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.

Correction :

L'élément $\sqrt{t}$ a pour polynôme minimal $X^2 - t$ sur $\mathbb{F}_2(t)$, donc non séparable.

De plus l'extension n'est pas normale, car par exemple $t^{1/3}$ est racine de $X^3 - t$, et les autres racines dans une cloture algébrique sont les $\zeta t^{1/3}$ et $\zeta^2 t^{1/3}$ où ζ racine primitive de $X^3 - 1$. Si par l'absurde $\zeta t^{1/3} \in L$, alors $\zeta \in L$. Mais ζ serait alors forcément dans F_2, absurde

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 $\bar{\mathbb{Q}}$?

Correction :

Les extensions $K/\mathbb{Q}$ et L/K sont de degré 2 et donc normales. Le polynôme minimal de $\sqrt{1+\sqrt{5}}$ sur $\mathbb{Q}$ est $X^4 - 2X^2 - 4$. On vérifie facilement que les racines de ce polynôme (dans $\mathbb{C}$) sont $\pm\sqrt{1+\sqrt{5}}$ et $\pm i\sqrt{-1+\sqrt{5}}$. Et comme $L \subset \mathbb{R}$, L ne contient pas ces deux dernière racines et donc n'est pas une extension normale de $\mathbb{Q}$. La clôture normale de L est alors $L(i\sqrt{-1+\sqrt{5}})$.

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 $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ est purement inséparable.

Correction :

1. Soit r maximal tel que $h(X) = g(X^{p^r})$. Alors g est irréductible car h l'est, et g est séparable par maximalité de r. g s'écrit alors $\prod_{i=1}^{n}(X - a_i)$ avec les a_i deux à deux distincts dans une clôture algébrique. Alors $h(X) = \prod_{i=1}^{n}\left(X^{p^r} - a_i\right)$, mais comme il est purement inséparable, cela implique $n = 1$ et on obtient la forme demandée de h.

2. On écrit $f(X) = f_1(X)\dots f_m(X)$ sa décomposition en polynômes irréductibles sur K. Si on appelle x son unique racine dans $\overline{K}$, alors pour tout i, $f_i = \pi_x$ le polynôme minimal de x sur K. Par question précédente, $\pi_x(X) = X^{p^n} - c$, et donc $f(X) = (X^{p^n} - c)^m$.

3. Supposons que l'extension soit purement inséparable. Soit $x \in L$, alors son polynôme minimal est de la forme $X^{p^n} - c \in K[X]$ et donc $x^{p^n} = c \in K$. Réciproquement, si $\forall x \in K, \exists n \in \mathbb{N}^*, x^{p^n} \in K$, alors x est racine du polynôme purement inséparable $X^{p^n} - c$, donc son polynôme minimal est aussi pureent inséparable. D'où l'extension l'est aussi.

✉clement.chivet@ens.fr

4. Pour tout élément $\frac{f(t)}{g(t)} \in \mathbb{F}_p(t)$ on a

$$\left(\frac{f(t)}{g(t)}\right)^p = \left(\frac{\sum_i a_i t^i}{\sum_j b_j t^j}\right)^p = \frac{\sum_i a_i^p (t^p)^i}{\sum_j b_j^p (t^p)^j} \in \mathbb{F}_p(t^p)$$

par proposé de morhpisme du Frobenius.

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 $[L_s : K] = [L : K]_s$ dans le cas où l'extension L/K est finie. 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 $\overline{K}^{\text{rad}}$.

Correction :

1. Si x, y sont séparables, $K(x, y)$ est une extension séparable et donc $xy, x - y$ sont séparables et donc dans K^s.

2.

a. Soit $\beta \in L$ séparable sur L_s, alors $L(\beta)/L_s$ est séparable, mais comme L_s/K est séparable, $L(\beta)/K$ est séparable et β est dans K^s. Finalement $\beta \in L_s = L \cap K^s$.

b. Soit $x \in L$. Soit f le polynôme minimal de x sur L_s. Soit r maximal tel que $f(X) = g(X^{p^r})$. Alors g est irréductible séparable, donc x^{p^r} est séparable sur L_s, donc appartient à L_s. On a donc montré que $\forall x \in L, \exists n > 0, x^{p^n} \in L_s$, d'où l'extension est purement inséparable par question 3 de l'exercice précédent.

c. Si l'extension L'/K est purement inséparable, un morphisme $L' \to \overline{K}$ envoie tout élément $x \in L'$ sur l'unique racine de $\pi_x \in K[X]$ dans $\overline{K}$. D'où l'unicité d'un tel morphisme.

