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

Corrigé du contrôle continu n°1
Mercredi 21 février 2018, 17h15 – 18h15

Exercice 1

Soit $\mathbf{K}$ *un corps. Combien d'idéaux l'anneau* $\mathbf{K}[X]/\langle X^4 - X^2\rangle$ *possède-t-il ?*

D'après le cours, on sait que l'ensemble des idéaux de l'anneau $\mathbf{K}[X]/\langle X^4 - X^2\rangle$ est en bijection avec l'ensemble des idéaux de l'anneau $\mathbf{K}[X]$ qui contiennent l'idéal $\langle X^4 - X^2\rangle$, et que ce dernier ensemble est en bijection avec l'ensemble des diviseurs unitaires du polynôme $X^4 - X^2$.

Si $\mathbf{K}$ n'est pas de caractéristique 2, la factorisation en irréductibles de ce dernier polynôme s'écrit $X^4 - X^2 = X^2(X-1)(X+1)$. L'unicité de la factorisation entraîne que l'application

$$\begin{array}{rcl} \{0,1,2\}\times\{0,1\}\times\{0,1\} & \longrightarrow & \mathbf{K}[X] \\ (a,b,c) & \longmapsto & X^a(X-1)^b(X+1)^c \end{array}$$

induit une bijection de $\{0,1,2\}\times\{0,1\}\times\{0,1\}$ sur l'ensemble des diviseurs unitaires de $X^4 - X^2$. On en déduit que l'anneau $\mathbf{K}[X]/\langle X^4 - X^2\rangle$ possède $3\times 2\times 2 = 12$ idéaux.

Si $\mathbf{K}$ est de caractéristique 2, la factorisation en irréductibles du polynôme $X^4 - X^2$ s'écrit $X^4 - X^2 = X^2(X+1)^2$. Un raisonnement similaire au cas précédent montre alors que l'anneau $\mathbf{K}[X]/\langle X^4 - X^2\rangle$ possède $3\times 3 = 9$ idéaux.

Exercice 2

Soit A *un anneau et* $e \in A$*. On dit que* e *est un* idempotent non trivial *si* $e^2 = e$ *et* $e \notin \{1_A, 0_A\}$.

1. *Déterminer la liste des idempotents non triviaux de* A *dans les cas suivants :* $A = \mathbf{Z}$*,* $A = \mathbf{Z}/p^n\mathbf{Z}$ *(*p *premier,* $n \in \mathbf{N}\setminus\{0\}$*),* $A = \mathbf{Z}/n\mathbf{Z}$ *(*$n \in \mathbf{N}\setminus\{0,1\}$*).*

   Notons que si A est un anneau et $e \in A$, la relation $e^2 = e$ équivaut à $e(e-1_A) = 0_A$. En particulier, si A est intègre, on a $e^2 = e$ si et seulement si $e = 0_A$ ou $e - 1_A = 0_A$. Ainsi un anneau intègre ne possède pas d'idempotent non triviaux. Ceci répond à la question pour $A = \mathbf{Z}$ et $A = \mathbf{Z}/p\mathbf{Z}$ (p premier).

   Soit p un nombre premier et $n \geqslant 2$ un entier. Soit $x \in \mathbf{Z}$ tel que $[x(x-1)]_p^n = [0]_{p^n}$. Ainsi, p^n divise $x(x-1)$. Si p^n divise x, on a $[x]_{p^n} = [0]_{p^n}$. Si p^n divise $x-1$, on a $[x]_{p^n} = [1]_{p^n}$. Si aucune des deux propriétés précédentes n'a lieu, comme on a $n \geqslant 2$, p divise nécessairement x et $x-1$, donc p divise 1, ce qui est une contradiction. On en conclut que $\mathbf{Z}/p^n\mathbf{Z}$ ne possède pas d'idempotents non triviaux.

   De manière générale, si A et B sont des anneaux et $(e,f) \in A\times B$, on a, par définition de la structure d'anneau produit, $(e,f)^2 = (e,f)$ si et seulement si $e^2 = e$ et $f^2 = f$. La généralisation à un produit fini d'anneaux est immédiate.

