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

CORRIGÉ de l'EXAMEN du 23 avril 2022

I

Soit k un corps fini à q éléments. Soit n un entier ≥ 1. On dit que $P \in k[X_1, ..., X_n]$ est *réduit* si, pour tout $i \in \{1, ..., n\}$ le degré de P en X_i est $\leq q-1$. Notons R l'ensemble des polynômes réduits de $k[X_1, ..., X_n]$. Notons Γ_q l'idéal de $k[X_1, ..., X_n]$ engendré par $X_1^q - X_1$,..., $X_n^q - X_n$.

Pour I idéal de $k[X_1, ..., X_n]$, on note $V(I)$ l'ensemble algébrique affine (dans k^n) associé à un idéal I de $k[X_1, ..., X_n]$.

Pour V, un ensemble algébrique affine de k^n, on note $I(V)$ l'idéal des polynômes de $k[X_1, ..., X_n]$ qui s'annulent sur V.

On fixe I_0 un idéal de $k[X_1, ..., X_n]$.

1. Montrer qu'il n'y a qu'un nombre fini d'ensembles algébriques affines dans k^n.
L'ensemble k^n est fini. Il n'a donc qu'un nombre fini de sous-ensembles.
2. Montrer que tout polynôme irréductible de $k[X_1, ..., X_n]$ engendre un idéal radical de $k[X_1, ..., X_n]$.
Soit $P \in k[X_1, ..., X_n]$ irréductible. Soit $Q \in k[X_1, ..., X_n]$ et m un entier ≥ 1 tels que $Q^m \in Pk[X_1, ..., X_n]$. Alors P divise Q^m et donc P divise Q puisque P est irréductible. Donc $Q \in Pk[X_1, ..., X_n]$. Donc $P \in Pk[X_1, ..., X_n]$ est un idéal radical.
3. Montrer qu'il existe V un ensemble algébrique affine de $k[X_1, ..., X_n]$ et une infinité d'idéaux radicaux distincts I de $k[X_1, ..., X_n]$ avec $V = V(I)$.
L'anneau $k[X_1, ..., X_n]$ possède une infinité de polynômes irréductibles et donc une infinité d'idéaux radicaux distincts. Ainsi, l'application qui à un idéal radical I associe $V(I)$ a des fibres qui ne sont pas toutes finies.
4. Montrer que R est un k-espace vectoriel de dimension q^n.
L'ensemble R est un espace vectoriel de base $\prod_{i=1}^n X_i^{d_i}$ avec $0 \leq d_i \leq q-1$. Il y a q^n éléments dans cette base.
5. Soit $P \in R$ tel que $P(x_1, ..., x_n) = 0$ pour tout $(x_1, ..., x_n) \in k^n$. Montrer que $P = 0$.
Par récurrence sur n. Fixons $(x_1, ..., x_{n-1}) \in k^{n-1}$. La fonction $x_n \mapsto P(x_1, ..., x_n)$ est nulle. C'est un polynôme en x_n de degré $< q$. Il ne peut avoir q racines que s'il est nul. Posons $P(X_1, ..., X_n) = \sum_{i=0}^{q-1} P_i(X_1, ..., X_{n-1}) X_n^i$. Cela montre le résultat pour $n = 1$. Si le résultat est vrai pour $n-1$ indéterminées, on a $P_i = 0$ pour tout i. Il est vrai pour n indéterminées.
6. Montrer que $k[X_1, ..., X_n] = R \oplus \Gamma_q$.
On a $R \cap \Gamma_q = 0$. Il reste à montrer que $k[X_1, ..., X_n] = R + \Gamma_q$. Comme on a $X_i^m = (X_i^q - X_i)D + S$ (division euclidienne dans $k[X_1, ..., X_n]$), avec S de degré $\leq q-1$ en X_i, on a $S \in R$. On a bien $\prod_{i=1}^n X_i^{m_i} \in \Gamma_q + R$. Ainsi $k[X_1, ..., X_n] \subset R + \Gamma_q$.
7. Montrer que $I(k^n) = \Gamma_q$.

