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

Examen terminal
Seconde session
Corrigé

Exercice 1

On pourra se reporter à la correction de l'exercice 1 du terminal de première session (identique aux données numériques près).

La question 2 (avec en outre exactement les mêmes données numériques) avait d'ailleurs aussi été posée dans le premier contrôle continu, et on pourra donc également se reporter au corrigé de ce contrôle continu, qui développe l'approche élémentaire de la résolution dans le cas $A = \mathbf{Z}/5\mathbf{Z}$ (à savoir calculer tous les cubes modulo 5).

Complément : soit p un nombre premier, n un entier premier avec $p-1$ et x_0 un élément non nul de $\mathbf{Z}/p\mathbf{Z}$; on souhaite résoudre l'équation $x^n = x_0, \quad x \in \mathbf{Z}/p\mathbf{Z}$. La méthode présentée dans le corrigé du terminal de première session a l'avantage de s'adapter facilement à une résolution explicite de ce type d'équations qui ne nécessite pas de calculer toutes les puissances n-èmes modulo p.

Exercice 2

On se reportera à la correction de l'exercice 2 du terminal de première session.

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.*

   Soit $a \in A$. On va montrer par récurrence la propriété suivante : pour tout entier strictement positif m, si $a^m = 0$ alors $a = 0$. L'hypothèse de récurrence est $\mathcal{H}_m$: « Si $a^m = 0$ alors $a = 0$ ». $\mathcal{H}_1$ est clairement vérifiée. Soit m un entier strictement positif tel que $\mathcal{H}_m$ est vérifiée. Montrons que $\mathcal{H}_{m+1}$ est encore vérifiée. Supposons donc $a^{m+1} = 0$. Il s'agit de montrer que $a = 0$. L'intégrité de A et le fait que $a^m = a.a^m = 0$ permettent de conclure que $a = 0$ ou $a^m = 0$. Dans le premier cas on a terminé. Dans le second cas, $\mathcal{H}_m$ permet de conclure que $a = 0$.

   Vu la définition d'un élément nilpotent, la propriété précédente montre aussitôt que tout élément nilpotent de A est nul, ce qu'il fallait démontrer.

   Donner un exemple d'anneau non intègre, non nul et réduit.

   Considérons l'anneau produit $\mathbf{Z} \times \mathbf{Z}$. Il est clairement non nul. Il est non intègre car $(1,0)$ et $(0,1)$ sont non nuls et leur produit est nul.

   Montrons que $\mathbf{Z} \times \mathbf{Z}$ est réduit. Notons que $\mathbf{Z}$ est intègre donc réduit d'après la question précédente.

   Soit $(a,b) \in \mathbf{Z} \times \mathbf{Z}$ un élément nilpotent. Il existe donc m entier strictement positif tel que $(a,b)^m = (0,0)$. Or $(a,b)^m = (a^m, b^m)$, donc $a^m = 0$ et $b^m = 0$. Comme $\mathbf{Z}$ est réduit, on en déduit que a et b sont nuls, donc $(a,b) = (0,0)$. Ceci achève de montrer que $\mathbf{Z} \times \mathbf{Z}$ est 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 $\mathbf{Z}/p^2\mathbf{Z}$.*

   On va montrer la propriété suivante : soit d un entier strictement positif. Alors $[d]_{p^2}$ est nilpotent si et seulement si p divise d

   Supposons tout d'abord $[d]_n$ nilpotent. Il existe donc un entier strictement positif m tel que $[d]_{p^2}^m = 0$ d'où $[d^m]_{p^2} = 0$. Ainsi p^2 divise d^m, donc p divise d^m, et finalement, par le lemme d'Euclide, p divise d.

   Supposons à présent que p divise d. Alors p^2 divise d^2, donc $[d^2]_{p^2} = [0]_{p^2}$ soit $[d]_{p^2}^2 = [0]_{p^2}$, donc $[d]_{p^2}$ est nilpotent.

