**Corrigé Examen 6L23 : Arithmétique dans les anneaux** mardi 26 juin 2012
9h00–12h00

**1. Problème.** Soit $u$ l'endomorphisme de $V = \mathbf{Q}^3$ tel que, si $B_c$ est la base canonique de $\mathbf{Q}^3$, on ait

$$\mathrm{Mat}_{B_c}(u) = A = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix} \in \mathcal{M}(3, \mathbf{Q}).$$

*a.* Montrer que le polynôme caractéristique $\chi_A$ de $A$ est de la forme $(X-a)^2(X-b)$ dans $\mathbf{Q}[X]$.

√ *En développant* $\det(I_3 X - A)$ *par sa second ligne on trouve*

$$\chi_A = (X-1)\begin{vmatrix} X-2 & -1 \\ -1 & X-2 \end{vmatrix} = (X-1)(X^2-4X+3) = (X-1)^2(X-3),$$

*comme voulu avec* $a = 1$ *et* $b = 3$.

*b.* Déterminer le polynôme minimal $\min_A$ de $A$.

√ *Le polynôme* $\min_A$ *doit avoir les même racine* $1, 3$, *et diviser* $\chi_A$ *(Cayley-Hamilton), donc la seule question qui reste est la multiplicité de la racine* $1$ *de* $\min_A$. *Or on calcule* $(A-I)(A-3I) = 0$, *donc* $(X-1)(X-3) = \min_A$.

*c.* $A$ est-elle trigonalisable sur $\mathbf{Q}$? Est-elle diagonalisable?

√ *Comme* $\chi_A$ *est scindé sur* $\mathbf{Q}$, $A$ *est trigonalisable sur* $\mathbf{Q}$. *Comme* $\min_A$ *est à racines simples,* $A$ *est diagonalisable.*

On note $\mathbf{Q}[A]$ la $\mathbf{Q}$-sous-algèbre de $\mathcal{M}(3, \mathbf{Q})$ engendrée par $A$, c'est-à-dire le $\mathbf{Q}$-sous-espace vectoriel de $\mathcal{M}(3, \mathbf{Q})$ engendré par les puissances de $A$.

*d.* Montrer que $\mathbf{Q}[A]$ est isomorphe à on produit direct d'anneaux, qu'on spécifiera.

√ *On a toujours* $\mathbf{Q}[A] = \mathbf{Q}[X]/(\min_A)$, *car* $\min_A$ *est par définition le noyau du morphisme surjectif* $\mathbf{Q}[X] \to \mathbf{Q}[A]$ *de substitution* $X := A$ *(on a appliqué le théorème d'isomorphisme). On a donc* $\mathbf{Q}[A] = \mathbf{Q}[X]/((X-1)(X-3))$, *ce qui d'après le lemme des noyaux (car* $X-1$ *est premier avec* $X-3$*) est isomorphe à* $(\mathbf{Q}[X]/(X-1)) \times (\mathbf{Q}[X]/(X-3))$. *On peut simplifier cela à* $\mathbf{Q}[A] \cong \mathbf{Q} \times \mathbf{Q}$, *car en général* $\mathbf{Q}[X]/(X-a)$ *isomorphe à* $\mathbf{Q}$ *parce que* $(X-a)$ *est le noyau du morphisme surjectif* $\mathbf{Q}[X] \to \mathbf{Q}$ *de substitution* $X := a$ *; on l'applique ici pour* $a = 1$ *et pour* $a = 3$. *L'isomorphisme* $\mathbf{Q}[A] \to \mathbf{Q} \times \mathbf{Q}$ *envoie donc explicitement* $P \mapsto (P[X := 1], P[X := 3])$.

On note $V_a$ (resp. $C_a$) et $V_b$ (resp. $C_b$) les sous-espaces propres (resp. caractéristiques) attachés aux valeurs propres $a$ et $b$.

*e.* Montrer que $V = C_a \oplus C_b$. Déterminer les dimensions $d_a = \dim_{\mathbf{Q}}(V_a)$, $c_a = \dim_{\mathbf{Q}}(C_a)$, $d_b = \dim_{\mathbf{Q}}(V_b)$, et $c_b = \dim_{\mathbf{Q}}(V_b)$.