   Si maintenant $n \geqslant 2$ est un entier, notant $n = \prod_{i\in I} p_i^{\nu_i}$ sa factorisation en produit de nombres premiers (I ensemble fini non vide, pour $i \in I$, p_i premier et ν_i entier strictement positif, pour $i \neq j \in I$, $p_i \neq p_j$) on a d'après le théorème chinois $\mathbf{Z}/n\mathbf{Z} \cong \prod_{i\in I} \mathbf{Z}/p_i^{\nu_i}\mathbf{Z}$. La notion d'idempotent non trivial étant invariante par isomorphisme d'anneaux, il suffit [1] de donner la liste des idempotents non triviaux de $\prod_{i\in I} \mathbf{Z}/p_i^{\nu_i}\mathbf{Z}$. Dans ce qui suit, pour alléger l'écriture, on note pour $i \in I$, $0_i := [0]_{p_i^{\nu_i}}$ et $1_i := [1]_{p_i^{\nu_i}}$. Si $e = (e_i)_{i\in I} \in \prod_{i\in I} \mathbf{Z}/p_i^{\nu_i}\mathbf{Z}$, on a $e^2 = e$ si et seulement si pour tout $i \in I$ on a $e_i^2 = e_i$ si et seulement si (d'après ce qui

1. Si l'on souhaite vraiment expliciter les idempotents non triviaux obtenus dans $\mathbf{Z}/n\mathbf{Z}$, il faut faire intervenir des relations de Bézout ad hoc.

précède) pour tout $i \in I$, on a $e_i \in \{0_i, 1_i\}$. Ainsi l'ensemble des idempotents non triviaux de $\prod_{i\in I} \mathbf{Z}/p_i^{\nu_i}\mathbf{Z}$ est

$$\prod_{i\in I}\{0_i, 1_i\} \setminus \{(0_i)_{i\in I}, (1_i)_{i\in I}\}.$$

Noter qu'en particulier le cardinal de cet ensemble est $2^{\mathrm{card}(I)-1}$.

2. *Soit e un idempotent non trivial de A. Montrer que l'idéal eA est propre.*

   Il suffit de montrer que e n'est pas inversible. Si $e \in A^\times$ vérifie $e^2 = e$, on en déduit en simplifiant par e que $e = 1_A$, et e n'est pas un idempotent non trivial.

3. *Montrer que les propriétés suivantes sont équivalentes :*

   (a) il existe des anneaux B et C non nuls *tels que A est isomorphe à $B \times C$;*

   (b) il existe des idempotents non triviaux $e, f \in A$ tels que $e + f = 1_A$.

   Supposons qu'il existe des anneaux B et C non nuls tels que A est isomorphe à $B \times C$. Clairement $e := (1_B, 0_C)$ et $f := (0_B, 1_C)$ vérifient $e^2 = e$, $f^2 = f$ et $e + f = 1$. Comme B et C sont non nuls, on a $1_B \neq 0_B$ et $1_C \neq 0_C$, ce qui montre que e et f sont des idempotents non triviaux de $B \times C$ tels que $e + f = 1$. Les images de e et f par l'isomorphisme réciproque d'un isomorphisme $A \to B \times C$ donnent alors ce qu'il faut.

   Supposons qu'il existe des idempotents non triviaux $e, f \in A$ tels que $e + f = 1_A$. En multiplipliant par e, on trouve $e^2 + ef = e$, soit $e + ef = e$, donc $ef = 0$. Ainsi l'idéal produit $eA \cdot fA$ est nul, et $A/(eA \cdot fA)$ est isomorphe à A. Par ailleurs, comme $e + f = 1_A$, on a $eA + fA = A$. D'après le théorème chinois, $A/(eA \cdot fA)$ est isomorphe à $A/eA \times A/fA$. D'après la question précédente, eA et fA sont des idéaux propres de A, donc A/eA et A/fA sont des anneaux non nuls.

Exercice 3

1. *Résoudre l'équation*

$$x^3 = 3, \quad x \in A$$

   pour les anneaux A suivants : $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/5^2\mathbf{Z}$.

   Pour $A = \mathbf{Z}/5\mathbf{Z}$, on peut calculer les cubes dans l'anneau fini $\mathbf{Z}/5\mathbf{Z}$:

$$[0]_5^3 = [0]_5,\ [1]_5^3 = [1]_5,\ [2]_5^3 = [8]_5 = [3]_5,\ [3]_5^3 = [27]_5 = [2]_5,\ [4]_5^3 = [-1]_5^3 = [-1]_5 = [4]_5.$$

   L'ensemble des solutions de l'équation proposée est donc $\{[2]_5\}$.

