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 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.

Solution.

(a) By our structure theorem for simple extensions, $[K(\alpha) : K] = \deg q(x)$, and so $\deg q(x) = d$. If $q(x)$ has no repeated roots, then $q(x)$ has $\deg q(x) = d$ roots.

(b) As part of our proof of the structure theorem for simple extensions, we've seen that for any root β of $q(x)$, we have an isomorphism of fields $K(\beta) \cong \frac{K[x]}{(q(x))}$ acting as the identity on K. In particular we have such an isomorphism for the root α. For any other root β, if we compose these isomorphisms we get an isomorphism $K(\alpha) \cong \frac{K[x]}{(q(x))} \cong K(\alpha)$ taking α to β and acting as the identity on K. Since $\overline{K}$ is an algebraically closed field, $\beta \in \overline{K}$ and so $K(\beta)$ is a subfield of $\overline{K}$. Thus, by combining the isomorphism $K(\alpha) \cong K(\beta)$ with the inclusion map $K(\beta) \hookrightarrow \overline{K}$ we obtain a homomorphism $K(\alpha) \longrightarrow K(\beta) \subseteq \overline{K}$ acting as the identity on K.

(c) By part (b), for any root β of $q(x)$ we get a homomorphism $\psi\colon K(\alpha) \longrightarrow \overline{K}$ such that $\psi|_K = \mathrm{Id}_K$ and $\psi(\alpha) = \beta$. In particular for different roots β we get different maps ψ. By part (a) the polynomial $q(x)$ has d distinct roots, and hence we get at least d field homomorphisms $\psi\colon K(\alpha) \longrightarrow \overline{K}$ acting as the identity on K. Thus we have

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

By our theorem characterizing separable extensions, we know that the set of such maps has size at most $[K(\alpha) : K] = d$, with equality if and only if $K(\alpha)/K$ is a separable extension. Thus, since we have at least d such maps, we must have exactly d such maps, and $K(\alpha)/K$ is a separable extension.

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 $\psi\colon \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{R}$?

Solution.

(a) Let $q(x) = x^2 - \sqrt{5}$. Then $q(x) \in K[x]$ and $q(\alpha) = \alpha^2 - \sqrt{5} = \sqrt{5} - \sqrt{5} = 0$. To see that $q(x)$ is the minimal polynomial of α over K we therefore just need to show that $q(x)$ is irreducible over K. Since $q(x)$ has degree 2, if $q(x)$ factors in $K[x]$ this implies that α (a root of $q(x)$)) is in K. But then we would have $K(\alpha) = K$, i.e., that $\mathbb{Q}(\sqrt[4]{5}) = \mathbb{Q}(\sqrt{5})$. We already know that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, and since the mimimal polynomial of α over $\mathbb{Q}$ is $x^4 - 5$, we have that $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$. Therefore $\mathbb{Q}(\sqrt[4]{5}) \neq \mathbb{Q}(\sqrt{5})$, and so $q(x)$ is irreducible over K.

(b) We have $\varphi(q(x)) = \varphi(x^2 - \sqrt{5}) = \varphi(1)x^2 - \varphi(\sqrt{5}) = x^2 - (-\sqrt{5}) = x^2 + \sqrt{5}$.

(c) Any lift of φ to a map $K(\alpha) \longrightarrow \mathbb{R}$ will therefore have to take α to a root of $x^2+\sqrt{5}$, i.e., to one of $\pm i\alpha$, where $i^2 = -1$. Since both roots are purely imaginary, and not in $\mathbb{R}$, there is *no* lift of φ to a field homomorphism $\psi\colon K(\alpha) \longrightarrow \mathbb{R}$.

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?

Solution.

