Université de Rennes 1 — Année universitaire 2017-2018
Licence de mathématiques – Module ANAR

Examen terminal
Seconde session

Le sujet comporte deux pages et cinq exercices. La qualité de la rédaction et de l'argumentation entre dans une part importante de l'appréciation des copies ; en particulier, *sauf mention expresse du contraire, toutes les réponses doivent être justifiées.* Documents de cours, calculatrices, téléphones portables et assimilés ne sont pas autorisés.

Exercice 1

1. Résoudre le système de congruences d'inconnue $x \in \mathbf{Z}$: $\begin{cases} x & \equiv & 4\ [11] \\ x & \equiv & 7\ [13]\,. \end{cases}$
2. Résoudre l'équation $x^3 = 3, \quad x \in A$ pour les anneaux A suivants : $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/25\mathbf{Z}$.

Exercice 2

Soit $\mathbf{K}$ un corps à 4 éléments. On note 0 l'élément neutre pour l'addition, 1 l'élément neutre pour la multiplication, et $\mathbf{K} \setminus \{0,1\} = \{\alpha, \beta\}$. En respectant ces notations, donner les tables d'addition et de multiplication de $\mathbf{K}$. *Aucune justification, aucun calcul annexe n'est demandé sur la copie.*

Exercice 3

Soit A un anneau. Un élément a de A est dit *nilpotent* s'il existe un entier strictement positif m tel que $a^m = 0$. L'anneau A est dit *réduit* s'il n'a pas d'éléments nilpotents non nuls.

1. Montrer que si A est un anneau intègre, alors A est réduit. Donner un exemple d'anneau non intègre, non nul et réduit.
2. Soit p un nombre premier. Décrire explicitement les éléments nilpotents de $\mathbf{Z}/p^2\mathbf{Z}$. Déterminer en particulier le nombre d'éléments nilpotents de $\mathbf{Z}/p^2\mathbf{Z}$.
3. Soit a un élément nilpotent de A. Montrer que $1 + a$ est un élément inversible de A.
4. Montrer que l'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents de A est un idéal de A. Montrer que l'anneau quotient $A/\mathrm{Nil}(A)$ est réduit.

Exercice 4

Soit A un anneau intègre, $\mathcal{I}$ un idéal de A, S une partie multiplicative de A ne contenant pas 0_A et $\iota\colon A \to S^{-1}A$ le morphisme de localisation.

1. Donner un exemple explicite montrant que $\iota(\mathcal{I})$ n'est pas nécessairement un idéal de $S^{-1}A$.
2. On note $S^{-1}\mathcal{I}$ le sous-ensemble de $S^{-1}A$ décrit par $S^{-1}\mathcal{I} := \{\frac{a}{s}\}_{a\in\mathcal{I}, s\in S}$. Montrer que $S^{-1}\mathcal{I}$ est l'idéal de $S^{-1}A$ engendré par $\iota(\mathcal{I})$.
3. On suppose dans cette question que $\mathcal{I}$ est un idéal premier de A et que $S = A \setminus \mathcal{I}$. Montrer que tout élément de $S^{-1}A \setminus S^{-1}\mathcal{I}$ est un élément inversible de $S^{-1}A$. En déduire que $S^{-1}\mathcal{I}$ est l'unique idéal maximal de $S^{-1}A$.

4. On suppose dans cette question que $\mathcal{I}$ est un idéal maximal de A et que $S = A \setminus \mathcal{I}$. Soit $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient. Montrer qu'il existe un unique morphisme
$$\varphi\colon S^{-1}A \to A/\mathcal{I}$$
tel que $\varphi \circ \iota = \pi$, et que φ est surjectif. En déduire que les anneaux $S^{-1}A/S^{-1}\mathcal{I}$ et $A/\mathcal{I}$ sont isomorphes.
5. On suppose dans cette question que $\mathcal{I}$ est un idéal premier de A et que $S = A \setminus \mathcal{I}$. Les anneaux $S^{-1}A/S^{-1}\mathcal{I}$ et $A/\mathcal{I}$ sont-ils nécessairement isomorphes ?

Exercice 5

Si p est un nombre premier et $P \in \mathbf{Z}[X]$, on rappelle que l'on dit que P est *réductible modulo p* si l'image de P par le morphisme $\mathbf{Z}[X] \to (\mathbf{Z}/p\mathbf{Z})[X]$ de « réduction des coefficients modulo p » est un élément réductible de $(\mathbf{Z}/p\mathbf{Z})[X]$.

On considère désormais l'élément P de $\mathbf{Z}[X]$ défini par $P := X^4 + 1$.

1. Montrer qu'on a dans $\mathbf{R}[X]$ l'égalité $P = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ et que les polynômes $X^2 + \sqrt{2}X + 1$ et $X^2 - \sqrt{2}X + 1$ sont des éléments irréductibles de $\mathbf{R}[X]$.
2. En déduire que P est un élément irréductible de $\mathbf{Z}[X]$.
3. Soit p un nombre premier. Si $a \in \mathbf{Z}$, on rappelle qu'on dit que *a est un carré modulo p* s'il existe $b \in \mathbf{Z}$ tel que $a \equiv b^2\ [p]$, en d'autres termes si $[a]_p$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$.

   On suppose que l'*une* des propriétés suivantes est vraie :

   (a) -1 est un carré modulo p ;

   (b) 2 est un carré modulo p ;

   (c) -2 est un carré modulo p.

   En utilisant des identités remarquables, montrer qu'alors P est réductible modulo p.
4. Soit $\mathbf{K}$ un corps fini. Soit $\alpha, \beta \in \mathbf{K}$ des éléments qui ne sont pas des carrés dans $\mathbf{K}$. Montrer qu'alors $\alpha\beta$ est un carré dans $\mathbf{K}$.
5. Déduire de ce qui précède que pour tout nombre premier p, P est réductible modulo p.