Université Louis Pasteur
Département de Mathématiques

3 septembre 2008

Master de mathématiques 1ère année

Algèbre M1S2

Durée : 3 heures

Documents, calculatrices et téléphones portables sont interdits

Il sera tenu compte de la qualité et de la rigueur de la rédaction. En particulier toutes les réponses doivent être justifiées d'après les résultats prouvés dans le cours ou en TD.

1. Soient p un nombre premier, $d \geq 1$ un entier tel que p ne divise pas d, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et K un corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^d - 1$.

(a) Montrer que $K/\mathbb{F}_p$ est une extension galoisienne finie et que $\mathrm{Gal}(K/\mathbb{F}_p)$ est isomorphe à un sous-groupe de $(\mathbb{Z}/d\mathbb{Z})^\times$.

(b) Montrer que $\mathrm{Gal}(K/\mathbb{F}_p)$ est cyclique, engendré par le morphisme défini par $x \mapsto x^p$.

(c) Montrer que $\mathrm{Gal}(K/\mathbb{F}_p)$ est isomorphe au sous-groupe de $(\mathbb{Z}/d\mathbb{Z})^\times$ engendré par p.

(d) Soit e le plus petit entier strictement positif tel d divise $p^e - 1$. Montrer que K est d'ordre p^e.

2. On considère $p, q \in \mathbb{Q}$ et on pose $P(X) = X^4 + pX^3 + qX^2 + pX + 1 \in \mathbb{Q}[X]$. Dans tout l'exercice on supposera que P soit *irréductible* sur $\mathbb{Q}$. On note $L \subset \mathbb{C}$ le corps de décomposition de P sur $\mathbb{Q}$ dans $\mathbb{C}$ et $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) Monter que $L/\mathbb{Q}$ est une extension galoisienne.

(b) Montrer qu'il existe $\alpha, \beta \in \mathbb{C}$ tels que les racines de P sont $\alpha, \alpha^{-1}, \beta$ et β^{-1}.

(c) On pose $A = \alpha + \alpha^{-1}$. En étudiant les orbites sous l'opération de G, trouver le polynôme minimal de A sur $\mathbb{Q}$ et le polynôme minimal de α sur $\mathbb{Q}(A)$.

t.s.v.p.

(d) Soit $B = \beta + \beta^{-1} \in L$. Montrer que $\mathbb{Q}(A) = \mathbb{Q}(B)$ et en déduire que $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$ sont des extensions de $\mathbb{Q}(A)$ contenues dans L.

(e) Montrer que $[L : \mathbb{Q}(A)] = 2$ ou 4 et que $[L : \mathbb{Q}] = 4$ ou 8.

Dans la suite on supposera que $[L : \mathbb{Q}] = 8$***.***

On pose $M = \mathbb{Q}(A)$ et $H = \mathrm{Gal}(L/M)$.

(f) Monter que L/M est une extension galoisienne et que $[L : M] = 4$.

(g) Montrer que $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ et en déduire que $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(h) Montrer qu'il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$ et $\sigma(\beta) = \alpha$.

(i) Montrer que $H \subset G$ est un sous-groupe distingué et que $G = H \cup \sigma H$.

D'après le cours, le groupe de Galois G s'identifie à un sous-groupe du groupe symétrique S_4. Pour rendre explicite cette identification, on fixe la bijection ϕ entre l'ensemble $\{1, 2, 3, 4\}$ et l'ensemble $\{\alpha, \alpha^{-1}, \beta, \beta^{-1}\}$ des racines de P donnée par

$$\phi(1) = \alpha, \quad \phi(2) = \beta, \quad \phi(3) = \alpha^{-1}, \quad \phi(4) = \beta^{-1}.$$

(j) Montrer que moyennant cette bijection, σ correspond à la permutation $(1, 2)(3, 4)$ et H au sous-groupe

$$\{(1), (1, 3), (2, 4), (1, 3)(2, 4)\}.$$

(k) Montrer qu'avec cette identification, le groupe G s'identifie au sous-groupe

$$\{(1, 3), (2, 4), (1, 2)(3, 4), (1, 4)(2, 3), (1, 2, 3, 4)^i \mid i = 0, \ldots, 3\} = \{(1, 2, 3, 4)^i, (1, 3)(1, 2, 3, 4)^i \mid i = 0, \ldots, 3\}$$

de S_4.

(l) Existe-t-il un sous-corps $M' \subset L$ avec $\mathrm{Gal}(L/M') \cong \mathbb{Z}/4\mathbb{Z}$?

(m) Déterminer le nombre de sous-corps $M' \subset L$ avec $[M' : \mathbb{Q}] = 2$.