(a) The minimal polynomial of $\alpha = \sqrt[6]{5}$ over $\mathbb{Q}$ is $q(x) = x^6 - 5$. (This is irreducible by Eisenstein's criterion with the prime $p = 5$.) Therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. The minimal polynomial for ω over $\mathbb{Q}$ is $p(x) = x^2 + x + 1$. The roots of $p(x)$ are ω and ω^2, neither of which are real. Therefore $p(x)$ has no root in $\mathbb{Q}(\alpha)$, since $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Since $p(x)$ has degree 2, this is the same thing as saying that $p(x)$ is irreducible over $\mathbb{Q}(\alpha)$. Therefore $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$. By the tower law we then compute that

$$[L : K] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

(b) By our theorem characterizing normal extensions, to check that L/K is normal, it is enough to look at the roots of the minimal polynomials of α and ω, since α and ω generate L over $\mathbb{Q}$. In part (a) we've seen that the minimal polynomial of α over $\mathbb{Q}$ is $q(x) = x^6 - 5$. The polynomial $q(x)$ has roots $\pm\alpha$, $\pm\alpha\omega$, and $\pm\alpha\omega^2$, all of which are in L. The minimal polynomial of ω over $\mathbb{Q}$ is $p(x) = x^2 + x + 1$ with roots ω, ω^2, both of which are in L. Thus L/K is a normal extension.

(c) In part (a) we have already seen that $p(x) = x^2 + x + 1$ is the minimal polynomial of ω over $M_2 = \mathbb{Q}(\alpha)$. We know that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ and from part (a) that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. The tower law then gives us that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] = 3$. This means that the minimal polynomial of α over $M_1 = \mathbb{Q}(\sqrt{5})$ must have degree 3. The polynomial $q_{M_1}(x) = x^3 - \sqrt{5}$ is a monic polynomial of degree 3 in $M_1[x]$ with α as a root. Therefore $q_{M_1}(x)$ is the minimal polynomial of α over M_1.

(d) By the inductive step of the Key Lifting Lemma, φ_1 can be lifted to a map $\varphi_2 \colon M_2 \longrightarrow L$ which takes α to any root of

$$\varphi_1(q_{M_1}(x)) = \varphi_1(x^3 - \sqrt{5}) = \varphi_1(1)x^3 - \varphi_1(\sqrt{5}) = x^3 + \sqrt{5}.$$

The roots of $x^3 + \sqrt{5}$ are $-\alpha$, $-\alpha\omega$, and $-\alpha\omega^2$. Thus there are three such lifts of φ_1, say $\varphi_{2,1}$, $\varphi_{2,2}$ and $\varphi_{2,3}$, with $\varphi_{2,2}(\alpha) = -\alpha$, $\varphi_{2,2}(\alpha) = -\alpha\omega$, and $\varphi_{2,3}(\alpha) = -\alpha\omega^2$.

(e) By the inductive step of the Key Lifting Lemma, any of the maps $\varphi_{2,j}$, $j = 1, 2, 3$, from part (d) can be lifted to a map $\psi \colon L \longrightarrow L$ taking ω to any root of

$$\varphi_{2,j}(p(x)) = \varphi_{2,j}(x^2 + x + 1) = \varphi_{2,j}(1)x^2 + \varphi_{2,j}(1)x + \varphi_{2,j}(1) = x^2 + x + 1.$$

(Note that, since all the coefficients of $p(x)$ are in $\mathbb{Q}$, each $\varphi_{2,j}$ does the same thing to $p(x)$.) The roots of $p(x)$ are ω and ω^2. Thus each $\varphi_{2,j}$ lifts to two automorphisms $\psi \colon L \longrightarrow L$, say $\psi_{j,1}$ and $\psi_{j,2}$ with $\psi_{j,1}(\omega) = \omega$ and $\psi_{j,2}(\omega) = \omega^2$.

