Université de Sciences et Technologie de Chine
Classe sino-française Année 2021-22

Corrigé de l'EXAMEN du 22 mai 2022

I

Soit n un entier ≥ 1. Soit K un corps. Posons $A = K[X_1, ..., X_n]$. Soit m un entier ≥ 1. On identifie $M_m(K)$ à K^{m^2} et on le munit de la topologie de Zariski.

Soient M, $N \in M_m(K)$. Pour $L \in M_m(K)$, on note P_L le polynôme caractéristique de L. On a $P_L(X) = \det(M - X\mathrm{Id})$, où Id est la matrice identité de $M_m(K)$.

On dit qu'un polynôme de $K[X]$ a des *facteurs multiples* s'il admet des zéros multiples dans une clôture algébrique de K.

Le but de cet exercice est de donner une nouvelle démontration du théorème de Cayley-Hamilton. Il faut donc traiter les questions 4 et 8 directement, sans utiliser ce théorème.

1. Montrer que l'idéal (0) est premier dans A.

Si R est un anneau intègre, $R[X]$ est un anneau intègre. Donc A est intègre, ce qui revient à dire que (0) est premier.

2. Supposons K algébriquement clos. Montrer que K^n est un ensemble algébrique affine irréductible.

L'ensemble K^n est le lieu des zéros du polynôme 0, puisque K est algébriquement clos. D'après le Nullstellensatz, on a $I(K^n) = \sqrt{(0)}$. Comme (0) est premier, on a $I(K^n) = (0)$ et donc $I(K^n)$ est premier, si bien que K^n est un ensemble algébrique affine irréductible.

3. Donner un exemple de corps K tel que K^n n'est pas un ensemble algébrique affine irréductible.

Pour K corps fini, K^n est fini et est donc réunion finie de points. Or chaque point est fermé. Donc K^n est réductible.

4. Montrer que si P_M n'a pas de facteur multiple, on a $P_M(M) = 0$.

Soit $\bar{K}$ une clôture algébrique de K. Alors P_M a pour racines a_1, ..., a_m dans $\bar{K}$ deux à deux distincts. Notons e_1,..., e_m les vecteurs propres associés de M dans $\bar{K}^m$. On a, pour tout $i \in \{1, ..., m\}$, $P_M(M)e_i = \prod_{j=1}^{m}(M - a_j)e_i = 0$. Comme e_1,..., e_m est une base de $\bar{K}^m$, on a $P_M(M) = 0$.

5. Montrer que l'application déterminant $M_m(K) \to K$ est continue pour la topologie de Zariski.

Le déterminant d'une matrice M est un polynôme en les coefficients de M. Tout application polynomiale est continue pour la topologie de Zariski. Ici, il suffit de montrer que l'image réciproque par le déterminant d'un voisinage de $\det(M)$ (par exemple le complémentaire d'un ensemble fini de K) est un voisinage de M. C'est immédiat.

6. Montrer que $Z = \{M \in M_m(K)/P_M(M) = 0\}$ est un ensemble algébrique affine de $M_m(K)$.

Notons $c_{i,j}$ la coordonnée (i,j) de la matrice $P_M(M)$. Notons $m_{i,j}$ la coordonnée (i,j) de la matrice M. On a $P_M(X) \in K[(m_{i,j})_{1\leq i,j\leq m}, X]$ (les coefficients de $P_M(X)$ sont des polynômes en les coefficients de M). On peut poser $P_M(X) = \sum_{k=0}^{m} a_k X^k$, avec $a_k \in K[(m_{i,j})_{1\leq i,j\leq m}]$. Comme les coefficients de M^k sont dans $K[(m_{i,j})_{1\leq i,j\leq m}]$, les coefficients de $P_M(M)$ sont dans $K[(m_{i,j})_{1\leq i,j\leq m}]$. Donc Z est l'ensemble algébrique affine défini par l'annulation de tous les coefficients de $P_M(M)$.

