Université Lyon 1
M1G. Théorie de Galois.

Le 9 mars 2016

PARTIEL

Durée : 1h30

Documents non admis.
Les résultats d'une question peuvent être utilisés pour les questions suivantes.

Problème 1

Soit K un corps et P un polynôme unitaire de $K[X]$. On note P' le polynôme dérivé de P.

1. Soit $Q \in K[X]$. Montrer que si Q^2 divise P, alors Q divise P'.
2. En déduire que si $\mathrm{pgcd}(P, P') = 1$, alors P n'a pas de facteur carré dans sa décomposition en produits d'irréductibles dans $K[X]$.

Problème 2

On rappelle qu'un élément α est *constructible* (à la règle et au compas) si et seulement s'il est contenu dans une tour d'extensions de degré deux sur $\mathbb{Q}$. Soit P un polynôme irréductible sur $\mathbb{Q}$.

1. Montrer que si une racine α de P est constructible, alors toutes les racines de $\mathbb{Q}$ sont constructibles.
2. Montrer que si une racine de P est constructible, alors K admet une tour d'extensions de degré deux sur $\mathbb{Q}$, où K est le corps de décomposition de P sur $\mathbb{Q}$. En déduire que $[K : \mathbb{Q}]$ est une puissance de 2.

Problème 3

Soient $p_1, \ldots, p_n$ dans $\mathbb{Q}$, et $K_i = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})$ pour $i \leq n$. On pose $K_0 = \mathbb{Q}$ et $K = K_n$. Pour $I \subseteq \{1, \ldots, n\}$ soit $a_I = \prod_{i \in I} \sqrt{p_i}$ (en particulier $a_\emptyset = 1$).

1. Montrer que K est le corps de décomposition d'un polynôme (réductible) sur $\mathbb{Q}$. En déduire que K est une extension normale.
2. On suppose que $\sqrt{p_{i+1}} \notin K_i$ pour tout $i < n$.
   (a) Calculer $[K : \mathbb{Q}]$ et $|\mathrm{Gal}(K/\mathbb{Q})|$.
   (b) Montrer que $(a_I : I \subseteq \{1, \ldots, n\})$ est une $\mathbb{Q}$-base linéaire de K.
   (c) Pour $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ soit $\sigma_i = \sigma(\sqrt{p_i})/\sqrt{p_i}$ pour $i \in \{1, \ldots, n\}$. Montrer que $\sigma_i \in \{\pm 1\}$ et que $\sigma \mapsto (\sigma_1, \ldots, \sigma_n)$ est un isomorphisme de groupes entre $\mathrm{Gal}(K/\mathbb{Q})$ et le groupe multiplicatif $\{+1, -1\}^n$.
3. On suppose que $p_1, \ldots, p_n$ sont des nombres premiers distincts et on propose de montrer que $[K : \mathbb{Q}] = 2^n$.
   (a) Montrer que c'est vrai pour $n = 0$ et $n = 1$.
   (b) Supposons, pour une contradiction, que $i < n$ est minimal avec $\sqrt{p_{i+1}} \in K_i$. Montrer qu'il y a une combinaison $\mathbb{Q}$-linéaire s de $\{a_I : I \subseteq \{1, \ldots, i\}\}$ telle que $\sqrt{p_i} = s$. En considérant les images de s par $\mathrm{Gal}(K/\mathbb{Q})$ et l'indépendance linéaire de $\{a_I : I \subseteq \{1, \ldots, i\}\}$ sur $\mathbb{Q}$, montrer que $s = qa_I$ pour un certain $q \in \mathbb{Q}$ et $I \subseteq \{1, \ldots, i\}$. Conclure que c'est impossible.
4. Soient $p_1, \ldots, p_n$ comme dans la question 3., et $\alpha_1, \ldots, \alpha_n$ dans $\mathbb{Q}$ non nuls. Déterminer les images de $\alpha := \sum_i \alpha_i \sqrt{p_i}$ sous l'action de $\mathrm{Gal}(K/\mathbb{Q})$. En déduire que α est un élément primitif de K sur $\mathbb{Q}$.
5. (Bonus) Est-ce que $\sqrt{15} \in \mathbb{Q}(\sqrt{10}, \sqrt{42})$? Justifier la réponse.