HW 4 problem 3 (selected solution)

⇒

K normal extension \( F \) \( \Rightarrow \)

Suppose \( K \) is a splitting over \( F \) for \( g(x) \in F[x] \)

Aside: suppose \( K/F \) finite normal extension

Thus \( K = F(\alpha_1, \ldots, \alpha_n) \) some \( \alpha_1, \ldots, \alpha_n \in K \)

since \( K/F \) finite.

Choose \( f_1 \ldots f_n \) minimal polynomials.

Say \( K \) is splitting field for collection \( S \) of polynomials in \( F[x] \)

For each \( f_i \in S \), let \( \{\alpha_{i1}, \ldots, \alpha_{it_i}\} \) be the set of roots in \( K \) for \( f_i \).

Then \( K = F(\alpha_{11}, \ldots, \alpha_{1t_1}, \ldots) \)

Since \( K/F \) finite, can choose finite subset of \( \alpha_i \)

and finitely many \( f_i \)

Then set \( g(x) = \text{product of finitely many } f_i \) above
Then $K$ is the splitting field for $g(x)$ over $F$ irreducible.

- Choose $f(x) \in F[X]$ with at least one root $a \in K$.

- Let $L$ be an algebraic closure for $K$.

- Since $K$ is algebraic over $F$, $K$ is also an algebraic closure for $F$.

- So naturally $f(x)$ splits completely in $L[X]$.

- $\beta \in L$ be any root of $f(x)$. We prove already in class that there is an isomorphism $F(a) \cong F(\beta)$ that restricts to the identity on $F$, with $\sigma(a) = \beta$.

- Now view $\sigma$ as an embedding of $FK \rightarrow L$.

We have:

```
\begin{array}{c}
K \xrightarrow{\sigma} K' \subseteq L \\
\downarrow \quad \downarrow \\
F(a) \xrightarrow{\sigma} F(\beta) \subseteq L \\
\downarrow \quad \downarrow \\
F \xrightarrow{id} F \\
\end{array}
```

where $\hat{\sigma}$ extends $\sigma$ to an embedding $K \rightarrow L$ with $\check{\sigma}$ image $K'$. Existence of $\hat{\sigma}$ follows from this index.

- $K$ splitting for $g(x)$, since $\hat{\sigma}(g(x)) = g(x)$ and $\check{\sigma}$ splitting for $g(x)$ over $F$, $K'$ is a splitting field for $g(x)$ over $F$ also.
Note that \( g(x) = \lambda (x - \alpha_1) \cdots (x - \alpha_n) \) for \( \lambda \in F \), \( \alpha_1, \ldots, \alpha_n \in K \) and \( K = (\alpha_1, \ldots, \alpha_n) \).

So \( K' = F(\hat{\alpha_1}, \ldots, \hat{\alpha_n}) \) and in \( K'[x] \),
\[
g(x) = \lambda (x - \hat{\alpha_1}) \cdots (x - \hat{\alpha_n})
\]

But \( K, K' \) splitting fields for \( g(x) \) both subfields of \( L \).

In problem 2, learned that splitting fields are unique in \( L \).

So \( K = K' \), so \( \sigma \) an \( \text{automorphism} \).

\( \sigma \in K' = K \), \( \alpha \in K \) : hence \( f(x) \)

splits completely since all roots of \( f(x) \) \( \sigma \) and \( \alpha \) are in \( K \). \[ \square \]
K a field

If F is a subfield of K

Aut(K/F) automorphisms of K fixing F pointwise.

Prop: E splitting field over F for f(x) ∈ F[x]. Then

|Aut(E/F)| ≤ [E:F] with equality when f(x) is separable.

Def

Let F be a subfield of K, [K:F] < ∞.

Then K/F is a Galois extension if |Aut(K/F)| = [K:F].

If K/F is Galois, we refer to Aut(K/F) as the Galois group of K over F, denoted

Gal(K/F).

Example

K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} (non-example)

Then Aut(K/\mathbb{Q}) = \langle \text{id} \rangle since each automorphism must send \sqrt{2} to itself.
So \( |\text{Aut}(K/F)| = 1 < 3 = [K:Q] \)

so \( K/Q \) is not Galois

From earlier proposition, we know that \( K/F \) is a Galois extension when \( K \) is the splitting field over \( F \) for some \( f(x) \in F[x] \) that \( K/F \) is Galois for \( f(x) \) separable

i.e. a splitting field over \( Q \) for \( x^3 - 2 \) is a Galois extension.

