**Agrégation Externe**

**Éléments algébriques sur un corps**

[1]Ce problème est en relation avec les leçons d'oral suivante :
– 122 Anneaux principaux. Exemples et applications.
– 125 Extensions de corps. Exemples et applications.
– 141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

On pourra consulter les ouvrages suivants.
S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).
S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).
P. Samuel. *Théorie algébrique des nombres.* Hermann (1971).
A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).
P. Tauvel. *Mathématiques générales pour l'agrégation.* Masson (1993).

1. Le 05/10/2013

# 1 Énoncé

**Notations et définitions**

**Définition 1** *Une algèbre unitaire sur un corps commutatif* $\mathbb{K}$ *est un* $\mathbb{K}$*-espace vectoriel* $(A, +, \cdot)$ *muni d'une multiplication interne* $\times$ *telle que* $(A, +, \times)$ *soit un anneau unitaire et :*

$$\forall \lambda \in \mathbb{K},\ \forall (a, b) \in A^2,\ \lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b)$$

Une $\mathbb{K}$-algèbre $A$ est intègre si l'égalité $ab = 0$ dans $A$ équivaut à $a = 0$ ou $b = 0$.

Les algèbres considérées dans ce problème sont supposées unitaires. Si $A$ est une $\mathbb{K}$-algèbre, on note 1 l'unité pour la multiplication de $\mathbb{K}$ ou de $A$ et $\lambda a$, $ab$ pour $\lambda \cdot a$ et $a \times b$ respectivement.

On note $\mathbb{K}[X]$ l'algèbre des polynômes à coefficients dans un corps $\mathbb{K}$ et pour tout entier naturel $n$, $\mathbb{K}_n[X]$ est le sous-espace vectoriel de $\mathbb{K}[X]$ formé des polynômes de degré au plus égal à $n$.

Pour tout polynôme $P$ à coefficients dans un corps $\mathbb{K}$, on note :

$$(P) = \mathbb{K}[X] \cdot P$$

l'idéal principal de $\mathbb{K}[X]$ engendré par $P$.

Si $A$ est une algèbre sur un corps $\mathbb{K}$, pour tout élément $\alpha$ de $A$, $\mathbb{K}[\alpha]$ est l'image du morphisme d'algèbres :

$$\begin{array}{cccc} \varphi_\alpha : & \mathbb{K}[X] & \to & A \\ & P = \sum\limits_{k=0}^{n} a_k X^k & \mapsto & P(\alpha) = \sum\limits_{k=0}^{n} a_k \alpha^k \end{array}$$

avec la convention que $\alpha^0 = 1$ (c'est la sous-$\mathbb{K}$-algèbre de $A$ engendrée par $\alpha$).

**– I – Extensions de corps**

**Définition 2** *Si* $\mathbb{K}, \mathbb{L}$ *sont deux corps tels que* $\mathbb{K} \subset \mathbb{L}$, *on dit alors que* $\mathbb{L}$ *est une extension de* $\mathbb{K}$.

De manière plus générale, une extension d'un corps $\mathbb{K}$ est la donnée d'un couple $(\mathbb{L}, \varphi)$ où $\mathbb{L}$ est un corps et $\varphi$ est un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$ (un tel morphisme est toujours injectif puisqu'on impose $\varphi(1) = 1$, ce qui permet d'identifier $\mathbb{K}$ au sous-corps $\varphi(\mathbb{K})$ de $\mathbb{L}$).

Une telle extension $\mathbb{L}$ est une algèbre sur $\mathbb{K}$. Sa dimension est appelée degré de l'extension et est notée $[\mathbb{L} : \mathbb{K}]$.

Dans le cas où ce degré est fini, on dit que $\mathbb{L}$ est une extension finie de $\mathbb{K}$.

Le sous-corps premier d'un corps $\mathbb{K}$ est le sous-corps de $\mathbb{K}$ engendré par 1, c'est-à-dire l'intersection de tous les sous-corps de $\mathbb{K}$ (ou encore le plus petit sous-corps de $\mathbb{K}$).

Pour tout nombre premier $p \geq 2$, $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ désigne le corps commutatif des classes résiduelles modulo $p$.

