Feuille d'exercices n° 5

Extensions de corps

Exercice 1.

1) Prouver qu'il existe un corps à 4 éléments, unique à isomorphisme près.

2) Existe-t-il un corps à 6 éléments ?

Exercice 2.

1) Soit p un nombre premier et soit $n \geqslant 2$. Décrire $\mathbb{Q}[\sqrt[n]{p}]$ comme quotient de $\mathbb{Q}[X]$ et montrer que l'extension $\mathbb{Q}[\sqrt[n]{p}]/\mathbb{Q}$ est de degré n.

2) On pose $S = \{2^{1/n}; n \in \mathbb{N}^*\}$. Montrer que l'extension $\mathbb{Q}(S)/\mathbb{Q}$ est algébrique. Est-elle finie ?

Exercice 3. Montrer que l'ensemble des nombres réels algébriques est dénombrable. En déduire que les nombres transcendants forment une partie non dénombrable de $\mathbb{R}$.

Exercice 4. On appelle nombre de Liouville un réel x tel que pour tout entier $n > 0$ il existe un rationnel $p_n/q_n \in \mathbb{Q}$, où $p_n, q_n \in \mathbb{Z}$ et $q_n > 1$, vérifiant

$$0 < |x - p_n/q_n| < 1/q_n^n.$$

On se propose de démontrer qu'un nombre de Liouville est transcendant.

1) Soit $\alpha \in \mathbb{R}$ un nombre algébrique.

(a) Montrer qu'il existe un polynôme $P(X) \in \mathbb{Z}[X]$ de degré $d \geqslant 1$ tel que $P(\alpha) = 0$.

(b) Établir que quels que soient $a, b \in \mathbb{Z}$ vérifiant $b > 0$ et $P(a/b) \neq 0$, on a $|P(a/b)| \geqslant 1/b^d$.

(c) Soit $\varepsilon > 0$ tel que α soit la seule racine de $P(X)$ dans $[\alpha - \varepsilon, \alpha + \varepsilon]$. Prouver qu'il existe $K > 0$ tel que $|P(x)| \leqslant K|x - \alpha|$ pour tout $x \in [\alpha - \varepsilon, \alpha + \varepsilon]$.

(d) En déduire qu'il existe $C > 0$ tel que $|\alpha - a/b| \geqslant C/b^d$ pour tout $a, b \in \mathbb{Z}$ vérifiant $b > 0$ et $a/b \neq \alpha$.

2) Montrer qu'un nombre de Liouville est transcendant.

3) Soient $b \in \mathbb{N}$, $b \geqslant 2$, et une suite $(a_n)_{n \geqslant 1}$ d'entiers vérifiant $1 \leqslant a_n \leqslant b - 1$. Montrer que

$$x = \sum_{k=1}^{\infty} a_k/b^{k!}$$

est transcendant. Exemple (premier transcendant connu) :

$$\sum_{k=1}^{\infty} 1/10^{k!} = 0.110001000000000000000001000000\dots$$

Exercice 5. Soient L/K une extension et $x \in L$.

1) Montrer que x est algébrique sur K si et seulement si x^2 est algébrique sur K.

2) Montrer que si x est algébrique sur K et si $[K(x) : K]$ est impair, alors $K(x^2) = K(x)$.

3) Est-ce encore vrai si $[K(x) : K]$ est pair ?

4) Montrer que si x est transcendant sur K, alors $K(x^2) \subsetneq K(x)$.

Exercice 6.

1) Que vaut $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$? Donner une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ vu comme $\mathbb{Q}$-espace vectoriel.

2) Quel est le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$?

3) En déduire que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Exercice 7. Soient K un corps de caractéristique différente de 2 et $P(X) \in K[X]$ unitaire de degré 2. Soit L/K une extension de degré 2.

1) Montrer qu'il existe $a, b \in K$ tels que $P(X) = (X - a)^2 - b$.

2) Montrer qu'il existe $x \in L \setminus \{0\}$ tel que $x^2 \in K$ et $L = K(x)$.

3) Soit $y \in L$ tel que $y^2 \in K$ et $L = K(y)$. Montrer que $y/x \in K$.

4) Soient p et q deux nombres premiers distincts. Que vaut $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}]$?

5) Soit $z \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ tel que $z^2 \in \mathbb{Q}$. Montrer que l'un des quatre éléments suivants appartient à $\mathbb{Q}$: z, $z/\sqrt{p}$, $z/\sqrt{q}$, $z/\sqrt{pq}$.

6) En déduire la liste des extensions de $\mathbb{Q}$ incluses dans $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

7) Quelles sont les extensions de $\mathbb{Q}$ incluses dans $\mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Exercice 8. Soit a une racine de $X^3 + X + 1$ dans $\mathbb{C}$. Quel est le degré d de l'extension $\mathbb{Q}(a)/\mathbb{Q}$? Soit $b = a^5 + a^2 + 1$. Montrer que b est non nul et exprimer son inverse sous la forme $b^{-1} = P(a)$, où $P(X) \in \mathbb{Q}[X]$ est de degré au plus $d - 1$.

Exercice 9. Soit $\alpha \in \mathbb{C}$ une racine du polynôme $X^3 + 2X - 1$.

1) Montrer que $L = \mathbb{Q}[\alpha]$ est une extension de degré 3 de $\mathbb{Q}$.

2) Exprimer les inverses de α, $1 + \alpha$ et $\alpha + \alpha^2$ dans la base $(1, \alpha, \alpha^2)$ de L sur $\mathbb{Q}$.

3) Prouver que pour tout $\beta \in L \setminus \mathbb{Q}$ on a $\mathbb{Q}(\beta) = L$.

4) Donner une condition nécessaire et suffisante pour que le polynôme minimal de $x = a + b\alpha + c\alpha^2$ $(a, b, c \in \mathbb{Q})$ soit de degré 3. Déterminer ce polynôme pour $x = 1 - \alpha^2$.