In more detail:
\[
\xi = \frac{-1 + \sqrt[3]{3}}{2} \in \mathbb{C}
\]

\( \xi \) is a primitive 3rd root of \( 1 \), so the roots in \( \mathbb{C} \) of \( x^3 - 2 \) are \( \sqrt[3]{2}, \sqrt[3]{2}^{\frac{2}{3}}, \sqrt[3]{2}^{\frac{2}{3}} \)

Let \( K = \mathbb{Q}(\sqrt[3]{2}, \xi \sqrt[3]{2}, \xi^{\frac{2}{3}} \sqrt[3]{2}) \)

\( = \mathbb{Q}(\xi, \sqrt[3]{2}) \)

Then \( K \) is a splitting field for \( x^3 - 2 \) over \( \mathbb{Q} \).

The minimal polynomial for \( \xi \) over \( \mathbb{Q} \) is the cyclotomic polynomial \( \Phi_3(x) = x^3 + x + 1 \) (check)

we see that \( [K: Q] = 6 \)
We see that $[K : \mathbb{Q}] \leq 6$
(since generated by elements degrees 2, 3)
Also see that 2 and 3 both divide $[K : \mathbb{Q}]$, by multiplicity of degrees, using both orders of construction
As noted at the start, $K/F$ has a Galois, and so we conclude $|\text{Gal}(K/F)| = 6$.

As proved last time, each $\sigma \in \text{Gal}(K/\mathbb{Q})$
acts as a permutation of the roots $\sqrt[3]{2}, \sqrt[3]{2} \cdot \sqrt[3]{2}, \sqrt[3]{2} \cdot \sqrt[3]{2}$

Also, each $\sigma \in \text{Gal}(K/\mathbb{Q})$ is completely determined by its action on these roots, since $K = (\sqrt[3]{2}, \sqrt[3]{2} \cdot \sqrt[3]{2}, \sqrt[3]{2} \cdot \sqrt[3]{2})$

Now consider the assignment
\[
\begin{align*}
\sqrt[3]{2} &\mapsto \sqrt[3]{2} \\
\sqrt[3]{2} \cdot \sqrt[3]{2} &\mapsto \sqrt[3]{2} \\
\sqrt[3]{2} \cdot \sqrt[3]{2} \cdot \sqrt[3]{2} &\mapsto \sqrt[3]{2}
\end{align*}
\]
and $q \mapsto q$, \( q \in \mathbb{Q} \).

Can check this assignment produces an automorphism $\sigma$ of $K$.
Also, $|\sigma| = 3$.
Next consider the assignment
\[
\begin{align*}
\frac{\sqrt[3]{3}}{2} & \mapsto \frac{\sqrt[3]{3}}{2} \\
\sqrt[3]{\frac{3}{2}} & \mapsto \sqrt[3]{\frac{3}{2}} \\
\sqrt[3]{\frac{2}{3}} & \mapsto \sqrt[3]{\frac{2}{3}} \\
q & \mapsto q
\end{align*}
\]
produces an automorphism \( \sigma \).

Can check that \( \sigma \) produces an automorphism of order 2.

However, we know since extension is Galois, \( |\text{Aut}(K/F)| = 6 \), and we know that it is a homomorphism of the three roots of \( x^3 - 2 \) produces a homomorphism from \( \text{Gal}(K/F) \) into \( S_3 \), further, since these permutations of the roots completely determine the automorphism of \( K/F \), we see that the above homomorphism must be injective.

So conclude in general
\[
\text{Gal}(K/F) \cong S_3
\]
and that every one of the 6 permutations of \( \frac{\sqrt[3]{3}}{2}, \sqrt[3]{\frac{3}{2}}, \frac{\sqrt[3]{2}}{3} \)
produces an automorphism of \( K/F \).
But it is clear that \( \Theta, \sigma \) give us all the automorphisms.

\[ \text{Gal}(K/F) = \langle \Theta, \sigma \rangle \]