7. Montrer que Z est fermé dans $M_m(K)$ pour la topologie de Zariski.

C'est un fermé puisque c'est l'intersection d'ensembles définis chacun par l'annulation d'un polynôme.

8. Soit Y l'ensemble des éléments $L \in M_m(K)$ tels que P_L a des facteurs multiples. Montrer que Y est un ensemble algébrique fermé de $M_m(K)$.

Le polynôme P_L a des facteurs multiples si et seulement si P_L et P'_L ont une racine commune, c'est-à-dire si et seulement si $\prod_{i=1}^{m} P'_L(a_i) = 0$ (où a_1, ..., a_m dans $\bar{K}$ sont les racines avec multiplicités de P_L). Comme le polynôme $\prod_{i=1}^{m} P'_L(X_i) = 0$ est symétrique en X_1,...,X_m, il s'écrit comme un polynôme en les polynômes symétriques élémentaires en X_1,...,X_m. Or les polynômes symétriques élémentaires en a_1,...,a_m sont les coefficients du polynôme P_M (au signe près). Comme $P_M(X) \in K[(m_{i,j})_{1\leq i,j\leq m}, X]$, on a $\prod_{i=1}^{m} P'_L(a_i) \in K[(m_{i,j})_{1\leq i,j\leq m}]$. Ainsi Y est le lieu des zéros de ce dernier polynôme. C'est donc un ensemble algébrique fermé. (Autre méthode : Y est le lieu d'annulation du discriminant.)

9. En déduire que $P_M(M) = 0$.

D'après les deux questions précédentes, on a $M_m(\bar{K}) = Y \cup Z$. Comme $M_m(\bar{K})$ est irréductible d'après la question 2, on a $M_m(\bar{K}) = Y$, ce qui est absurde, ou $M_m(\bar{K}) = Z$. Donc $P_M(M) = 0$.

10. Supposons N inversible. Montrer que $P_{MN} = P_{NM}$.

On a alors $P_{MN}(X) = \det(MN - X\mathrm{Id}) = \det(N(MN - X\mathrm{Id})N^{-1}) = \det(NM - X\mathrm{Id}) = P_{NM}$.

11. En déduire, par des arguments analogues que $P_{MN} = P_{NM}$.

L'ensemble des matrices non-inversibles est un ensemble algébrique fermé de $M_n(K)$ puisque c'est le lieu d'annulation du déterminant. L'ensemble $\{N \in M_m(K)/P_{MN} = P_{NM}\}$ est algébrique fermé puisque les coefficients des polynômes P_{MN} et P_{NM} sont des polynômes en les coefficients de N. On conclut en utilisant l'irréductibilité de $M_m(\bar{K})$.

II

Posons $A = \mathbf{Z}[X,Y]$. Posons $\epsilon : A \to \mathbf{Z}$ donné par $\epsilon(P(X,Y)) = P(1,1)$. Posons $B = \mathbf{Z}[X,Y,X^{-1},Y^{-1}]$. Soit M un A-module. Soient G et H deux groupes isomorphes à $\mathbf{Z}$ de générateurs g_0 et h_0 respectivement.

1. Montrer que l'application $A\times\mathbf{Z} \to \mathbf{Z}$ qui à (P,n) associe $P(1,1)n$ fait de $\mathbf{Z}$ un A-module.

Cela résulte du fait que $P \mapsto P(1,1)$ est un morphisme d'anneaux $A \to \mathbf{Z}$.

2. Pour P, Q, $R \in A$, posons $\alpha(P,Q) = (X-1)P(X,Y) + (Y-1)Q(X,Y) \in A$ et $\beta(R) = ((Y-1)R, -(X-1)R) \in A^2$. Montrer qu'on obtient ainsi une résolution projective

de $\mathbf{Z}$ comme A-module

$$0 \to A \to A^2 \to A \to \mathbf{Z} \to 0.$$

Montrons qu'on a une suite exacte. L'application $A \to \mathbf{Z}$ qui à P associe $P(1,1)$ est surjective et son noyau est formé par les polynômes qui s'annulent en $(1,1)$, c'est-à-dire l'image de α. Si (P,Q) est dans le noyau de α, on a $(Y-1)|P$ et $(X-1)|Q$, et donc (P,Q) est dans l'image de β. Il est immédiat que $\alpha \circ \beta = 0$. De plus β est injective puisque c'est un couple d'applications injectives. La suite est bien exacte.

