§3. Extending field homomorphisms and the Galois group of an extension.

Definition 16. For $i = 1, 2$, let $L_i : K_i$ be a field extension relative to the embedding $\varphi_i : K_i \to L_i$.

Suppose $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are isomorphisms.

We say $\tau$ extends $\sigma$ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$.

In such circumstances, $L_1 : K_1$ and $L_2 : K_2$ are isomorphic field extensions.

Diagram commutes.
Suppose $K_i \leq L_i \quad (i = 1, 2)$

\[ \tau \mid_{K_i} \quad \text{defined by} \quad \tau \mid_{K_i}(k) = \tau(k) \quad \text{for } k \in K_i. \]

restriction of $\tau$ to $K_i$

From the diagram: if $\tau$ extends $\sigma$

then \[ \tau \mid_{K_i} = \sigma \]
Definition 17. Let $L: K$ be a field extension relative to the embedding $\varphi: K \to L$, and let $M$ be a subfield of $L$ containing $\varphi(K)$. Then, when $\sigma: M \to L$ is a homomorphism, we say that $\sigma$ is a $K$-homomorphism if $\sigma$ leaves $\varphi(K)$ pointwise fixed, i.e., for all $\alpha \in \varphi(K)$, we have $\sigma(\alpha) = \alpha$.

\[
\begin{align*}
K \xrightarrow{\varphi} \varphi(K) \xhookrightarrow{\iota} L \\
\downarrow \sigma \\
M \xrightarrow{\sigma} L
\end{align*}
\]
Proposition 3.1 Suppose that $L:K$ is a field extension with $K \subseteq L$, and $\tau: L \to L$ is a $K$-homomorphism. Suppose that $f \in K[t]$ has $\text{deg} (f) \geq 1$, and $\alpha \in L$. Then:

(i) if $f(\alpha) = 0$, one has $f(\tau(\alpha)) = 0$;

(ii) when $\tau$ is a $K$-automorphism of $L$, one has $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

Theorem 3.2  Let $\sigma : K_1 \to K_2$ be a field isomorphism.
Suppose $L_i$ is a field with $K_i \subseteq L_i$ ($i = 1, 2$).
Suppose also that $\alpha \in L_1$ is algebraic over $K_1$, and $\beta \in K_2$ is algebraic over $K_2$.

Then we can extend $\sigma$ to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ in such a manner that $\tau(\alpha) = \beta$ (if and only if) $m_\beta(K_2) = \sigma(m_\alpha(K_1))$. 

\[
\begin{array}{c}
K_2 \xrightarrow{\varphi_2} K_2(\beta) \xleftarrow{\varphi_2^*} L_2 \\
\uparrow \sigma \quad \uparrow \tau \\
K_1 \xrightarrow{\varphi_1} K_1(\alpha) \xleftarrow{\varphi_1^*} L_1
\end{array}
\]
Definition 18. Suppose that $L:K$ is a field extension. Write $\text{Aut}(L)$ to denote the automorphism group of $L$. Set

$$\text{Gal}(L:K) = \{ \sigma \in \text{Aut}(L) : \sigma \text{ is a } K \text{-homomorphism} \}$$

Then we call $\text{Gal}(L:K)$ the Galois group of $L:K$. 
Proof of Theorem 3.2. \((\Rightarrow)\) Suppose we have an isomorphism \(\tau: K_1(\kappa) \rightarrow K_2(\beta)\) s.t. \(\tau\) extends \(\sigma\) and \(\tau(\alpha) = \beta\).

Let \(m_\alpha(K_1) = c_0 + c_1 \tau t + \ldots + c_d \tau^d t^d \in K_1[\tau t]\).

Then \(\tau\left(\frac{c_0 + c_1 \tau t + \ldots + c_d \tau^d t^d}{\in K_1(\kappa)}\right) = \tau((m_\alpha(K_1))(\alpha)) = \tau(c_0) + \tau(c_1) \tau(\alpha) + \ldots + \tau(c_d) \tau(\alpha)^d \thicksim 0\)

\(\Rightarrow\)

\(\sigma(c_0) + \sigma(c_1) \beta + \ldots + \sigma(c_d) \beta^d = 0\)

Hence \(\sigma(m_\alpha(K_1))\) has \(\beta\) as a root.

Since \(m_\alpha(K_1)\) is monic and irreducible over \(K_1\), and so \(\sigma(m_\alpha(K_1))\) is monic and irreducible over \(K_2\). Hence \(\sigma(m_\alpha(K_1)) = m_\beta(K_2)\).
8. Suppose that \( \beta \) is a root of \( \sigma(m_\alpha(K_1)) \).

(holds when \( m_\beta(K_2) = \sigma(m_\alpha(K_1)) \)).

For convenience write \( f_1 = m_\alpha(K_1) \) and \( f_2 = \sigma(m_\alpha(K_1)) \).

Then \( f_1 \) monic and irreducible over \( K_1 \).

\( f_2 \) monic and irreducible over \( K_2 \).

The map \( \psi_1 : K_1[t]/(f_1) \to K_1(\alpha) \)

\[ g + (f_1) \mapsto g(\alpha) \]

is an isomorphism, and

\[ \psi_2 : K_2[t]/(f_2) \to K_2(\beta) \]

\[ h + (f_2) \mapsto h(\beta) \]
Define $\varphi : K_2[t] \to K_2[t]/(f_2)$

$$h \mapsto h + (f_2)$$

Easy to see that $\varphi$ is surjective, so

$$\varphi \circ \sigma : K_1[t] \to K_2[t]/(f_2)$$

is also surjective. But

$$\ker \left( \varphi \circ \sigma \right) = \left\{ g \in K_1[t] : \sigma(g) + (f_2) = 0 + (f_2) \right\}$$

$$= \left\{ g \in K_1[t] : \sigma(g) \in (f_2) \right\}$$

$$= \left\{ g \in K_1[t] : \sigma(g) = f_1 h_1 \text{ for some } h_1 \in K_2[t] \right\}$$
is an isomorphism.

By the Fundamental Homomorphism Theorem, it follows that $\omega : K[[t]]/(f_1) \rightarrow K[[t]]/(f_2) \rightarrow (g) + (f_1) = \ker (f_1)$.

But $\omega (f_1) = f_2$, and $\ker (f_1) = K[[t]]/(f_1) = K[[t]]/(f_2) = \{ h \in K[[t]] : h = f_2 \text{ some } g \in K[[t]] \}$.

$= f_2.1 = (f_1).g \in K[[t]]$. 
Thus \( \tau = \psi_2 \circ \omega \circ \psi_1^{-1} \) is an isomorphism.

Finally,

\[
\tau (x) = \psi_2 \circ \omega \circ \psi_1^{-1} (x) \\
= \psi_2 \circ \omega (t + (f_1)) \\
= \psi_2 (\sigma(t) + (f_1)) \\
= \psi_2 (t + (f_1)) = \beta.
\]

Also, when \( c \in K_1 \), we have

\[
\tau (c) = \psi_2 \circ \omega \circ \psi_1^{-1} (c) \\
= \psi_2 \circ \omega (c + (f_1)) \\
= \psi_2 (\sigma(c) + (f_1)) = \sigma(c).
\]

Thus \( \tau \) extends \( \sigma \), and \( \tau(\alpha) = \beta \). \( \square \)