Extensions séparables, extensions normales (TD6)

FIMFA Algèbre 2 (Tony Ly), Mars 2014

Exercice 1
Trouver une infinité d'extensions intermédiaires entre $\mathbb{F}_p(X^p, Y^p)$ et $\mathbb{F}_p(X, Y)$.

Exercice 2
Soit $F \subseteq E$ une extension finie de corps de caractéristique $p > 0$.
a) Montrer qu'un élément $x \in E$ est séparable si et seulement si on a $F(x) = F(x^p)$.
b) Montrer l'équivalence des assertions suivantes :
(i) il existe une base $(x_1, \ldots, x_n)$ de E sur F telle que $(x_1^p, \ldots, x_n^p)$ est aussi une F-base de E ;
(ii) pour toute base $(y_1, \ldots, y_n)$ de E sur F, $(y_1^p, \ldots, y_n^p)$ est aussi une F-base de E.
c) Montrer que (i) est vraie si et seulement si l'extension $F \subseteq E$ est séparable.

Exercice 3
Soient K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et K^s la clôture séparable de K dans $\overline{K}$.
a) Rappeler pourquoi K^s est bien définie.
Soit $P \in K[X]$ un polynôme unitaire irréductible.
b) Montrer que P a une unique racine dans $\overline{K}$ si et seulement si il existe $r \in \mathbb{N}$ et $a \in K$ tels que $P = X^{p^r} - a$.
Soit $K \subseteq L$ une extension algébrique. L'extension $K \subseteq L$ est dite *purement inséparable* si pour tout $x \in L$, il existe $r \in \mathbb{N}$ tel que $x^{p^r} \in K$.
c) Montrer que $K \subseteq L$ est purement inséparable si et seulement si il n'existe qu'un homomorphisme de K-algèbres de L dans $\overline{K}$.
d) Montrer que L est une extension purement inséparable de $K^s \cap L$.
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 $x^{p^r} \in K$.
e) Montrer que $\overline{K}$ est une extension séparable de $\overline{K}^{\text{rad}}$.
f) Est-ce vrai pour $L \subsetneq \overline{K}$ et L^{rad} ?

Exercice 4
Soit $F \subseteq E$ une extension finie de corps de caractéristique $p > 0$. On suppose l'inclusion $E^{\times p} \subseteq F^{\times}$, de sorte que $F \subseteq E$ est purement inséparable.
On dit qu'une famille $(x_1, \ldots, x_n)$ de E est une *p-base* de E/F si elle engendre la tour d'extensions

$$F \subsetneq F(x_1) \subsetneq F(x_1, x_2) \subsetneq \cdots \subsetneq F(x_1, \ldots, x_n) = E.$$

a) Montrer que si E/F possède une p-base $(x_1, \ldots, x_n)$, alors on a la relation $[E : F] = p^n$.
Cela permet en particulier de parler de *p-dimension* de E/F, qui est toujours définie en vertu du point suivant.
b) Montrer que E/F possède une p-base.

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

Exercice 6
Déterminer les groupes d'automorphismes suivants :

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}), \quad \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})), \quad \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3})), \quad \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}).$$

Exercice 7
Soient $n \geq 1$ un entier et $p \geq 2$ un nombre premier.

a) Montrer que n divise l'ordre de tout sous-groupe transitif de $\mathfrak{S}_n$.

b) Montrer qu'un p-cycle et une transposition engendrent toujours $\mathfrak{S}_p$.

c) En déduire le groupe de Galois du polynôme $X^5 - 4X + 2 \in \mathbb{Q}[X]$.

Exercice 8
Soit $n \geq 1$ un entier. Soient $F \subseteq E$ une extension galoisienne (ie. normale et séparable) finie, de base $\{1, x_1, \ldots, x_{n-1}\}$. En particulier le groupe $G = \mathrm{Gal}(E/F)$ est d'ordre n et le corps fixe $E^G = \{e \in E \mid \forall g \in G,\, ge = e\}$ est exactement F.

a) Montrer que les éléments de G sont linéairement indépendants.

Soit V un espace vectoriel sur E, muni d'une action semi-linéaire de G. On définit son sous-F-espace vectoriel des G-invariants $V^G = \{v \in V \mid \forall g \in G,\, gv = v\}$.

b) Vérifier que l'application E-linéaire $V^G \otimes_F E \xrightarrow{\eta} V$ canonique est compatible à l'action de G.

c) Montrer que η est un isomorphisme.

Exercice 9 (Cyclotomie sur $\mathbb{Q}$)
Soient $n \geq 1$ un entier et μ_n l'ensemble des racines primitives n-èmes de l'unité dans $\mathbb{C}$. On note Φ_n le n-ème polynôme cyclotomique, c'est-à-dire le polynôme unitaire de $\mathbb{C}[X]$ dont les racines sont les éléments de μ_n.

a) Calculer le degré de Φ_n.

b) Montrer l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$ et en déduire que Φ_n est à coefficients entiers.

c) Montrer que le corps de rupture de Φ_n est égal à son corps de décomposition.

Soient $\xi \in \mu_n$ et f son polynôme minimal sur $\mathbb{Q}$. Soit $h \in \mathbb{Z}[X]$ vérifiant $X^n - 1 = fh$. Soient p un nombre premier ne divisant pas n et g le polynôme minimal de ξ^p.
On suppose $f \neq g$.

d) Montrer les divisibilités $g \mid h$ et $f(X) \mid g(X^p)$.

e) Etablir une contradiction, et en déduire l'irréductibilité de Φ_n.

f) Déterminer le groupe de Galois de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$.

Exercice 10
On se propose d'établir deux résultats qui utilisent les polynômes cyclotomiques sur $\mathbb{Q}$.

a) Montrer que tout sous-groupe G de $\mathrm{GL}_n(\mathbb{Q})$ dont tous les éléments sont d'ordre fini est d'exposant fini.

Le second résultat est ce qui est appelé le théorème de Dirichlet faible. Soient $P \in \mathbb{Z}[X] \smallsetminus \mathbb{Z}$ et $n \geq 1$ un entier.

b) Montrer que l'ensemble $\{d \in \mathbb{N} \mid \exists n \in \mathbb{N},\ d \mid P(n)\}$ est infini.

c) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

Exercice 11
Soit p un nombre premier impair. Pour $n \geq 1$ un entier, on note ξ_n une racine primitive n-ème de l'unité dans $\mathbb{C}$.

a) En calculant le discriminant de Φ_p, montrer que $\sqrt{(-1)^{\frac{p-1}{2}} p}$ appartient à $\mathbb{Q}[\xi_p]$.

b) Montrer que $\sqrt{2}$ et $\sqrt{-1}$ appartiennent à $\mathbb{Q}[\xi_8]$.

c) En déduire que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique.