Examen 6L23 : Arithmétique dans les anneaux jeudi 10 mai 2012
9h00–12h00

Le polycopié ou un résumé du cours sont autorisés comme documents.

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.

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

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

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

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

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

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

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.

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

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 $\mathbf{Z}[\mathbf{i}]$.

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 $R = 0$.

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

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 $x, y \in \mathbf{Z}[\mathbf{i}]$.

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 $-\mathbf{i}$.

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 $N(r) < N(c + d\mathbf{i})$.

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.

Fin.