ENS Lyon 2011 - 2012
Master 1

Algèbre Approfondie

30.09 et 04.10.2011

TD 3

Corps finis, extensions séparables

Exercice 1.
Soit p un nombre premier. Les affirmations suivantes sont-elles exactes ?

1. Les corps $\mathbb{F}_7[X]/(X^3-2)$ et $\mathbb{F}_7[X]/(X^3-3)$ sont isomorphes.
2. Le corps $\mathbb{F}_{p^2}$ est un sous-corps de $\mathbb{F}_{p^3}$.
3. Il existe un élément $a \in \mathbb{F}_{p^2}$ tel que $a^2 = -1$.
4. Il existe un isomorphisme de groupes entre le corps $\mathbb{F}_4$ et $\mathbb{Z}/4\mathbb{Z}$.
5. Pour tout nombre premier p, $\bar{\mathbb{F}}_p = \cup_{n\geq 1}\mathbb{F}_{p^n}$.

Exercice 2.
Vérifier que les polynômes X^2+1 et X^2+X+2 sont irréductibles sur le corps $\mathbb{F}_3$, puis construire explicitement un isomorphisme entre les corps $\mathbb{F}_3[X]/(X^2+1)$ et $\mathbb{F}_3[X]/(X^2+X+2)$.

Exercice 3.
Soit K un corps fini de caractéristique $p > 0$. Soit $\mathcal{A}$ l'ensemble des $\alpha \in K$ tels que $K = \mathbb{F}_p[\alpha]$ (*éléments primitifs*), et soit $\mathcal{B}$ l'ensemble des générateurs du groupe multiplicatif K^* (*racines primitives*). O a donc $\mathcal{B} \subset \mathcal{A}$. Quels sont les cardinaux des ensembles $\mathcal{A}$ et $\mathcal{B}$ pour les corps $K = \mathbb{F}_4$ et $K = \mathbb{F}_9$?

Exercice 4. Limites de la réduction modulo p.
Soit P un polynôme de degré n à coefficients dans $\mathbb{Z}$. Soit p un nombre premier. On note $\bar{P}$ la réduction de P modulo p, $\bar{P}$ est un polynôme de $\mathbb{F}_p[X]$.

On considère le polynôme $P(X) = X^4 + 1 \in \mathbb{Z}[X]$.

1. Si $p = 2$, montrer que $\bar{P}$ n'est pas irréductible.
2. On suppose $p \neq 2$.
   (a) Montrer la congruence $p^2 - 1 \equiv 0 \pmod 8$. En déduire que le polynôme $X^8 - 1$ divise $X^{p^2-1} - 1$.
   (b) Soit α une racine de $\bar{P}$ dans une extension de $\mathbb{F}_p$. Montrer que l'extension $\mathbb{F}_p[\alpha]$ est de degré au plus 2 sur $\mathbb{F}_p$. En déduire que le polynôme $X^4 + 1$ n'est pas irréductible modulo p.

Exercice 5.
Soit K un corps de caractéristique 0 ou fini.

1. Montrer que tout polynôme irréductible sur K est séparable.
2. En déduire que toute extension finie de K est séparable.

Exercice 6.
Soit K un corps fini. Soit $P \in K[X]$ un polynôme irréductible et soit L/K une extension de K qui contient une racine de P. Montrer que P est scindé dans cette extension. Est-ce que cette propriété reste vraie si K n'est pas fini ?

Exercice 7.

Soit L/K une extension de corps.

1. Montrer que l'ensemble L_s des éléments de L qui sont séparables sur K forme un sous-corps de L. Est-ce que cette propriété est vraie pour les éléments qui ne sont pas séparables ?
2. Vérifier que L_s est la plus grande sous-extension de L qui est séparable sur K.
3. On appelle *degré séparable* de l'extension L/K le degré $[L_s : K]$, et *degré inséparable* de L/K le degré $[L : L_s]$. On suppose le corps K de caractéristique p, montrer qu'alors $[L : L_s]$ est une puissance de p.

Exercice 8.

1. Soit K un corps et soit L/K une extension séparable. On suppose qu'il existe un entier $n > 0$ tel que $\deg_K(x) \leq n$ pour tout $x \in L$. Montrer : $[L : K] \leq n$.
2. Soit $L = \mathbb{F}_p(X, Y)$ et soit K le sous-corps de L engendré par X^p et Y^p. Montrer que l'extension L/K admet une infinité de corps intermédiaires ; en déduire qu'elle est finie non monogène.

Exercice 9.

Soit K un corps et soit $\bar{K}$ une clôture algébrique de K. Soit L/K une extension séparable finie. Montrer que les propositions suivantes sont équivalentes :

1. $L = K(x)$;
2. l'application $\mathrm{Hom}_K(L, \bar{K}) \to \bar{K}$ donnée par $\sigma \mapsto \sigma(x)$ est injective.

Exercice 10.

Soit K un corps de caractéristique $\neq 2$. Soient a, b deux éléments de K tels aue a, b et ab ne soient pas des carrés dans K. On note $\sqrt{a}$ et $\sqrt{b}$ des racines carrées de a et b dans une clôture algébrique de K.

1. Vérifier que l'extension $K(\sqrt{a}, \sqrt{b})/K$ est de degré 4.
2. Déterminer tous les K-homomorphismes de $K(\sqrt{a}, \sqrt{b})$ dans $\bar{K}$, puis en déduire que l'on a $K(\sqrt{a}, \sqrt{b}) = K(\sqrt{a} + \sqrt{b})$.

Exercice 11. Caractérisation des extensions monogènes finies.

1. Soit L/K une extension de corps telle que l'ensemble des sous-corps de L contenant K est fini. Montrer que l'extension L/K est monogène.

   On pourra d'abord montrer que cette extension est finie.
2. Réciproquement, soit L/K une extension finie monogène. Soit $\alpha \in L$ un élément tel que $L = K(\alpha)$.
   (a) Soit M une extension intermédiaire, c'est-à-dire $K \subset M \subset L$. Montrer que M est le sous-corps de L engendré sur K par les coefficients du polynôme minimal de α sur M.
   (b) En déduire que l'ensemble des sous-corps de L contenant K est fini.