

Corrigé du contrôle de maths L3 : anneaux, idéaux et polynômes irréductibles

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours : idéaux premiers et maximaux	3 points
Exercice 2 : Les idéaux de $\mathbb{Z}/12\mathbb{Z}$	3 points
Exercice 3 : Idéaux de $\mathbb{Z}[X]$ et anneau quotient $\mathbb{R}[X]/(X^2+1)$	4 points
Exercice 4 : L'anneau des entiers de Gauss	5 points
Exercice 5 : Problème : irréductibilité de polynômes à coefficients entiers	5 points
Total	20 points

Exercice 1 : Question de cours : idéaux premiers et maximaux (3 points)

- a. Un idéal $I \neq A$ est **premier** si, pour tous $a, b \in A$, la condition $ab \in I$ entraîne $a \in I$ ou $b \in I$. Il est **maximal** s'il n'existe aucun idéal J tel que $I \subsetneq J \subsetneq A$.

Supposons d'abord I maximal. Comme $I \neq A$, l'anneau A/I n'est pas nul. Soit $\bar{x} \neq \bar{0}$, c'est-à-dire $x \notin I$. L'idéal $I + xA$ contient strictement I , donc il est égal à A par maximalité. Il existe alors $i \in I$ et $a \in A$ tels que $1 = i + xa$. Ainsi $\bar{x}\bar{a} = \bar{1}$: **A/I est un corps.**

Réciproquement, supposons que A/I soit un corps. Soit J un idéal tel que

$I \subsetneq J$, et $x \in J \setminus I$. Alors $\bar{x}$ est inversible : il existe $a \in A$ et $i \in I$ tels que $xa = 1 + i$. Donc $1 = xa - i \in J$, d'où $J = A$. Ainsi I est maximal.

- b. Si I est maximal, A/I est un corps d'après a). Or un corps est intègre : si $\bar{a}\bar{b} = \bar{0}$ avec $\bar{a} \neq \bar{0}$, on multiplie par $\bar{a}^{-1}$ et on obtient $\bar{b} = \bar{0}$. Donc A/I est intègre. **Par conséquent I est premier.**

Barème : a) 0,5 point pour les définitions, 0,75 point pour chaque sens de l'équivalence ; b) 0,5 point pour « un corps est intègre », 0,5 point pour la conclusion.

Exercice 2 : Les idéaux de $\mathbb{Z}/12\mathbb{Z}$ (3 points)

- a. Soit J un idéal de $\mathbb{Z}/12\mathbb{Z}$. Son image réciproque $\pi^{-1}(J)$ est un idéal de $\mathbb{Z}$ qui contient $12\mathbb{Z}$. Or $\mathbb{Z}$ est principal, donc $\pi^{-1}(J) = d\mathbb{Z}$ avec $d \geq 1$. De plus, $12 \in d\mathbb{Z}$ signifie que d divise 12. Comme π est surjective, $J = \pi(\pi^{-1}(J)) = \pi(d\mathbb{Z})$.

Réciproquement, l'image d'un idéal par un morphisme surjectif est un idéal. Enfin, deux diviseurs distincts donnent deux idéaux distincts, car $\pi^{-1}(\pi(d\mathbb{Z})) = d\mathbb{Z} + 12\mathbb{Z} = d\mathbb{Z}$.

Les diviseurs positifs de 12 sont 1, 2, 3, 4, 6 et 12. **On obtient six idéaux :**

$$\mathbb{Z}/12\mathbb{Z} : (\bar{2}) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} ; (\bar{3}) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} ; (\bar{4}) = \{\bar{0}, \bar{4}, \bar{8}\} ; (\bar{6}) = \{\bar{0}, \bar{6}\} ; \{\bar{0}\}.$$

- b. Le morphisme composé $\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z} \rightarrow (\mathbb{Z}/12\mathbb{Z})/(\bar{d})$ est surjectif, de noyau $d\mathbb{Z}$. Le premier théorème d'isomorphisme donne donc $(\mathbb{Z}/12\mathbb{Z})/(\bar{d}) \simeq \mathbb{Z}/d\mathbb{Z}$.

