulo 4. Donc 49725 se décompose en somme de carrés d'entiers.

(c) (1 point) Donner la décomposition de 49725 en facteurs irréductibles dans l'anneau de Gauss $\mathbb{Z}[i]$.

Solution: $49725 = 3^2 \times (2+i)^2(2-i)^2(3+2i)(3-2i)(4+i)(4-i)$

(d) (2 points) En déduire tous les entiers de Gauss $A+iB$ tel que

$$49725 = (A+iB)(A-iB).$$

Solution: L'entier de Gauss $A+iB$ est égal à 12 entiers de Gauss :
$3(2+i)^2(3+2i)(4+i) = 3(3+4i)(10+11i) = 3(30+33i+40i+44i^2) = 3(-14+73i) = -42+219i$ ou son conjugué
ou
$3(2+i)^2(3+2i)(4-i) = 3(3+4i)(14+5i) = 3(42+15i+56i+20i^2) = 3(22+71i) = 66+213i$ ou son conjugué
ou
$3(2+i)^2(3-2i)(4+i) = 3(3+4i)(14-5i) = 3(42-15i+56i-20i^2) = 3(62+41i) = 186+123i$ ou son conjugué
ou
$3(2+i)^2(3-2i)(4-i) = 3(3+4i)(10-11i) = 3(30-33i+40i-44i^2) = 3(74+7i) = 222+21i$ ou son conjugué
ou
$3(2+i)(2-i)(3+2i)(4+i) = 3 \times 5(10+11i) = 150+165i$ ou son conjugué
ou
$3(2+i)(2-i)(3+2i)(4-i) = 3 \times 5(14+5i) = 210+75i$ ou son conjugué
Car $(2+i)^2 = 4+4i+i^2 = 3+4i$.
$(3+2i)(4+i) = 12+8i+3i+2i^2 = 10+11i$ et $(3+2i)(4-i) = 12+8i-3i-2i^2 = 14+5i$.

(e) (1 point) En déduire toutes les décompositions de 49725 en sommes de carrés d'entiers.

Solution: $49725 = 42^2+219^2 = 66^2+213^2 = 186^2+123^2 = 222^2+21^2 = 150^2+165^2 = 210^2+75^2$ admet 6 decompositions comme somme de carres d'entiers.