DUE DATE: FEB. 11, 2016

The problems in this assignment revolve around the Key Lifting Lemma and related arguments. It may be helpful to review the inductive step of the lemma, and in particular the (often used) result that if α has minimal polynomial $q(x)$ over K, and if $\varphi\colon K \xrightarrow{\sim} K'$ is an isomorphism, then for any root β of $\varphi(q(x))$ there exists a composite isomorphism

$$\varphi_1 : K(\alpha) \cong \frac{K[x]}{(q(x))} \cong \frac{K'[x]}{(\varphi(q(x))} \cong K'(\beta)$$

lifting φ and which takes α to β. (As a special case, if $K = K'$ and φ is the identity, we have an isomorphism $K(\alpha) \cong K(\beta)$ taking α to β and acting as the identity on K.)

1. Our proof of Corollary 2 in Thursday's class on 'Galois Extensions' had a gap, in that I repeatedly used a fact which we did not prove. The fact was this :

> Suppose that $K \subseteq L$ is an algebraic extension, $\alpha \in L$ an element, and that the minimal polynomial $q(x)$ of α over K has distinct roots. Then $K(\alpha)/K$ is a separable extension.

This fact is a special case of of Corollary 2, but we have to establish it independently since we use it to prove the corollary. In this problem we will fix the gap by proving the result above.

(a) Let $d = [K(\alpha) : K]$. If all roots of $q(x)$ are distinct, how many roots does $q(x)$ have?

(b) Let $\overline{K}$ be the algebraic closure of K. For each root β of $q(x)$, explain why there is a homomorphism of fields $K(\alpha) \longrightarrow K(\beta) \subseteq \overline{K}$ taking α to β and acting as the identity on K.

(c) From parts (a) and (b), you have computed a lower bound for

$$\left|\left\{\psi : K(\alpha) \longrightarrow \overline{K} \,\middle|\, \psi|_K = \mathrm{Id}_K\right\}\right|.$$

Use this lower bound and the theorem characterizing separable extensions to prove that $K(\alpha)/K$ is separable.

2. In this problem we will see why "$\varphi(q_\alpha)$ splits completely in F" was part of the hypothesis of the lifting lemma. Consider the fields $K = K' = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$, and $F = \mathbb{R}$. As we have seen several times, there is an isomorphism $\varphi\colon K \longrightarrow K'$ sending $\sqrt{2}$ to $-\sqrt{2}$.

(a) Let $\alpha = \sqrt[4]{2}$. What is the minimal polynomial of α over K?

(b) Let $q(x) \in K[x]$ be your answer from (a). Compute $\varphi(q(x))$.

According to the inductive step in the lifting lemma, any lift ψ of φ will have to send α to a root of $\varphi(q(x))$ in F.

(c) Can φ be lifted to a field homomorphism $\psi\colon \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{R}$?

3. Let $\alpha = \sqrt[6]{5}$, $\omega = e^{\frac{2\pi i}{3}}$, and $L = \mathbb{Q}(\alpha, \omega)$. In this problem we will repeat the inductive step of the lifting lemma in order to construct some automorphisms of L over $\mathbb{Q}$. Set $M_1 = \mathbb{Q}(\sqrt{5})$ and $M_2 = \mathbb{Q}(\alpha)$, so that we have the tower of extensions $\mathbb{Q} \subset M_1 \subset M_2 \subset L$. Note that $M_2 = M_1(\alpha)$, and $L = M_2(\omega)$.

(a) Compute $[L : \mathbb{Q}]$.

(b) Show that $L/\mathbb{Q}$ is a normal extension.

(c) Find the minimal polynomials of α over M_1 and of ω over M_2.

Let $\varphi_1\colon M_1 \longrightarrow M_1$ be the automorphism sending $\sqrt{5}$ to $-\sqrt{5}$. (We know that there is such an automorphism by **H4** Q3.)

(d) How many lifts of φ_1 to a homomorphism $\varphi_2\colon M_2 \longrightarrow L$ are there? For each of them, describe what φ_2 does to α.

(e) For each of your answers in (d), how many lifts of φ_2 to an automorphism $\psi\colon L \longrightarrow L$ are there? What does each of these do to ω?

(f) Are your counts in (d) and (e) consistant with the fact that L/M_1 is a separable normal extension? (I.e., how many lifts of φ_1 did we expect?)

(g) How many automorphisms of L over $\mathbb{Q}$ should there be?

(h) The automorphisms in (e) do not account for all of the automorphisms of L over $\mathbb{Q}$. What choice have we made above which restricts the automorphisms we obtained?