1. Montrer qu'un corps $\mathbb{K}$ de caractéristique nulle (resp. de caractéristique $p$) est une extension de $\mathbb{Q}$ (resp. de $\mathbb{Z}_p$). Préciser, dans chaque cas, le sous-corps premier $\mathbb{K}_0$ de $\mathbb{K}$.
2. Soit $P$ un polynôme irréductible dans $\mathbb{K}[X]$. Montrer que $\mathbb{L} = \dfrac{\mathbb{K}[X]}{(P)}$ est une extension de $\mathbb{K}$ dans laquelle le polynôme $P$ a une racine $\alpha$ (corps de rupture de $P$ sur $\mathbb{K}$), puis que $\mathbb{L} = \mathbb{K}[\alpha]$. Quel est le degré $[\mathbb{L} : \mathbb{K}]$ de cette extension ?
   Que dire du corps de rupture de $P(X) = X^2 + bX + c$ irréductible dans $\mathbb{R}[X]$ ?
3. Montrer $[\mathbb{R} : \mathbb{Q}]$ est infini.

4. Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps. Montrer que :
$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] [\mathbb{L} : \mathbb{K}]$$
5. Soit $p \geq 2$ un nombre premier. Montrer que les polynômes $X^2 - p$ et $X^3 - p$ sont irréductibles dans $\mathbb{Q}[X]$. Peut-on avoir un morphisme de corps de $\dfrac{\mathbb{Q}[X]}{(X^2 - p)}$ dans $\dfrac{\mathbb{Q}[X]}{(X^3 - p)}$ ?
6. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ de degré $p \geq 2$ premier. Quels sont les corps $\mathbb{K}$ tels que $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$.
7. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $P$ un polynôme irréductible dans $\mathbb{K}[X]$ de degré $n \geq 1$. Montrer que si $m = [\mathbb{L} : \mathbb{K}]$ est premier avec $n$, alors $P$ est irréductible dans $\mathbb{L}[X]$.

## – II – Nombres algébriques

**Définition 3** *On dit qu'un élément $\alpha$ d'une algèbre $A$ sur un corps $\mathbb{K}$ est algébrique sur $\mathbb{K}$, s'il existe un polynôme non nul $P$ dans $\mathbb{K}[X]$ tel que $P(\alpha) = 0$.*

**Définition 4** *Un élément non algébrique d'une $\mathbb{K}$-algèbre $A$ est dit transcendant.*

1. Soient $A$ une $\mathbb{K}$-algèbre et $\alpha$ un élément de $A$ algébrique sur $\mathbb{K}$.
   (a) Montrer qu'il existe un unique polynôme unitaire $\pi_\alpha$ dans $\mathbb{K}[X]$ tel que :
   $$\{P \in \mathbb{K}[X] \mid P(\alpha) = 0\} = (\pi_a)$$
   On dit que $\pi_\alpha$ est le polynôme minimal de $\alpha$ sur $\mathbb{K}$ et le degré de ce polynôme est le degré de $\alpha$ sur $\mathbb{K}$.
   (b) Montrer que, si $A$ est intègre, alors le polynôme minimal de $\alpha$ est l'unique polynôme unitaire irréductible de $\mathbb{K}[X]$ qui annule $\alpha$.
   (c) Pour $A$ non intègre, le polynôme minimal est-il irréductible ?
   (d) Montrer que :
   $$\dim_{\mathbb{K}} \left( \frac{\mathbb{K}[X]}{(\pi_a)} \right) = \dim_{\mathbb{K}} (\mathbb{K}[\alpha]) = \deg(\pi_\alpha)$$
   (e) Montrer que, si $A$ est intègre, $\mathbb{K}[\alpha]$ est alors un corps.
   (f) Montrer que tout élément $\beta$ de $\mathbb{K}[\alpha]$ est algébrique sur $\mathbb{K}$. Comparer les degrés de $\beta$ et $\alpha$.
2. Soient $A$ une $\mathbb{K}$-algèbre intègre et $\alpha$ un élément de $A$. Montrer que les assertions suivantes sont équivalentes :
   (a) $\alpha$ est algébrique sur $\mathbb{K}$ ;
   (b) $\mathbb{K}[\alpha]$ est de dimension finie ;
   (c) $\mathbb{K}[\alpha]$ est un corps.
3. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Montrer que si $[\mathbb{L} : \mathbb{K}]$ est fini, alors tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.
4. Montrer que les réels $\alpha = \sqrt{\dfrac{1+\sqrt{5}}{2}}$, $\beta = \sqrt{2} + \sqrt{3}$, $\gamma = \sqrt{2} + \sqrt[3]{7}$ et $\delta = \sqrt[3]{2} + \sqrt[3]{4}$ sont algébriques sur $\mathbb{Q}$ et calculer les polynômes minimaux correspondants.
5. Montrer que l'ensemble des nombres réels algébriques sur $\mathbb{Q}$ est dénombrable et en déduire qu'il existe une infinité de nombres réels transcendants.

