# Algèbre approfondie.

Le sujet est volontairement long 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 — Corps fini.** Soit $p$ un nombre premier impair. On note $\mathbb{F}_p$ le corps fini à $p$ éléments.

**a)** (Question de cours) Montrer qu'il existe $s \in \mathbb{F}_p$ tel que $s$ n'est pas un carré dans $\mathbb{F}_p$.

**b)** Montrer que le polynôme $\mathrm{X}^2 - s$ est irréductible sur $\mathbb{F}_p$.

Dans la suite de l'exercice, on désigne par K un corps de rupture de $\mathrm{X}^2 - s$ sur $\mathbb{F}_p$ et $\alpha$ une racine de $\mathbb{F}_p$ dans K.

**c)** Déterminer le cardinal de K.

**d)** (Question de cours) Montrer que l'application

$$\mathrm{F}\colon \begin{cases} \mathrm{K} \longrightarrow \mathrm{K} \\ x \longmapsto x^p \end{cases}$$

est un automorphisme de corps.

**e)** Montrer que $\mathrm{F} \circ \mathrm{F} = \mathrm{id}_{\mathrm{K}}$.

**f)** (Question de cours) Caractériser les éléments de $\mathbb{F}_p$ à l'aide de F.

**g)** Montrer que $\mathrm{F}(\alpha)$ est racine de $\mathrm{X}^2 - s$. En déduire la valeur de $\mathrm{F}(\alpha)$ en fonction de $\alpha$.

**h)** Montrer que l'application

$$\mathrm{N}\colon \begin{cases} \mathrm{K}^\times \longrightarrow \mathrm{K}^\times \\ x \longmapsto x^{p+1} \end{cases}$$

Montrer que N est un morphisme de groupes à valeurs dans ${\mathbb{F}_p}^\times$.

**i)** En utilisant la relation $|\mathrm{Ker}\,\mathrm{N}||\mathrm{Im}\,\mathrm{N}| = |\mathrm{K}^\times|$, montrer que l'image de N est ${\mathbb{F}_p}^\times$ (on pourra majorer $|\mathrm{Ker}\,\mathrm{N}|$).

**j)** Montrer que pour tout $x \in \mathrm{K}$, il existe un unique couple $(u, v) \in {\mathbb{F}_p}^2$ tel que $x = u + v\alpha$.

**k)** Calculer $\mathrm{F}(x)$ en fonction de $u, v$ et $\alpha$.

**l)** En déduire que pour $x \in \mathrm{K}^\times$, on a $\mathrm{N}(x) = u^2 - sv^2$.

**Exercice 2 — Extension de $\mathbb{Q}$.**

**a)** Montrer que le polynôme $\mathrm{X}^4 - 2$ est irréductible sur $\mathbb{Q}$.

**b)** On note K le corps de décomposition sur $\mathbb{Q}$ de $\mathrm{X}^4 - 2$. Montrer que $\mathrm{K} = \mathbb{Q}(i, \sqrt[4]{2})$ et déterminer $[\mathrm{K} : \mathbb{Q}]$.

**c)** Montrer que K est une extension galoisienne de $\mathbb{Q}$.

**d)** Déterminer le cardinal du groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

**e)** Pour chacun des éléments $\sigma$ du groupe du Galois. Déterminer $\sigma(i)$ et $\sigma(\sqrt[4]{2})$.

**f)** Déterminer toutes les sous-extension de K.

**Exercice 3 — Constructibilité : théorème de Wanzel.** On note $\overline{\mathbb{Q}}$ l'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$. Si $z, z' \in \overline{\mathbb{Q}}$, on dit que $z, z'$ sont conjugués sur $\mathbb{Q}$ si $z$ et $z'$ ont le même polynôme minimal sur $\mathbb{Q}$.

**a)** (Question de cours) En utilisant le fait que $\mathbb{C}$ est algébriquement clos, montrer que $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

**b)** Montrer que si $z$ et $z'$ sont conjugués sur $\mathbb{Q}$, il existe $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ automorphisme de corps tel que $\sigma(z) = z'$.

**c)** Montrer que si $z$ et $z'$ sont conjugués et $z$ est constructible alors $z'$ est constructible.

**d)** Soit $z \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et P le polynôme minimal de $z$. On note K le corps de décomposition de P sur $\mathbb{Q}$. On suppose que $z$ est constructible. Montrer que K est engendré sur $\mathbb{Q}$ par des éléments constructibles. En déduire que tout élément de K est constructible.

**e)** En utilisant le théorème de l'élément primitif, montrer que $[\mathrm{K} : \mathbb{Q}]$ est une puissance de 2.

**f)** Inversement, on suppose que $[\mathrm{K} : \mathbb{Q}]$ est une puissance de 2. Montrer que $z$ est constructible (on pourra montrer que K est une extension galoisienne de $\mathbb{Q}$ dont le groupe de Galois est un 2-groupe).

**Exercice 4 – Extension séparable et puissance $p$.** Soient $p$ un nombre premier, $k$ un corps de caractéristique $p$ et K une extension de $k$.

**Rappel :** On rappelle qu'un polynôme $\mathrm{P} \in k[\mathrm{X}]$ irréductible est dit séparable sur $k$ si P et $\mathrm{P}'$ n'ont pas de racines communes. On rappelle qu'un élément $x \in \mathrm{K}$ est dit séparable sur $k$ si le polynôme minimal $x$ sur $k$ est séparable sur $k$.

**a)** (Question de cours) Montrer que si P est séparable alors $\mathrm{P}' = 0$.

**b)** (Question de cours) Soit $a \in \mathrm{K}$ algébrique sur $k$. On suppose que $a$ n'est pas séparable et on note P le polynôme minimal de P sur $k$. Montrer qu'il existe un unique $\mathrm{Q} \in k[\mathrm{X}]$ tel que $\mathrm{P} = \mathrm{Q}(\mathrm{X}^p)$.

