Université de Rennes 1 Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°2
Mercredi 3 avril 2019, 17h15 – 18h15

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.

Il n'est pas nécessaire de répondre à toutes les questions pour avoir la note maximale. L'appréciation des copies valorisera le fait de traiter des portions significatives des exercices proposés, plutôt que de tenter de « grapiller » des points de-ci de-là.

Exercice 1

Soit $A = \mathbf{Z}[X]$ et I l'idéal de A engendré par 2 et X. Montrer qu'il n'existe pas d'élément $P \in \mathbf{Z}[X]$ tel que $I = P\,\mathbf{Z}[X]$.

Exercice 2

1. Soit $P = X^2 + [2]_5 \in \mathbf{F}_5[X]$ et $A = \mathbf{F}_5[X]/\langle P\rangle$. On note α l'image de X dans A par le morphisme d'anneaux quotient $\mathbf{F}_5[X] \to A$.
   (a) A est-il un corps ?
   (b) Déterminer l'ordre en tant qu'élément du groupe $A^\times$ de chacun des éléments de l'ensemble $\{[3]_5, \alpha, \alpha + [2]_5\}$. *On ne demande pas sur la copie le détail des calculs des puissances d'éléments de A ; on pourra se contenter d'indiquer clairement les résultats nécessaires.*
2. Soit $P = X^2 + [1]_5 \in \mathbf{F}_5[X]$ et $A = \mathbf{F}_5[X]/\langle P\rangle$. Le groupe $A^\times$ est-il cyclique ?

Exercice 3

Soit p un nombre premier et $\mathbf{Z}_{(p)}$ le localisé de l'anneau $\mathbf{Z}$ par rapport à la partie multiplicative $\mathbf{Z} \setminus p\mathbf{Z}$. Soit $\mathfrak{M}_p = p\mathbf{Z}_{(p)}$ l'idéal engendré par p dans $\mathbf{Z}_{(p)}$.

1. Soit A un anneau. Rappeler la définition d'une partie multiplicative de A. Justifier que $\mathbf{Z}\setminus p\mathbf{Z}$ est une partie multiplicative de $\mathbf{Z}$.
2. Donner une description explicite de $\mathbf{Z}_{(p)}$ en tant que sous-anneau de $\mathbf{Q}$ (*aucune justification n'est demandée*).
3. Soit $\pi\colon \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ le morphisme d'anneaux quotient et $\iota\colon \mathbf{Z} \to \mathbf{Z}_{(p)}$ le morphisme de localisation. Montrer qu'il existe un unique morphisme d'anneaux $\varphi\colon \mathbf{Z}_{(p)} \to \mathbf{Z}/p\mathbf{Z}$ tel que $\varphi \circ \iota = \pi$.
4. Montrer que $\mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$ est contenu dans $\mathbf{Z}_{(p)}^\times$.
5. Soit A un anneau et I un idéal propre de A tel que $A \setminus I \subset A^\times$. Montrer que I est un idéal maximal de A, et que c'est l'unique idéal maximal de A.
6. Déduire des questions 3, 4 et 5 que l'anneau quotient $\mathbf{Z}_{(p)}/\mathfrak{M}_p$ est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.
7. Soit q un nombre premier distinct de p. Déduire des questions 4, 5 et 6 que les anneaux $\mathbf{Z}_{(p)}$ et $\mathbf{Z}_{(q)}$ ne sont pas isomorphes.

Université de Rennes 1 Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°2
Mercredi 3 avril 2019, 17h15 – 18h15

Exercice 1

Soit $A = \mathbf{Z}[X]$ et I l'idéal de A engendré par 2 et X. Montrer qu'il n'existe pas d'élément $P \in \mathbf{Z}[X]$ tel que $I = P\,\mathbf{Z}[X]$.

Correction : Raisonnons par l'absurde et supposons l'existence d'un élément $P \in \mathbf{Z}[X]$ tel que $I = P\,\mathbf{Z}[X]$. Comme I est l'idéal engendré par 2 et X, on a en particulier $2 \in I$ et $X \in I$. Ainsi il existe $Q_1, Q_2 \in \mathbf{Z}[X]$ tels que $2 = P\,Q_1$ et $X = P\,Q_2$. Comme $\mathbf{Z}$ est intègre, on en tire notamment $0 = \deg(2) = \deg(P) + \deg(Q_1)$. Comme $\deg(P), \deg(Q_1) \in \mathbf{N} \cup \{-\infty\}$, on en déduit que $\deg(P) = 0$ et $\deg(Q_1) = 0$, en d'autres termes $P, Q_1 \in \mathbf{Z}$ et l'égalité $2 = P\,Q_1$ est une égalité dans $\mathbf{Z}$. Comme 2 est premier, on en tire $P = \pm 1$ ou $P = \pm 2$. Si $P = \pm 2$, tous les coefficients du polynôme $P\,Q_2$ sont divisibles par 2. Comme $P\,Q_2 = X$, on aboutit alors à une contradiction. Donc $P = \pm 1$. Mais comme $P \in I$ et que I est engendré par 2 et X, on en déduit l'existence de $S_1, S_2 \in \mathbf{Z}[X]$ tels que