√ *Le fait que* $V = C_a \oplus C_b$ *est juste le fait général que, si le polynôme caractéristique est scindé, l'espace entier est somme direct des espaces caractéristiques pour les valeurs propres distinctes. On a* $C_a = \ker((u-I)^2)$, $V_a = \ker(u-I)$ *et* $C_b = V_b = \ker(u-3I)$. *Or*

$$A - I = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad (A-I)^2 = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 0 & 0 \\ 2 & 2 & 2 \end{pmatrix} \quad A - 3I = \begin{pmatrix} -1 & 1 & 1 \\ 0 & -2 & 0 \\ 1 & 1 & -1 \end{pmatrix},$$

*dont on voit facilement que les deux premiers sont de rang* $1$ *avec le même noyau (confirmant le fait que la dimension de l'espace propre pour la valeur propre* $a = 1$ *est égale à la multiplicité* $2$ *de celle-ci comme racine de* $\chi_A$, *et que cet espace propre est donc le même que l'espace caractéristique), et que* $A - 3I$ *sont de rang* $2$ *(confirmant que la dimension de l'espace propre pour la valeur propre* $b = 3$ *est forcément* $1$*). Par conséquent* $d_a = c_a = 2$ *et* $d_b = c_b = 1$.

*f.* Trouver une base $B = B_a \cup B_b$ de $V$ (avec $B_a$ base de $C_a$, et $B_b$ base de $C_b$), telle que $\mathrm{Mat}_B(u)$ soit triangulaire supérieure, et écrire $\mathrm{Mat}_B(u)$.

√ *L'espace propre* $V_a$ *est de dimension* $2$, *des générateurs sont par exemple* $b_1 = (1, -1, 0)$ *et* $b_2 = (0, 1, -1)$. *L'autre espace propre (et caractéristique)* $C_b = V_b$ *est engendré par* $b_3 = (1, 0, 1)$. *Avec ces choix de vecteurs on a* $(A-I) \cdot b_2 = -b$, *et donc avec* $B_a = (b_1, b_2)$ *et* $B_b = (b_3)$,

$$\mathrm{Mat}_B(u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

*On trouve cette forme quelle que soit la base de vecteurs propres de* $V = V_1 \oplus V_3$ *choisie.*

**2.** On considère le système suivant de deux congruences, pour $x \in \mathbf{Z}$ :

$$74x \equiv 22 \pmod{84} \tag{1}$$
$$x \equiv 33 \pmod{65} \tag{2}$$

*a.* Calculer $d = \text{pgcd}(74, 84)$, et simplifier la congruence (1) en divisant par $d$ (la congruence simplifiée est équivalente à (1)).

$\surd$ *On a* $\text{pgcd}(74, 84) = 2$ *qui divise aussi* 22*, et la congruence se simplifie en divisant par* 2 *à* $37x \equiv 11 \pmod{42}$.

*b.* Argumenter sans calcul que, considéré séparément, la congruence (1) possède des solutions, et que l'ensemble des solutions forme une classe de congruence, modulo en entier $n$ qu'on spécifiera.

$\surd$ *Le coefficient* 37 *de* $x$ *est premier avec le modulus* 42*, donc* 37 *est inversible dans* $\mathbf{Z}/42\mathbf{Z}$*, et en multipliant* 22 *par un représentant de cet inverse modulo* 42 *on trouvera une solution. La multiplication correspondante dans* $\mathbf{Z}/42\mathbf{Z}$ *transformera la relation de congruence en une congruence simple modulo* 42*, qui détermine l'ensemble des solutions (une classe modulo* 42*).*

*c.* Déterminer l'inverse de (la classe de) 37 dans $\mathbf{Z}/42\mathbf{Z}$.