La résolution obtenue est projective, puisque A et A^2 sont des A-modules libres.

3. Montrer que les groupes $\mathrm{Ext}^i_A(\mathbf{Z}, M)$ (dans la catégorie des A-modules) se déduisent de la cohomologie du complexe

$$0 \to \mathrm{Hom}_A(A, M) \to \mathrm{Hom}_A(A \oplus A, M) \to \mathrm{Hom}_A(A, M) \to 0$$

où $\mathrm{Hom}_A(A, M) \to \mathrm{Hom}_A(A \oplus A, M)$ se déduit de α et $\mathrm{Hom}_A(A \oplus A, M) \to \mathrm{Hom}_A(A, M)$ se déduit de β.

Cela se déduit du fait qu'on a une résolution projective de $\mathbf{Z}$ comme A-module obtenue dans la question 2.

4. En déduire que les groupes $\mathrm{Ext}^i_A(\mathbf{Z}, M)$ se déduisent de la cohomologie du complexe :

$$0 \to M \to M \oplus M \to M \to 0$$

où $d^0 : M \to M \oplus M$ est donné par $d^0(m) = ((X-1)m, (Y-1)m)$ et $d^1 : M \oplus M \to M$ est donné par $d^1(m \oplus n) = (X-1)m - (Y-1)n$.

Comme on a $d^1 \circ d^0 = 0$, on a bien un complexe. L'application $\mathrm{Hom}_A(A, M) \to M$ qui à P associe $P(1,1)$ est un isomorphisme. Ainsi le complexe de la question 3 devient

$$0 \to M \to M \oplus M \to M \to 0.$$

Il reste à vérifier que les flèches $\delta^0 : M \to M \oplus M$ et $\delta^1 : M \oplus M \to M$ sont bien d^0 et d^1.

5. Déterminer $\mathrm{Ext}^i_A(\mathbf{Z}, \mathbf{Z})$ pour tout $i \geq 0$.

On applique la question 4 pour $M = \mathbf{Z}$. On a alors $(X-1)n = (Y-1)n = 0$ pour tout $n \in \mathbf{Z}$. On a donc $d^0 = 0$ et $d^1 = 0$. Le complexe de la question 4 devient

$$0 \to \mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Z} \to \mathbf{Z} \to 0,$$

où toutes les flèches sont nulles. Donc $\mathrm{Ext}^0_A(\mathbf{Z}, \mathbf{Z}) = \mathbf{Z}$, $\mathrm{Ext}^1_A(\mathbf{Z}, \mathbf{Z}) = \mathbf{Z} \oplus \mathbf{Z}$, $\mathrm{Ext}^2_A(\mathbf{Z}, \mathbf{Z}) = \mathbf{Z}$, et $\mathrm{Ext}^i_A(\mathbf{Z}, \mathbf{Z}) = 0$ si $i \geq 3$.

6. Montrer qu'on a une résolution projective de $\mathbf{Z}$ comme B-module

$$0 \to B \to B^2 \to B \to \mathbf{Z} \to 0.$$

C'est analogue à la question 1.

7. Montrer que l'application $\mathbf{Z}$-linéaire $\mathbf{Z}[G \times H] \to \mathbf{Z}[X, Y, X^{-1}, Y^{-1}]$ qui, pour i, $j \in \mathbf{Z}$, à $[(g_0^i, h_0^j)]$ associe $X^i Y^j$ est un isomorphisme d'anneaux.

Comme cette application envoie un élément de la base canonique de $\mathbf{Z}[G \times H]$ vers un élément de la base canonique de $\mathbf{Z}[X, Y, X^{-1}, Y^{-1}]$, c'est évidemment une bijection. On vérifie immédiatement que c'est un isomorphisme d'anneaux.

8. Montrer que tout $G \times H$-module est ainsi un A-module.

Un $G \times H$-module est la même chose qu'un $\mathbf{Z}[G \times H]$-module et donc qu'un B-module. Comme on a un homomorphisme injectif d'anneaux $A \to B$, on obtient un A-module.

9. Supposons que M est un $G \times H$-module. Montrer que les groupes de cohomologie $\mathrm{H}^i(G \times H, M)$ se déduisent de la cohomologie du complexe $C(M)$

$$0 \to M \to M \oplus M \to M \to 0.$$

On utilise la question 6 et on adapte les arguments de la question 4.

10. Soit c un 1-cocycle $G \times H \to M$. Montrer que c est déterminé par $c(g_0)$ et $c(h_0)$.

Soit $g \in G$. On a $c(gg_0) = g.c(g_0) + c(g)$. On a des formules analogues pour $c(gh_0)$, $c(gg_0^{-1})$, $c((gh_0^{-1})$. Ainsi si $c(g)$ est déterminé par $c(g_0)$ et $c(h_0)$, il en est de même pour $c(gg_0)$, $c(gh_0)$, $c(gg_0^{-1})$, $c(gh_0^{-1})$. Comme G est engendré par $\{g_0, h_0\}$, on en déduit que c est déterminé par $c(g_0)$ et $c(h_0)$.

11. Donner explicitement $\mathrm{Z}^1(G \times H, M) \to \mathrm{H}^1(C(M))$ qui produit l'isomorphisme $\mathrm{Z}^1(G \times H, M)/\mathrm{B}^1(G \times H, M) \to \mathrm{H}^1(G \times H, M)$.

Soit $c \in \mathrm{Z}^1(G \times H, M)$. On a $c(g_0 h_0) = g_0 c(h_0) + c(g_0)$ et $c(h_0 g_0) = h_0 c(g_0) + c(h_0)$ et donc $(g_0 - 1)c(h_0) = (h_0 - 1)c(g_0)$. Donc l'image de $(c(g_0), c(h_0))$ par $M \oplus M \to M$ est nulle. Donc $(c(g_0), c(h_0))$ définit une classe de cohomologie dans $\mathrm{H}^1(C(M))$. Si c est un cobord, il existe $m \in M$ tel que $c(g) = g.m - m$ pour tout $m \in M$. Alors on a $(c(g_0), c(h_0)) = ((g_0 - 1)m, (h_0 - 1)m)$, qui est l'image de $m \in M$ par $M \to M \oplus M$ et donc la classe de cohomologie de $(c(g_0), c(h_0))$ est nulle. On a donc une application bien définie $\mathrm{Z}^1(G \times H, M)/\mathrm{B}^1(G \times H, M) \to \mathrm{H}^1(C(M))$. L'application inverse est construite ainsi. Soit $(m, n) \in M \oplus M$ tel que $(g_0 - 1)n = (h_0 - 1)m$. On lui associe la classe d'un cocycle c défini par $c(g_0) = m$ et $c(h_0) = n$. Cela définit bien un cocycle par la formule $c(g_0^k h_0^l) = g_0^k(1 + h_0 + ... + h_0^{l-1})n + (1 + g_0 + ... + g_0^{k-1})m$. Un tel cocycle est un cobord si et seulement si il existe $l \in M$ tel que $m = (h_0 - 1)l$ et $n = (g_0 - 1)l$, c'est-à-dire si et seulement si (m, n) est dans l'image de $M \to M \oplus M$. On a bien trouvé un isomorphisme $\mathrm{Z}^1(G \times H, M)/\mathrm{B}^1(G \times H, M) \to \mathrm{H}^1(G \times H, M)$.