$$X\,S_1 + 2\,S_2 = 1.$$

En évaluant ce qui précède en $X = 0$, on trouve $1 = 2\,S_2(0)$. Comme $S_2(0) \in \mathbf{Z}$ et 2 ne divise pas 1 dans $\mathbf{Z}$, c'est une contradiction.

Exercice 2

1. Soit $P = X^2 + [2]_5 \in \mathbf{F}_5[X]$ et $A = \mathbf{F}_5[X]/\langle P\rangle$. On note α l'image de X dans A par le morphisme d'anneaux quotient $\mathbf{F}_5[X] \to A$.
   (a) A est-il un corps ?

   Correction : En calculant $[i]_5^2$ pour $i \in \{0, 1, 2, 3, 4\}$, on trouve que les éléments de $\mathbf{F}_5$ qui s'écrivent comme le carré d'un élément de $\mathbf{F}_5$ sont les éléments de l'ensemble $\{[0]_5, [1]_5, [4]_5\}$. Comme $-[2]_5 = [3]_5$ n'est pas un élément de cet ensemble, le polynôme P n'a pas de racine dans $\mathbf{F}_5$. Comme P est en outre un polynôme de degré 2 à coefficients dans $\mathbf{F}_5$, ceci montre que P est un élément irréductible de $\mathbf{F}_5[X]$. On sait alors d'après le cours que $\langle P\rangle$ est un idéal maximal de $\mathbf{F}_5[X]$ et donc que $A = \mathbf{F}_5[X]/\langle P\rangle$ est un corps.

   (b) Déterminer l'ordre en tant qu'élément du groupe $A^\times$ de chacun des éléments de l'ensemble $\{[3]_5, \alpha, \alpha + [2]_5\}$. *On ne demande pas sur la copie le détail des calculs des puissances d'éléments de A ; on pourra se contenter d'indiquer clairement les résultats nécessaires.*

   Correction : On a $[3]_5^2 = [4]_5 \neq [1]_5$ et $[3]_5^4 = [4]_5^2 = [1]_5$. Ainsi l'ordre de $[3]_5$ divise 4 (ceci découle bien sûr aussi directement du petit théorème de Fermat) et comme $[3]_5^2 \neq [1]_5$ ce n'est ni 1, ni 2, c'est donc 4.

   En utilisant la relation $\alpha^2 = -[2]_5 = [3]_5$ on obtient d'après ce qui précède $\alpha^4 = [3]_5^2 = [4]_5 \neq [1]_5$ et $\alpha^8 = [3]_5^4 = [1]_5$. Donc l'ordre de α divise 8, et n'est ni 1, ni 2, ni 4. Donc α est d'ordre 8.

   Comme $\{[1]_5, \alpha\}$ est une base du $\mathbf{F}_5$-espace vectoriel A, on a $\alpha + [2]_5 \neq 1$. Toujours en utilisant $\alpha^2 = -[2]_5$, on obtient

$$(\alpha + [2]_5)^2 = [2]_5 + [4]_5\alpha$$

et

$$(\alpha + [2]_5)^3 = (\alpha + [2]_5)([2]_5 + [4]_5\alpha) = [4]_5\alpha^2 + [10]_5\alpha + [4]_5 = [1]_5.$$

Donc l'ordre de $\alpha + [2]_5$ divise 3 et n'est pas 1, c'est donc 3.

2. Soit $P = X^2 + [1]_5 \in \mathbf{F}_5[X]$ et $A = \mathbf{F}_5[X]/\langle P\rangle$. Le groupe $A^\times$ est-il cyclique ?
Correction : Montrons que $A^\times$ n'est pas cyclique. On a

