Examen 6L23 : Arithmétique dans les anneaux mardi 26 juin 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

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

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

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

c. 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.

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

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

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

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

$$74x \equiv 22 \pmod{84} \quad (1)$$
$$x \equiv 33 \pmod{65} \quad (2)$$

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

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.

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

d. Résoudre la congruence (1).

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

$$x \equiv a \pmod{n} \quad (1')$$
$$x \equiv 33 \pmod{65} \quad (2)$$

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.

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 $x \equiv a + y(33-a) \pmod{m}$.

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

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

 continué au verso

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.)

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

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.

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.

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

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.*]

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

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

 Fin.