Pour $d \neq 1$, l'anneau $\mathbb{Z}/d\mathbb{Z}$ est intègre si et seulement si d est premier, et c'est alors un corps. Par exemple, $\{\bar{0}\}$ n'est pas premier, car $\bar{3} \times \bar{4} = \bar{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Les idéaux premiers sont $(\bar{2})$ et $(\bar{3})$, et ce sont aussi les idéaux maximaux.

Barème : a) 1 point pour la correspondance, 0,5 point pour la liste ; b) 0,5 point pour le quotient, 1 point pour les idéaux premiers et maximaux.

Exercice 3 : Idéaux de $\mathbb{Z}[X]$ et anneau quotient $\mathbb{R}[X]/(X^2+1)$ (4 points)

- a. L'évaluation $\text{ev}_0 : \mathbb{Z}[X] \rightarrow \mathbb{Z}, P \rightarrow P(0)$, est un morphisme d'anneaux. Il est surjectif, car l'entier n est l'image du polynôme constant n .

Calculons son noyau. Si $P = a_0 + a_1 X + \dots + a_n X^n$, alors $P(0) = 0$ équivaut à $a_0 = 0$, donc à $P = X Q$ avec $Q \in \mathbb{Z}[X]$. Ainsi $\text{Ker}(\text{ev}_0) = (X)$. Le premier théorème d'isomorphisme donne $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$.

Or $\mathbb{Z}$ est intègre sans être un corps, car 2 n'y est pas inversible. D'après l'exercice 1, (X) est premier mais n'est pas maximal. On a d'ailleurs $(X) [\subsetneq] (2, X) [\subsetneq] \mathbb{Z}[X]$.

- b. Considérons $\psi : \mathbb{Z}[X] \rightarrow \mathbb{Z}/2\mathbb{Z}$, qui associe à P la classe de $P(0)$ modulo 2. C'est un morphisme surjectif.

Son noyau est formé des P dont le coefficient constant est pair. Un tel P s'écrit $P = 2k + X Q$, donc il appartient à $(2, X)$. Inversement, tout élément $2U + X V$ de $(2, X)$ a un coefficient constant pair. Ainsi $\text{Ker} \psi = (2, X)$ et $\mathbb{Z}[X]/(2, X) \simeq \mathbb{Z}/2\mathbb{Z}$, qui est un corps. **Donc $(2, X)$ est maximal.**

- c. L'évaluation $\text{ev}_i : \mathbb{R}[X] \rightarrow \mathbb{C}, P \rightarrow P(i)$, est un morphisme d'anneaux. Il est surjectif, car $a + b i$ est l'image de $a + b X$.

Pour le noyau, effectuons la division euclidienne $P = (X^2 + 1) Q + a + b X$, avec a, b réels. Comme $i^2 + 1 = 0$, on obtient $P(i) = a + b i$. Ainsi $P(i) = 0$ équivaut à $a = b = 0$, c'est-à-dire à $X^2 + 1 \mid P$. Le noyau est donc $(X^2 + 1)$.

Par le premier théorème d'isomorphisme, $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

