Algèbre approfondie

Le sujet est volontairement long (35 questions) pour évoquer les différents thèmes du cours. Il ne s'agit pas de tout traiter. Chaque question rapporte un point. Un exercice traité entièrement et correctement rapporte un bonus.

Exercice 1 — Questions de cours. Toutes les réponses sont à justifier.

a) Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. Montrer que $k[\mathrm{X}]/(\mathrm{P})$ est un corps si et seulement si P est irréductible.

b) Le nombre $\sqrt[4]{2+\sqrt{5}}$ est-il constructible ? Le nombre $\sqrt[4]{2+\sqrt[3]{5}}$ est-il constructible ?

c) Soit A un anneau intègre et $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$. Montrer que P a au plus $\deg \mathrm{P}$ racines dans A.

d) Montrer que dans un anneau intègre, un élément premier est irréductible.

e) Soient K une extension de k et E un K-espace vectoriel. Montrer que

$$[\mathrm{E} : k] = [\mathrm{E} : \mathrm{K}][\mathrm{K} : k]$$

f) Soit k un corps, Ω une extension algébriquement close de k et $\mathrm{K} = \{x \in \Omega, \quad x \text{ algébrique sur } k\}$. Montrer que K est une clôture algébrique de k.

g) Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. Montrer que si a est une racine commune de P et P' alors a est une racine multiple de P.

h) Soit $\mathrm{P} = \mathrm{X}^3 + \mathrm{X} + 1 \in \mathbb{Q}[\mathrm{X}]$ et α, β, γ ses racines dans $\mathbb{C}$. Déterminer les coefficients du polynôme dont les racines sont $\alpha^2, \beta^2, \gamma^2$.

Exercice 2 — Corps fini.

a) Déterminer la liste des polynômes irréductibles de degré 2, 3 sur $\mathbb{F}_2$.

b) En déduire une factorisation en irréductibles du polynôme $\mathrm{X}^8 - \mathrm{X} \in \mathbb{F}_2[\mathrm{X}]$.

c) À partir de cette liste proposer deux constructions du corps $\mathbb{F}_8$ comme quotient de $\mathbb{F}_2[\mathrm{X}]$.

d) Pour chacune des deux constructions de la question précédente, déterminer l'ordre dans le groupe multiplicatif $\mathbb{F}_8^\times$ de x la classe de X dans le quotient.

e) On considère le polynôme $\mathrm{X}^3 + \mathrm{X}^2 + 1 \in \mathbb{F}_2[\mathrm{X}]$. Montrer que $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X}^2 + 1)$ est isomorphe à $\mathbb{F}_8$. On note x la classe de X dans le quotient $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X}^2 + 1)$.

f) Montrer que si y est une racine de $\mathrm{X}^3+\mathrm{X}^2+1$ dans $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3+\mathrm{X}^2+1)$ alors y^2 est aussi racine de $\mathrm{X}^3+\mathrm{X}^2+1$.

g) En déduire que $\mathrm{X}^3 + \mathrm{X}^2 + 1$ est scindé dans $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X}^2 + 1)$ et que ses racines sont x, x^2, x^4.

h) Montrer que $(1, x, x^2)$ est une base de $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X}^2 + 1)$.

i) Déterminer les coordonnées de x^4 dans la base $(1, x, x^2)$.

j) En déduire que la famille $\mathscr{B} = (x, x^2, x^4)$ est une base de $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^3 + \mathrm{X}^2 + 1)$?

k) Déterminer le produit est trois éléments de $\mathscr{B}$. En déduire que le produit de deux éléments de $\mathscr{B}$ est soit dans $\mathscr{B}$, soit l'inverse d'un élément de $\mathscr{B}$

Exercice 3 — Arithmétique. On considère l'ensemble $\mathrm{A} = \left\{a + i\sqrt{5}b, \quad a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$.

a) Montrer que A est un sous-anneau intègre de $\mathbb{C}$.

b) Pour $z = a + i\sqrt{5}b \in \mathrm{A}$, on pose $\mathrm{N}(z) = a^2 + 5b^2$. Montrer que $\mathrm{N}(z) \in \mathbb{N}$ et $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ pour tout $z, z' \in \mathrm{A}$.

c) Soit $z \in \mathrm{A}$. Montrer que est inversible dans A si et seulement si $\mathrm{N}(z) = 1$.

d) Déterminer l'ensemble des éléments inversible de A.

e) Montrer que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont des éléments irréductibles de A non associés (on pourra utiliser N).

f) Déterminer deux factorisations de 6 en irréductibles dans A.

g) 2 est-il premier dans A ?

h) A est-il factoriel ?

Exercice 4 – Extension de $\mathbb{Q}$. On considère $\alpha = \sqrt{3+\sqrt{3}} \in \mathbb{C}$.

a) Déterminer le polynôme minimal P de α sur $\mathbb{Q}$.

b) Déterminer les racines de P dans $\mathbb{C}$.

c) Montrer que $\sqrt{2} \notin \mathbb{Q}(\alpha)$.

d) Montrer que $\mathbb{Q}(\alpha, \sqrt{2})$ est un corps de décomposition de P sur $\mathbb{Q}$.

e) Montrer que $\mathbb{Q}(\alpha, \sqrt{2})$ est une extension galoisienne de $\mathbb{Q}$.

f) Déterminer le cardinal du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\alpha, \sqrt{2})/\mathbb{Q})$.

g) Pour chacun des éléments σ du groupe du Galois, déterminer $\sigma(\sqrt{2})$ et $\sigma(\alpha)$.

h) Déterminer toutes les sous-extensions de K.