   Compte tenu de ce qui précède et du fait que l'application qui à d entier compris entre 0 et $p^2 - 1$ associe $[d]_{p^2}$ est une bijection, on voit que l'ensemble des éléments nilpotents de $\mathbf{Z}/p^2\mathbf{Z}$ est en bijection avec l'ensemble des entiers qui s'écrivent ep, où e est un entier compris entre 0 et $p - 1$. Ainsi $\mathbf{Z}/p^2\mathbf{Z}$ possède exactement p éléments nilpotents.

3. *Soit a un élément nilpotent de A. Montrer que $1 + a$ est un élément inversible de A.*

   Soit m un entier strictement positif tel que $a^m = 0_A$. On a l'identité remarquable

$$(1 - (-1)^m a^m) = (1 + a)(\sum_{k=0}^{m-1} (-1)^k a^k).$$

   Comme $a^m = 0$, ceci montre que $1 + a$ est inversible dans A, d'inverse $\sum_{k=0}^{m-1}(-1)^k a^k$.

4. *Montrer que l'ensemble* $\mathrm{Nil}(A)$ *des éléments nilpotents de A est un idéal de A.*

   On a $0_A^1 = 0$ donc $0_A \in \mathrm{Nil}(A)$

   Soit $a \in \mathrm{Nil}(A)$. Montrons que $-a \in \mathrm{Nil}(A)$. Soit m un entier strictement positif tel que $a^m = 0$. Alors $(-a)^m = (-1)^m.a^m = (-1)^m.0_A = 0_A$ donc $-a \in \mathrm{Nil}(A)$.

   Soit $a, b \in \mathrm{Nil}(A)$. Montrons que $a + b \in \mathrm{Nil}(A)$.

   Soit m_1 un entier strictement positif tel que $a^{m_1} = 0_A$ et m_2 un entier strictement positif tel que $b^{m_2} = 0$. Remarquons alors pour tout entier d positif, on a $a^{m_1+d} = a^{m_1}a^d = 0_A$ et similairement pour b.

   La formule du binôme de Newton donne

$$(a+b)^{m_1+m_2} = \sum_{k=0}^{m_1+m_2} \binom{m_1+m_2}{k} a^k b^{m_1+m_2-k}$$

   Soit k un entier compris entre 0 et $m_1 + m_2$. Si $k \geqslant m_1$, la remarque ci-dessus montre que $a^k = 0_A$. Sinon, on a $m_1 + m_2 - k > m_1 + m_2 - m_1 = m_2$. Toujours d'après la remarque ci-dessus, on a alors $b^{m_1+m_2-k} = 0_A$. Dans tous les cas, on a $a^k b^{m_1+m_2-k} = 0_A$. Ainsi tous les termes de la somme du membre de droite de l'égalité ci-dessus sont nuls, ce qui montre que $(a + b)^{m_1+m_2}$ est nul. Donc $a + b \in \mathrm{Nil}(A)$.

   Soit $a \in \mathrm{Nil}(A)$ et $b \in A$. Montrons que $ab \in \mathrm{Nil}(A)$. Soit m un entier strictement positif tel que $a^m = 0$. On a $(ab)^m = a^m.b^m = 0_A.b^m = 0_A$, donc $ab \in \mathrm{Nil}(A)$

   Ce qui précède montre bien que $\mathrm{Nil}(A)$ est un idéal de A.

   Montrer que l'anneau quotient $A/\mathrm{Nil}(A)$ est réduit.

   Soit $\pi\colon A \to A/\mathrm{Nil}(A)$ le morphisme quotient. Soit b un élément nilpotent de $A/\mathrm{Nil}(A)$. Il s'agit de montrer que b est nul. Soit m un entier strictement positif tel que $b^m = 0$. Soit $a \in A$ tel que $b = \pi(a)$. On a donc $\pi(a^m) = \pi(a)^m = b^m = 0$ donc $a^m \in \mathrm{Ker}(\pi) = \mathrm{Nil}(A)$. Il existe donc n un entier strictement positif tel que $(a^m)^n = 0$. Comme $(a^m)^n = a^{mn}$, ceci montre que $a \in \mathrm{Nil}(A) = \mathrm{Ker}(\pi)$. Donc $b = \pi(a) = 0$, ce qui conclut.

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.