$$P = X^2 + [1]_5 = X^2 - [4]_5 = (X + [2]_5)(X - [2]_5)$$

d'où on déduit que $\langle P\rangle = \langle X - [2]_5\rangle \cdot \langle X - [2]_5\rangle$. Les polynômes $X + [2]_5$ et $X - [2]_5$ sont de degré 1 donc irréductibles, et distincts donc non associés car ils sont unitaires. Il sont donc premiers entre eux, et d'après le théorème de Bezout pour les anneaux de polynômes en une variable à coefficients dans un corps, on a $\langle X + [2]_5\rangle + \langle X - [2]_5\rangle = \mathbf{F}_5[X]$. Ainsi, d'après le théorème chinois, l'anneau A est isomorphe à $\mathbf{F}_5[X]/\langle X + [2]_5\rangle \times \mathbf{F}_5[X]/\langle X - [2]_5\rangle$. De manière générale, si B est un anneau et $b \in B$, le morphisme $B[X] \to B$ d'évaluation en b est surjectif (car il induit l'identité sur $B \subset B[X]$) et induit donc un isomorphisme de $B[X]/\langle X - b\rangle$ sur B (résultat du cours : pour tout $P \in B[X]$, $P(b) = 0$ si et seulement si $P \in \langle X - b\rangle$). Ainsi A est isomorphe à $\mathbf{F}_5 \times \mathbf{F}_5$, donc le groupe $A^\times$ est isomorphe à $\mathbf{F}_5^\times \times \mathbf{F}_5^\times$. Comme le groupe $\mathbf{F}_5^\times$ est de cardinal 4, on a pour tout $(x, y) \in \mathbf{F}_5^\times \times \mathbf{F}_5^\times$ la relation $(x, y)^4 = (x^4, y^4) = (1, 1)$. Ainsi l'ordre de tout élément de $A^\times$ divise 4, mais par ailleurs $A^\times$ est de cardinal $4 \times 4 = 16$. Donc $A^\times$ n'est pas cyclique.

Remarque : On sait d'après le cours qui si A est un anneau fini qui est un corps, alors $A^\times$ est cyclique. Mais il existe des anneaux finis qui ne sont pas des corps et dont le groupe des éléments inversibles est cyclique, tel que $\mathbf{Z}/4\mathbf{Z}$, dont le groupe des éléments inversibles est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

Exercice 3

Soit p un nombre premier et $\mathbf{Z}_{(p)}$ le localisé de l'anneau $\mathbf{Z}$ par rapport à la partie multiplicative $\mathbf{Z} \setminus p\mathbf{Z}$. Soit $\mathfrak{M}_p = p\mathbf{Z}_{(p)}$ l'idéal engendré par p dans $\mathbf{Z}_{(p)}$.

1. Soit A un anneau. Rappeler la définition d'une partie multiplicative de A. Justifier que $\mathbf{Z}\setminus p\mathbf{Z}$ est une partie multiplicative de $\mathbf{Z}$.
Correction : Une partie multiplicative de A est une partie S de A qui contient 1_A et qui est stable par multiplication.
Comme p est premier, 1 n'est pas divisible par p. Par ailleurs la contraposée du lemme d'Euclide (valable puisque p est premier) s'écrit : soit $a, b \in \mathbf{Z}$ tel que p ne divise ni a, ni b ; alors p ne divise pas ab. Ainsi $\mathbf{Z} \setminus p\mathbf{Z}$ est bien une partie multiplicative de $\mathbf{Z}$.
2. Donner une description explicite de $\mathbf{Z}_{(p)}$ en tant que sous-anneau de $\mathbf{Q}$ (*aucune justification n'est demandée*).
Correction : On a

$$\mathbf{Z}_{(p)} = \{\frac{a}{b}\}_{\substack{a\in\mathbf{Z}\\ b\in\mathbf{Z}\setminus p\mathbf{Z}}} \subset \mathbf{Q}.$$

3. Soit $\pi\colon \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ le morphisme d'anneaux quotient et $\iota\colon \mathbf{Z} \to \mathbf{Z}_{(p)}$ le morphisme de localisation. Montrer qu'il existe un unique morphisme d'anneaux $\varphi\colon \mathbf{Z}_{(p)} \to \mathbf{Z}/p\mathbf{Z}$ tel que $\varphi \circ \iota = \pi$.
Correction : Par la propriété universelle de l'anneau localisé et la définition de $\mathbf{Z}_{(p)}$, il suffit de montrer qu'on a $\pi(\mathbf{Z} \setminus p\mathbf{Z}) \subset (\mathbf{Z}/p\mathbf{Z})^\times$. Mais comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps, donc $(\mathbf{Z}/p\mathbf{Z})^\times = \mathbf{Z}/p\mathbf{Z} \setminus \{0\}$. Or par définition du morphisme quotient on a $\pi^{-1}(\{0\}) = \mathrm{Ker}(\pi) = p\mathbf{Z}$. Donc $\pi(\mathbf{Z} \setminus p\mathbf{Z}) \subset \mathbf{Z}/p\mathbf{Z} \setminus \{0\}$, ce qui conclut.

