Université de Poitiers, Année 2024-2025

3e année de Licence de Mathématiques, Anneaux

Corrigé de l'examen du mercredi 7 mai 2025

Exercice 1 – Questions de cours (4 points)

1. Donner la définition d'un polynôme sur un anneau commutatif A.

   Un *polynôme sur A* (ou *à coefficients dans A*) est une suite presque nulle $P = (a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, ..., a_i, ...)$ d'éléments de A. *Autrement dit, la suite n'a qu'un nombre fini de termes non nuls : il existe un entier $n \in \mathbb{N}$ tel que $a_i = 0_A$ pour tout $i > n$.*

2. Soit A un anneau factoriel.

   (a) Donner la définition d'un polynôme primitif $P \in A[X]$.
   Un polynôme $P \in A[X]$ est dit *primitif* si 1_A est un $PGCD$ de ses coefficients.

   (b) Énoncer le Lemme de Gauss.
   Soient P et Q deux polynômes sur K_A et $C(P)$ et $C(Q)$ des contenus de P et Q. Alors $C(P)C(Q)$ est un contenu de PQ.

   (c) Démontrer que, si U et V sont deux polynômes unitaires à coefficients dans $\mathbb{Q}$ tels que $UV \in \mathbb{Z}[X]$, alors U et V appartiennent à $\mathbb{Z}[X]$.
   Soient $C(U)$ et $C(V)$ des contenus de U et V respectivement et U^* et V^* des polynômes primitifs tels que $U = C(U)U^*$ et $V = C(V)V^*$. On note a et b les coefficients des termes de plus haut degré de U^* et V^*. Comme U et V sont unitaires, on a $C(U) = a^{-1}$ et $C(V) = b^{-1}$. Le fait que U et V soient unitaires implique aussi que $UV \in \mathbb{Z}[X]$ est unitaire, donc UV est un polynôme primitif. Le lemme de Gauss donne alors $a^{-1}b^{-1} = \pm 1$, d'où $a = \pm 1$ et $b = \pm 1$. On en déduit que $U = \pm U^*$ et $V = \pm V^*$ appartiennent à $\mathbb{Z}[X]$.

Exercice 2 – *Exercice issu du DM* (3 points)
Soit A un anneau intègre. Une application $N : A^* \to \mathbb{N}$ est dite être une *norme de Dedekind-Hasse* si, pour tout couple (a, b) d'éléments non nuls de A :

- soit b divise a ;
- soit il existe $x, y \in A$ tels que $ax - by \neq 0_A$ et $N(ax - by) < N(b)$.

Nous montrons que tout anneau principal possède une norme de Dedekind-Hasse.
On fixe un anneau principal A.

1. Pourquoi tout $x \in A$ non nul se décompose en un produit d'un élément inversible u par un produit d'éléments irréductibles $p_1, \cdots, p_r$, et que l'entier r est indépendant de la décomposition choisie de x ? *On note alors* $N(x) = r$.

   Cette décomposition et son unicité (et, en particulier, l'indépendance de l'entier r) sont valables dans tout anneau factoriel. Or A est un anneau principal, donc c'est un anneau factoriel, d'où le résultat.

2. Soient (a, b) un couple d'éléments non nuls de A. On suppose que b ne divise pas a.

   (a) Pourquoi a et b admettent-il un $PGCD$? *On fixe d un $PGCD$ de a et b.*

   Les anneaux principaux sont des anneaux à $PGCD$, donc a et b admettent un $PGCD$.

   (b) Justifier l'existence d'éléments x et y de A tels que $ax - by = d$.

   Comme A est un anneau principal, il existe $c \in A$ tel que $(a) + (b) = (c)$. En particulier, on a $a \in (c)$ et $b \in (c)$, donc c est un diviseur commun de a et b. Alors c divise d par définition d'un $PGCD$, d'où $(d) \subseteq (c) = (a) + (b)$. On obtient $d \in aA + bA$, d'où l'existence de x et y tels que $ax - by = d$.

   (c) Démontrer que N est une norme de Dedekind-Hasse. D'après la question 1, on peut décomposer b sous la forme $b = up_1 \dots p_r$ pour $u \in A$ inversible et des éléments irréductibles $p_1, \cdots, p_r$. Comme d divise b et que l'anneau A est factoriel (car principal), alors il existe $v \in A$ inversible et des entiers distincts $i_1, \dots, i_s$ dans $\{1, \dots, r\}$ tels que $d = vp_{i_1} \dots p_{i_s}$. Si on a $s = r$, alors on a $d = vp_1 \dots p_r = vu^{-1}b$, donc b divise d, ce qui implique que b divise a, en contradiction avec le choix de a et b. On en déduit que $s < r$, ce qui signifie que $N(d) = N(ax - by) < N(b)$. On a démontré que N est une norme de Dedekind-Hasse.

