Algèbre approfondie.

Le sujet est composé de cinq exercices indépendants. Le sujet est volontairement très long pour aborder un maximum de thèmes. Le traitement en profondeur d'un exercice apportera des bonus. Enfin, les questions sont posées de manière volontairement ouvertes : il est possible de demander des indications.

Exercice 1 — Dérivation. Soit k un corps et (K, i) une extension de k. Une k-dérivation de (K, i) est une application k-linéaire $\mathrm{D} : \mathrm{K} \to \mathrm{K}$ vérifiant $\mathrm{D}(xy) = x\mathrm{D}(y) + \mathrm{D}(x)y$ pour tous $x, y \in \mathrm{K}$. On note $\mathrm{Der}_k(\mathrm{K})$ l'ensemble des k-dérivations de (K, i).

a) On note $\mathscr{L}_k(\mathrm{K})$ l'ensemble des applications k-linéaires de K dans K. Munir $\mathscr{L}_k(\mathrm{K})$ d'une structure de K-espace vectoriel.

b) Montrer que l'ensemble des $\mathrm{Der}_k(\mathrm{K})$ est un sous-K-espace vectoriel de $\mathscr{L}_k(\mathrm{K})$.

c) Montrer que $i(k)$ est dans le noyau de tous les éléments de $\mathrm{Der}_k(\mathrm{K})$.

d) Soit $\mathrm{D} \in \mathrm{Der}_k(\mathrm{K})$. Montrer que $\operatorname{Ker} \mathrm{D}$ est un sous-extension de K.

e) En déduire que s'il existe $x \in \mathrm{K}$ tel que $\mathrm{K} = k(x)$, on a $\dim_{\mathrm{K}} \mathrm{Der}_k(\mathrm{K}) \leqslant 1$.

f) Soit $\mathrm{P} \in k[\mathrm{X}]$, $x \in \mathrm{K}$ et $\mathrm{D} \in \mathrm{Der}_k(\mathrm{K})$. Exprimer $\mathrm{D}(\mathrm{P}(x))$ en fonction $\mathrm{D}(x)$.

g) Soient $(x, y) \in \mathrm{K} \times \mathrm{K}^\times$. Montrer que

$$\mathrm{D}(xy^{-1}) = \frac{\mathrm{D}(x)y - x\mathrm{D}(y)}{y^2}.$$

h) Déduire de ce qui précède que $\mathrm{Der}_k(k(\mathrm{X}))$ est un $k(\mathrm{X})$-espace vectoriel de dimension 1.

i) Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme **irréductible**. On suppose que l'une des racines de P dans un corps de décomposition de P est multiple. Montrer que $\mathrm{P}' = 0$ et que $\mathrm{car}(k)$ est un nombre premier p. En déduire que tous les racines de P dans son corps de décomposition sont multiples.

Dans les questions **j** et **k**, on suppose qu'il existe $x \in \mathrm{K}$ tel que $\mathrm{K} = k(x)$ et x est algébrique sur k. On note π le polynôme minimal de x sur K.

j) On suppose que π est à racines simples dans son corps de décomposition. Montrer que $\mathrm{Der}_k(\mathrm{K}) = \{0\}$ (Indication : on pourra utiliser la question **f**).

k) On suppose que π est à racines multiples dans son corps de décomposition. Montrer que $\dim_{\mathrm{K}} \mathrm{Der}_k(\mathrm{K}) = 1$ (Indication : on pourra utiliser la question **f**).

l) Déterminer $\dim_{\mathrm{K}} \mathrm{Der}_{\mathbb{F}_p(\mathrm{X}^p)}(\mathbb{F}_p(\mathrm{X}))$.

Exercice 2 Soit k un corps et $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}, \mathrm{Y}]$.

a) Justifier que $k[\mathrm{X}, \mathrm{Y}]$ est factoriel.

b) Trouver $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}, \mathrm{Y}]$ tels que $\mathrm{pgcd}(\mathrm{P}, \mathrm{Q}) = 1$ et il n'existe pas $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}, \mathrm{Y}]$ tels que $\mathrm{UP} + \mathrm{VQ} = 1$?

On suppose jusqu'à la fin de l'exercice que $\mathrm{pgcd}(\mathrm{P}, \mathrm{Q}) = 1$.

c) Montrer qu'il existe $\mathrm{U}, \mathrm{V} \in k(\mathrm{X})[\mathrm{Y}]$ tels que $\mathrm{UP} + \mathrm{VQ} = 1$.

d) En déduire qu'il existe $\mathrm{A}, \mathrm{B} \in k[\mathrm{X}, \mathrm{Y}]$ et $\mathrm{D} \in k[\mathrm{X}] \smallsetminus \{0\}$ tels que $\mathrm{AP} + \mathrm{BQ} = \mathrm{D}$

e) Montrer que $\{(x, y) \in k^2, \quad \mathrm{P}(x, y) = \mathrm{Q}(x, y) = 0\}$ est fini.