Réciproquement, on sait que l'on pour tout $x \in L'$ a une surjection $\text{Hom}_K(L', \overline{K}) \to \text{Hom}_K(K(x), \overline{K})$ via l'application de restriction (par propriété d'extension des morhpsimes à valeurs dans un corps algébriquement clos). Alors $|\text{Hom}_K(K(x), \overline{K})| = 1$, mais ce cardinal est aussi le nombre de racines distinctes de π_x le polynôme minimal de x sur K : d'où π_x est purement inséparable et L'/K aussi.

d. Comme L/L_s est purement inséparable, $[L : L_s]_s = |\text{Hom}_{L_s}(L, \overline{L_s})| = 1$ par question précédente. De plus par multiplicité du degré séparable, $[L : K]_s = [L : L_s]_s[L_s : K]_s = [L_s : K]_s$. Comme l'extension L_s/K est séparable, on a $[L_s : K]_s = [L_s : K]$ ce qui conclut.

e. Il est multiplcatif car $[L : K]_i = \frac{[L:K]}{[L:K]_s}$ et ces deux degrés le sont, de plus on montre par récurrence que le degré d'une extension finie purement inséparable est une puissance de p : si L/K est de degré $\leqslant n$, on se donne $x \in L \backslash K$, alors le polynôme minimal de x est de la forme $X^{p^r} - c$, donc $[K(x) : K] = p^r$, et l'extension $L/K(x)$ reste purement inséparable (car tout y est dans K quand on le met a la puissance p^k assez grand donc à fortiori dans $K(x)$) et on conclut par hypothèse de récurrence.

3. le point clé est que Fr est surjectif de $\overline{K}^{\mathrm{rad}} \to \overline{K}^{\mathrm{rad}}$. Supposons par l'absurde qu'il existe P un polynôme irréductible non-séparable sur $\overline{K}^{\mathrm{rad}}$. Alors $P(X) = \sum_i a_i X^{ip}$, mais alors en prenant b_i tel que $b_i^p = a_i$, $P(X) = \left(\sum_i b_i X^i\right)^p$ n'est donc pas irréductible, absurde. Comme $\overline{K}/\overline{K}^{\mathrm{rad}}$ est algébrique, cela suffit pour conclure.

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 $x, x+1, \dots, x+p-1$.

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 $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$.

Correction :

1. $P(x+1) = x^p + 1^p - x - 1 - a = 0 + 1^p - 1 = 0$, puis par récurrence car $x+1$ est une racine donc on peut appliquer le même résultat. On obtient alors p racines distinctes car $\mathrm{car}(K) = p$ pour le polynôme P de degré p, on les a bien toutes.

2. Si P a une racine dans K, P est scindé sur K par question 1. Supposons alors que P n'a pas de racine sur K. Supposons par l'asurde que $P = RQ$ sur $K[X]$ avec R unitaire irréductible. Si x est une racine de R dans L, alors $R(X) = X^{\deg R} - \left((\deg R)x + \underbrace{\sum_{i=1}^{\deg R} k_i}_{k_i \in \{0,\dots,p-1\}} \right) + \dots$.

Alors $(\deg R)x \in K$ et $\deg R = p = \deg P$ sinon $x \in K$ absurde. D'où P irréductible.

3. Si P n'a pas de racine dans K, il est irréductible par question précédente, séparable car $P'(X) = -1 \neq 0$, donc L est une extension galoisienne de degré p, et le morphisme induit par $x \to x+1$ où x est une racine de P est d'ordre p d'où $\mathrm{Gal}(L/K) = \mathbb{Z}/p\mathbb{Z}$ ·

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.

Correction :

Soit $P \in (K \cap K')[X]$ un polynôme unitaire irréductible qui a une racine a_1 dans L. On écrit $P(X) = Q(X) \prod_{i=1}^n (X - a_i)$ avec $a_i \in L$ et $Q(X) \in L[X]$ qui n'a pas de racine dans L. Cette décomposition est unique. Soit $P = P_1 \dots P_k$ la factorisation irréductible (unitaire) de P dans $K[X]$. Alors pour tout i, par normalité, soit P_i a toutes ses racines dans L, soit il n'en a aucune. On a donc un sous ensemble $I \subset \{1, \dots, k\}$ tel que $i \in I \iff P_i$ est scindé sur L. Alors $P(X) = \prod_{i \in I} P_i \times \prod_{i \notin I} P_i$. Mais alors par unicité de la décomposition de P en un poylnôme scindé et un polynôme sans racines, on en déduit

$$\begin{cases} Q(X) = \prod_{i \notin I} P_i \\ \prod_{i=1}^n (X - a_i) = \prod_{i \in I} P_i \end{cases}$$

Finalement, $Q \in K[X]$. De manière symétrique, $Q \in K'[X]$, donc $Q \in (K \cap K')[X]$, or P est irréductible sur $(K \cap K')[X]$ et $\deg Q < \deg P$, donc Q est constant, et tous les conjugués de a_i sont bien dans L ce qui conclut.

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.

