TD4 : Extensions séparables et Corps finis

16/10/2023

Exercice 1 : Extensions finie non normale ni séparable

Montrer que l'extension $\mathbb{F}_2(t^{1/6})/\mathbb{F}_2(t)$ n'est ni séparable ni normale.

Exercice 2 :

Soit $K = \mathbb{Q}(\sqrt{5})$ et $L = \mathbb{Q}(\sqrt{1+\sqrt{5}})$. Montrer que les extensions $\mathbb{Q} \subset K$ et $K \subset L$ sont normales, mais que $\mathbb{Q} \subset L$ ne l'est pas. Quelle est sa clôture normale dans $\bar{\mathbb{Q}}$?

Exercice 3 : Polynômes purement inséparables

Soit K un corps de caractéristique $p > 0$, $f \in K[X]$ est dit purement inséparable si il a exactement une seule racine dans la clôture algébrique $\overline{K}$.

1. Soit $h \in K[X]$ un polynôme unitaire irréductibe purement inséparable. Montrer qu'il existe $n \in \mathbb{N}, c \in K$ tel que $h(X) = X^{p^n} - c$.

2. Soit $f \in K[X]$ un polynôme purement inséparable unitaire. Montrer que $f(X) = (X^{p^n} - c)^m$ pour certains $n, m \in \mathbb{N}$, $c \in K$.

Soit L/K une extension. On dit que $\alpha \in L$ est purement inséparable si son polynôme minimal est purement inséparable, et que l'extension l'est si cette propriété est vraie pour tous les $\alpha \in L$.

3. Montrer que L/K est purement inséparable ssi pour tout $x \in L$, il existe $n \in \mathbb{N}$ tel que $x^{p^n} \in K$.

4. Montrer que l'extension $\mathbb{F}(t)/\mathbb{F}(t^p)$ est purement inséparable.

Exercice 4 : Extensions purement inséparables

Soit K un corps de caractéristique $p > 0$, et $\overline{K}$ une clôture algébrique de K. On note $K^s = \{x \in \overline{K}, x \text{ est séparable sur } K\}$.

1. Rappeler pourquoi K^s est bien un corps.

2. Soit L/K une extension algébrique. On note $L_s = K^s \cap L$.

a. Montrer que si $\beta \in L$ est séparable sur L_s, alors $\beta \in L_s$.

b. Montrer que L/L_s est purement inséparable.

c. Montrer le fait général : une extension algébrique L'/K est purement inséparable si et seulement si il n'existe qu'un seul K-morphisme de $L' \to \overline{K}$.

d. Montrer que $[L : L_s]_s = 1$ et que $[L_s : K] = [L : K]_s$. En particulier, en déduire que le degré séparable divise le degré.

e. On note alors $[L : K]_i := [L : L_s]$ le degré d'inséparabilité. Montrer que ce degré est multiplicatif et que c'est une puissance de p. On note L^{rad} le sous-corps de L constitué de tous les éléments $x \in L$ tels qu'il existe $r \in \mathbb{N}$ avec $x^{p^r} \in K$.

3. Montrer que $\overline{K}$ est une extension séparable de $\overline{K}^{\text{rad}}$.

Exercice 5 :

Soit K un corps de caractéristique p, et soit $a \in K$. On pose $P(X) = X^p - X - a$ et on note L un corps de décomposition de P sur K.

1. Si x est une racine de P dans L, montrer que les racines de P sont $x, x+1, \ldots, x+p-1$.

2. Montrer que P est soit scindé soit irréductible sur $K[X]$.

3. Dans le cas où P n'a pas de racine dans K, montrer que $[L : K] = p$ et que $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$.

Exercice 6 :

Soient K et K' des sous-corps d'un corps L, tels que les extensions L/K et L/K' soient normales. Montrer que $L/(K \cap K')$ est normale.

Exercice 7 : Corps finis

Soit p un nombre premier.
1. Rappeler pourquoi deux corps finis de même cardinal sont isomorphes.
2. Soient $n, n' \in \mathbb{N}$ tels que n' soit un multiple de n. Justifier l'écriture $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$.
3. Réciproquement, montrer que si $\mathbb{F}_{p^n}$ s'identifie à un sous-corps de $\mathbb{F}_{p^{n'}}$ alors n divise n'.
4. Montrer qu'un corps fini n'est jamais algébriquement clos.
5. Déterminer les corps de cardinal $4, 8, 16$ et 9.

Exercice 8 : Un isomorphisme

Montrer que les anneaux $\mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont isomorphes et exhiber un isomorphisme explicite.

Exercice 9 : Clôture algébrique de $\mathbb{F}_p$

Soit p un nombre premier et $q := p^n, n \geqslant 1$.
1. Soit $\bar{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Montrer que si $x \in \bar{\mathbb{F}_p}$, $x \neq 0$, alors x est une racine de l'unité.
2. Montrer que $\mathbb{F}_q \subset \mathbb{F}_{p^{n!}}$.
3. Montrer que $K := \bigcup_{n \geqslant 1} \mathbb{F}_{p^{n!}}$ est naturellement muni d'une structure de corps. Conclure que K est une clôture algébrique de $\mathbb{F}_p$ et même de tout corps fini de caractéristique p.

Exercice 10 : Polynômes irréductibles sur $\mathbb{F}_q$

Pour $n \in \mathbb{N}^*$, on note $A(n, q)$ l'ensemble des polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$ et $I(n, q) = \sharp A(n, q)$. On note μ la fonction de Möbius. Soit $n \geqslant 1$.
1. Soit d un diviseur de n et $P \in A(d, q)$. Montrer que P divise $X^{q^n} - X$.
2. Soit P un facteur irréductible (unitaire) de $X^{q^n} - X$. Montrer que $\deg P$ divise n.
3. Déduire des questions précédentes que $\sum_{d|n} dI(d, q) = q^n$. Montrer qu'on a

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d. \tag{1}$$

Exercice 11 : Irréductibilité des polynômes cyclotomiques sur les corps finis

Soit p un nombre premier, $n \in \mathbb{N}^*$, et $q := p^n$. On considère une extension finie $\mathbb{F}_p \subset K$. Soit $\alpha \in K$. On note π_α le polynôme minimal de α sur $\mathbb{F}_p$ et $d = deg(\pi_\alpha)$.
1. Montrer que $\{r \in \mathbb{Z}, \alpha^{p^r} = \alpha\} = d\mathbb{Z}$. En déduire que le degré du polynôme minimal de α sur $\mathbb{F}_p$ est égal à l'ordre de p dans $(\mathbb{Z}/od(\alpha)\mathbb{Z})^*$, où $od(\alpha)$ désigne l'ordre de α dans le groupe multiplicatif K^*.
2. Montrer que $\pi_\alpha = (X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{d-1}})$.
3. Montrer que

$$p^n = \sum_{d|n} dI(d, p) \tag{2}$$

(avec les notations de l'exercice précédent). En déduire que pour tout $n \geqslant 1$ il existe un polynôme de degré n irréductible sur $\mathbb{F}_p$ et donc l'existence d'un corps fini cardinal p^n pour tout $n \geqslant 1$.