Exercice 3 – *Exercice 3 de la fiche de TD n° 5* (5 points)

1. Soit A un anneau principal.

   (a) Soit p un élément irréductible de A. Montrer que (p) est un idéal maximal de A.

   Comme p est un élément irréductible, il est non inversible et (p) est un idéal propre de A.

   Si M est un idéal propre de A contenant (p) alors, comme A est principal, il existe $\alpha \in A$ tel que $M = (\alpha)$. On obtient $p \in (p) \subseteq M = (\alpha) = A\alpha$, donc $p = u\alpha$ pour $u \in A$. Par irréductibilité de p, l'un des éléments u ou α est inversible, et comme $(\alpha) = M \neq A$, ce ne peut pas être α. Ceci démontre que p et α sont associés, donc $(p) = (\alpha) = M$ est un idéal maximal de A.

   (b) En déduire que les idéaux premiers non nuls de A sont maximaux.

   Soit I un idéal premier non nul de A. Alors $I = (p)$ pour $p \in A$ puisque A est principal. Comme I est un idéal premier et non nul, on en déduit que p est un élément premier de A, c'est donc un élément irréductible. D'après la question 1.(a), l'idéal $I = (p)$ est donc maximal, ce qui démontre que idéaux premiers non nuls de A sont maximaux.

2. Soit $\mathrm{ev}_0 : \mathbb{Z}[X] \to \mathbb{Z}$ l'évaluation en 0. *On rappelle que* ev_0 *est un morphisme d'anneaux.*

   (a) Montrer que ev_0 est surjectif et que $\operatorname{Ker} \mathrm{ev}_0 = (X)$.

   Pour tout $a \in \mathbb{Z}$, si on note $P_a \in \mathbb{Z}[X]$ le polynôme constant égal à a, on a $\mathrm{ev}_0(P_a) = P_a(0) = a$, donc ev_0 est surjectif.

   L'ensemble $\operatorname{Ker} \mathrm{ev}_0$ est constitué des polynômes $P \in \mathbb{Z}[X]$ ayant 0 comme racine, ce qui équivaut à dire que $X = X - 0$ divise P, ou encore que P appartient à (X). Ainsi on a bien $\operatorname{Ker} \mathrm{ev}_0 = (X)$.

   (b) En déduire que (X) est un idéal premier de $\mathbb{Z}[X]$, mais n'est pas un idéal maximal.

   D'après la question 2.(a) et le théorème d'isomorphisme, les anneaux $\mathbb{Z}[X]/(X)$ et $\mathbb{Z}$ sont isomorphes. En particulier, l'anneau $\mathbb{Z}[X]/(X)$ est intègre sans être un corps, donc (X) est un idéal premier de $\mathbb{Z}[X]$ qui n'est pas maximal.

   (c) Conclure que $\mathbb{Z}[X]$ n'est pas un anneau principal.

   Comme (X) est un idéal premier non nul, l'élément X est premier dans $\mathbb{Z}[X]$, et il est donc irréductible. Comme (X) n'est pas maximal, l'anneau $\mathbb{Z}[X]$ n'est pas principal d'après la question 1.(a).

Exercice 4 – (10 points)

On rappelle que $\mathbb{Z}[i]$ *est le sous-anneau de* $\mathbb{C}$ *engendré par* $\mathbb{Z}$ *et* i*, que* $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ *et que l'écriture de ses éléments sous la forme* $a + ib$ *pour* a *et* b *dans* $\mathbb{Z}$ *est unique. En outre, ses éléments inversibles sont ceux de module* 1*, c'est-à-dire* $+1$*,* -1*,* i *et* $-i$*.*

1. On considère l'application $\varphi : \mathbb{Z}[i] \to \mathbb{N}$ définie par $\varphi(z) = |z|^2$.

   (a) Vérifier que, pour tout couple d'éléments non nuls (a, b) de $\mathbb{Z}[i]$, si b divise a, alors $\varphi(b) \leqslant \varphi(a)$.

   Si b divise a, il existe $d \in \mathbb{Z}[i]$ tel que $a = bd$ avec d non nul puisque $a \neq 0$. On a donc $\varphi(d) \geqslant 1$ et $\varphi(b) = \frac{\varphi(a)}{\varphi(b)} \leqslant \varphi(a)$.

   (b) Démontrer que, pour tout couple $(a, b) \in \mathbb{Z}[i]^2$ avec b non nul, il existe des éléments q et r de $\mathbb{Z}[i]$ tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$.