Soit $P \in \Gamma_q$. Comme le polynôme $X_i^q - X_i$ s'annule en tout $x_i \in k$, on a bien $P \in I(k^n)$. Réciproquement, soit $P \in I(k^n)$. Posons $P = S + T$ avec $S \in R$ et $T \in \Gamma_q$. On a alors $T \in I(k^n)$, puisque $\Gamma_q \subset I(k^n)$ et que $I(k^n)$ est un idéal. Donc $S \in I(k^n)$. Mais on a vu que cela entraîne $S = 0$.
8. Montrer que $I(V(I_0)) = I_0 + \Gamma_q$.
On a $I_0 \in I(V(I_0))$ et $\Gamma_q = I(k^n) \subset I(V(I_0))$. Donc $I_0 + \Gamma_q \subset I(V(I_0))$. Réciproquement, soit $P \in I(V(I_0))$. Par le théorème de la base normale, l'idéal I_0 est de type fini. Soient P_1, P_2,..., P_m un système de générateurs de I_0. Posons $Q = 1 - \prod_{i=1}^m (1 - P_i^{q-1}) \in k[X_1, ..., X_n]$. On a $Q(x_1, ..., x_n) = 0$ si et seulement si $P_1(x_1, ..., x_n) = ... = P_m(x_1, ..., x_n) = 0$, c'est-à-dire si et seulement si $(x_1, ..., x_n) \in V(I_0)$. Sinon, on a $Q(x_1, ..., x_n) = 1$. On a $P = PQ + P(1 - Q)$. On a $P(1 - Q) \in \Gamma_q$ car $1 - Q$ s'annule sur le complémentaire de $V(I_0)$. Donc $P \in I_0 + \Gamma_q$.
9. En déduire que $I_0 + \Gamma_q$ est un idéal radical de $k[X_1, ..., X_n]$.
Tout idéal de la forme $I(V)$ est radical.
10. Soit m un entier ≥ 1. Soit d un entier $< q$. Soient $P_1, ..., P_m$ de degré total $\leq d$. Posons $S = \sum_{i=1}^m P_i^{q-1} \prod_{j=i+1}^m (1 - P_j^{q-1})$. Montrer que $S(x_1, ..., x_n) = 1$ si $(x_1, ..., x_n) \in V(P_1, ..., P_m) \cap k^n$ et $S(x_1, ..., x_n) = 0$ si $(x_1, ..., x_n) \in k^n - V(P_1, ..., P_n)$.
Si $(x_1, ..., x_n) \in V(P_1, ..., P_m) \cap k^n$, on a bien $S(x_1, ..., x_n) = 0$. Si $(x_1, ..., x_n) \in k^n - V(P_1, ..., P_n)$, soit i_0 le plus grand entier tel que $P_{i_0}(x_1, ..., x_n) \neq 0$. On a $S(x_1, ..., x_n) = (\sum_{i=1}^m P_i^{q-1} \prod_{j=i+1}^m (1 - P_j^{q-1}))(x_1, ..., x_n)$. Les termes pour $i > i_0$ sont nuls. Les termes pour $i < i_0$ sont nuls car $(1 - P_{i_0}^{q-1})(x_1, ..., x_n) = 0$. Le terme pour $i = i_0$ est égal à 1. Donc on a bien $S(x_1, ..., x_n) = 1$.
11. Soit $Q \in k[X_1, ..., X_n]$ de degré total $\leq d$, avec $V(P_1, ..., P_m) \subset V(Q)$. Montrer qu'il existe $U_1, ..., U_m \in k[X_1, ..., X_n]$ de degré total $\leq md(q - 1)$ tels que pour tout $(x_1, ..., x_n) \in k^n$, on a $Q(x_1, ..., x_n) = \sum_{i=1}^m (P_i U_i)(x_1, ..., x_n)$.
Comme $V(P_1, ..., P_m) \subset V(Q)$, les polynômes Q et $QS = Q \sum_{i=1}^m P_i^{q-2} \prod_{j=i+1}^m (1 - P_j^{q-1}) P_i$ coïncident sur k^n. Posons $U_i = QP_i^{q-2} \prod_{j=i+1}^m (1 - P_j^{q-1})$. C'est un polynôme de degré total $\leq d(q - 1)m$.

II

Soit L_2 le groupe libre (non-abélien) sur deux générateurs α et β. Notons H le sous-groupe normal de G engendré par $\{\alpha^2, \beta^3\}$. Notons respectivement a et b les images de α et β dans $G = L_2/H$. (On dit que G un groupe de présentation $< a, b | a^2, b^3 >$.) Notons A le sous-groupe engendré par a et B le sous-groupe engendré par b. Soit R un anneau commutatif. On admettra qu'on a la suite exacte de G-modules (déduite des surjections canoniques $G \to G/A$ et $G \to G/B$)

$$0 \to R[G] \to R[G/A] \times R[G/B] \to R \to 0,$$

où l'application $R[G/A] \times R[G/B] \to R$ associe à (x, y) le degré de x - le degré de y. Pour $t \in \mathbf{Z}[G]$, on note $M[t] = \{m \in M / t.m = 0\}$.