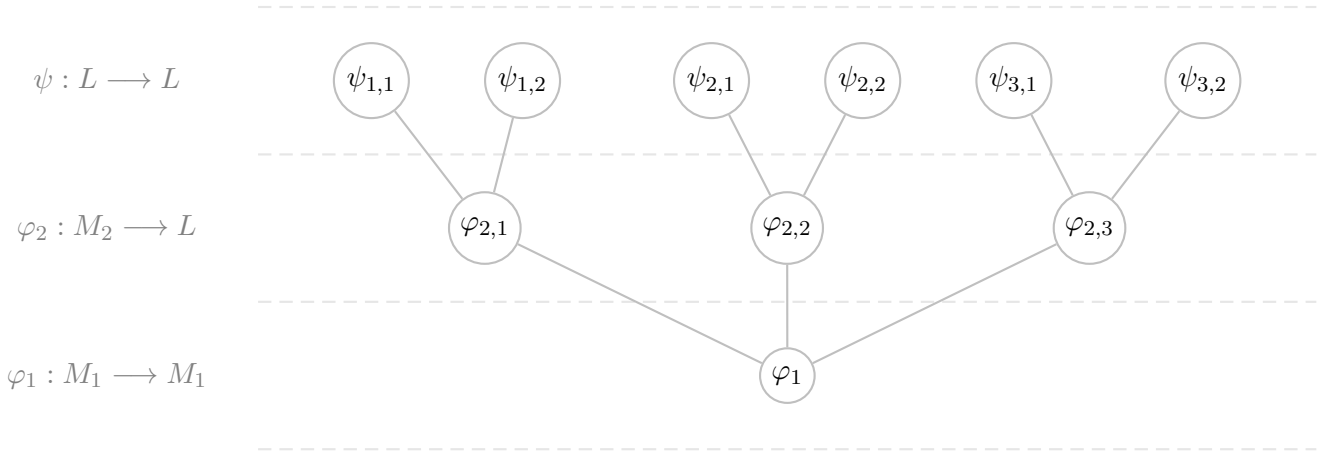
Note that if $j \neq j'$ then $\psi_{j,1} \neq \psi_{j',1}$; even though these maps do the same thing to ω, they do different things to α, and so are different automorphisms of L. Similarly $\psi_{j,2} \neq \psi_{j',2}$ whenever $j \neq j'$.

(f) Since L/M_1 is a separable extension, any map $\varphi_1 \colon M_1 \longrightarrow \overline{K}$ lifts to $[L : M_1] = 6$ different maps $\psi : L \longrightarrow \overline{L}$. Since L/M_1 is a normal extension, each of these maps has image L, and can be thought of as an automorphism of L. Thus we expect 6 different lifts of φ_1 to an automorphism $\psi \colon L \longrightarrow L$.

In part (e) we did find 6 lifts of φ_1 to an automorphism of L. The three lifts $\varphi_{2,1}$, $\varphi_{2,2}$, and $\varphi_{2,3}$ of φ_1 to a map from M_1 to L each lift in two ways to an automorphism of L. If we organize the lifts by "what each lift does to M_1", we see that there are three "boxes" (for the three different possible maps $M_1 \longrightarrow L$), and in each box

there are two automorphisms (the corresponding lifts to an automorphism of L), for a total of $3 \cdot 2 = 6$ automorphisms.

We can also visualize the lifting process as a tree, where at each stage we represent the choice of different lifts by having a different branch :



At the top of the tree we see a total of 6 lifts of φ_1 to an automorphism of L, as expected.

(g) Since L/K is a Galois extension of degree 12, there are 12 automorphisms of L over K.

(h) Any automorphism of L over $\mathbb{Q}$ must take the intermediate field M_1 somewhere. Since M_1 is a normal extension over $\mathbb{Q}$, any such automorphism of L must take M_1 to itself, i.e., induce an automorphism of M_1. In the calculations above we have required that this automorphism of M_1 be the one which takes $\sqrt{5}$ to $-\sqrt{5}$, and our computations show that there are six lifts of this automorphism to an automorphism of L. However, there is another automorphism of M_1, namely the identity map on M_1, taking $\sqrt{5}$ to $\sqrt{5}$. If we start with this automorphism of M_1 and again try to lift, we would find six different automorphism of L, for a total of 12. In particular, the tree of lifts above is only half of the tree of lifts of the identity map on $\mathbb{Q}$ to an automorphism of L.