Note : les hypothèses « A intègre » et « S ne contient pas 0_A » n'étaient pas nécessaire dans la suite et étaient seulement destinées à vous « rassurer ».

1. *Donner un exemple explicite montrant que $\iota(\mathcal{I})$ n'est pas nécessairement un idéal de $S^{-1}A$.*

   Notons que comme A est supposé intègre et S est supposé ne pas contenir 0_A, le morphisme de localisation est injectif. Notons que A est un idéal de A et que $\iota(A)$ contient $\iota(1_A) = 1_{S^{-1}A}$. Ainsi, si $\iota(A)$ est un idéal de A, on a $\iota(A) = S^{-1}A$ et ι est surjectif.

   Il sufit donc d'expliciter un exemple où ι n'est pas surjectif. Prenons par exemple $A = \mathbf{Z}$ et $S = 2^n{}_{n\in\mathbf{N}}$. On identifie $S^{-1}\mathbf{Z}$ au sous-ensemble de $\mathbf{Q}$ donné par $\{\frac{a}{2^n}\}_{a\in\mathbf{Z},n\in\mathbf{N}}$. Le morphisme ι est alors le morphisme induit par l'inclusion de $\mathbf{Z}$ dans $S^{-1}\mathbf{Z}$

   On a alors $\frac{1}{2} \in S^{-1}(\mathbf{Z})$ et $\frac{1}{2} \notin \iota(\mathbf{Z}) = \mathbf{Z}$ donc ι n'est pas surjectif et $\iota(\mathbf{Z})$ n'est pas un idéal de $S^{-1}\mathbf{Z}$.

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 $\iota(\mathcal{I})$.*

   Soit $\mathcal{J}$ l'idéal de $S^{-1}A$ engendré par $\iota(\mathcal{I})$. On sait que $\mathcal{J}$ est l'ensemble des éléments x de $S^{-1}A$ tel qu'il existe un entier positif n, $(b_i) \in (S^{-1}A)^n$ et $(a_i) \in \mathcal{I}^n$ tels que

   $$x = \sum_{i=1}^{n} b_i \frac{a_i}{1}.$$

   Le cas $n = 1$, $a_1 = a \in \mathcal{I}$ et $b_1 = \frac{1}{s}$ où $s \in S$ montre que $S^{-1}\mathcal{I}$ est inclus dans $\mathcal{J}$.

   En général, prenant un élément $x \in \mathcal{J}$ qui s'écrit comme ci-dessus et notant $b_i = \frac{c_i}{s_i}$ avec $c_i \in A$ et $s_i \in S$, on obtient

   $$x = \frac{\sum_{i=1}^{n} a_i c_i \prod_{j\neq i} s_j}{\prod_{i=1}^{n} s_i}.$$

   Pour tout $i \in \{1, \ldots, n\}$, comme $a_i \in \mathcal{I}$ et $\mathcal{I}$ est un idéal de A, on a $a_i c_i \prod_{j\neq i} s_j \in \mathcal{I}$, d'où on déduit ensuite que le numérateur dans l'expression de x ci-dessus est dans $\mathcal{I}$. Comme S est une partie multiplicative, le dénominateur est un élément de S, donc $x \in S^{-1}\mathcal{I}$. Ainsi $\mathcal{J}$ est inclus dans $S^{-1}\mathcal{I}$, ce qui conclut.

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 $S^{-1}A$.*

   Soit x un élément de $S^{-1}A \setminus S^{-1}\mathcal{I}$. Par la question précédente et la description générale de $S^{-1}A$, x s'écrit $\frac{a}{s}$ avec $a \notin \mathcal{I}$ et $b \in S$, en d'autres termes avec $a \in S$ et $b \in S$. Ceci montre aussitôt que x est inversible dans $S^{-1}A$, d'inverse $\frac{s}{a}$. Au passage, on constate que $S^{-1}A \setminus S^{-1}\mathcal{I}$ est non vide, en d'autres termes $S^{-1}\mathcal{I}$ est un idéal propre de $S^{-1}A$.

   En déduire que $S^{-1}\mathcal{I}$ est l'unique idéal maximal de $S^{-1}A$.

