Lecture 10

Author
Tom Jeong

February 10, 2025

Contents

1 house keeping

- exam next monday
- no materials from this lecture

2 From Previous Lecture

Discussion of $\mathbb{Q}(\sqrt[4]{2})$:

- $\sqrt[4]{2}$ is a root of $x^4 - 2$
- Consider $-\sqrt[4]{2}$

Interesting maps $\mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ that fix $\mathbb{Q}$:

1. $\sqrt[4]{2} \to \sqrt[4]{2}$ (identity homomorphism)
2. $\sqrt[4]{2} \to -\sqrt[4]{2}$

Intermediate subfields:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

2.1 L/K Field Extension

$Aut(L : K)$ or $Aut(L/K)$ or $Aut(L, K)$ = Automorphisms of L fixing K

Definition 2.1 (In case you forgot)**.** Automorphisms are isomorphisms to itself:

$$Aut(L : K) = \{\sigma : L \to L : \sigma \text{ is an isomorphism and } \sigma(x) = x \text{ for all } x \in K\}$$

Note: $Aut(L, K)$ is a group under composition (the book calls this the Galois group of L/K).

In our example:

$$Aut(\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}) = \mathbb{Z}_2$$

Working with finite degrees $[L : K] < \infty$:

- $\alpha \in L$ has a minimal polynomial $f_\alpha \in K[x]$
- f_α has same roots in L
- For $\sigma \in Aut(K, L)$, σ permutes the roots of $f_\alpha \in L$

$$f_\alpha(r) = 0 \Rightarrow f_\alpha(\sigma(r)) = 0$$

For $f(x) \in K[x]$ and $f(r) = 0$, then

$$\begin{aligned}
f(\sigma(r)) &= 0 \text{ for all } \sigma \in Aut(L:K) \\
f(x) &= a_0 + a_1 x + \cdots + a_n x^n \\
f(r) &= a_0 + a_1 r + \cdots + a_n r^n = 0 \\
f(\sigma(r)) &= a_0 + a_1 \sigma(r) + \cdots + a_n \sigma(r)^n = 0 \\
&= a_0 + a_1 \sigma(r) + \cdots + a_n \sigma(r)^n = 0 \quad \text{(by the definition of } \sigma) \\
&= \sigma(a_0) + \sigma(a_1)\sigma(r) + \sigma(a_2)\sigma(r^2) + \cdots + \sigma(a_n)\sigma(r^n) = 0 \\
&= \sigma(a_0 + a_1 r + \cdots + a_n r^n) = \sigma(0) = 0
\end{aligned}$$

Since we have that $\sigma(r^k) = [\sigma(r)]^k$ because $\sigma(r^2) = \sigma(r) \cdot \sigma(r)$

Question:

1. How big can this group be ?
2. For now we will show that $|Aut(L:K)|$ is finite if $[L:K] < \infty$

Theorem 2.1. If $[L:K] < \infty$, then $|Aut(L:K)| < \infty$

Proof.

$$\begin{aligned}
&L = K(\alpha_1, \ldots, \alpha_n) \\
&\sigma \in Aut(L:K) \text{ has minimal polynomial } f_{\alpha_i} \\
&\forall \alpha \in Aut(L:K) \text{is sepcific if we know } \sigma(\alpha_1), \ldots, \sigma(\alpha_n) \\
&\sigma \text{ permutes the roots of } f_{\alpha_i} \text{ in } L \\
&\Rightarrow \forall \alpha_i \text{ there are infiniitely many possiblities for } \sigma(\alpha_i) \\
&\Rightarrow \text{finitely many possibilities for } \sigma \in Aut(L:K) \\
&\Rightarrow \text{Not every possible permutation of roots leads to a field automorphism}
\end{aligned}$$

□

2.2 relationship between subfields, subgroups, and Automorphisms

$$\begin{tikzcd}
L \arrow[d, dotted] & Aut(L:K) \arrow[d, dotted] \\
\text{intermediate fields} \arrow[d, dotted] & \text{subgroups} \\
K &
\end{tikzcd}$$

$$\Gamma := \{M : K \subseteq M \subseteq L\} \to \text{Subgroups of } Aut(L:K)$$

$$M \to \Gamma(M) = \{\sigma \in Aut(L : K) : \sigma(x) = x \text{ for all } x \in M\}$$

Φ : subgroups of $Aut(L : K) \to$ subfields of L/K

$$H \rightarrowtail \Phi(H) := \{x \in L : \sigma(x) = x \quad \forall \sigma \in H\}$$

we see that Φ fixed subfield of H
We want to show that the mapping Φ is a bijection. Note that the mapping *is not always a bijection.* When is it a bijection?

$$M \xrightarrow{\Gamma} \Gamma(M) \xrightarrow{\Phi} \Phi(\Gamma(M)) = M?$$
$$H \xrightarrow{\Phi} \Phi(H) \xrightarrow{\Gamma} \Gamma(\Phi(H)) = H?$$

$H < Aut(L : K)$, $\Phi(H) = \{x \in L : \sigma(x) = x \quad \forall \sigma \in H\}$

$\Gamma(\Phi(H)) = \{\tau \in Aut(L : K) | \tau(x) = x \quad \forall x \in \Phi(H)\}$

- we have a structure: subgroup $H \to$ fixed subfield $\Gamma(\Phi(H)) \to$ subgroup that fixes the fixed subfield
- $H \leq \Gamma(\Phi(H)) \leq Aut(L : K)$

$M \to \Gamma(M) \to \Phi(\Gamma(M)) = M$

- subfield $\to$ subgroup that fixes the subfield $\to$ fixed subfield of this group
- $M \subseteq \Phi(\Gamma(M))$

Example 2.2. $L = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}$ and $Aut(L : K) = \mathbb{Z}_2$ $\sigma^2 = e$

$\mathbb{Q}(\sqrt{2}) \xleftrightarrow[\Phi]{\Gamma} \{e\}$

right is gamma left is phi

$\mathbb{Q} \xleftrightarrow[\Phi]{\Gamma} \mathbb{Z}_2$

Example 2.3. $L = \mathbb{Q}(\sqrt[4]{2}), K = \mathbb{Q}$

$\mathbb{Q}(\sqrt[4]{2}) \xleftrightarrow[\Phi]{\Gamma} \{e\}$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}) \arrow[dr, leftrightarrow, "\Gamma", "\Phi"'] & \\
\mathbb{Q} \arrow[r, leftrightarrow, "\Phi", "\Gamma"'] & \mathbb{Z}_2
\end{tikzcd}$$