Corrigé Examen 6L23 : Arithmétique dans les anneaux jeudi 10 mai 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

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

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

$\surd$ *En développant* $\det(I_3X - A)$ *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* $b = 3$. *Le polynôme* $\min_A$ *doit avoir les même racine* $1, 3$, *et diviser* χ_A *(Cayley-Hamilton), donc la seule question qui reste est la multiplicité de la racine* 1 *de* $\min_A$. *Or on calcule* $(A-I)(A-3I) \neq 0$, *donc* $(X-1)(X-3) \neq \min_A$, *et* $\min_A = \chi_A = (X-1)^2(X-3)$.

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

$\surd$ *Comme* $\min_A$ *(ou* χ_A *est scindé sur* $\mathbf{Q}$, A *est trigonalisable sur* $\mathbf{Q}$. *Comme* $\min_A$ *n'est pas à racines simples,* A *n'est pas 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.

c. Expliquer pourquoi les anneaux $\mathbf{Q}[A]$ et $\mathbf{Q}[X]/((X-a)^2) \times \mathbf{Q}$ sont isomorphes.

$\surd$ *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* $\mathbf{Q}[A] = \mathbf{Q}[X]/((X-1)^2(X-3))$, *ce qui d'après le lemme des noyaux (car* $(X-1)^2$ *est premier avec* $X-3$*) est isomorphe à* $(\mathbf{Q}[X]/((X-1)^2)) \times (\mathbf{Q}[X]/(X-3))$. *Il ne reste qu'à montrer* $\mathbf{Q}[X]/(X-3)$ *isomorphe à* $\mathbf{Q}$, *or* $(X-3)$ *est le noyau du morphisme surjectif* $\mathbf{Q}[X] \to \mathbf{Q}$ *de substitution* $X := 3$.

d. Déterminer les idéaux premiers de $\mathbf{Q}[X]/((X-a)^2)$ et de $\mathbf{Q}$.

$\surd$ *Le seul idéal premier du corps* $\mathbf{Q}$ *est* $\{0\}$. *Les idéaux de* $\mathbf{Q}[X]/((X-1)^2)$ *sont en bijection avec les idéaux de* $\mathbf{Q}[X]$ *contenant* $((X-1)^2)$, *et cette bijection préserve la propriété d'être premier ou non, car les quotients correspondants sont isomorphes. Les idéaux de* $\mathbf{Q}[X]$ *sont tous de la forme* (P) *avec* $P \in \mathbf{Q}[X]$ *(car* $\mathbf{Q}[X]$ *est un anneau principal); or demander* $(P) \supseteq ((X-1)^2)$ *veut dire que* P *divise* $(X-1)^2$, *et demander* (P) *idéal premier de* $\mathbf{Q}[X]$ *veut dire* P *irréductible ou nul, donc le seule idéal premier de* $\mathbf{Q}[X]$ *contenant* $((X-1)^2)$ *est* $(X-1)$, *et son image* $(X-1)/((X-1)^2)$ *dans* $\mathbf{Q}[X]/((X-1)^2)$ *est le seul idéal premier de cet anneau.*

e. En déduire les idéaux premiers de $\mathbf{Q}[X]/((X-a)^2) \times \mathbf{Q}$.

$\surd$ *On a la propriété (non démontrée dans le cours) que les idéaux d'un anneau produit* $R \times S$ *sont tous de la forme* $I \times J$ *avec* I *un idéal de* R *et* J *un idéal de* S, *et le quotient* $(R \times S)/(I \times J)$ *est isomorphes à* $(R/I) \times (S/J)$. *Ce dernier anneau produit ne peut être intègre que si l'un des deux facteurs est l'anneau trivial (mais pas les deux), car* $(1,0)*(0,1) = (0,0)$ *dans tout anneau produit, et l'autre facteur est intègre. Par conséquent les idéaux premiers de* $R \times S$ *sont obtenus comme* $I \times S$ *où* I *est idéal premier de* R *ou comme* $R \times J$ *avec* J *idéal premier de* S. *Dans le cas concret les idéaux premiers de* $\mathbf{Q}[X]/((X-1)^2) \times \mathbf{Q}$ *sont* $(X-1)/((X-1)^2) \times \mathbf{Q}$ *(pour l'idéal premier de* $\mathbf{Q}[X]/((X-1)^2)$*) et* $\mathbf{Q}[X]/((X-1)^2) \times \{0\}$ *(pour l'idéal premier de* $\mathbf{Q}$*). On pourrait démontrer la propriété utilisée ainsi : si* $X \subseteq R \times S$ *est un idéal, alors* $X \subseteq (X \cap (R \times \{0\})) + (X \cap (\{0\} \times S))$ *car* $(x_1, x_2) \in X$ *s'écrit* $(x_1, x_2) = (x_1, 0) + (0, x_2) = (1, 0) * (x_1, x_2) + (0, 1) * (x_1, x_2)$.