   On a déjà remarqué que $S^{-1}\mathcal{I}$ était un idéal propre de $S^{-1}A$.

   Soit $\mathcal{J}$ un idéal de $S^{-1}A$ contenant $S^{-1}\mathcal{I}$ et distinct de $S^{-1}\mathcal{I}$. En particulier $\mathcal{J}$ rencontre $S^{-1}A \setminus S^{-1}\mathcal{I}$. Ainsi, d'après la question précédente, $\mathcal{J}$ contient un élément inversible, donc $\mathcal{J} = S^{-1}(A)$.

   Ainsi $S^{-1}\mathcal{I}$ est bien un idéal maximal de $S^{-1}A$.

Soit à présent $\mathcal{J}$ un idéal maximal de $S^{-1}A$. Montrons que $\mathcal{J} = S^{-1}\mathcal{I}$. Comme $\mathcal{J}$ est maximal, $\mathcal{J}$ est en particulier propre et donc n'intersecte pas $(S^{-1}A)^\times$. D'après la question précédente, $\mathcal{J}$ est inclus dans $S^{-1}\mathcal{I}$, qui est un idéal propre. Comme $\mathcal{J}$ est maximal, ceci montre que $\mathcal{J} = S^{-1}\mathcal{I}$.

Ainsi $S^{-1}\mathcal{I}$ est bien 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 $S = A\backslash\mathcal{I}$. 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 $\varphi \circ \iota = \pi$,*

   Par la propriété universelle du localisé, il suffit de montrer que l'image par π de tout élément de S est inversible dans $A/\mathcal{I}$. Or, si $a \in S = A \setminus \mathcal{I} = A \setminus \operatorname{Ker}(\pi)$, on a $\pi(a) \neq 0$. Mais comme $\mathcal{I}$ est maximal, $A/\mathcal{I}$ est un corps. Donc $\pi(a)$ est inversible dans $A/\mathcal{I}$.

   et que φ est surjectif.

   On sait que π est surjectif. Comme $\varphi \circ \iota = \pi$, ceci entraîne que φ est surjectif.

   En déduire que les anneaux $S^{-1}A/S^{-1}\mathcal{I}$ et $A/\mathcal{I}$ sont isomorphes.

   Le morphisme $\varphi\colon S^{-1}A \to A/\mathcal{I}$ étant surjectif, il induit un isomorphisme de $S^{-1}A/\operatorname{Ker}(\varphi)$ sur $A/\mathcal{I}$. Or $\mathcal{I}$ est maximal donc $A/\mathcal{I}$ est un corps. Donc $S^{-1}A/\operatorname{Ker}(\varphi)$ est un corps et ainsi $\operatorname{Ker}(\varphi)$ est maximal. Par la question précédente, on a $\operatorname{Ker}(\varphi) = S^{-1}\mathcal{I}$, ce qui conclut.

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 ?*

   Non. En fait, si ces anneaux sont isomorphes, comme $S^{-1}\mathcal{I}$ est un idéal maximal de $S^{-1}A$, $\mathcal{I}$ est alors nécessairement un idéal maximal de A (*cf.* le raisonnement ci-dessus). Le cas où $A = \mathbf{Z}$ et $\mathcal{I} = \{0\}$ (qui est premier mais non maximal) donne donc un exemple explicite où les deux quotients considérés ne sont pas isomorphes.

   En complément à cette question, on pourra essayer de montrer que sous les mêmes hypothèse, l'anneau quotient $S^{-1}A/S^{-1}\mathcal{I}$ est en fait isomorphe au corps des fractions de $A/\mathcal{I}$.

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 $P = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$*

   On a

   $$P = (X^2+1)^2 - 2X^2 = (X^2+1)^2 - (\sqrt{2}X)^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

   et que $(X^2 + \sqrt{2}X + 1)$ et $(X^2 - \sqrt{2}X + 1)$ sont des éléments irréductibles de $\mathbf{R}[X]$.

   On a affaire à des polynômes de degré 2 à coefficients dans un corps. On sait qu'ils sont irréductibles si et seulement s'ils n'ont pas de racine dans ce corps. C'est bien le cas ici car le discriminant $2 - 4 = -2$ est strictement négatif.