$\surd$ *On a*

$$\begin{array}{rrcl} & 42 & = & 1 \times 42 \; + \; 0 \times 37 \\ & 37 & = & 0 \times 42 \; + \; 1 \times 37 \\ 42 - 1 \times 37 = & 5 & = & 1 \times 42 \; - \; 1 \times 37 \\ 37 - 7 \times 5 = & 2 & = & -7 \times 42 \; + \; 8 \times 37 \\ 5 - 2 \times 2 = & 1 & = & 15 \times 42 \; - 17 \times 37 \end{array}$$

*ou plus simplement la suite des congruences modulo* 42*:* $42 \equiv 0 \times 37$*,* $37 \equiv 1 \times 37$*,* $5 \equiv -1 \times 37$*,* $2 \equiv 8 \times 37$*,* $1 \equiv -17 \times 37$*. En final, l'inverse cherché est la classe de* $-17$*, ou de* 25*, modulo* 42*.*

*d.* Résoudre la congruence (1).

$\surd$ *On vérifie que pour* $x = -17 \times 11 = -187$ *on a* $37x = 37 \times -17 \times 11 \equiv 11 \pmod{42}$*. La solution* $-187$ *est congruente modulo* 42 *à* 23*, donc la solution complète est donnée par* $x \equiv 23 \pmod{42}$.

*e.* On considère maintenant le système des deux congruences (1) et (2), dont on peut remplacer (1) pas sa solution trouvée. Ainsi le système a la forme

$$x \equiv a \pmod{n} \tag{1'}$$
$$x \equiv 33 \pmod{65} \tag{2}$$

avec $a, n \in \mathbf{Z}$. Montrer qu'il existe des solutions pour ce système de congruences (il n'est pas nécessaire de calculer explicitement une solution), et que l'ensemble des solutions forme une classe de congruence, modulo un entier $m$ qu'on spécifiera.

$\surd$ *Comme* $n = 42$ *et* 65 *sont premiers entre eux, l'existence d'une solution est affirmé par le théorème chinois, et l'ensemble des solutions sera une classe modulo* $m = 42 \times 65 = 2730$.

*f.* Montrer que si $y \in \mathbf{Z}$ vérifie $y \equiv 0 \pmod{n}$ et $y \equiv 1 \pmod{65}$, alors l'ensemble des solutions du système ((1′),(2)) est formé des $x \in \mathbf{Z}$ vérifiant $x \equiv a + y(33 - a) \pmod{m}$.

$\surd$ *Modulo* $n = 42$ *on a* $a + y(33 - a) \equiv a$ *(car par hypothèse* $y \equiv 0 \pmod{n}$*), et modulo* 65 *on a* $a + y(33 - a) \equiv a + 33 - a = 33$ *(car* $y \equiv 1 \pmod{65}$*). Donc* $x = a + y(33 - a)$ *est une solution du système de congruences ; concrètement on a* $a = 23$ *donc* $x = 23 + 10y$*. La solution entière est donnée par sa classe modulo* $m = 2730$*, c'est-à-dire par* $x \equiv 23 + 10y \pmod{2730}$.

*g.* Trouver un tel $y$ (à l'aide d'une relation de Bezout pour $(n, 65)$), et ensuite $x = a + y(33 - a)$.

$\surd$ *On trouve une relation de Bezout* $1 = -17 \times 42 + 11 \times 65$ *par la méthode de la question b. Alors* $y = -17 \times 21 = -714$ *convient, et* $x \equiv 23 - 10 \times 714 = -7117$.

*h.* Décrire la solution du système (1),(2).

$\surd$ *On obtient* $x \equiv -7117 \equiv 1073 \pmod{2730}$*. On vérifie que* $x = 1073$ *est effectivement une solution du système de départ.*

**3.** Dans cette partie $R$ désigne un anneau commutatif quelconque. Notre but est de montrer que l'intersection des idéaux principaux est égal à l'ensemble des éléments nilpotents de $R$. On admet le résultat suivant,qui est mentionné dans le cours sans être démontré, connu comme le théorème de Krull : tout anneau commutatif non trivial contient un idéal maximal.

*a.* Déduire du théorème de Krull sa généralisation suivante : pour tout idéal propre $I$ de $R$ il existe un idéal maximal de $R$ qui contient $I$. (Indication : penser aux anneaux quotient.)

√ *L'anneau $R/I$ contient un idéal maximal, dont l'image réciproque par la projection canonique $R \to R/I$ est un idéal maximal de $R$ contenant $I$ (correspondance de la proposition 1.3.3). Autrement dit, il existe un morphisme surjectif $R/I \to K$ où $K$ est un corps (dont le noyau est l'idéal de $R/I$ produit par le théorème de Krull), et composition avec la projection canonique donne un morphisme surjectif $R \to K$, dont le noyau est un idéal maximal de $R$ contenant $I$.*

*b.* Soit $a \in R$ un élément contenu dans *aucun* idéal maximal. Montrer que $a$ est inversible dans $R$.