   Il existe des entiers rationnels x et y tels que $\frac{a}{b} = x + iy$. On considère des entiers x' et y' tels que $|x - x'| \leqslant \frac{1}{2}$ et $|y - y'| \leqslant \frac{1}{2}$, et on note $q = x' + iy' \in \mathbb{Z}[i]$ et $r = a - bq$. On a donc $a = bq + r$ et, comme $r = b(\frac{a}{b} - q)$, on a aussi $\varphi(r) = \varphi(b)\varphi((x-x')+i(y-y')) = \varphi(b)(|x-x'|^2+|y-y'|^2) \leqslant \varphi(b)(\frac{1}{2^2}+\frac{1}{2^2}) < \varphi(b)$.

   (c) En déduire que $\mathbb{Z}[i]$ est un anneau euclidien.

   Il suit de 1.(a) et 1.(b) que la restriction de φ à $\mathbb{Z}[i]^*$ est un stathme euclidien pour $\mathbb{Z}[i]$, donc $\mathbb{Z}[i]$ est un anneau euclidien.

2. Pour tout idéal I de $\mathbb{Z}[i]$, on note $\mathrm{Tr}(I) = I \cap \mathbb{Z}$ la *trace de* I *sur* $\mathbb{Z}$.

   (a) Expliquer pourquoi la trace de tout idéal de $\mathbb{Z}[i]$ est un idéal de $\mathbb{Z}$.

   Comme I est un idéal de $\mathbb{Z}[i]$ et $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$, ce sont des sous-groupes de $(\mathbb{Z}[i], +)$, et $I \cap \mathbb{Z}$ est donc un sous-groupe de $(\mathbb{Z}[i], +)$. Pour tous $x \in I \cap \mathbb{Z}$ et tout $a \in \mathbb{Z}$, on a $xa \in I$ puisque I est un idéal de $\mathbb{Z}[i]$ et $xa \in \mathbb{Z}$ puisque $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$, donc $xa \in I \cap \mathbb{Z}$. Ceci montre que $\mathrm{Tr}(I) = I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.

   (b) Montrer que la trace de tout idéal non nul de $\mathbb{Z}[i]$ est un idéal non nul de $\mathbb{Z}$.

   Si I est un idéal non nul de $\mathbb{Z}[i]$, il existe $z \in I$ non nul. On a donc $\varphi(z) = |z]^2 \in \mathbb{N}^*$. Or, comme $z \in \mathbb{Z}[i]$, on a aussi $\overline{z} \in \mathbb{Z}[i]$, d'où $\varphi(z) = z\overline{z} \in I$. Ainsi $\varphi(z)$ est un élément non nul de $\mathrm{Tr}(I) = I \cap \mathbb{Z}$, et $\mathrm{Tr}(I)$ est donc un idéal non nul de $\mathbb{Z}$.

3. On fixe un élément irréductible α de $\mathbb{Z}[i]$ et on note $M = (\alpha)$.

   (a) Montrer l'existence d'un morphisme d'anneaux injectif de $\mathbb{Z}/\mathrm{Tr}(M)$ dans $\mathbb{Z}[i]/M$.

   La surjection canonique de $\mathbb{Z}[i]$ dans $\mathbb{Z}[i]/M$ est un morphisme d'anneaux, donc sa restriction $f : \mathbb{Z} \to \mathbb{Z}[i]/M$ à $\mathbb{Z}$ aussi. D'après le théorème d'isomorphisme, il y a un isomorphisme d'anneaux de $\mathbb{Z}/\mathrm{Ker}\, f$ dans $\mathrm{Im}\, f$, ce qui donne un morphisme d'anneaux injectif $g : \mathbb{Z}/\mathrm{Ker}\, f \to \mathbb{Z}[i]/M$.

   Or, comme f est une restriction de la surjection canonique $\mathbb{Z}[i] \to \mathbb{Z}[i]/M$, on a $\mathrm{Ker}\, f = M \cap \mathbb{Z} = \mathrm{Tr}(M)$ et g est le morphisme d'anneaux recherché.

   (b) En déduire que $\mathrm{Tr}(M)$ est un idéal premier et non nul de $\mathbb{Z}$.

   Comme M est un idéal non nul de $\mathbb{Z}[i]$, la question 2.(b) montre que $\mathrm{Tr}(M)$ est un idéal non nul de $\mathbb{Z}$.