Exercice 3

a) Montrer que les polynômes $\mathrm{P}_1 = \mathrm{X}^4 + \mathrm{X}^3 + 1$, $\mathrm{P}_2 = \mathrm{X}^4 + \mathrm{X} + 1$ et $\mathrm{P}_3 = \mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1$ sont irréductibles sur $\mathbb{F}_2$.

b) Pour $i = 1, 2, 3$, on note $\mathrm{L}_i = \mathbb{F}_2[\mathrm{X}]/\mathrm{P}_i$ et x_i la classe de X dans L_i, Montrer que x_i est inversible dans L_i et déterminer l'ordre de x_i dans le groupe ${\mathrm{L}_i}^\times$.

c) Montrer que L_1, L_2 et L_3 sont trois corps isomorphes.

d) Construire trois isomorphismes $\alpha : \mathrm{L}_3 \to \mathrm{L}_1$, $\beta : \mathrm{L}_3 \to \mathrm{L}_2$ et $\gamma : \mathrm{L}_1 \to \mathrm{L}_2$ (on pourra considérer les éléments ${x_1}^3$ et ${x_2}^3$).

Exercice 4

a) Soit A un anneau commutatif unitaire, $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ et $a \in \mathrm{A}$. Montrer que $\mathrm{P}(a) = 0$ si et seulement si $(\mathrm{X}-a) \mid \mathrm{P}$.

b) Soit $n \in \mathbb{N}$ et $\mathrm{P} \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Soit $1 \leqslant i < j \leqslant n$. Montrer que

$$\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_i, \ldots, \mathrm{X}_{j-1}, \mathrm{X}_i, \mathrm{X}_{j+1}, \ldots, \mathrm{X}_n) = 0 \text{ si et seulement si } (\mathrm{X}_j - \mathrm{X}_i) \mid \mathrm{P}.$$

c) Soit $\mathrm{P} \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tel que, pour tout $\sigma \in \mathfrak{S}_n$, $\mathrm{P}(\mathrm{X}_{\sigma(1)}, \ldots, \mathrm{X}_{\sigma(n)}) = \varepsilon(\sigma)\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. Montrer que $\prod\limits_{1 \leqslant i < j \leqslant n} (\mathrm{X}_j - \mathrm{X}_i) \mid \mathrm{P}$.

d) Soit

$$\mathrm{V} = \begin{vmatrix} 1 & \mathrm{X}_1 & \ldots & {\mathrm{X}_1}^{n-1} \\ 1 & \mathrm{X}_2 & \ldots & {\mathrm{X}_2}^{n-1} \\ \vdots & & & \vdots \\ 1 & \mathrm{X}_n & \ldots & {\mathrm{X}_n}^{n-1} \end{vmatrix}$$

Montrer que V vérifie $\mathrm{V}(\mathrm{X}_{\sigma(1)}, \ldots, \mathrm{X}_{\sigma(n)}) = \varepsilon(\sigma)\mathrm{V}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ pour tout $\sigma \in \mathfrak{S}_n$. En déduire que

$$\mathrm{V} = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_j - \mathrm{X}_i).$$

e) Soit $\mathrm{P} \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tel que, pour tout $\sigma \in \mathfrak{S}_n$, $\mathrm{P}(\mathrm{X}_{\sigma(1)}, \ldots, \mathrm{X}_{\sigma(n)}) = \varepsilon(\sigma)\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. Montrer qu'il existe $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathfrak{S}_n}$ tel que $\mathrm{P} = \mathrm{VQ}$.

f) Soit

$$\mathrm{W} = \begin{vmatrix} 1 & \mathrm{X}_1 & \ldots & {\mathrm{X}_1}^{n-2} & {\mathrm{X}_1}^{n} \\ 1 & \mathrm{X}_2 & \ldots & {\mathrm{X}_2}^{n-2} & {\mathrm{X}_2}^{n} \\ \vdots & & & & \vdots \\ 1 & \mathrm{X}_n & \ldots & {\mathrm{X}_n}^{n-2} & {\mathrm{X}_n}^{n} \end{vmatrix}$$

Montrer qu'il existe $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathfrak{S}_n}$ tel que $\mathrm{W} = \mathrm{VQ}$ et déterminer Q.

Exercice 5 Soit ζ une racine n^{e} primitive de l'unité dans $\mathbb{C}$ et ξ une racine m^{e} primitive de l'unité dans $\mathbb{C}$. Déterminer $[\mathbb{Q}(\zeta, \xi) : \mathbb{Q}]$.