Algèbre approfondie.

Le sujet est composé de quatre exercices. Il s'agit d'en traiter trois parmi les quatre avec les contraintes suivantes : les exercices 1 et 2 sont obligatoires, il faut choisir entre l'exercice 3 et l'exercice 4.

Exercice 1 On considère le polynôme $\mathrm{P} = \mathrm{X}^6 + \mathrm{X}^5 + \mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1$.

a) Soit K un corps. On suppose que P a une racine z dans K. Déterminer l'ordre de z dans le groupe K^* (on distinguera le cas de la caractéristique 7).

b) Soit K un corps. On suppose que le groupe K^* admet un élément z d'ordre 7. Montrer que z est racine de P.

c) Montrer que si P admet une racine dans K alors P est scindé dans K (indication : montrer que si z est une racine de P dans K alors, pour $1 \leqslant k \leqslant 6$, z^k est aussi une racine de P).

d) Soit K un corps et L un corps de décomposition de P sur K. Montrer que L est un corps de rupture pour tous les facteurs irréductibles de P sur K.

e) Montrer que P est irréductible sur $\mathbb{Q}$ (on pourra considérer le polynôme $\mathrm{P}(\mathrm{X}+1)$).

f) Déterminer la factorisation de P en irréductible sur $\mathbb{F}_7$.

g) Justifier que ${\mathbb{F}_8}^*$ admet un élément d'ordre 7. En déduire que P n'est pas irréductible sur $\mathbb{F}_2$ (indication : on pourra considérer le polynôme minimal sur $\mathbb{F}_2$ d'un élément d'ordre 7 de $\mathbb{F}_8$) et déterminer la factorisation de P en irréductible sur $\mathbb{F}_2$.

h) Déterminer le plus petit entier n tel que 7 divise $3^n - 1$. En déduire que P est irréductible sur $\mathbb{F}_3$ (indication : on pourra considérer le corps de rupture d'un facteur irréductible de P). Montrer alors que $\mathbb{F}_3[\mathrm{X}]/\mathrm{P}$ est un corps dont on déterminera le cardinal.

i) Que peut-on dire de la factorisation de P en irréductible sur $\mathbb{F}_{29}$?

Exercice 2 On considère le polynôme $\mathrm{P} = 1 + \mathrm{X} + \mathrm{X}^2 + \mathrm{X}^3 + \mathrm{X}^4 \in \mathbb{Q}[\mathrm{X}]$.

a) Montrer que P est irréductible sur $\mathbb{Q}$.

b) Déterminer un sous-corps K de $\mathbb{C}$ qui est un corps de rupture de P sur $\mathbb{Q}$. Est-ce un corps de décomposition de P sur $\mathbb{Q}$?

c) Déterminer la factorisation en irréductibles de P sur $\mathbb{C}$.

d) Soit $z \in \mathrm{K}$ une racine de P. Calculer $(2(z + z^4) + 1)^2$.

e) En déduire que $\mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}(\sqrt{5})$ et déterminer une expression de $\cos(2\pi/5)$ en fonction de $\sqrt{5}$.

f) Soit L un sous-corps de K différent de K et $\mathbb{Q}$. Déterminer $[\mathrm{L} : \mathbb{Q}]$ et $[\mathrm{K} : \mathrm{L}]$.

g) Montrer que le polynôme minimal de z sur L divise P. En déduire que $\mathrm{L} = \mathbb{Q}(\sqrt{5})$.

Exercice 3 On considère le polynôme $\mathrm{P} = \mathrm{X}^4 - 3 \in \mathbb{Q}[\mathrm{X}]$ et L le corps de décomposition de P sur $\mathbb{Q}$.

a) Montrer que P est irréductible sur $\mathbb{Q}$.

b) Déterminer $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]$.

c) Déterminer $[\mathrm{L} : \mathbb{Q}]$.

d) Déterminer tous les corps de rupture de P contenu dans L.

Exercice 4 On considère $\mathrm{P} = \mathrm{Y}^2 - \mathrm{X}^3 + \mathrm{X} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$.

a) Montrer que P est irréductible dans $\mathbb{C}[\mathrm{X}, \mathrm{Y}]$.

b) En déduire que $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{P})$ est un anneau intègre (on rappelle que $\mathbb{C}[\mathrm{X}, \mathrm{Y}]$ est factoriel).

c) On note y la classe de Y dans $\mathbb{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{P})$. Montrer que y est irréductible dans $\mathbb{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{P})$.

d) Montrer que le morphisme $\varphi : \mathbb{C}[\mathrm{X}, \mathrm{Y}] \to \mathbb{C}[\mathrm{X}]/(\mathrm{X}^3 - \mathrm{X})$ qui envoie X sur la classe de X et Y sur 0 induit par passage au quotient un isomorphisme entre $\mathrm{A}/(y)$ et $\mathbb{C}[\mathrm{X}]/(\mathrm{X}^3 - \mathrm{X})$. En déduire que A n'est pas factoriel.