Comme $\mathbb{Z}[i]$ est euclidien, c'est un anneau à $PGCD$ et ses éléments irréductibles sont premiers. En particulier, l'élément α est premier et M est donc un idéal premier de $\mathbb{Z}[i]$. Ainsi, l'anneau quotient $\mathbb{Z}[i]/M$ est intègre, et ses sous-anneaux sont donc aussi intègres. En particulier, si $g : \mathbb{Z}/\mathrm{Tr}(M) \to \mathbb{Z}[i]/M$ est un morphisme injectif (un tel morphisme existe d'après la question 3.(a)), alors $\mathbb{Z}/\mathrm{Tr}(M)$ est isomorphe au sous-anneau $\mathrm{Im}\, f$ de $\mathbb{Z}[i]/M$ d'après le théorème d'isomorphisme, donc $\mathbb{Z}/\mathrm{Tr}(M)$ est un anneau intègre. Ainsi $\mathrm{Tr}(M)$ est un idéal premier de $\mathbb{Z}$.

(c) Justifier l'existence d'un nombre premier p tel que $\mathrm{Tr}(M) = p\mathbb{Z}$.

Comme les idéaux premiers de $\mathbb{Z}$ sont l'idéal nul et les idéaux de la forme $p\mathbb{Z}$ pour un nombre premier p, l'existence de p découle de la question 3.(b).

(d) Vérifier que α divise p.

On a $p \in \mathrm{Tr}(M) \subseteq M = (\alpha)$, donc α divise p.

4. On suppose $p \equiv 3$ [4]. Montrer que α est associé à p.

D'après la question 3.(d), il existe $u \in \mathbb{Z}[i]$ tel que $p = u\alpha$. Alors on a $\varphi(u)\varphi(\alpha) = \varphi(u\alpha) = \varphi(p) = p^2$. Comme α n'est pas inversible, et comme p est un nombre premier, on a $\varphi(\alpha) \in \{p, p^2\}$. Or, il existe des entiers a et b tels que $\alpha = a + ib$ et on a $\varphi(\alpha) = a^2 + b^2$. Tous les carrés dans $\mathbb{Z}$ étant congrus à 0 ou 1 modulo 4, l'entier $a^2 + b^2$ ne peut pas être congru à 3 modulo 4, ce qui interdit $\varphi(\alpha) = p$. On en déduit que $\varphi(\alpha) = p^2$, donc $\varphi(u) = 1$ et u est inversible. Ceci démontre que α est associé à p.

5. On suppose que $p = 2$. Montrer que α est associé à $1 + i$.

On rappelle que, comme α est irréductible dans l'anneau euclidien $\mathbb{Z}[i]$, c'est un élément premier de $\mathbb{Z}[i]$. Ainsi comme α divise $p = 2 = (1 + i)(1 - i)$, il divise $1 + i$ ou $1 - i$. Or on a $1 + i = i(1 - i)$, donc α divise $1 + i$, d'où $1 + i = u\alpha$ pour $u \in \mathbb{Z}[i]$. On en déduit que $\varphi(u)\varphi(\alpha) = \varphi(u\alpha) = \varphi(1 + i) = 2$, et α n'étant pas inversible, on obtient $\varphi(u) = 1$ et $\varphi(\alpha) = 2$, donc u est inversible et α est associé à $1 + i$.

6. On suppose $p \equiv 1$ [4].

On rappelle que -1 est alors un carré dans $\mathbb{Z}/p\mathbb{Z}$.

(a) Pourquoi p n'est-il pas irréductible dans $\mathbb{Z}[i]$?

D'après le rappel, il existe $x \in \mathbb{Z}$ tel que x^2 est congru à -1 modulo p. Alors p divise $x^2 + 1 = (x + i)(x - i)$. Pourtant, aucun des éléments $x + i$ et $x - i$ n'est divisible par p dans $\mathbb{Z}[i]$, donc p n'est pas premier dans $\mathbb{Z}[i]$ et, comme $\mathbb{Z}[i]$ est un anneau euclidien (et donc aussi à $PGCD$), ce n'est pas un élément irréductible dans $\mathbb{Z}[i]$.

(b) Montrer que les diviseurs irréductibles de p sont les nombres complexes de la forme $a + ib$ pour $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.

Si $a + ib$ est un diviseur irréductible de p pour $(a, b) \in \mathbb{Z}^2$, alors $\varphi(a + ib) = a^2 + b^2$ divise $\varphi(p) = p^2$ (dans $\mathbb{Z}$), donc on a $a^2 + b^2 \in \{1, p, p^2\}$.

- Si $a^2 + b^2 = 1$, alors $a + ib$ est inversible, ce qui contredit son irréductibilité.
- Si $a^2 + b^2 = p^2$, alors $a + ib$ est associé à p, ce qui contredit la non-irréductibilité de p.

On en déduit que $a^2 + b^2 = p$. Dans ce cas, l'élément $a + ib$ est non inversible et ses diviseurs non inversibles sont de module p, ils sont donc associés à $a + ib$, ce qui démontre l'irréductibilité de $a + ib$.