Université Joseph Fourier

Préparation à l'agrégation de mathématiques
Devoir d'algèbre à rendre le 25 mars 2004

I Il s'agit ici de prouver le théorème de Cayley-Hamilton par "spécialisation" de la matrice générique : on fixe un entier $n \geq 2$, on note $\mathcal{A}$ l'anneau de polynômes $\mathbb{Z}[X_{i,j}]_{1\leq i,j\leq n}$, et $\mathcal{X}$ la matrice $(X_{i,j})_{1\leq i,j\leq n}$ de $M_n(\mathcal{A})$.

1. Pour A un anneau commutatif unitaire et $M = (m_{i,j})_{1\leq i,j\leq n}$ dans $M_n(A)$, on note

$$C_M(X) = \det(M - XI_n) \in A[X]$$

le polynôme caractéristique de M. On définit un homomorphisme d'anneaux f (ou $f_{A,M}$) de $\mathcal{A}$ dans A par $f(X_{i,j}) = m_{i,j}$ pour tout $(i,j) \in \{1,\ldots,n\}^2$, puis un homomorphisme d'anneaux F (ou $F_{A,M}$) : $\mathcal{A}[X] \to A[X]$ par $F_{|\mathcal{A}} = f$ et $F(X) = X$.

a) Montrer que $F(C_\mathcal{X}) = C_M$.

b) On note f_n l'application $M_n(\mathcal{A}) \to M_n(A)$ qui envoie toute matrice $(P_{k,l})_{k,l}$ sur la matrice $(f(P_{k,l}))_{k,l}$. Montrer que f_n est un homomorphisme d'anneaux qui vérifie $f_n(u\mathcal{Y}) = f(u)f_n(\mathcal{Y})$ $(u \in \mathcal{A},\ \mathcal{Y} \in M_n(\mathcal{A}))$.

c) Montrer que si $C_\mathcal{X}(\mathcal{X})$ est la matrice nulle alors pour tout choix du couple (A, M) comme ci-dessus on a $C_M(M) = 0$ dans $M_n(A)$.

2. On garde les notations de **1.** et on va prouver que $C_\mathcal{X}(\mathcal{X})$ est la matrice nulle de $M_n(\mathcal{A})$. D'après **1**c) ceci établira le théorème de Cayley-Hamilton. On note $\mathcal{K} = \mathbb{Q}(X_{i,j})_{1\leq i,j\leq n}$ le corps des fractions de l'anneau intègre $\mathcal{A}$.

a) Exhiber une matrice $M \in M_n(\mathbb{Z})$ telle que $C_M(X) = (-1)^n(X^n - 2)$. On notera F l'homomorphisme $F_{\mathbb{Z},M}$ associé (*cf* **1.**).

b) En utilisant l'homomorphisme F, démontrer que le polynôme $C_\mathcal{X}$ est irréductible sur $\mathcal{K}$ (on détaillera soigneusement l'argument).

c) Déduire de b) que $C_\mathcal{X}$ a toutes ses racines simples dans son corps de décomposition sur $\mathcal{K}$.

d) Conclure que $C_\mathcal{X}(\mathcal{X}) = 0$.

II Dans ce qui suit on se donne un entier $n \geq 1$, on désigne par k un corps de caractéristique p **avec** $p \not| n$, et on note K le corps de décomposition sur k du polynôme $X^n - 1$.

1. Rappeler pourquoi le corps K contient des racines primitives n-ièmes de 1 (éléments d'ordre multiplicatif exactement n). Quel est leur nombre?

On note $\Phi_{n,k}$ le polynôme $\prod_\zeta (X - \zeta)$ de $K[X]$, où ζ parcourt les racines primitives n-ièmes de 1 dans K. On a alors l'égalité $X^n - 1 = \prod_{d|n} \Phi_{d,k}(X)$ (pourquoi?).

L'existence et l'unicité de la division euclidienne permettent d'en déduire par récurrence les propriétés suivantes, admises:
(i) si $p = 0$, on a $\Phi_{n,k} = \Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$; on note Φ_n ce polynôme.
(ii) si k est le corps fini $\mathbb{F}_q$, alors $\Phi_{n,k} = \Phi_{n,\mathbb{F}_p}$ coïncide avec la reduction de Φ_n modulo p; on le notera $\Phi_{n,p}$.

2. Dans la suite on garde les notations de **1.** et on prend pour k un corps fini $\mathbb{F}_q$. Montrer que toutes les racines de $\Phi_{n,p}$ dans K ont le même degré sur $\mathbb{F}_q$.

3.a) Soit ζ une racine de $\Phi_{n,p}$ dans K. Montrer que les ζ^{q^i}, où $0 \leq i \leq s-1$ et s est l'ordre de q modulo n, sont tous distincts.

b) On pose $P(x) = \prod_{i=0}^{s-1}(X - \zeta^{q^i})$. Montrer que $P \in \mathbb{F}_q[X]$ et que P est le polynôme minimal de ζ sur $\mathbb{F}_q$.

c) Montrer que $\Phi_{n,p}$ se décompose sur $\mathbb{F}_q$ en $\varphi(n)/s$ facteurs irréductibles unitaires distincts, de degré s.

4.a) Ecrire le polynôme Φ_3 et la condition pour que $\Phi_{3,p}$ soit scindé sur $\mathbb{F}_q$. Expliciter le polynôme Φ_9 en fonction de Φ_3 et factoriser $\Phi_{9,k}$ en irréductibles sur les corps $\mathbb{F}_2$, $\mathbb{F}_4$ (qu'on construira) et $\mathbb{F}_7$.

b) Expliciter le polynôme Φ_7 et factoriser de même sa réduction $\Phi_{7,2}$ sur les corps $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_8$.

*****