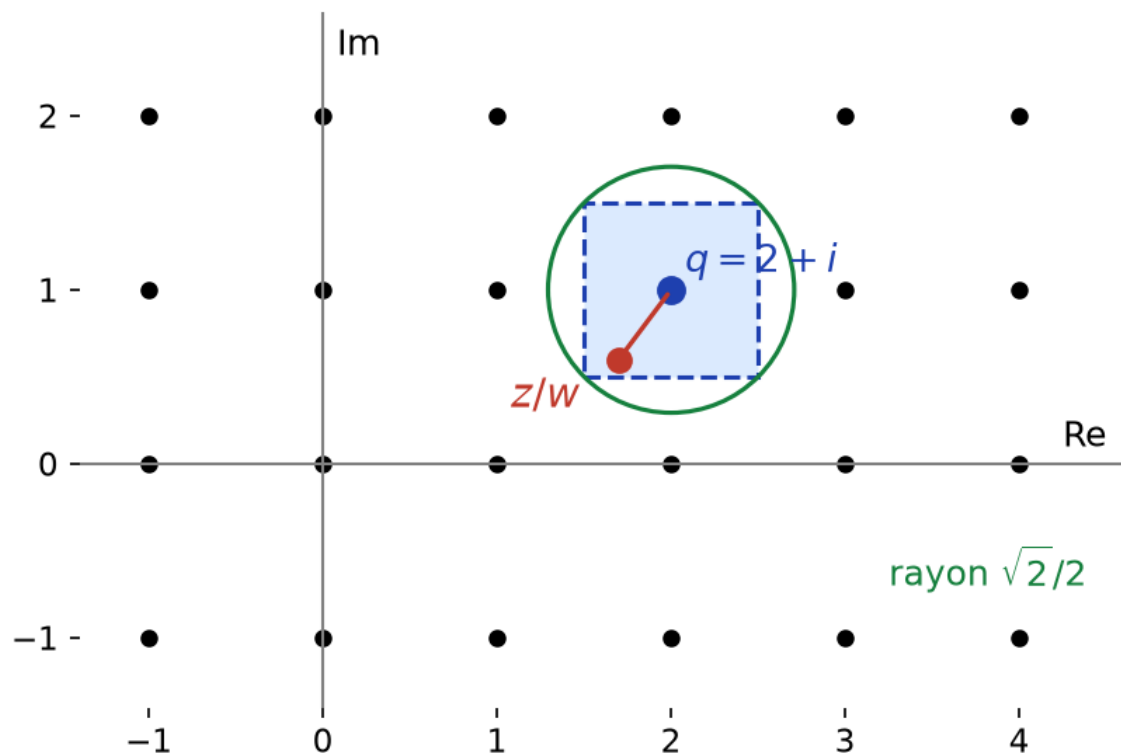
Barème : a) 0,5 point pour le morphisme, 0,5 point pour le noyau, 0,5 point pour premier non maximal ; b) 1 point ; c) 0,5 point pour la surjectivité, 0,5 point pour le noyau, 0,5 point pour la conclusion.

Exercice 4 : L'anneau des entiers de Gauss (5 points)

a. La conjugaison est multiplicative, donc $N(z w) = z w \overline{z w} = z \overline{z} w \overline{w} = N(z) N(w)$.

Si $u v = 1$, alors $N(u) N(v) = N(1) = 1$, avec $N(u), N(v)$ entiers naturels. Donc $N(u) = 1$, soit $a^2 + b^2 = 1$. Cela donne $u \in \{1, -1, i, -i\}$. Réciproquement, ces quatre éléments sont inversibles, puisque $i \times (-i) = 1$. **Les inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$.**

b. Soit $z \in \mathbb{Z}[i]$ et $w \neq 0$. Écrivons $\frac{z}{w} = x + i y$ avec x, y rationnels. On choisit des entiers a et b tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. On pose ensuite $q = a + i b$ et $r = z - q w$.



D'une part, $r \in \mathbb{Z}[i]$, car z et q sont. D'autre part,

$N(r) = |w|^2 \left| \frac{z}{w} - q \right|^2 \leq N(w) \left(\frac{1}{4} + \frac{1}{4} \right) = \frac{N(w)}{2}$. Donc $N(r) < N(w)$. Ainsi $\mathbb{Z}[i]$ est euclidien pour N .

c. On a $5 = (2 + i)(2 - i)$ et $13 = (3 + 2i)(3 - 2i)$.

Montrons que $2 + i$ est irréductible. Si $2 + i = uv$, alors $N(u)N(v) = 5$. Comme 5 est premier, $N(u) = 1$ ou $N(v) = 1$, donc u ou v est inversible. Le même argument s'applique à $2 - i$ (norme 5) et à $3 \pm 2i$ (norme 13, premier). Les facteurs ne sont pas inversibles, car leur norme diffère de 1.

Donc $5 = (2 + i)(2 - i)$ et $13 = (3 + 2i)(3 - 2i)$ sont des décompositions en irréductibles. En particulier, 5 et 13 ne sont pas irréductibles dans $\mathbb{Z}[i]$.

d. On a $N(3) = 9$. Supposons $3 = uv$ avec u et v non inversibles. Alors

$N(u)N(v) = 9$ et $N(u) \neq 1$, $N(v) \neq 1$. Donc $N(u) = 3$, soit $a^2 + b^2 = 3$.