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

f. 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 $c_b = \dim_{\mathbf{Q}}(V_b)$.

$\surd$ *On a $C_a = \ker((u-I)^2)$, $V_a = \ker(u-I)$ et $C_b = V_b = \ker(u-3I)$. Or*

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

dont on voit facilement que $A - I$ et $A - 3I$ sont de rang 2 (on sait que ces matrices ne sont pas inversibles, donc le rang n'est pas 3, et le rang est > 1 puisque on trouve facilement deux lignes ou deux colonnes indépendantes) et $(A-I)^2$ de rang 1 (une ligne est nulle et les deux autres sont linéairement dépendantes). Par conséquent $d_a = 1 = d_b = c_b$ et $c_a = 2$.

g. 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 $\mathrm{Mat}_B(u)$.

$\surd$ *L'espace propre V_a est engendré par $b_1 = (1, 0, -1)$ (vecteur annulé par $A - I$ pendant que C_a est engendré par ce même vecteur accompagné de par exemple $b_2 = (3, -2, 0)$ (vecteur indépendant annulé par $(A-I)^2$. 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 $B_b = (b_3)$,*

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

(pour d'autre choix de b_1, b_2, le coefficient -1 peut prendre toute autre valeur, sauf 0).

h. Écrire explicitement une identité de Bézout $S(X-a)^2 + T(X-b) = 1$, avec S et T dans $\mathbf{Q}[X]$.

$\surd$ *Division euclidienne de $(X-1)^2$ par $(X-3)$ donne $(X_1)^2 = (X-3)(X+1) + 4$ et on en déduit la relation de Bezout $1 = \mathrm{pgcd}((X-1)^2, X-3) = S(X-1)^2 + T(X-3)$ avec $S = \frac{1}{4}$ et $T = -\frac{1}{4}(X+1)$.*

i. Exprimer les projections de V dans V, définies respectivement par $p_a : v_a + v_b \mapsto v_a$ et $p_b : v_a + v_b \mapsto v_b$, pour $v_a \in C_a$ et $v_b \in C_b$, comme des polynômes en u.

$\surd$ *Avec la relation $S(X-a)^2 + T(X-b) = 1$ on a $p_a = (T(X-b))[X := u] = T(u)(u - bI)$ et $p_b = (S(X-a)^2)[X := u] = S(u)(u - aI)^2$. On a donc concrètement*

$$p_1 = -\frac{1}{4}(u+I)(u-3I) = \left(-\frac{1}{4}X^2 + \frac{1}{2}X + \frac{3}{4}\right)[X := u]$$
$$p_3 = \frac{1}{4}(u-I)^2 = \left(\frac{1}{4}X^2 - \frac{1}{2}X + \frac{1}{4}\right)[X := u].$$

j. Montrer que $p_a \circ (u - a\,\mathrm{Id})$ est nilpotent.

$\surd$ *Par définition de C_1, l'endomorphisme $(u - \mathrm{Id})^2$ s'annule sur C_1. Or, comme p_1, qui est une polynôme en u d'après la question précédente, commute avec u on a $(p_1 \circ (u - \mathrm{Id}))^2 = p_1 \circ (u - \mathrm{Id}) \circ p_1 \circ (u - \mathrm{Id}) = (u - \mathrm{Id}))^2 \circ p_1^2 = 0$, car l'image de $p_1^2 = p_1$ est C_1, où $(u - \mathrm{Id})^2$ s'annule.*

2. On considère le sous-anneau $\mathbf{Z}[\mathbf{i}] = \{\, a + b\mathbf{i} \mid a, b \in \mathbf{Z} \,\}$ de $\mathbf{C}$, dont les éléments son appelés des entiers de Gauss.

a. Soit $g : \mathbf{Z}[X] \to \mathbf{C}$ le morphisme d'anneaux de substitution de $\mathbf{i}$ pour X, qui vérifie donc $g(n) = n$ pour $n \in \mathbf{Z}$ ainsi que $g(X) = \mathbf{i}$. Si $P = \sum_{i=0}^{d} p_i X^i \in \mathbf{Z}[X]$, décrire explicitement $g(P)$. En déduire que l'image $g(\mathbf{Z}[X])$ est égale à $\mathbf{Z}[\mathbf{i}]$.

