Examen Algèbre 2
Responsable : Mr O. DEBARRE

Important : vous avez droit de consulter le cours et d'utiliser sans démonstration ses résultats (sauf ceux des exercices ou des TD). Si vous voulez utiliser des résultats hors du cours, il faut les démontrer.

Exercice. Soit A un anneau noethérien qui n'a qu'un seul idéal premier, que l'on note $\mathfrak{p}$.

a) Montrer qu'il existe un entier $n > 0$ tel que $\mathfrak{p}^n = (0)$.

b) Montrer que toute suite décroissante d'idéaux de A est stationnaire (*Indication :* on pourra procéder par récurrence sur un entier n tel que $\mathfrak{p}^n = (0)$).

Problème 1. Soit K un corps. Le but de cet problème est de donner une démonstration directe de l'égalité

$$\dim(K[X_1, \dots, X_n]) = n$$

pour tout entier n.

Soit A un anneau.

a) Soit x un élément de A. Montrer que $S_x := \{x^m(1 + ax) \mid m \in \mathbf{N},\ a \in A\}$ est une partie multiplicative de A.

b) Soit $\mathfrak{p}$ un idéal premier de A contenu dans un idéal maximal $\mathfrak{m}$ de A. Montrer que pour tout $x \in A$, on a $\mathfrak{m} \cap S_x \neq \varnothing$ et que pour tout $x \in \mathfrak{m} - \mathfrak{p}$, on a $\mathfrak{p} \cap S_x = \varnothing$.

c) Soit n un entier ≥ 0. Montrer que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) pour tout $x \in A$, on a $\dim(S_x^{-1}A) \leq n - 1$.

d) Soit n un entier ≥ 0. En déduire que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) pour tous $x_0, \dots, x_n \in A$, il existe $a_0, \dots, a_n \in A$ et $m_0, \dots, m_n \in \mathbf{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(x_n^{m_n}(1 + a_n x_n) + a_{n-1}x_{n-1}) + a_{n-2}x_{n-2}) + \cdots) + a_1 x_1) + a_0 x_0) = 0.$$

e) On suppose que A est une K-algèbre et que toute famille $(x_0, \dots, x_n)$ d'éléments de A est algébriquement dépendante sur K. Montrer que l'on a $\dim(A) \leq n$ (*Indication :* on pourra ordonner les monômes intervenant dans une relation de dépendance algébrique entre $x_0, \dots, x_n$ selon l'ordre lexicographique).

f) En déduire $\dim(K[X_1, \dots, X_n]) = n$.

Problème 2. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme unitaire à coefficients entiers. Notons $z_1, \dots, z_n$ ses racines complexes (non nécessairement simples) et $K := \mathbf{Q}(z_1, \dots, z_n) \subset \mathbf{C}$ le corps de décomposition de P et posons $G := \mathrm{Gal}(K/\mathbf{Q})$.

Soit p un nombre premier. Le but de ce problème est de comparer le groupe G au groupe de Galois $\bar{G}$ du polynôme

$$\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_0 \in \mathbf{F}_p[X],$$

où $\bar{a}_i$ désigne la classe de l'entier a_i dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Soit A le sous-anneau $\mathbf{Z}[z_1, \dots, z_n]$ de K.

a) Montrer que l'action du groupe G sur K laisse A stable.

b) Pour tout a dans A, on pose $N(a) = \prod_{g \in G} g(a)$. Montrer $N(a) \in \mathbf{Z}$.

c) Soit p un nombre premier. En déduire que l'idéal pA de A est distinct de A.

d) Soit $\mathfrak{m}$ un idéal maximal de A contenant pA. Montrer que $k := A/\mathfrak{m}$ est un corps de décomposition pour le polynôme $\bar{P}$ défini plus haut.

On pose $D_{\mathfrak{m}} := \{g \in G \mid g(\mathfrak{m}) = \mathfrak{m}\}$. Lorsque g décrit $G - D_{\mathfrak{m}}$, les $g(\mathfrak{m})$ décrivent un ensemble fini $\{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$, peut-être vide, d'idéaux maximaux de A distincts deux à deux et distincts de $\mathfrak{m}$.

e) Montrer que $D_{\mathfrak{m}}$ est un sous-groupe de G.

f) Pour tout $i \in \{1, \dots, r\}$, montrer que l'on a $\mathfrak{m} + \mathfrak{m}_i = A$.

g) Montrer $\mathfrak{m} + \mathfrak{m}_1 \cdots \mathfrak{m}_r = A$.

h) Montrer qu'il existe $x \in A$ dont la classe $\bar{x}$ dans k engendre l'extension $\mathbf{F}_p \subset k$.

i) Montrer qu'il existe $z \in A$ tel que $\bar{z} = \bar{x}$ et $g(z) \in \mathfrak{m}$ pour tout $g \in G - D_{\mathfrak{m}}$.

j) Montrer que le polynôme $\mu(X) := \prod_{g \in G}(X - g(z))$ est à coefficients dans $\mathbf{Z}$.

Tout $g \in D_{\mathfrak{m}}$ laisse stable A et $\mathfrak{m}$, donc définit un élément de $\bar{G}$ que l'on note $\bar{g}$.

k) Si $\sigma \in \bar{G}$, déduire de j) qu'il existe $g \in D_{\mathfrak{m}}$ tel que $\sigma(\bar{x}) = \bar{g}(\bar{x})$, puis que le morphisme

$$\begin{array}{rcl} \psi : D_{\mathfrak{m}} & \to & \bar{G} \\ g & \mapsto & \bar{g} \end{array}$$

est surjectif.

l) Si le polynôme $\bar{P}$ est séparable, montrer que ψ est un isomorphisme.

m) Quelle est la nature du groupe $\bar{G}$?