Algèbre approfondie.

Exercice 1 — Corps finis. Soit $\mathrm{P} = \mathrm{X}^9 - \mathrm{X} + 1 \in \mathbb{F}_3[\mathrm{X}]$.

a) Soit K un corps fini à p^n éléments. Montrer que tout élément x de K est racine de $\mathrm{X}^{p^n} - \mathrm{X}$.

b) Montrer que P n'a pas de racines dans $\mathbb{F}_3$ ni dans $\mathbb{F}_9$.

c) Montrer que le polynôme $\mathrm{Q} = \mathrm{X}^3 - \mathrm{X} - 1$ est irréductible sur $\mathbb{F}_3$. En déduire que $\mathrm{L} := \mathbb{F}_3[\mathrm{X}]/(\mathrm{Q})$ est un corps fini dont on déterminera le cardinal. On note $\alpha \in \mathrm{L}$ la classe de X modulo Q.

d) Déterminer les racines de Q dans L (on pourra étudier la différence de deux racines de Q).

e) Montrer que toute racine de Q dans L est une racine de P.

f) Déterminer toutes les racines de P dans L (on pourra utiliser le morphisme de Frobenius pour construire une racine de Q à partir d'une racine de P).

g) En déduire une factorisation de P en irréductible sur $\mathbb{F}_3[\mathrm{X}]$ (on pourra utiliser sans le démontrer le résultat suivant : soit k un corps ; un polynôme $\mathrm{P} \in k[\mathrm{X}]$ est irréductible sur k si et seulement si il n'a pas de racine dans toutes les extensions de degré inférieur ou égal à $\deg \mathrm{P}/2$).

h) Déterminer l'ordre de α dans le groupe $\mathrm{L}^\times$. En déduire l'ordre de $-\alpha$ dans $\mathrm{L}^\times$.

i) Trouver i tel que $\alpha^2 - \alpha = (-\alpha)^i$.

Exercice 2 — Extension de corps.

a) Déterminer la liste des polynômes irréductibles sur $\mathbb{F}_2$ de degré inférieur ou égal à 4.

b) En déduire que $\mathrm{P} = \mathrm{X}^4 + \mathrm{X}^3 - 4\mathrm{X}^2 - 4\mathrm{X} + 1$ est irréductible sur $\mathbb{Q}$.

c) Montrer que P divise $\mathrm{P}(2 - \mathrm{X}^2) = \mathrm{X}^8 - 9\mathrm{X}^6 + 26\mathrm{X}^4 - 24\mathrm{X}^2 + 1$. En déduire que si z est une racine de P dans $\mathbb{C}$ alors $2 - z^2$ aussi.

Soit a une racine de P dans $\mathbb{C}$.

d) Déterminer $[\mathbb{Q}(a) : \mathbb{Q}]$

e) On pose $b = 2 - a^2$, $c = 2 - b^2$ et $d = 2 - c^2$. Exprimer c comme un polynôme en a de degré inférieur ou égal à 3.

f) Montrer que a, b, c, d sont des racines distincts de P (indication : on pourra utiliser sans la justifier l'égalité suivante $d = -a^3 + a^2 + 3a - 2$).

g) Justifier sans calcul que $a = 2 - d^2$.

h) Montrer que les corps $\mathbb{Q}(a)$, $\mathbb{Q}(b)$, $\mathbb{Q}(c)$ et $\mathbb{Q}(d)$ sont égaux.

i) Montrer que $\mathbb{Q}(a)$ est un corps de rupture et un corps de décomposition pour P.

j) Les éléments a, b, c, d sont-ils constructibles à la règle et au compas ? (On pourra calculer $(-3a + a^3)^2$, pour cela, on pourra utiliser sans la justifier l'égalité : $a^6 = -5a^3 + 15a^2 + 21a - 5$).

k) On note G l'ensemble des morphismes de $\mathbb{Q}$-algèbres de $\mathbb{Q}(a)$ dans $\mathbb{C}$. Déterminer le nombre et la forme des éléments de G.

l) Montrer que P est scindé dans $\mathbb{R}$ (On pourra calculer $\mathrm{P}(3/2)$).

Exercice 3 On considère la courbe paramétrée donnée par

$$x(t) = \frac{1 + t^2}{1 - t^2}, \quad y(t) = \frac{2t}{1 - t^2}$$

a) Montrer que la courbe est contenue dans un ensemble de la forme $\{(x, y) \in \mathbb{R}^2,\ \mathrm{P}(x, y) = 0\}$ où $\mathrm{P} \in \mathbb{R}[\mathrm{X}, \mathrm{Y}]$ est un polynôme que l'on déterminera.

b) Le polynôme P obtenu est-il irréductible dans $\mathbb{R}[\mathrm{X}, \mathrm{Y}]$?