$\surd$ *Excuses pour la maladresse d'utiliser i comme indice dans un sommation concernant des nombres complexes! En le remplaçant par k on aura $g(P) = \sum_{k=0}^{d} p_k \mathbf{i}^k$ ce qui est visiblement dans $\mathbf{Z}[\mathbf{i}]$ (car les coefficients p_k sont dans $\mathbf{Z} \subseteq \mathbf{Z}[\mathbf{i}]$ et les puissances de $\mathbf{i}$ sont aussi dans $\mathbf{Z}[\mathbf{i}]$ par définition). Pour montrer que aussi $g(\mathbf{Z}[X]) \supseteq \mathbf{Z}[\mathbf{i}]$, il suffit de considérer les polynômes de degré ≤ 1, pour lesquels on a $g(bX + a) = a + b\mathbf{i}$, ce qui montre que tout élément de $\mathbf{Z}[\mathbf{i}]$ est dans $g(\mathbf{Z}[X])$.*

b. Vérifier que $g(X^2+1) = 0$. Comme X^2+1 est un polynôme *unitaire*, on peut effectuer la division euclidienne par $X^2 + 1$ dans $\mathbf{Z}[X]$, c'est-à-dire pour tout $P \in \mathbf{Z}[X]$ il existe $Q, R \in \mathbf{Z}[X]$ tels que $P = (X^2 + 1)Q + R$ et $\deg R < 2$, et ces polynômes Q, R sont uniques. Montrer que pour de tels P, Q, R on a $g(P) = 0$ si et seulement si $R = 0$.

$\surd$ *On a $g(X^2 + 1) = \mathbf{i}^2 + 1 = -1 + 1 = 0$. Application de g à l'équation $P = (X^2 + 1)Q + R$ donne $g(P) = g(X^2 + 1)g(Q) = g(R) = g(R)$, donc $g(P) = 0$ si et seulement si $g(R) = 0$. Or comme $\deg(R) < 2$, disons $R = bX + a$, la condition $g(R) = 0$ veut dire $a + b\mathbf{i} = 0$ et donc $R = 0$.*

c. En déduire que $\mathbf{Z}[\mathbf{i}]$ est isomorphe à $\mathbf{Z}[X]/(X^2+1)$.

$\surd$ *On vient de montrer que $g(P) = 0$ si et seulement si les reste R de la division euclidienne de P par X^2+1 est nul, donc si $p \in (X^2+1)$. On a $\mathbf{Z}[\mathbf{i}] = g(\mathbf{Z}[X]) = \mathbf{Z}[X]/\ker(g) = \mathbf{Z}[X]/(X^2+1)$ d'après le théorème d'isomorphisme.*

On définit $N : \mathbf{Z}[\mathbf{i}] \to \mathbf{Z}$ par $N(a+b\mathbf{i}) = |a+b\mathbf{i}|^2 = a^2+b^2$ pour $a, b \in \mathbf{Z}$.

d. Montrer que N vérifie $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbf{Z}[\mathbf{i}]$.

$\surd$ *$N(xy) = |xy|^2 = (|x|\,|y|)^2 = |x|^2|y|^2 = N(x)N(y)$, ou en utilisant $N(x) = x\overline{x}$ on peur le trouver ainsi : $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$. Cette identité peut aussi être obtenue directement ainsi pour les plus courageux : $N(xy) = N(ac-bd+(ad+bc)\mathbf{i}) = (ac-bd)^2+(ad+bc)^2 = a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2 = (a^2+2b^2)(c^2+2d^2) = N(x)N(y)$.*

e. Montrer que les éléments inversibles de $\mathbf{Z}[\mathbf{i}]$ sont les $z \in \mathbf{Z}[\mathbf{i}]$ avec $N(z) = 1$, puis que ces éléments inversibles sont 1, $\mathbf{i}$, -1, et $-\mathbf{i}$.

