Université Claude Bernard Lyon I — 2nd semestre 2014/2015
Master I — Théorie de Galois

Partiel, 31 mars 2015, 14h00-16h30

Les règles du jeu :

1. Vous pouvez utiliser tout résultat du cours... sauf si la question est de démontrer un tel résultat.

2. Les documents ainsi que la communication avec les autres étudiants ne sont pas autorisés.

3. Les questions à l'enseignant sont encouragées.

4. Il y a 4 exercices (34 points à gagner sur 20) qui attendent vos réponses. A vous de vous organiser. Bon travail...

Exercice 1 (Révisions (6 pts)).

1. (0.5 pt) Montrer que si $K \leq L \leq M$ sont des extensions algébriques des corps K, L, M et que M est une extension séparable de K, alors M est une extension séparable de L.
2. (1 pt) Montrer que si $K \leq L \leq M$ sont des extensions algébriques des corps K, L, M et que M est une extension normale de K, alors M est une extension normale de L.
3. *Un corps K est dit parfait si toute extension algébrique de K est séparable.*
   (a) (0.5 pt) Montrer que toute extension algébrique d'un corps parfait est parfait.
   (b) (1 pt) Soit K un corps de caractéristique p non nulle. Si f est un polynôme irréductible dans $K[X]$, alors f est inséparable si et seulement si $f(X) \in K[X^p]$. (*Rappelons qu'un polynôme est dit inséparable s'il n'est pas séparable.*)
   (c) (2 pts) Soit K un corps de caractéristique p. Montrer alors l'équivalence suivante : K est parfait si et seulement si l'endomorphisme de Frobenius $F : x \longmapsto x^p$ est surjectif.
   (d) (1 pt) Montrer que les corps finis sont parfaits.

Exercice 2 (Corps finis (5 pts)).

Soit K un corps fini de caractéristique p impaire. On dira que $x \in K$ est un carré s'il existe $y \in K$ tel que $y^2 = x$. On notera K^2 les carrés de K

1. (1 pt) Montrer que le nombre de carrés dans K est $\frac{|K|+1}{2}$ où $|\ |$ note le nombre d'éléments dans l'ensemble en question.
2. (0.5 pt) Soit $\delta \in K \setminus K^2$. Montrer que l'extension $K(\sqrt{\delta})/K$ est galoisienne de degré 2.
3. (1.5 pts) Montrer, en considérant l'action des éléments de $\mathrm{Gal}(K(\delta)/K)$ sur $K(\sqrt{\delta})$, que l'application $x + y\sqrt{\delta} \longmapsto x^2 - y^2\delta$ $(x, y) \in K^2$ définit un homomorphisme du groupe multiplicatif de $K(\sqrt{\delta})$ dans le groupe multiplicatif de K.
4. (1 pt) Montrer que le morphisme du point précédent est surjectif.
5. (1 pt) Montrer que pour chaque $c \in K^\times$, le nombre de solutions dans $K \times K$ de l'équation $x^2 - y^2\delta = c$ est $|K| + 1$.

Exercice 3 (Groupes de Galois (13 pts)).
On pose $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

1. (3 pts) On commence avec une révision rapide. Montrer que $K/\mathbb{Q}$ est une extension galoisienne de degré 4, de groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ et engendré par les deux automorphismes

$$\sigma \ : \ \begin{cases} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{cases} \qquad\qquad \tau \ : \ \begin{cases} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{cases} \quad ,$$

   dont on justifiera l'existence.

   On définit $\theta = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ et $L = K(\theta)$. Clairement $\theta^2 \in K$.

2. (1 pt) Montrer que $\frac{\sigma(\theta^2)}{\theta^2} = (\sqrt{2}-1)^2$ et $\frac{\tau(\theta^2)}{\theta^2} = \left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)^2$.
3. (1 pt) Déduire du point précédent que $\theta \notin K$. (*Vous pouvez utiliser le raisonnement par l'absurde ce qui légitimera l'écriture $\sigma(\theta)$ et permettra de calculer $\sigma^2(\theta)$.*)
4. (1 pt) Si $\mu : L \longrightarrow \mathbb{C}$, montrer que $\mu_{|L}$ prolonge un élément de $\mathrm{Gal}(K/\mathbb{Q})$. Déduire de ceci et des calculs du point 2 que $L/\mathbb{Q}$ est une extension normale, et par conséquent galoisienne.

   On notera $G = \mathrm{Gal}(L/\mathbb{Q})$.

5. (3 pts) Déduire du point précédent que σ (resp. τ) s'étend à un automorphisme de $L/\mathbb{Q}$ qu'on notera $\bar{\sigma}$ (resp. $\bar{\tau}$). Montrer ensuite que $\bar{\sigma}$ et $\bar{\tau}$ sont d'ordre 4 et qu'ils ne commutent pas. (*Vous pouvez vous inspirer des calculs du point 2, et aussi calculer $\bar{\sigma}\bar{\tau}(\theta)$ et $\bar{\tau}\bar{\sigma}(\theta)$.*).
6. (2 pts) Montrer en les explicitant en fonction de $\bar{\sigma}$ et $\bar{\tau}$ que G a six éléments d'ordre 4 et 1 d'ordre 2. (*Il suffira de déterminer l'ordre de $\bar{\sigma}\bar{\tau}$.*)
7. (2 pts) Montrer que G est isomorphe au groupe $\mathbf{Q}_8$ (de présentation $\langle\, a, b \mid a^2 = b^2 = (ab)^2 \rangle$). Montrer que si $\mathbb{Q} \leq M \leq L$, alors $M/\mathbb{Q}$ est galoisienne.

Exercice 4 (Séparable/Inséparable (10 pts)).
Soit t un élément transcendant sur $\mathbb{F}_5$. On définit $K = \mathbb{F}_5(t)$.

1. (2 pts) Montrer que le polynôme $P = X^3 + tX + t$ est irréductible dans $K[X]$. Montrer que P est séparable.
2. (3 pts) Montrer que le corps de décomposition L de P sur K est de degré 6 en utilisant son discriminant. (*Voir ci-dessous pour la formule générale du discriminant pour les polynômes de degré 3.*)
3. (2 pts) On définit $Q = P(X^{5^2})$. Montrer que Q est irréductible dans $K[X]$. Déterminer le nombre de racines de Q et leurs multiplicités.
4. (3 pts) Soit M le corps de décomposition de Q sur K. Déterminer $[M : K]$ et $[M : K]_s$.

Formule du discriminant pour $X^3+pX+q \in K[X]$ séparable avec K de caractéristique différente de 2 et 3 : $-4p^3 - 27q^2$.