UNIVERSITÉ DE NICE SOPHIA ANTIPOLIS **2010/2011**
Faculté des Sciences Préparation à l'agrégation
Département de Mathématiques
TD : corps de rupture, corps de décomposition, corps finis

Exercice 1. Nombres algébriques (Gourdon)
Soient $\mathbb{K} \subset \mathbf{L}$ deux corps commutatifs. Pour $\alpha \in \mathbf{L}$, on pose $\mathbb{K}[\alpha] = \{P(\alpha), P \in \mathbb{K}[X]\}$. On dit que $\alpha \in \mathbf{L}$ est *algébrique sur* $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X]$, $P \neq 0$, tel que $P(\alpha) = 0$.

1. (a) Soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Montrer que $\{P \in \mathbb{K}[X], P(\alpha) = 0\}$ est un idéal principal engéndré par un polynôme unitaire irréductible (appelé polynôme minimal de α).
   Montrer que $\mathbb{K}[\alpha]$ est un corps, de dimension finie en tant que $\mathbb{K}$-espace vectoriel.
   (b) Montrer que si $\mathbb{K}[\alpha]$ est de dimension finie en tant que $\mathbb{K}$-espace vectoriel, α est algébrique sur $\mathbb{K}$.
2. Soient $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}_3$ trois corps commutatifs. Montrer l'équivalenece
$$([\mathbb{K}_2 : \mathbb{K}_1] < +\infty \text{ et } [\mathbb{K}_3 : \mathbb{K}_2] < +\infty) \iff [\mathbb{K}_3 : \mathbb{K}_1] < +\infty.$$
   Si ces conditions sont satisfaites alors $[\mathbb{K}_2 : \mathbb{K}_1][\mathbb{K}_3 : \mathbb{K}_2] = [\mathbb{K}_3 : \mathbb{K}_1]$.
3. Si $a_1, \ldots, a_n \in \mathbf{L}$, on note $\mathbb{K}(a_1, \ldots, a_n)$ le plus petit sous-corps de $\mathbf{L}$ contenant $\mathbb{K}$ et $a_1, \ldots, a_n$. Montrer que $a_1, \ldots, a_n$ sont algébriques sur $\mathbb{K}$ ssi $[\mathbb{K}(a_1, \ldots, a_n) : \mathbb{K}] < \infty$.
4. Montrer que $\mathbf{A}$, l'ensemble des nombres algébriques sur $\mathbb{K}$, est un corps.
5. Si $\mathbf{L}$ est algébriquement clos, montrer que $\mathbf{A}$ est algébriquement clos.

Exercice 2. Soient f, g deux polynômes unitaires de $\mathbb{K}[X]$. Soit $\alpha_1, \ldots, \alpha_n$ et $\beta_1, \ldots, \beta_m$ les racines de f et g dans une extension $\mathbf{L}$ de $\mathbb{K}$.

1. On introduit les nouvelles indéterminées U et T et on considère
$$h(U) = Res_U(g(U), Res_T(f(T), X - (T + U))).$$
   Montrer que les zéros de h dans $\mathbf{L}$ sont les sommes $\alpha_i + \beta_j$, $i = 1, \ldots n, j = 1, \ldots m$.
2. Proposer une formule similaire pour un polynôme dont les zéros sont les produits $\alpha_i \beta_j$, $i = 1, \ldots n, j = 1, \ldots m$.
3. Calculer le polynôme minimal de $\sqrt[3]{7} + \sqrt{2}$ sur $\mathbb{Q}$.

Exercice 3. Structure des corps finis (Demazure)
Soit $\mathbb{K}$ un corps (commutatif) fini. Montrer que

1. La caractéristique p de $\mathbb{K}$ est $\neq 0$ et le nombre des éléments de $\mathbb{K}$ est de la forme $q = p^s$ avec s entier > 0.
2. On a $X^q - X = \prod_{\alpha \in \mathbb{K}} (X - \alpha)$.
3. Le groupe $\mathbb{K}^*$ est cyclique, d'ordre $q - 1$

4. Les nombre des éléments de tout sous-corps de $\mathbb{K}$ est de la forme p^r où r divise s.
5. Inversement, pour tout diviseur r de s, il existe un unique sous-corps de $\mathbb{K}$ à p^r éléments.

Exercice 4. Théorème de l'élément primitif pour les corps finis.
Soit $\mathbf{L}$ une extension algébrique d'un coprs fini $\mathbb{K}$. Montrer qu'il existe $\alpha \in \mathbf{L}$ tel que $\mathbf{L} = \mathbb{K}[\alpha]$.

Exercice 5. Polynômes sans facteurs multiples (Demazure)
Soit $\mathbb{K}$ un corps et soit P un polynôme unitaire de $\mathbb{K}[X]$, $\deg P > 1$.

1. Montrer que les conditions suivantes sont équivalentes
   (a) P et P' sont premiers entre eux
   (b) les facteurs irreductibles de P apparaissent tous avec la multiplicité 1
   (c) il n'existe pas de polynôme non constant Q tel que Q^2 divise P.
   (d) P n'a pas de racines multiples dans aucun corps contenant $\mathbb{K}$.

   Un polynôme satisfaisant ces conditions est dit *sans facteurs multiples*.
2. Prouver que tout polynôme unitaire P s'écrit de façons unique Q^2R, où Q est R sont unitaires, et R est sans facteurs multiples.
3. Montrer que le nombre de polynômes unitaires sans facteurs multiples de degré n sur $\mathbf{F}_p$ est p pour $n = 1$ et $p^n - p^{n-1}$ pour $n > 1$.