Examen Partiel – 13 Novembre 2007

Documents autorisés : polycopié du cours, une feuille manuscrite personnelle.

Exercice I

Soit A un anneau intègre. Soient $x \in A^*$ et n un entier ≥ 1. L'élément x est dit d'*ordre* n si on a $x^n = 1$ et $x^d \neq 1$ pour tout entier d divisant n, $d \neq n$. Une *racine primitive* n^e *de l'unité* dans un corps $\mathbb{K}$ est par définition un élément d'ordre n de $\mathbb{K}^*$.

Considérons le polynôme $\Phi_9(X) = X^6 + X^3 + 1 \in \mathbb{Z}[X]$. Soit ζ une racine primitive 9^e de l'unité dans $\mathbb{C}$.

1. Soit $x \in A^*$ tel que $x^n = 1$ et $x \neq 1$. Montrer que $x^{n-1} + \cdots + x^2 + x + 1 - n = -n$, puis que $x - 1$ divise n dans A.
2. Soit $\mathbb{F}$ un corps de caractéristique finie p qui est un quotient de l'anneau A. Soit n un entier premier à p. Soit $x \in A^*$ d'ordre n. Si d est un diviseur > 0 de n, $d \neq n$, montrer que l'image de $x^d - 1$ dans $\mathbb{F}$ divise n/d, puis que cette image est inversible.
3. En déduire que tout élément d'ordre n dans A a pour image dans $\mathbb{F}$ un élément d'ordre n.
4. Montrer que les racines de Φ_9 dans $\mathbb{C}$ sont les racines primitives 9^e de l'unité.
5. Montrer que Φ_9 est irréductible sur $\mathbb{Q}$. (On pourra s'intéresser à $\Phi_9(X + 1)$.) Est-il irréductible sur $\mathbb{Z}$?
6. Montrer que l'anneau quotient $\mathbb{Z}[X]/(\Phi_9)$ est isomorphe au sous-anneau $\mathbb{Z}[\zeta]$ de $\mathbb{C}$ engendré par ζ.
7. Montrer que le groupe $\mathbb{Z}[\zeta]^*$ des éléments inversibles de $\mathbb{Z}[\zeta]$ contient un groupe cyclique d'ordre 18.
8. Montrer que l'image de Φ_9 dans $\mathbb{F}_2[X]$ est irréductible. En déduire que l'anneau $k = \mathbb{Z}[X]/(\Phi_9, 2)$ est un corps fini à 2^6 éléments. Montrer que l'ordre de tout élément de k^* divise 63.
9. Montrer que l'image de Φ_9 dans $\mathbb{F}_{19}[X]$ est scindée. En déduire que l'anneau $\mathbb{Z}[X]/(\Phi_9)$ possède un corps quotient à 19 éléments.
10. Montrer que les éléments d'ordre fini du groupe $\mathbb{Z}[\zeta]^*$ sont au nombre de 18.

Exercice II

Soit $\mathbb{K}$ un corps commutatif. Pour $n \geq 1$, on notera $(e_1, \ldots, e_n)$ la base canonique du $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$. Pour $A \in M(n, \mathbb{K})$, on notera $\mathcal{I}_1(A)$ l'ensemble des polynômes $Q \in \mathbb{K}[X]$ tels que $Q(A)(e_1) = 0$. Enfin, pour $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$, on notera $C_P(T) \in M(n, \mathbb{K}[T])$ la matrice

$$C_P(T) = \begin{bmatrix} -T & 0 & \cdots & 0 & -a_0 \\ 1 & -T & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & -T & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} - T \end{bmatrix}.$$

La matrice $c_P = C_P(0)$ est appelée la *matrice compagnon* du polynôme P.

1. On fixe $A \in M(n, \mathbb{K})$. Montrer que l'application $\mathbb{K}[X] \times \mathbb{K}^n \to \mathbb{K}^n$ qui à (Q, e) associe $Q(A)e$ fait de $\mathbb{K}^n$ un $K[X]$-module. Montrer que l'application $\mathbb{K}[X] \to \mathbb{K}^n$ qui à Q associe $Q(A)(e_1)$ est un homomorphisme de $\mathbb{K}[X]$-modules. En déduire que $\mathcal{I}_1(A)$ est un idéal de $\mathbb{K}[X]$.
2. Écrire la matrice de Sylvester associée aux polynômes $X - T$ et $P(X)$ (vus comme polynômes en l'indéterminée X à coefficients dans le corps $\mathbb{K}(T)$). Montrer alors que le déterminant de la matrice $C_P(T)$ est le résultant des polynômes $X - T$ et $P(X)$. En déduire (sans calcul) que le polynôme caractéristique de c_P est P.
3. Montrer que, lorsque $A = c_P$, le $\mathbb{K}[X]$-module $\mathbb{K}^n$ est engendré par e_1. (On pourra montrer que ce $\mathbb{K}[X]$-module contient e_2, e_3, …, e_n.)
4. Montrer que tout élément non nul de $\mathcal{I}_1(c_P)$ est de degré $\geq n$.
5. Montrer que $P \in \mathcal{I}_1(c_P)$.
6. En déduire que le polynôme minimal de c_P est P et que $\mathcal{I}_1(c_P)$ est l'idéal principal engendré par P.
7. Si P est irréductible, montrer que le sous-anneau $\mathbb{K}[c_P]$ de $M(n, \mathbb{K})$ est un corps. Quelle est sa dimension comme $\mathbb{K}$-espace vectoriel ?
8. Donner un exemple de polynôme irréductible de degré n dans $\mathbb{Q}[X]$.
9. Soit F un sous-espace vectoriel de $M(n, \mathbb{Q})$, de dimension $\geq n^2 - n + 1$. Démontrer qu'il contient un élément inversible de $M(n, \mathbb{Q})$.
10. Y a-t-il des sous-espaces vectoriels de dimension $n^2 - n$ de $M(n, \mathbb{Q})$ sans élément inversible ?