   Pour $A = \mathbf{Z}/25\mathbf{Z}$, plutôt que de calculer les cubes dans $\mathbf{Z}/25\mathbf{Z}$, ce qui est un peu long, on va chercher une solution sous la forme $[x]_{25}$, où $x \in \{0, \ldots, 25\}$, en remarquant que si $[x]_{25}^3 = [3]_{25}$, on a en particulier nécessairement $[x]_5^3 = [3]_5$, donc $[x]_5 = [2]_5$. On peut donc chercher les solutions parmi les éléments de la forme $[2 + 5y]_{25}$, avec $y \in \{0, \ldots, 4\}$. On a, d'après la formule du binôme de Newton

$$(2 + 5y)^3 = 2^3 + 3.2^2.5.y \pmod{25\mathbf{Z}} = 3 + 5(1 + 12y) \pmod{25}.$$

   Ceci montre que $[x]_{25}^3 = [3]_{25}$ si et seulement si 5 divise $1 + 12y$ si et seulement si 5 divise $3(1 + 12y)$ (noter que 3 est l'inverse de 12 modulo 5) si et seulement si 5 divise $3 + y$ si et seulement si $y = 2$. Ainsi l'ensemble des solutions de l'équation proposée est $\{[12]_{25}\}$.

2. *Soit $P \in \mathbf{Z}[X]$ et p un nombre premier. On suppose qu'il existe $a \in \mathbf{Z}$ tel que*

$$P(a) = 0 \pmod{p\mathbf{Z}} \quad \textit{et} \quad P'(a) \neq 0 \pmod{p\mathbf{Z}}.$$

Montrer que pour tout entier strictement positif n, il existe un unique élément $a_n \in \mathbf{Z}/p^n\mathbf{Z}$ tel que

$$P(a_n) = 0 \pmod{p^n\mathbf{Z}} \quad \textit{et} \quad a_n = a \pmod{p\mathbf{Z}}.$$

Le résultat visé est en fait le cas particulier du résultat de la question suivante où $A = \mathbf{Z}$ et $\mathcal{I} = p\mathbf{Z}$, sachant que $(\mathbf{Z}/p\mathbf{Z})^\times = (\mathbf{Z}/p\mathbf{Z}) \setminus \{0\}$. On pourrait donc reprendre mot pour mot la démonstration du résultat de la question suivante. Ici on propose une approche qui bien qu'essentiellement équivalente est légèrement plus élémentaire par certains aspects, et généralise la technique utilisée à la question précédente dans $\mathbf{Z}/25\mathbf{Z}$.

Raisonnons par récurrence sur n, le cas $n = 1$ étant donné par les hypothèses. Soit n un entier strictement positif tel que la propriété est vraie au rang n. Montrons que la propriété est vraie au rang $n + 1$.

Par hypothèse de récurrence, il existe un entier $x_n \in \mathbf{Z}$ vérifiant $x_n = a \pmod{p\mathbf{Z}}$ et $P(x_n) = 0 \pmod{p^n\mathbf{Z}}$, et tout autre entier vérifiant ces propriétés est congru à x_n modulo $p^n\mathbf{Z}$. On a en particulier $P'(x_n) = P'(a) \pmod{p\mathbf{Z}}$, donc $P'(x_n) \neq 0 \pmod{p\mathbf{Z}}$. Soit $z_n \in \mathbf{Z}$ tel que $P(x_n) = p^n z_n$.

Cherchons les éléments $x_{n+1} \in \mathbf{Z}$ vérifiant $x_{n+1} = a \pmod{p\mathbf{Z}}$ et $P(x_{n+1}) = 0 \pmod{p^{n+1}\mathbf{Z}}$. Un tel élément vérifie en particulier $P(x_{n+1}) = 0 \pmod{p^n\mathbf{Z}}$. Ainsi on a nécessairement $x_{n+1} = x_n \pmod{p^n\mathbf{Z}}$. Par ailleurs, si $x_{n+1} = x_n \pmod{p^n\mathbf{Z}}$, on a nécessairement $x_{n+1} = a \pmod{p\mathbf{Z}}$.

On est donc ramené à chercher les éléments $x_{n+1} \in \mathbf{Z}$ vérifiant $x_{n+1} = x_n \pmod{p^n\mathbf{Z}}$ et $P(x_{n+1}) = 0 \pmod{p^{n+1}\mathbf{Z}}$. Pour un tel élément x_n, soit $y_n \in \mathbf{Z}$ tel que $x_{n+1} = x_n + p^n y_n$. Pour tout entier $d \geqslant 1$, on a d'après la formule du binôme de Newton

$$(x_n + p^n y_n)^d = x_n^d + p^n d x_n^{d-1} y_n \pmod{p^{n+1}\mathbf{Z}}.$$

On en déduit

$$P(x_n + p^n y_n) = P(x_n) + p^n P'(x_n) y_n \pmod{p^{n+1}\mathbf{Z}} = p^n(z_n + p^n P'(x_n) y_n) \pmod{p^{n+1}\mathbf{Z}}$$

On a donc $P(x_n + p^n y_n) = 0 \pmod{p^{n+1}\mathbf{Z}}$ si et seulement si

$$z_n + P'(x_n) y_n = 0 \pmod{p\mathbf{Z}}.$$

Or $P'(x_n)$ est non nul donc inversible modulo p, donc l'équation ci-dessous possède une unique solution $\widetilde{y_n}$ modulo p. Comme cette solution est unique modulo p, la solution associée $\widetilde{x_{n+1}} = x_n + p^n \widetilde{y_n}$ de l'équation originelle est unique modulo p^n, ce qui conclut.