$\surd$ *Si $xy = 1$ on a $N(x)N(y) = N(1) = 1$, et comme $N(x), N(y) \in \mathbf{N}$ (l'expression pour $N(x)$ exclut toute valeur négative) cela n'est possible que si $N(x) = N(y) = 1$. Mais $a^2+b^2 = 1$ avec $a, b \in \mathbf{Z}$ n'a que les solutions $a = \pm 1$, $b = 0$ et $a = 0$, $b = \pm 1$.*

On désignera par $\rho : \mathbf{R} \to \mathbf{Z}$ l'opération d'arrondir vers l'entier le plus proche (plus précisément $\rho(x)$ est la partie entière de $x+\frac{1}{2}$), et par $\rho_{\mathbf{C}} : \mathbf{C} \to \mathbf{Z}[\mathbf{i}]$ l'opération d'arrondir vers l'entier de Gauss le plus proche, donnée par $\rho_{\mathbf{C}}(x+y\mathbf{i}) = \rho(x)+\rho(y)\mathbf{i}$ pour $x, y \in \mathbf{R}$. On a pour tout $x \in \mathbf{R}$ que $|x-\rho(x)| \leq \frac{1}{2}$ et donc pour tout $z \in \mathbf{C}$ que $|z-\rho_{\mathbf{C}}(z)| \leq \frac{1}{2}\sqrt{2}$.

f. Soient $a+b\mathbf{i}, c+d\mathbf{i} \in \mathbf{Z}[\mathbf{i}]$ avec $c+d\mathbf{i} \neq 0$. Montrer que si $q = \rho_{\mathbf{C}}(\frac{a+b\mathbf{i}}{c+d\mathbf{i}}) \in \mathbf{Z}[\mathbf{i}]$, alors on aura $a+b\mathbf{i} = (c+d\mathbf{i})q+r$ pour un entier de Gauss r qui vérifie $N(r) < N(c+d\mathbf{i})$.

$\surd$ *Il est clair que $r = a+b\mathbf{i}-(c+d\mathbf{i})q$ est un entier de Gauss, en on peut donc parler de $N(r)$. Soit $z = \frac{a+b\mathbf{i}}{c+d\mathbf{i}} \in \mathbf{Q}[\mathbf{i}]$ et $\delta = z-\rho_{\mathbf{C}}(z)$; d'après le texte du sujet on aura donc $|\delta| \leq \frac{1}{2}\sqrt{2}$. Or on a $q = z-\delta$, et donc $a+b\mathbf{i}-r = (c+d\mathbf{i})q = (c+d\mathbf{i})z-(c+d\mathbf{i})\delta = a+b\mathbf{i}-(c+d\mathbf{i})\delta$, d'où $r = (c+d\mathbf{i})\delta$ et $|r| = |c+d\mathbf{i}|\cdot|\delta| \leq \frac{1}{2}\sqrt{2}|c+d\mathbf{i}|$. En prenant le carré on trouve $N(r) \leq \frac{1}{2}N(c+d\mathbf{i}) < N(c+d\mathbf{i})$.*

g. Soit I un idéal non nul de $\mathbf{Z}[\mathbf{i}]$. Parmi les éléments non-nuls de I, choisissons un élément $s = c+d\mathbf{i}$ qui minimise la valeur de $N(s)$. Montrer que I est égal à l'idéal principal (s) de $\mathbf{Z}[\mathbf{i}]$ engendré par s, et conclure que $\mathbf{Z}[\mathbf{i}]$ est un anneau principal.

$\surd$ *Il est évident que les multiples de s sont des éléments de I, c'est-à-dire que $(s) \subseteq I$; prouvons donc l'inclusion opposée $I \subseteq (s)$. Soit $a+b\mathbf{i} \in I$ un élément quelconque de l'idéal ; on est dans la situation de la question précédente, donc $r = a+b\mathbf{i}-s\rho_{\mathbf{C}}(\frac{a+b\mathbf{i}}{s})$ est un élément de I (par construction, car $a+b\mathbf{i}, s \in I$) qui vérifie $N(r) < N(c+d\mathbf{i})$. Mais d'après le choix de s cela implique $r = 0$, donc $a+b\mathbf{i} = s\rho_{\mathbf{C}}(\frac{a+b\mathbf{i}}{s}) \in (s)$, et on a montré $I \subseteq (s)$. Cela établit que I (et donc tout idéal non nul) est un idéal principal de $\mathbf{Z}[\mathbf{i}]$, et comme $\{0\} = (0)$ est aussi un idéal principal de $\mathbf{Z}[\mathbf{i}]$, les entiers de Gauss forment un anneau principal.*

Fin.