Université de Rennes 1 — Année universitaire 2019-2020
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°3
Mercredi 6 mai 2020, 13h – 18h

On veillera à la qualité de la rédaction et de l'argumentation, de même qu'au soin apporté à la présentation. *Sauf mention expresse du contraire, une justification est attendue pour toutes les réponses.*

Les questions marquées du symbole **(*)** sont considérées comme plus difficiles. Traiter correctement une proportion raisonnable des *autres* questions assure déjà une bonne note.

Le symbole $\mathbf{C}$ désigne le corps des nombres complexes et i un élément de $\mathbf{C}$ tel que $i^2 = 1$. Les symbole $\mathbf{Z}$ et $\mathbf{N}$ désignent respectivement l'ensemble des entiers relatifs et naturels.

Exercice

1 On rappelle qu'on note $\mathbf{F}_3$ le corps $\mathbf{Z}/3\mathbf{Z}$. Déterminer, en expliquant soigneusement votre démarche, un élément P de $\mathbf{F}_3[X]$ de degré 3 et irréductible. On pose désormais $\mathbf{K} := \mathbf{F}_3[X]/\langle P\rangle$ et on note α l'image de X dans $\mathbf{K}$.

2 Donner *sans justification* la caractéristique et le cardinal de $\mathbf{K}$.

3 Choisir un triplet (a_0, a_1, a_2) d'éléments de $\mathbf{F}_3 \setminus \{0\}$; soit $x = a_0 + a_1.\alpha + a_2.\alpha^2$. Calculer les décompositions dans la $\mathbf{F}_3$-base $(1, \alpha, \alpha^2)$ de x^3 et de l'inverse de x. Le détail des calculs doit apparaître sur la copie.

4 **(*)** Soit $\varphi\colon \mathbf{F}_3[X] \to \mathbf{K}$ l'unique morphisme de $\mathbf{F}_3$-algèbres qui envoie X sur x. Déterminer l'image de φ.

Problème

Soit A le sous-ensemble de $\mathbf{C}$ défini par $A := \{a + i\,b\sqrt{2}, \quad (a,b) \in \mathbf{Z}^2\}$.

1 Montrer que A est un sous-anneau de $\mathbf{C}$ contenant $\mathbf{Z}$. En déduire que A est un anneau intègre.

2 *(la réponse à cette question n'est pas utilisée dans la suite)* **(*)** Décrire le corps des fractions de A ; déterminer en particulier s'il est ou non égal à $\mathbf{C}$.

3 Pour tout élément z de $\mathbf{C}$, on note $\overline{z}$ le conjugué de z et on pose $\mathcal{N}(z) := z\,\overline{z}$.

1. Montrer que pour tous $z_1, z_2 \in \mathbf{C}$, on a $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2)$.
2. Montrer qu'on a $\mathcal{N}(A) \subset \mathbf{N}$.
3. Déterminer, si c'est possible, un élément de z de A tel que $\mathcal{N}(z) = 3$, puis un élément z de A tel que $\mathcal{N}(z) = 5$.

4 Soit B un sous-anneau de $\mathbf{C}$ stable par conjugaison (c'est à dire que pour tout $z \in B$, on a $\overline{z} \in B$) et tel que $\mathcal{N}(B) \subset \mathbf{N}$.

1. Donner deux exemples d'un tel sous-anneau B.
2. Montrer que l'ensemble $B^\times$ des éléments inversibles de B est égal à $\{z \in B, \quad \mathcal{N}(z) = 1\}$.
3. Rappelons une caractérisation des éléments irréductibles d'un anneau intègre : un élément a d'un anneau intègre R est irréductible s'il est non nul, non inversible et pour tout couple (b, c) d'éléments de R tel que $a = bc$, b ou c est inversible.
   Soit $z \in B$ tel que $\mathcal{N}(z) > 1$. On suppose que pour tout diviseur positif d de $\mathcal{N}(z)$ distinct de 1 et de $\mathcal{N}(z)$ on a : $d \notin \mathcal{N}(B)$. Montrer qu'alors z est un élément irréductible de B.

5 Déduire de la question 4.2 une description de l'ensemble $A^\times$ des éléments inversibles de A. Déterminer un élément $d \in \mathbf{N}$ tel que le groupe $A^\times$ est isomorphe au groupe $\mathbf{Z}/d\mathbf{Z}$.

6 Soit n un entier naturel. On considère la propriété $(\mathcal{P})$ suivante : il existe $a, b \in \mathbf{Z}$ tel que $n = a^2 + 2\,b^2$.

