Partiel, 27 mars 2013, 14h-16h

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, sauf les notes de cours de M. Tchoudjem sur sa page web, 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 (25 points à gagner) qui attendent vos réponses. Bon travail...

Exercice 1 (Rappels élémentaires).
(2 pts) Soient L et K deux corps. On suppose que L est le corps de décomposition d'un polynôme séparable $P \in K[X]$. Montrer que l'action de $\mathrm{Gal}(L/K)$ sur les racines de P est transitive si, et seulement si, P est irréductible sur K.

Exercice 2 (Groupes de Galois, léger).
I. (3 pts) On considère le polynôme $P(X) = (X^2 - p_1)(X^2 - p_2)$ dans $\mathbb{Q}[X]$ où les p_i sont des nombres premiers distincts. On déterminera son groupe de Galois. Voici une recette :

1. Déterminer le corps L de décomposition de P.
2. Vérifier que $X^2 - p_2$ est irréductible sur le corps de décomposition L_1 de $X^2 - p_1$ sur $\mathbb{Q}$. En déduire le degré $[L : K]$.
3. Expliciter des automorphismes des L/L_1.
4. Conclure.

II. Soit $P[X]$ un polynôme séparable sur un corps K. On suppose que $P(X) = P_1(X) \dots P_k(X)$, où chaque P_i est irréductible dans $K[X]$ de degré n_i, et que son groupe de Galois G soit cyclique.

1. (0,5 pt) Montrer que le groupe de Galois de P agit transitivement sur les racines de chaque P_i.
2. (1 pt) Déduire que, quitte à réindexer les racines, G est engendré par un produit de k cycles de la forme

$$(1\ 2\ \dots\ n_1)(n_1+1\ \dots\ n_1+n_2)\ \dots\ (n_1+\dots+n_{k-1}+1\ \dots\ n_1+\dots+n_k)\ .$$

Exercice 3 (Corps finis).
On étudie le corps à 8 éléments.

1. (0,5 pt) Montrer, en les explicitant, qu'il existe deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2$.
2. (3 pts) Expliciter tous les isomorphismes possibles entre les deux présentations du corps à 8 éléments, fournies par les deux polynômes du point précédent.

Exercice 4 (Groupes de Galois, gastronomique).
On étudie des extensions de $\mathbb{Q}$. On commence avec le polynôme suivant dans $\mathbb{Q}[X]$.

$$P(X) \;=\; X^3 - 3X - 1 \;.$$

1. (1.5 pts) Montrer que ce polynôme est irréductible sur $\mathbb{Q}$. (*Changement de variable.*)

   On admettra que P a trois racines $\alpha_1, \alpha_2, \alpha_3$ telles que

   $$\alpha_3 < \alpha_2 < 0 < \alpha_1 \quad .$$

2. (1.5 pts) Montrer que si α est racine de P, alors il en est de même pour $-1 - \frac{1}{\alpha}$. En déduire que $K = \mathbb{Q}(\alpha_1)$ est une extension galoisienne de $\mathbb{Q}$, et le cardinal de $\mathrm{Gal}(K/\mathbb{Q})$.
3. (1 pt) On définit $\beta_1, \beta_2, \beta_3 \in \mathbb{C}$ tels que $\beta_i^2 = \alpha_i$. Montrer qu'on peut choisir les β_i telles que $\beta_1\beta_2\beta_3 = 1$. On définit $L = K(\beta_1, \beta_2, \beta_3)$. Montrer que $L/\mathbb{Q}$ est une extension galoisienne en explicitant un polynôme séparable dont L est le corps de décomposition sur $\mathbb{Q}$.
4. (2 pts) Montrer que $[K(\beta_1) : K] = 2$. (*Vous pouvez utiliser les images possibles de β_1 sous l'action des extensions des éléments de* $\mathrm{Gal}(K/\mathbb{Q})$ *à L.*)
5. (1 pt) Montrer que $L = \mathbb{Q}(\beta_1, \beta_2)$. Déterminer $[L : K]$, et en déduire $[L : \mathbb{Q}]$.
6. (i) (2 pts) On définit $G = \mathrm{Gal}(L/\mathbb{Q})$ et $H = \mathrm{Gal}(L/K)$. Le sous-groupe H est-il distingué dans G ? Quelle est sa structure ?

   (ii) (2 pts) Montrer que G n'est pas abélien. En déduire que les 3-Sylow de G ne sont pas distingués.
7. (4 pts) On définit $\theta = \beta_1 + \beta_2 + \beta_3$. Montrer en les explicitant que θ a quatre images possibles sous l'action de G. En déduire $[\mathbb{Q}(\theta) : \mathbb{Q}]$. Cette extension est-elle galoisienne ?