3. *Soit A un anneau et $\mathcal{I}$ un idéal de A. Soit $P \in A[X]$. On suppose qu'il existe $a \in A$ tel que $P(a) = 0 \pmod{\mathcal{I}}$ et l'image de $P'(a)$ dans $A/\mathcal{I}$ est inversible. Montrer que pour tout entier strictement positif n, il existe un unique élément $a_n \in A/\mathcal{I}^n$ tel que*

$$P(a_n) = 0 \pmod{\mathcal{I}^n} \quad \textit{et} \quad a_n = a \pmod{\mathcal{I}}.$$

Raisonnons par récurrence sur n, le cas $n = 1$ étant donné par hypothèse. Soit n un entier strictement positif tel que la propriété est vraie au rang n. Montrons que la propriété est vraie au rang $n + 1$.

Par hypothèse de récurrence, il existe un élément $x_n \in A$ vérifiant $x_n = a \pmod{\mathcal{I}}$ et $P(x_n) = 0 \pmod{\mathcal{I}^n}$, et tout autre élément de A vérifiant ces propriétés est congru à x_n

modulo $\mathcal{I}^n$. En particulier on a $P'(x_n) = P'(a) \pmod{\mathcal{I}}$, donc l'image de $P'(x_n)$ dans $A/\mathcal{I}$ est inversible. Soit $t_n \in A$ tel que $t_n P'(x_n) = 1 \pmod{\mathcal{I}}$. On a donc en particulier [2], pour tout $x \in \mathcal{I}^n$,

$$t_n P'(x_n) x = x \pmod{\mathcal{I}^{n+1}}.$$

Cherchons un élément $x_{n+1} \in A$ vérifiant $P(x_{n+1}) = 0 \pmod{\mathcal{I}^{n+1}}$ et $x_{n+1} = a \pmod{\mathcal{I}}$. Comme $\mathcal{I}^{n+1}$ est contenu dans $\mathcal{I}^n$, un tel élément vérifie en particulier $P(x_{n+1}) = 0 \pmod{\mathcal{I}^n}$. Ainsi on a nécessairement $x_{n+1} = x_n \pmod{\mathcal{I}^n}$. Par ailleurs, comme $\mathcal{I}^n$ est inclus dans $\mathcal{I}$, si $x_{n+1} = x_n \pmod{\mathcal{I}^n}$, on a nécessairement $x_{n+1} = a \pmod{\mathcal{I}}$.
On est donc ramené à chercher les éléments $x_{n+1} \in A$ vérifiant

$$P(x_{n+1}) = 0 \pmod{\mathcal{I}^{n+1}} \quad \text{et} \quad x_{n+1} = x_n \pmod{\mathcal{I}^n}.$$

Pour un tel élément, soit $y_n \in \mathcal{I}^n$ tel que $x_{n+1} = x_n + y_n$. Pour tout entier $d \geqslant 2$, on a $y_n^d \in \mathcal{I}^{n+1}$. Ainsi, pour tout entier $d \geqslant 1$, on a d'après la formule du binôme de Newton

$$(x_n + y_n)^d = x_n^d + d x_n^{d-1} y_n \pmod{\mathcal{I}^n}.$$

On en déduit

$$P(x_n + y_n) = P(x_n) + P'(x_n) y_n \pmod{\mathcal{I}^{n+1}}.$$

Ainsi, si $P(x_n + y_n) = 0 \pmod{\mathcal{I}^{n+1}}$, on en déduit que

$$0 = t_n P(x_n) + t_n P'(x_n) y_n \pmod{\mathcal{I}^{n+1}} = t_n P(x_n) + y_n \pmod{\mathcal{I}^{n+1}}.$$

Réciproquement, si $0 = t_n P(x_n) + y_n \pmod{\mathcal{I}^{n+1}}$, on a

$$0 = P'(x_n) t_n P(x_n) + P'(x_n) y_n \pmod{\mathcal{I}^{n+1}} = P(x_n) + P'(x_n) y_n \pmod{\mathcal{I}^{n+1}}.$$