Or un carré est congru à 0 ou 1 modulo 4. Une somme de deux carrés est donc congrue à 0, 1 ou 2 modulo 4, jamais à 3. C'est absurde. **Donc 3 est irréductible dans $\mathbb{Z}[i]$.**

Barème : a) 0,5 point pour la multiplicativité, 0,5 point pour les inversibles ; b) 0,5 point pour le choix de q , 1 point pour la majoration de $N(r)$; c) 0,5 point pour les décompositions, 1 point pour les justifications par la norme ; d) 1 point.

Erreur fréquente : conclure que 5 est irréductible dans $\mathbb{Z}[i]$ parce qu'il est premier dans $\mathbb{Z}$.

Exercice 5 : Problème : irréductibilité de polynômes à coefficients entiers (5 points)

- a. **Critère d'Eisenstein.** Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$, avec $n \geq 1$. On suppose qu'il existe un nombre premier p tel que p ne divise pas a_n , p divise $a_0, \dots, a_{n-1}$ et p^2 ne divise pas a_0 . Alors P est irréductible dans $\mathbb{Q}[X]$.

Pour $X^5 - 6X + 3$, on prend $p = 3$. En effet, 3 ne divise pas 1, 3 divise 0, -6 et 3, et 9 ne divise pas 3. **Donc $X^5 - 6X + 3$ est irréductible dans $\mathbb{Q}[X]$.**

- b. On a $(X - 1)\Phi = X^5 - 1$. En remplaçant X par $X + 1$, on obtient $(X + 1)\Phi(X + 1) = (X + 1)^5 - 1$. La formule du binôme donne alors :

$$\Phi(X + 1) = X^4 + 5X^3 + 10X^2 + 10X + 5.$$

Le critère d'Eisenstein s'applique avec $p = 5$: 5 divise 5, 10, 10 et 5, ne divise pas 1, et 25 ne divise pas 5. Donc $\Phi(X + 1)$ est irréductible.

Si l'on avait $\Phi = AB$ avec A et B non constants, alors

$\Phi(X + 1) = A(X + 1)B(X + 1)$ serait une factorisation en facteurs non constants. **Donc Φ est irréductible dans $\mathbb{Q}[X]$.**

- c. Le polynôme $X^3 + X + 1$ est de degré 3. S'il était réductible, il aurait un facteur de degré 1, donc une racine dans $\mathbb{F}_2$. Or il prend la valeur 1 en 0, et $1 + 1 + 1 = 1$ en 1. **Il n'a pas de racine, donc il est irréductible dans $\mathbb{F}_2[X]$.**

d. Modulo 2, on a $-4 \equiv 0$, $7 \equiv 1$ et $9 \equiv 1$. Donc $\bar{S} = X^3 + X + 1$, irréductible d'après c).

Supposons $S = AB$ dans $\mathbb{Q}[X]$, avec A et B non constants. Quitte à diviser A par son coefficient dominant et à multiplier B par ce même coefficient, on peut supposer A et B unitaires. Le lemme de Gauss donne alors $A, B \in \mathbb{Z}[X]$.

Réduisons modulo 2 : $\bar{S} = \bar{A} \bar{B}$. Comme A et B sont unitaires, $\bar{A}$ et $\bar{B}$ gardent leurs degrés, qui sont au moins 1. Cela contredit l'irréductibilité de $\bar{S}$. **Donc S est irréductible dans $\mathbb{Q}[X]$.**

Barème : a) 0,5 point pour l'énoncé, 0,5 point pour l'application ; b) 0,5 point pour le calcul de $\Phi(X+1)$, 0,5 point pour Eisenstein, 0,5 point pour le retour à Φ ; c) 1 point ; d) 0,5 point pour la réduction, 1 point pour l'argument (unitaires, lemme de Gauss, degrés conservés).

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : anneaux, idéaux et polynômes irréductibles

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Anneaux et idéaux](#) » en L3 puis entraînez-vous avec les **exercices corrigés** [anneaux et idéaux](#).

Retrouvez tous les [contrôles de maths de L3 classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).

Autres contrôles de maths de L3 sur ce thème

- [Contrôle de maths L3 : partiel d'algèbre : groupes, anneaux et corps](#)