4. Montrer que $\mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$ est contenu dans $\mathbf{Z}_{(p)}^\times$.

   Correction : Soit $x \in \mathbf{Z}_{(p)} \setminus p\mathbf{Z}_{(p)}$. Soit (question 2) $a \in \mathbf{Z}$ et $b \in \mathbf{Z} \setminus p\mathbf{Z}$ tel que $x = \frac{a}{b}$. S'il existe $a' \in \mathbf{Z}$ tel que $a = pa'$, on a $x = p\frac{a'}{b} \in p\mathbf{Z}_{(p)}$. Comme $x \notin p\mathbf{Z}_{(p)}$, p ne divise pas a. D'après la question 2, $y := \frac{b}{a} \in \mathbf{Z}_{(p)}$. Clairement $xy = 1$, donc $x \in \mathbf{Z}_{(p)}^\times$. Ceci montre bien l'inclusion demandée.

5. Soit A un anneau et I un idéal propre de A tel que $A \setminus I \subset A^\times$. Montrer que I est un idéal maximal de A, et que c'est l'unique idéal maximal de A.

   Correction : Soit J un idéal de A contenant strictement I. En particulier, il existe un élément $x \in J$ qui n'est pas dans I. Comme $A \setminus I \subset A^\times$, on a donc $x \in A^\times$. Comme $x \in J$, on a $J = A$. Comme I est propre, ceci achève de montrer que I est un idéal maximal de A.

   Soit J un idéal maximal de A. Montrons que $I = J$. Supposons que J n'est pas inclus dans I. Il existe donc $x \in J$ qui n'est pas dans I. En raisonnant comme précédemment, on en déduit que $J = A$. C'est une contradiction, car J est maximal et en particulier propre. Ainsi J est inclus dans I. Comme I est maximal, donc propre, et que J est maximal, on en déduit $J = I$. Ainsi I est bien l'unique idéal maximal de A.

6. Déduire des questions 3, 4 et 5 que l'anneau quotient $\mathbf{Z}_{(p)}/\mathfrak{M}_p$ est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

   Correction : En reprenant les notations de la question 3, soit $\varphi\colon \mathbf{Z}_{(p)} \to \mathbf{Z}/p\mathbf{Z}$ l'unique morphisme d'anneaux tel que tel que $\varphi \circ \iota = \pi$. Comme π est un morphisme quotient, π est surjectif. Comme $\varphi \circ \iota = \pi$, φ est également surjectif. Ainsi φ induit un isomorphisme de $\mathbf{Z}_{(p)}/\operatorname{Ker}(\varphi)$ sur $\mathbf{Z}/p\mathbf{Z}$. Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps, et donc $\operatorname{Ker}(\varphi)$ est un idéal maximal de $\mathbf{Z}_{(p)}$. Mais d'après les questions 4 et 5, $\mathfrak{M}_p$ est l'unique idéal maximal de $\mathbf{Z}_{(p)}$. Donc $\operatorname{Ker}(\varphi) = \mathfrak{M}_p$ et $\mathbf{Z}_{(p)}/\mathfrak{M}_p$ est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

7. Soit q un nombre premier distinct de p. Déduire des questions 4, 5 et 6 que les anneaux $\mathbf{Z}_{(p)}$ et $\mathbf{Z}_{(q)}$ ne sont pas isomorphes.

   Correction : Raisonnons par l'absurde et supposons l'existence d'un isomorphisme d'anneaux $\psi\colon \mathbf{Z}_{(q)} \to \mathbf{Z}_{(p)}$. Soit $\theta\colon \mathbf{Z}_{(p)} \to \mathbf{Z}_{(p)}/\mathfrak{M}_p$ le morphisme quotient de $\mathbf{Z}_{(p)}$ par $\mathfrak{M}_p$. Ainsi, comme ψ est un isomorphisme, $\theta \circ \psi$ est un morphisme surjectif de $\mathbf{Z}_{(q)}$ sur le corps $\mathbf{Z}_{(p)}/\mathfrak{M}_p$. Le noyau de $\theta \circ \psi$ est donc un idéal maximal de $\mathbf{Z}_{(q)}$. D'après les questions 4 et 5, ce noyau est donc $\mathfrak{M}_q$. Ainsi $\theta \circ \psi$ induit un isomorphisme de $\mathbf{Z}_{(q)}/\mathfrak{M}_q$ sur $\mathbf{Z}_{(p)}/\mathfrak{M}_p$. D'après la question 6, les anneaux $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/q\mathbf{Z}$ sont donc isomorphes. Comme ils ont pour cardinal respectif p et q et que p est supposés distinct de q, c'est une contradiction.

   Remarque : on a en fait montré qu'il n'existait même pas de morphisme d'anneaux surjectif de $\mathbf{Z}_{(q)}$ sur $\mathbf{Z}_{(p)}$; on peut même montrer, en utilisant ce qui précède et en travaillant un tout petit peu plus, qu'il n'existe en fait aucun morphisme d'anneaux de $\mathbf{Z}_{(q)}$ vers $\mathbf{Z}_{(p)}$.