1. Traduire la propriété $(\mathcal{P})$ en termes de l'application $\mathcal{N}$ et de l'anneau A.
2. Donner trois exemples de nombres premiers vérifiant $(\mathcal{P})$, et trois exemples de nombres premiers ne vérifiant pas $(\mathcal{P})$.
3. En utilisant la question 4.3, en déduire un exemple explicite d'un élément de $\mathbf{Z}$ qui est un élément irréductible de A.
4. Montrer que si le nombre premier p vérifie $(\mathcal{P})$ alors -2 est un carré dans $\mathbf{F}_p$, c'est à dire il existe $x \in \mathbf{F}_p$ tel que $x^2 = [-2]_p$.

7 Soit p un nombre premier impair tel que -2 est un carré dans $\mathbf{F}_p$. Soit $c \in \mathbf{Z}$ tel que p divise $c^2 + 2$. Soit $\varphi\colon A \to \mathbf{Z}/p\mathbf{Z}$ l'application qui à $a + ib\sqrt{2} \in A$ associe $[a - c\,b]_p$.

1. Montrer que φ est un morphisme d'anneaux.
2. *On admet que l'idéal* $\mathrm{Ker}(\varphi)$ *est engendré par un élément* $\alpha \in A$. **(*)** En utilisant le fait que $\mathrm{Ker}(\varphi)$ contient p et $c + i\sqrt{2}$, en déduire que p vérifie la propriété $(\mathcal{P})$.

8 Soit $\mathbf{K}$ un corps et $x \in \mathbf{K}$. On dit que x est un carré dans $\mathbf{K}$ s'il existe $y \in \mathbf{K}$ tel que $x = y^2$. Soit Q l'anneau quotient $Q := \mathbf{K}[X]/\langle X^2 - x\rangle$.

1. Montrer que Q est un corps si et seulement si Q est intègre si et seulement si x n'est pas un carré dans $\mathbf{K}$.
2. *(la réponse à cette question n'est pas utilisée dans la suite)* **(*)** Si x est un carré dans $\mathbf{K}$, montrer qu'on est dans l'un des deux cas suivants, suivant une condition sur x et $\mathbf{K}$ que l'on précisera :
   - l'anneau Q est isomorphe à l'anneau produit $\mathbf{K} \times \mathbf{K}$; c'est un anneau réduit (on rappelle qu'un anneau est réduit si pour tout élément a de cet anneau et tout entier naturel n, si $a^n = 0$ alors $a = 0$) ;
   - l'anneau Q est un anneau non réduit.

9 Soit $\theta\colon \mathbf{Z}[X] \to \mathbf{C}$ l'unique morphisme d'anneaux qui envoie X sur $i\sqrt{2}$. Montrer que $\theta(\mathbf{Z}[X]) = A$ et que le noyau de θ est l'idéal engendré par $X^2 + 2$.

10 **(*)** Soit p un nombre premier. Déduire de la question précédente que l'idéal pA est un idéal premier de A si et seulement si -2 n'est pas un carré dans $\mathbf{F}_p$.

11 On considère un rectangle du plan euclidien dont les côtés ont pour longueur 1 et $\sqrt{2}$.

1. Montrer que pour tout point du rectangle (au sens large : intérieur et côtés compris) il existe un sommet du rectangle tel que ce point est à distance < 1 de ce sommet.
2. En déduire que pour tous $\alpha, \beta \in A$, avec $\beta \neq 0$, il existe $(q, r) \in A^2$ tel que $\alpha = \beta.q + r$ et $\mathcal{N}(r) < \mathcal{N}(\beta)$.
3. **(*)** En utilisant le résultat de la question précédente ainsi que ceux d'autres questions antérieures, en déduire que les conditions suivantes sont équivalentes :
   - (i) p est un élément irréductible de A ;
   - (ii) -2 n'est pas un carré modulo p ;
   - (iii) p ne vérifie pas la propriété $(\mathcal{P})$.

12 **(*)** Expliciter un algorithme permettant, connaissant c, de déterminer l'élément α de la question 7.2.

13 **(*)** Soit I_1 l'ensemble des nombres premiers qui ne vérifient pas la propriété $\mathcal{P}$ ainsi que les opposés de ces nombres premiers et I_2 l'ensemble des $z \in A$ tel que $\mathcal{N}(z)$ est un nombre premier qui vérifie la propriété $(\mathcal{P})$. Montrer que l'ensemble des éléments irréductibles de A est la réunion des ensembles I_1 et I_2.

14 **(*)** Le polynôme $P_1 := X^3 + 5i\sqrt{2}X + 5$ est-il un élément irréductible de $A[X]$? Même question pour les polynômes $P_2 := X^4 + (3 + 3i\sqrt{2})X^3 + 5 + 5i\sqrt{2}$ et $P_3 := (1 + i\sqrt{2})X + 3$.