Au final, on a donc $P(x_n + y_n) = 0 \pmod{\mathcal{I}^{n+1}}$ si et seulement si $y_n = -t_n P(x_n) \pmod{\mathcal{I}^{n+1}}$.
Ceci montre l'existence et l'unicité modulo $\mathcal{I}^n$ d'un élément $x_{n+1} \in A$ vérifiant

$$P(x_{n+1}) = 0 \pmod{\mathcal{I}^{n+1}} \quad \text{et} \quad x_{n+1} = x_n \pmod{\mathcal{I}^n},$$

ce qui conclut.
Remarques finales : 1) L'utilisation ci-devant décrite de la formule du binôme de Newton montre en fait le résultat général suivant : pour tout anneau A et tout polynôme $P \in A[X]$, il existe $R \in A[X, Y]$ tel que

$$P(X + Y) = P(X) + Y P'(X) + Y^2 R(X, Y).$$

Il s'agit de la formule de Taylor à l'ordre 1 pour le polynôme P, valable sans aucune hypothèse sur l'anneau A. Il existe aussi des formules de Taylor d'ordre supérieur, mais limitées à certains anneaux : pour la formule de Taylor à l'ordre n, on a besoin que $n!$ soit inversible dans A.
2) Le résultat démontré dans cet exercice porte le nom de *lemme de Hensel*. La technique de démonstration peut se rapprocher dans l'esprit de la méthode de Newton de résolution d'une

2. Autre approche possible, proposée par un étudiant : au lieu d'utiliser directement t_n ainsi, on peut relever t_n en un inversible de $A/\mathcal{I}^n$ en utilisant le fait (à démontrer) que tout antécédent d'un inversible par le morphisme naturel $A/\mathcal{I}^n \to A/\mathcal{I}$ est encore inversible ; soulignons si besoin que cette propriété est fausse pour un morphisme d'anneaux (même surjectif) en général.

équation par approximations successives. Un exemple éclairant est la résolution d'équations polynômiales à coefficients dans l'anneau de séries formelles $A[[T]]$, où A est un anneau.
On pourra ainsi montrer, à titre de prolongement, le résultat suivant. Si $\mathcal{F}(T) \in A[[T]]$, on note $\mathcal{F}(T)_{T=0} \in A$ le terme constant de $\mathcal{F}(T)$.
Soit $P \in A[[T]][X]$ un polynôme à une indéterminée à coefficients dans $A[[T]]$. On suppose qu'il existe $\mathcal{F}(T) \in A[[T]]$ tel que $P(\mathcal{F}(T))_{T=0} = 0$ et $P'(\mathcal{F}(T))_{T=0} \in A^\times$. Alors il existe un unique $\mathcal{G}(T) \in A[[T]]$ tel que $P(\mathcal{G}(T)) = 0$ et $\mathcal{G}(T)_{T=0} = \mathcal{F}(T)_{T=0}$.
Ici la série formelle $\mathcal{F}(T)$ peut être comprise comme une solution grossièrement approchée de l'équation

$$P(\mathcal{X}(T)) = 0, \quad \mathcal{X}(T) \in A[[T]],$$

plus précisément comme une solution modulo $TA[[T]]$. La solution $\mathcal{G}(T)$ est construite par le procédé décrit ci-dessus dans la correction de l'exercice, en déterminant des solutions approchées de plus en plus précises, c'est-à-dire modulo $T^n A[[T]]$ avec n de plus en plus grand. Quand « n tend vers l'infini », on obtient une solution exacte de l'équation $P(\mathcal{X}(T)) = 0$.
Comme exemple basique d'application, on a ainsi :
Soit $\mathbf{K}$ un corps de caractéristique différente de 2. Soit $\mathcal{H}(T) \in A[[T]]$ tel que $\mathcal{H}(T)_{T=0} = 1$. Alors l'équation

$$\mathcal{X}(T)^2 = \mathcal{H}(T), \quad \mathcal{X}(T) \in \mathbf{K}[[T]],$$

possède une unique solution telle que $\mathcal{X}(T)_{T=0} = 1$.
On pourra par exemple expliciter la solution lorsque $\mathcal{H}(T) = 1 + T$ et retrouver ainsi une formule bien connue. On pourra remarquer que si $\mathbf{K}$ est de caractéristique 2, l'équation

$$\mathcal{X}(T)^2 = 1 + T, \quad \mathcal{X}(T) \in \mathbf{K}[[T]]$$

n'admet pas de solution.