√ *Si $aR$ était un idéal propre, il serait contenu dans un idéal maximal (d'après la question précédente), et donc en particulier $a$ aussi, contredisant l'hypothèse. Donc on doit avoir au contraire $aR = R$, et comme alors $1 \in aR$ cela implique que $a$ est inversible.*

*c.* Soit $x \in R$ un élément nilpotent, disons $x^n = 0$. Montrer que tout idéal premier de $R$ contient $x$. Ceci établit l'une des deux inclusions à prouver : l'ensemble des éléments nilpotents de $R$ est contenu dans l'intersection des idéaux premiers de $R$.

√ *Quand un idéal premier contient un produit de plusieurs facteurs, il contient au moins un de ces facteurs (par récurrence immédiate basée sur le produit de deux facteurs). Tout idéal premier contient $0 = x^n$, et donc l'un des $n$ facteurs $x$ du produit ; il contient donc $x$. Ou encore : dans l'anneau quotient par un idéal premier, donc intègre, l'image nilpotente de $x$ est forcément nulle.*

Pour établir l'inclusion opposée, on suppose désormais que $a \in R$ est contenu dans tout idéal premier de $R$. On cherche à démontrer que $a$ est nécessairement nilpotent.

*d.* Soit $I$ un idéal premier de $R[X]$. Montrer que $I \cap R$ est un idéal premier de $R$.

√ *Le quotient $R[X]/I$ est un anneau intègre, et l'image du morphisme composé $R \to R[X] \to R[X]/I$, étant un sous-anneau de celui-ci, est aussi intègre. Le noyau du morphisme composé est $I \cap R$, et c'est un idéal premier dans $R$. On peut aussi raisonner directement si $a, b \in R$ avec $ab \in I \cap R$, alors en particulier $ab \in I$, donc $a \in I$ ou $b \in I$, et donc $a \in I \cap R$ ou $b \in I \cap R$, respectivement.*

*e.* Montrer que $a$ est contenu dans tout idéal maximal de $R[X]$ (on rappelle que $a \in R \subset R[X]$).

√ *Un idéal maximal $M$ de $R[X]$ est en particulier un idéal premier de $R[X]$, donc d'après la question d, $M \cap R$ est un idéal premier de $R$, et par conséquent il contient $a$.*

*f.* En déduire que pour cet élément $a \in R$, le polynôme $1-aX$ est inversible dans $R[X]$. [Indication : on peut utiliser la question *b*.]

√ *D'après la question b, il suffit de montrer que $1 - aX$ n'est dans aucun idéal maximal de $R[X]$. Mais tout tel idéal maximal $M$ contient $a$ (question e), et s'il contiendrait aussi $1 - aX$ on aurait $1 = (1 - aX) + Xa \in M$, contredisant le fait que les idéaux maximaux sont des idéaux propres.*

*g.* Trouver explicitement un inverse de $1 - aX$ dans l'anneau de séries formelles $R[[X]]$.

√ *Si $S = \sum_{i \in \mathbf{N}} a^i X^i$ désigne la série formelle suite de coefficients $(1, a, a^2, \ldots)$, on calcule coefficient par coefficient que $S(1 - aX) = 1$. Donc $S$ est l'inverse de $1 - aX$ dans $R[[X]]$.*

*h.* Conclure, en observant que $R[[X]]$ contient $R[X]$ comme sous-anneau.

√ *D'une part $R[[X]]$ ne peut contenir qu'un seul inverse de $1 - aX$, la série (géométrique) $S$ de la question f, et d'autre part $1 - aX$ possède un inverse dans le sous-anneau $R[X]$. On doit donc avoir $S \in R[X]$, ce qui veut dire que la suite de coefficients $(1, a, a^2, \ldots)$ devient nulle à partir d'un certain indice, c'est-à-dire $a^i = 0$ ; autrement dit $a$ est nilpotent.*



**Fin.**