1. Montrer que les R-modules ci-dessus sont libres.

Tout module de la forme $R[G/H]$ est libre, puisqu'il a pour base G/H.
2. Montrer que le foncteur $\mathrm{Hom}_R(.,M)$ donne lieu à une suite exacte de R-modules :

$$0 \to \mathrm{Hom}_R(R,M) \to \mathrm{Hom}_R(R[G/A],M) \times \mathrm{Hom}_R(R[G/B],M) \to \mathrm{Hom}_R(R[G],M) \to 0.$$

Cela résulte du fait qu'on applique le foncteur à une suite exacte de R-modules libres.
3. Soit H un sous-groupe de G. Identifier $\mathrm{Hom}_R(R[G/H],M)$ à $\mathrm{Hom}_{R[H]}(R[G],M)$.
Soit $\phi \in \mathrm{Hom}_R(R[G/H],M)$. On lui associe $\psi \in \mathrm{Hom}_{R[H]}(R[G],M)$ obtenue en composant avec la surjection canonique $R[G] \to R[G/H]$.
4. En déduire une suite exacte de $R[G]$-modules

$$0 \to M \to \mathrm{Hom}_{R[A]}(R[G],M) \times \mathrm{Hom}_{R[B]}(R[G],M) \to \mathrm{Hom}_R(R[G],M) \to 0.$$

C'est la suite exacte de la question 2, en utilisant l'identification de la question 3, avec $H=A$, $H=B$, $H=G$. On utilise l'identification $\mathrm{Hom}_{R[H]}(R[G],M)$
5. Montrer que, pour tout entier $i \geq 0$, $\mathrm{H}^i(G, \mathrm{Hom}_{R[H]}(R[G],M))$ s'identifie à $\mathrm{H}^i(H,M)$.
C'est le lemme de Shapiro.
6. Montrer que $\mathrm{H}^i(G, \mathrm{Hom}_R(R[G],M))$ est isomorphe à M si $i=0$.
On a $\mathrm{H}^0(G, \mathrm{Hom}_R(R[G],M)) = \mathrm{Hom}_R(R[G],M)^G$. Or on a $\mathrm{Hom}_R(R[G],M)^G \simeq M$ par l'application $\phi \mapsto \phi(1)$. Cette application est surjective. Elle est aussi injective car si $\phi(1)=0$, on a $\phi(g)=0$ pour tout $g \in G$, car ϕ est G-invariante, si bien que $\phi = 0$. D'où l'identification.
7. Montrer que $\mathrm{H}^i(G, \mathrm{Hom}_R(R[G],M))$ est nul si $i>0$.
C'est une propriété des modules coinduits.
8. Montrer que $\mathrm{H}^1(A,M)$ s'identifie à $M[1+a]/(1-a)M$ et que $\mathrm{H}^1(B,M)$ s'identifie à $M[1+b+b^2]/(1-b)M$.
Comme le groupe A est cyclique, on a $\mathrm{H}^1(A,M) \simeq \hat{\mathrm{H}}_0(A,M) = M[1+a]/(1-a)M$, puisque la norme est $1+a$. De même pour B.
9. Montrer qu'on a une suite exacte longue

$$0 \to M^G \to M^A \times M^B \to M \to \mathrm{H}^1(G,M) \to \frac{M[1+a]}{(1-a)M} \times \frac{M[1+b+b^2]}{(1-b)M} \to 0.$$

C'est la suite exacte longue de cohomologie déduite de la suite exacte courte de la question 5.

$$0 \to \mathrm{H}^0(G,M) = M^G \to \mathrm{H}^0(A,M) \times \mathrm{H}^0(B,M) \to \mathrm{Hom}_R(R[G],M)^G \simeq M \to$$

$$\mathrm{H}^1(G,M) \to \mathrm{H}^1(A,M) \times \mathrm{H}^1(B,M) \to \mathrm{H}^1(G, \mathrm{Hom}_R(R[G],M)) = 0.$$

10. Montrer que, pour $i \geq 2$, $\mathrm{H}^i(G,M)$ s'identifie à $\mathrm{H}^i(A,M) \times \mathrm{H}^i(B,M)$.
Il suffit d'écrire la suite exacte longue et d'utiliser la question 8 pour obtenir ces isomorphismes.
11. Montrer que, pour $i \geq 2$, $\mathrm{H}^i(G,M)$ est isomorphe à $\mathrm{H}^{i+2}(G,M)$.
Les groupes A et B sont cycliques. On a donc $\mathrm{H}^i(A,M)$ est isomorphe à $\mathrm{H}^{i+2}(A,M)$ pour $i \geq 1$. Idem pour B. D'où le résultat.

Remarque : Deux précisions manquaient dans l'énoncé. D'une part, M est un $R[G]$-module. D'autre part, on pouvait utiliser que la cohomologie est un foncteur additif, c'est-à-dire que $\mathrm{H}^i(G, M \times N)$ s'identifie à $\mathrm{H}^i(G,M) \times \mathrm{H}^i(G,N)$. Désolé pour ceux qui ont été troublés.