2. *En déduire que P est un élément irréductible de $\mathbf{Z}[X]$.* Le polynôme P est unitaire donc de contenu 1. Il suffit donc de montrer que P est irréductible dans $\mathbf{Q}[X]$. Pour tout $x \in \mathbf{R}$, on a $P(x) = x^4 + 1 > 0$ donc P n'a pas de racine dans $\mathbf{R}$ (en particulier pas de racines dans $\mathbf{Q}$). Raisonnons par l'absurde et supposons que P est réductible dans $\mathbf{Q}[X]$. D'après ce qui précède, P s'écrit nécessairement $P = P_1P_2$, où $P_1, P_2 \in \mathbf{Q}[X]$ sont de degré 2 et sans

racine dans $\mathbf{R}$, donc irréductibles dans $\mathbf{R}[X]$. D'après la question précédente et l'unicité de la factorisation en irréductibles dans $\mathbf{R}[X]$, quitte à échanger P_1 et P_2, il existe $\alpha \in \mathbf{R}^\times$ tel que $\alpha P_1 = X^2 + \sqrt{2}X + 1$ En comparant les coefficients dominants, on voit que $\alpha \in \mathbf{Q}^\times$. En comparant les coefficients de X, on voit que $\sqrt{2} \in \mathbf{Q}$ ce qui est une contradiction. Donc P est irréductible dans $\mathbf{Q}[X]$, ce qui conclut.

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 $a \equiv b^2\ [p]$.*

   *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 que P est réductible modulo p.

   Supposons qu'il existe $a \in \mathbf{Z}$ tel que $[-1]_p = [a]_p^2$. On a alors

   $$X^4 + [1]_p = (X^2)^2 - [a]_p^2 = (X^2 - [a]_p)(X^2 - [a]_p).$$

   Le polynôme $X^4 + [1]_p$, de degré 4, s'écrit donc comme produit de deux polynômes de degré strictement inférieur à 4, ce qui montre que P est réductible modulo p.

   Supposons qu'il existe $a \in \mathbf{Z}$ tel que $[2]_p = [a]_p^2$. On a alors

   $$X^4+[1]_p = (X^2+[1]_p)^2-[2]_pX^2 = (X^2+[1]_p)^2-([a]_pX)^2 = (X^2+[a]_pX+[1]_p)(X^2-[a]_pX+[1]_p).$$

   Là encore, on en déduit que P est réductible modulo p.

   Supposons qu'il existe $a \in \mathbf{Z}$ tel que $[-2]_p = [a]_p^2$. On a alors

   $$X^4+[1]_p = (X^2-[1]_p)^2+[2]_pX^2 = (X^2+[1]_p)^2-([a]_pX)^2 = (X^2+[a]_pX+[1]_p)(X^2-[a]_pX+[1]_p).$$

   On aboutit donc à la même conclusion.

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 $\mathbf{K}$.*

   Indication : si $\mathbf{K}$ est de caractéristique 2, en considérant le morphisme $x \mapsto x^2$, on montre que tout élément de $\mathbf{K}$ est un carré.

   Si $\mathbf{K}$ est de caractéristique impaire et de cardinal q, on pourra démonter que pour tout $x \in \mathbf{K}^\times$, on a $x^{\frac{q-1}{2}} \in \{1_K, -1_K\}$ et x est un carré si et seulement si $x^{\frac{q-1}{2}} = 1_K$ (ceci a essentiellement été fait dans le chapitre 3 du cours) et conclure de manière ad hoc.

5. *Déduire de ce qui précède que pour tout nombre premier p, P est réductible modulo p.*

   Soit p un nombre premier.

   Si -1 ou 2 est un carré modulo p, la question 3 permet de conclure.

   Supposons à présent que ni -1 ni 2 ne sont des carrés modulo p. Comme $\mathbf{Z}/p\mathbf{Z}$ est un corps fini, la question précédente montre que $(-1).2 = -2$ est un carré modulo p. On conclut grâce à la question 3.