**c)** Montrer que le polynôme Q obtenu à la question précédente est irréductible.

**d)** Soit $a \in \mathrm{K}$ algébrique sur $k$. On suppose que $a$ n'est pas séparable sur $k$. Déterminer le polynôme minimal de $a^p$ sur $k$.

**e)** En déduire $[k(a) : k(a^p)]$ et le polynôme minimal de $a$ sur $k(a^p)$.

**f)** Pour $a \in \mathrm{K}$. Montrer que les propriétés suivantes sont équivalentes

$(i)$ $a$ est séparable sur $k$ ;
$(ii)$ $k(a) = k(a^p)$ ;
$(iii)$ il existe $n \in \mathbb{N}^*$ tel que $k(a^{p^n}) = k(a)$ ;
$(iv)$ pour tout $n \in \mathbb{N}$, on a $k(a^{p^n}) = k(a)$.

Indication : pour $(i) \Rightarrow (iv)$, on pourra déterminer $[k(a) : k(a^{p^n})]_s$ en utilisant le polynôme $\mathrm{X}^{p^n} - a^{p^n}$.

**g)** On considère $x \in \mathrm{K}$ séparable sur $k$ et $y \in \mathrm{K}^\times$ tel qu'il existe $n \in \mathbb{N}$ tel que $y^{p^n} \in k$. Montrer que

$$k(x, y) = k(xy) = k(x + y).$$

**Exercice 5 – Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.** Soit $k$ un corps et $n \in \mathbb{N}^*$. On note

$$\mu_n(k) = \{x \in k,\ x^n = 1\} \qquad \text{et} \qquad \mu_n^\circ(k) = \{x \in k,\ x \text{ d'ordre } n \text{ dans } k^*\}$$

**a)** (Question de cours) Montrer que $\mu_n(k)$ est un sous-groupe de $k^\times$ et que $|\mu_n(k)| \leqslant n$.

**b)** (Question de cours) Montrer que si $\mu_n^\circ(k) \neq \varnothing$ alors $|\mu_n(k)| = n$.

**c)** (Question de cours) Montrer que si $|\mu_n(k)| = n$ alors $\mu_n^\circ(k) \neq \varnothing$ et qu'alors $|\mu_n^\circ(k)| = \varphi(n)$.

**d)** Montrer que $|\mu_n(\mathbb{C})| = n$ pour tout $n \in \mathbb{N}^*$.

**e)** Soit $k$ un corps algébriquement clos de caractéristique $p$. Pour quelle valeurs de $n$ a-t-on $|\mu_n(k)| = n$ ?

**Définition :** Pour $n \in \mathbb{N}^*$, on note $\Phi_n = \prod_{x \in \mu_n^\circ(\mathbb{C})} (\mathrm{X} - x) \in \mathbb{C}[\mathrm{X}]$.

**f)** Calculer $\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5$ et $\Phi_6$.

**g)** Montrer que pour tout $n \in \mathbb{N}^*$, on a $\prod_{d|n} \Phi_d = \mathrm{X}^n - 1$.

**h)** En déduire que $\Phi_n \in \mathbb{Z}[\mathrm{X}]$.

**i)** Déterminer $\Phi_p$ lorsque $p$ est premier.

**j)** Montrer que $\Phi_p$ est irréductible (on pourra calculer $\Phi_p(\mathrm{X} + 1)$).

**Programme :** Dans la suite, on cherche à démontrer que $\Phi_n$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$. On note P le polynôme minimal de $\zeta := \exp(2i\pi/n)$ sur $\mathbb{Q}$.

**k)** Soit $\mathrm{U} \in \mathbb{Z}[\mathrm{X}]$ et $\mathrm{V}, \mathrm{W} \in \mathbb{Q}[\mathrm{X}]$ unitaires tels que $\mathrm{U} = \mathrm{VW}$. Montrer que $\mathrm{V}, \mathrm{W} \in \mathbb{Z}[\mathrm{X}]$.

**l)** Soit $\mathrm{U} \in \mathbb{F}_p[\mathrm{X}]$. Comparer $\mathrm{U}(\mathrm{X})^p$ et $\mathrm{U}(\mathrm{X}^p)$.

**m)** Montrer que $\mathrm{P} \mid \Phi_n$ dans $\mathbb{Q}[\mathrm{X}]$. On note $\mathrm{Q} \in \mathbb{Q}[\mathrm{X}]$ tel que $\Phi_n = \mathrm{PQ}$. Montrer que $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}]$.

**n)** Soit $p$ un nombre premier qui ne divise pas $n$. On suppose que pour toute racine $x$ de P dans $\mathbb{C}$, on a $x^p$ qui est racine de P dans $\mathbb{C}$. Montrer que $\mathrm{P} = \Phi_n$ et conclure.

On suppose à présent qu'il existe $x$ une racine de P dans $\mathbb{C}$ et $p$ un nombre premier qui ne divise par $n$ tel que $x^p$ ne soit pas racine de P.

**o)** Montrer que $x$ est racine que $\mathrm{Q}(\mathrm{X}^p)$. En déduire qu'il existe $\mathrm{R} \in \mathbb{Z}[\mathrm{X}]$ tel que $\mathrm{PR} = \mathrm{Q}(\mathrm{X}^p)$.

**p)** Montrer que dans $\mathbb{F}_p[\mathrm{X}]$, on obtient une relation de la forme $\mathrm{X}^n - 1 = \mathrm{Q}^{p+1}\mathrm{S}$.

**q)** En déduire une contradiction.