Algèbre approfondie.

Exercice 1 — Racines de l'unité. Soit ζ une racine m^{e} primitive de l'unité dans $\mathbb{C}$ et ξ une racine n^{e} primitive de l'unité dans $\mathbb{C}$.

a) Montrer que le sous-groupe $\mathrm{G} = \langle \zeta, \xi \rangle$ de $\mathbb{C}^\times$ engendré par ζ et ξ est fini.

b) En déduire que G est cyclique.

c) Déterminer un générateur de G et l'ordre de G (indication : soit $d = \mathrm{pgcd}(m, n)$ et $d = rm + ns$ une relation de Bézout, on pourra considérer $\zeta^s \xi^r$).

d) En déduire la valeur de $[\mathbb{Q}(\zeta, \xi) : \mathbb{Q}]$.

Exercice 2 — Corps fini.

a) Montrer que le polynôme $\mathrm{P} = \mathrm{X}^4 + \mathrm{X} + 1$ est irréductible sur $\mathbb{F}_2$.

b) On note $\mathrm{K} = \mathbb{F}_2[\mathrm{X}]/\mathrm{P}$ et x la classe de X dans K. Justifier que $(1, x, x^2, x^3)$ est une $\mathbb{F}_2$-base de K et que K est un corps de cardinal 16.

c) Démontrer que l'ensemble $\mathrm{L} = \{y \in \mathrm{K},\ y^4 = y\}$ est un sous-corps de K dont on déterminera le cardinal.

d) Déterminer la liste de tous les sous-corps de K.

e) Déterminer pour chacun des éléments de L la décomposition dans la base $(1, x, x^2, x^3)$ (on pourra considérer l'élément $x^2 + x$).

f) Soit $\mathrm{Q} \in \mathbb{F}_2[\mathrm{X}]$. Montrer que si $z \in \mathrm{K}$ est une racine de Q alors z^2 l'est aussi. En déduire que une factorisation de P en irréductibles dans K[X] (les coefficients de la factorisation seront exprimés dans la base $(1, x, x^2, x^3)$).

g) Soit $\mathrm{Q} \in \mathrm{L}[\mathrm{X}]$. Montrer que si $z \in \mathrm{K}$ est une racine de Q alors z^4 l'est aussi.

h) Le polynôme P est-il irréductible sur L ou non ? Si oui, justifier l'irréductibilité, sinon déterminer une factorisation de P dans L[X].

Exercice 3 — Polynôme symétrique. On considère $\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ l'anneau des polynômes en n indéterminées à coefficients dans $\mathbb{Z}$.

Pour $j \in [\![1\,,\, n]\!]$, on note $\mathscr{P}_j$ l'ensemble des parties à j éléments de $\{1, \ldots, n\}$ et

$$\Sigma_j(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \sum_{\mathrm{J} \in \mathscr{P}_j} \prod_{\ell \in \mathrm{J}} \mathrm{X}_\ell \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]\,.$$

Pour $j \in \mathbb{N}^*$, on pose $\mathrm{S}_j(\mathrm{X}_1, \ldots, \mathrm{X}_n) = {\mathrm{X}_1}^j + \cdots + {\mathrm{X}_n}^j$.

a) Montrer que, pour tout $j \in \mathbb{N}^*$, S_j est un polynôme symétrique en $\mathrm{X}_1, \ldots, \mathrm{X}_n$.

b) Exprimer S_1, S_2 et S_3 en fonction de $\Sigma_1, \ldots, \Sigma_n$.

c) On considère le polynôme $\mathrm{P}(\mathrm{T}) = \prod_{\ell=1}^{n} (\mathrm{T} - \mathrm{X}_\ell)$. Exprimer P en fonction de T et de Σ_j pour $j \in [\![1\,,\, n]\!]$.

d) En déduire que, pour $j \geqslant n$, on a $\mathrm{S}_j - \Sigma_1 \mathrm{S}_{j-1} + \Sigma_2 \mathrm{S}_{j-2} - \Sigma_3 \mathrm{S}_{j-3} + \cdots + (-1)^n \Sigma_n \mathrm{S}_{j-n} = 0$ (on pourra utiliser le fait que X_ℓ est racine de P pour tout $\ell \in [\![1\,,\, n]\!]$).

e) Montrer que $\mathrm{P}'(\mathrm{T}) = \sum_{\ell=1}^{n} \dfrac{\mathrm{P}(\mathrm{T})}{\mathrm{T} - \mathrm{X}_\ell} = \sum_{\ell=1}^{n} \dfrac{\mathrm{P}(\mathrm{T}) - \mathrm{P}(\mathrm{X}_\ell)}{\mathrm{T} - \mathrm{X}_\ell}$.

f) Pour tout $m \in [\![0\,,\, n]\!]$, déterminer explicitement un polynôme $\mathrm{Q}_m(\mathrm{T}, \mathrm{X}_\ell)$ tel que

$$\mathrm{T}^m - {\mathrm{X}_\ell}^m = (\mathrm{T} - \mathrm{X}_\ell)\mathrm{Q}_m(\mathrm{T}, \mathrm{X}_\ell)\,.$$

g) En déduire que

$$\frac{\mathrm{P}(\mathrm{T})}{\mathrm{T} - \mathrm{X}_\ell} = \mathrm{T}^{n-1} + \sum_{p=1}^{n-1} \mathrm{A}_{p,\ell} \mathrm{T}^{n-1-p} \qquad \text{avec} \qquad \mathrm{A}_{p,\ell} = {\mathrm{X}_\ell}^p + \sum_{j=1}^{p} (-1)^j {\mathrm{X}_\ell}^{p-j} \sigma_j\,.$$

h) À l'aide de la question **e**, en déduire que $j \leqslant n-1$, on a $\mathrm{S}_j - \Sigma_1 \mathrm{S}_{j-1} + \Sigma_2 \mathrm{S}_{j-2} - \Sigma_3 \mathrm{S}_{j-3} + \cdots + (-1)^j j \Sigma_j = 0$.