Correction :

1. Tout corps fini de cardinal $q = p^r$ s'identifie au corps de décomposition (sur $\mathbb{F}_p$) de $X^q - X$ qui est par conséquent unique à isomorphisme près.
2. Le corps fini $\mathbb{F}_{p^n}$ est isomorphe au corps $\mathbb{F}_p[\zeta]$ où ζ est une racine $p^n - 1$ de l'unité. De même $\mathbb{F}_{p^{n'}}$ est engendré par une racine $p^{n'} - 1$ième ζ' de l'unité. On vérifie sans peine que $p^n - 1 | p^{n'} - 1$ et donc que ζ est une puissance de ζ' ce qui justifie l'inclusion.
3. On va dans l'autre sens si $p^n - 1 | p^{n'} - 1$, on écrit $n' = an + b$ la DE de n' par n, alors mod $p^n - 1$ on a $p^b = 1$ et comme $b < n$ on a $b = 0$ ie $n | n'$.
4. Un corps fini ne peut contenir qu'un nombre fini de racines de l'unité. Mais dans une clôture algébrique, il y en a un nombre infini.

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.

Correction :

Comme les polynômes $X^2 + X + 2$ et $X^2 + 2X + 2$ sont irréductibles sur $\mathbb{F}_3$ (car n'ont pas de racine), les deux anneaux proposés sont des extensions de corps de degré 2 sur $\mathbb{F}_3$: ils sont donc isomorphes à $\mathbb{F}_9$. On définit un isomorphisme par :

$$\begin{aligned} \mathbb{F}_3[X]/\left(X^2 + X + 2\right) &\to \mathbb{F}_3[X]/\left(X^2 + 2X + 2\right) \\ X &\mapsto -X \end{aligned}$$

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.

Correction :

1. Soit $x \in \bar{\mathbb{F}}_q$ alors $\mathbb{F}_q[x]$ est un corps fini et donc x est dans le groupe cyclique $\mathbb{F}_{q^n}^\times$ et ne particulier c'est une racine de l'unité.
2. Par la question 2. de l'exercice 7, comme $n | n!$ on a $\mathbb{F}_q \subset \mathbb{F}_{p^{n!}}$.
3. La tour d'extensions $\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \dots$ est d'union K. L'ensemble K est trivialement munit d'une structure de corps qui en fait une extension de tous les $\mathbb{F}_q$ simultanément. Par construction le corps K est certainement algébrique sur $\mathbb{F}_p$ et par la question il contient tout corps fini de caractéristique p. Par la question 1 il contient $\bar{\mathbb{F}}_p$ et comme K est algébrique sur $\mathbb{F}_p$ il en est une clôture algébrique.

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

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

Correction :

1. On a $X^{q^n} - X = \prod_{x \in \mathbb{F}_{q^n}} (X - x)$, remarquons que $\mathbb{F}_{q^n}$ est une extension normale de $\mathbb{F}_q$ et un corps de décomposition de $X^{q^n} - X$. Si $P \in A(d,q)$ alors $\mathbb{F}_{q^d}$ est un corps de rupture de P ce dernier est contenu dans $\mathbb{F}_{q^n}$ car $d|n$ qui est une extension normale de $\mathbb{F}_q$ et donc $P = \prod_i (X - x_i) | X^{q^n} - X$.

2. Si P est un facteur irréductible de $X^{q^n} - X$, alors $\mathbb{F}_{q^{deg P}}$ est un corps de rupture de P, il est contenu dans $\mathbb{F}_{q^n}$ et par l'exercice 1 question 2. on a $deg(P)|n$.

3. Par les questions précédentes, on a

$$X^{q^n} - X = \prod_d \prod_{P \in A(d,q)} P \tag{2}$$

en comparant les degrés on obtient la formule, la formule $I(n,q)$ est donnée par la formule d'inversion de Möbius.

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

$$p^n = \sum_{d|n} dI(d,p) \tag{3}$$

(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 $n \geqslant 1$.

Correction :

1. On sait que α est une racine primitive $p^d - 1$ de l'unité, cela implique immédiatement que $\{r, \alpha^{p^r}\} = d\mathbb{Z}$. On sait que $od(\alpha) = p^d - 1$ et donc l'ordre de p dans $\mathbb{Z}/od(\alpha)$ est d.

2. Le Frobenius $x \mapsto x^p$ est un morphisme de corps, ainsi tous les α^{p^r} sont conjugués. Comme l'ordre de p dans $\mathbb{Z}/od(\alpha)$ est d, on en déduit que $(X - \alpha)(X - \alpha^p) \dots (X - \alpha^{p^{d-1}}) | \pi_\alpha$ et ils sont égaux par égalité des degrés.

3. Voir exercice 3. pour l'équation (2). Pour l'existence des corps finis de cardinal fixé, il suffit d'extraire des racines de l'unité d'ordre $p^n - 1$.

4. Si $(\mathbb{Z}/n)^\times$ est cyclique et p en est un générateur, alors si ζ est une racine $p^n - 1$ de l'unité, son polynôme minimal est par 2. de la forme $(X - \zeta) \dots (X - \zeta^{p^{n-1}}) = \phi_n$. Réciproquement si ϕ est irréductible alors il est de cette forme et cela implique le résultat.