6.

   (a) Soit $\alpha$ un nombre réel algébrique sur $\mathbb{Q}$ de degré $d$. Montrer qu'il existe une constante $C_\alpha > 0$ telle que pour tout nombre rationnel $r = \dfrac{p}{q}$ distinct de $\alpha$, on ait $\left|\alpha - \dfrac{p}{q}\right| \geq \dfrac{C_\alpha}{q^d}$.

   (b) Soit $(a_n)_{n\geq 1}$ une suite d'entiers compris entre 0 et 9 telle que $a_n$ soit non nul à partir d'un certain rang. Montrer que le réel :

$$\xi = \sum_{n\geq 1} \frac{a_n}{10^{n!}}$$

   est transcendant.

7. Soit $\mathbb{L}$ une extension de degré 2 d'un corps $\mathbb{K}$ (une extension quadratique de $\mathbb{K}$). Montrer qu'il existe $\lambda \in \mathbb{L} \setminus \mathbb{K}$ tel que $\lambda^2 \in \mathbb{K}$ et $\mathbb{L} = \mathbb{K}[\lambda]$.

8. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $\mathbb{M}$ une extension du corps $\mathbb{L}$. Montrer que si $\alpha \in \mathbb{M}$ est algébrique sur $\mathbb{K}$, il est alors algébrique sur $\mathbb{L}$. Comparer les polynômes minimaux de $\alpha$ sur $\mathbb{K}$ et sur $\mathbb{L}$.

9. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Montrer que si $\alpha \in \mathbb{L} \setminus \{0\}$ est algébrique sur $\mathbb{K}$ alors $\dfrac{1}{\alpha}$ est aussi algébrique sur $\mathbb{K}$.

10. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Montrer que l'ensemble $\mathbb{A}$ des éléments de $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.

11. Soit $p$ un nombre premier.

   (a) Soit $\xi$ une racine $p$-ème de l'unité distincte de 1. Montrer que $\xi$ est algébrique sur $\mathbb{Q}$ et déterminer son polynôme minimal.

   (b) Soit $\xi$ une racine primitive $p^2$-ème de l'unité. Montrer que $\xi$ est algébrique sur $\mathbb{Q}$ et déterminer son polynôme minimal.

12. On admettra que pour tout entier $n \geq 2$ le polynôme cyclotomique :

$$\Phi_n(X) = \prod_{\substack{1\leq k\leq n-1 \\ k\wedge n=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

   est irréductible dans $\mathbb{Q}[X]$. On rappelle que ce polynôme est de degré $\varphi(n)$ où $\varphi$ est la fonction indicatrice d'Euler.

   Montrer que pour tout entier naturel non nul $n$, le réel $\alpha = \cos\left(\dfrac{2\pi}{n}\right)$ est algébrique sur $\mathbb{Q}$ et préciser son degré.

13.

   (a) Montrer que si $\mathbb{L}$ une extension finie d'un corps $\mathbb{K}$ alors tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et il existe des éléments $\alpha_1, \cdots, \alpha_p$ dans $\mathbb{L}$ algébriques sur $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_p]$.

   (b) Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$, $p$ un entier naturel non nul et $\alpha_1, \cdots, \alpha_p$ des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$. Montrer que $\mathbb{K}[\alpha_1, \ldots, \alpha_p]$ est une extension finie de $\mathbb{K}$ avec $\dim_{\mathbb{K}}(\mathbb{K}[\alpha_1, \ldots, \alpha_p]) \leq \prod_{k=1}^{p} \deg(\alpha_k)$.

14.

   (a) Montrer que si $n \in \mathbb{N} \setminus \{0, 1\}$ est sans facteur carré (i.e. $n = \prod_{k=1}^{r} p_k$ où les $p_k$ sont premiers deux à deux distincts), alors le réel $\sqrt{n}$ est algébrique sur $\mathbb{Q}$ de degré 2.

(b) Soit $p_1, \cdots, p_n$ des entiers sans facteur carré dans $\mathbb{N} \setminus \{0,1\}$ deux à deux premiers entre eux. Calculer le degré sur $\mathbb{Q}$ de $\mathbb{Q}\left[\sqrt{p_1}, \cdots, \sqrt{p_n}\right]$ en donnant une base de ce $\mathbb{Q}$-espace vectoriel.

(c) Montrer que la famille de réels $\mathcal{L} = \{\sqrt{m} \in \mathbb{N} \setminus \{0,1\} \mid m \text{ est sans facteur carré}\}$ est libre sur $\mathbb{Q}$.