Lecture 26: Automorphisms of normal extensions

Tuesday, March 6, 2018 1:56 PM

In the previous lectures we proved:

1. Any embedding of $E \hookrightarrow F$ can be extended to an automorphism of $F$ where $F \subseteq E \subseteq F$.

2. The following are equivalent:
   
   a) $\forall \sigma \in \text{Aut}(\overline{F}/F)$, $\sigma(E) = E$.
   
   b) $\forall \alpha \in E$, $\exists \alpha_i \in E$, $m_{\alpha_i F}(\alpha) = \prod (\alpha - \alpha_i)$
   
   c) $E$ is a splitting field of a non-empty subset $S \subseteq F^{\text{Gal}(F)}$.
   
   d) $\exists i \in E$, $\forall \ i \in I$ such that:
      
      d-1) $E_i$ is a splitting field of $f(x)$ over $F$ ($E_i \subseteq F$).
      
      d-2) $\forall i,j, \exists k$, $E_k \supseteq E_i \cup E_j$.
      
      d-3) $E = \bigcup_{i \in I} E_i$.

   ($E/F$ is called a normal extension if the above statements hold.)

Remark. (d-3) implies a finite extension $E/F$ is normal $\iff$

   $E$ is a splitting field of $f(x)$ over $F$. 
Cor. Suppose $F \subseteq E_1 \subseteq E_2 \subseteq \overline{F}$ is a tower of fields.

Suppose $E_1/F$ and $E_2/F$ are normal extensions. Then

1. \[ \text{Aut}(\overline{F}/F) \xrightarrow{r_{E_2}} \text{Aut}(E_2/F) \xrightarrow{r_{E_1}} \text{Aut}(E_1/F) \]

given by restrictions are well-defined group homomorphisms.

2. \[ \text{Aut}(\overline{F}/F) \rightarrow \bigoplus_{E/F \text{finite, normal}} \text{Aut}(E/F) | \begin{array}{c} \phi_{E_2} \\ \phi_{E_1} \end{array} \quad \text{such that} \quad \phi_{E_2} = \phi_{E_1} \]

\[ \phi \mapsto (\phi|_E) \]

is an isomorphism.

Proof. 1. Since $E_i/F$ are normal, $\forall \phi \in \text{Aut}(\overline{F}/F)$, $\phi(E_i) = E_i$;

And so $\phi|_{E_i} \in \text{Aut}(E_i/F)$.

For any $\theta \in \text{Aut}(E_i/F)$, $\exists \widetilde{\theta} : \overline{F} \xrightarrow{\sim} \overline{F}$ s.t. $\widetilde{\theta}|_{E_i} = \theta$. And so the restriction map is onto.

Since clearly $r_{E_1} = r_{E_2/E_1} \circ r_{E_2}$ and $r_{E_1}$ is onto, we get that $r_{E_2/E_1}$ is onto.

2. By part 1, we get that $\phi \mapsto (\phi|_E)$ is a well-defined group homomorphism. Since $\overline{F} = \bigcup_{E/F \text{finite, normal}} E$, we get that $\phi \mapsto (\phi|_E)$
is injective.

Suppose $(\phi_E) \in \prod \text{Aut}(E/F)$ and $\forall E_1 \subseteq E_2 \subseteq \overline{F}$, $\phi_{E_2}|_{E_1} = \phi_{E_1}$; we know that $\overline{F} = \bigcup E_i$; we "glue" $\phi_E$ s:

\[
\phi : \overline{F} \to \overline{F}, \quad \phi(\alpha) = \phi_E(\alpha) \text{ if } \alpha \in E_i.
\]

Since $\phi_E$ s are compatible, $\phi$ is well-defined. One can easily check that $\phi \in \text{Aut}(\overline{F}/F)$; and the claim follows. \(\blacksquare\)

**Def.** The group given in RHS of part 2 is called the inverse limit of $\text{Aut}(E/F)$'s; and it is denoted by $\lim_{\leftarrow} \text{Aut}(E/F)$.

So we proved $\text{Aut}(\overline{F}/F) \cong \lim_{\leftarrow} \text{Aut}(E/F)$.

Moreover the above proof implies:

**Theorem.** Suppose $F \subseteq E_1 \subseteq E_2 \subseteq \overline{F}$, and $E_i/F$ are normal.

Then $\text{Aut}(E_2/E_1) \trianglelefteq \text{Aut}(E_2/F)$ and

\[
\text{Aut}(E_2/F)/\text{Aut}(E_2/E_1) \cong \text{Aut}(E_1/F).
\]
Lecture 26: Topology on group of Automorphisms of normal extensions

Tuesday, March 6, 2018  2:05 PM

Pf. We have seen \( \sigma \mapsto \sigma|_{E_1} \) is an onto group hom \( \text{Aut}(E_2/F) \to \text{Aut}(E_1/F) \). Its kernel is precisely \( \text{Aut}(E_2/E_1) \). And so by the 1st isomorphism theorem, we are done. ■

We will see that, if \( E/F \) is a finite normal extension, then \( |\text{Aut}(E/F)| \) is finite. So, by Tychonoff theorem, \( \prod_{E_i/F: \text{finite normal}} \text{Aut}(E_i/F) \) is compact with respect to product topology. And for any \( E_0 \subseteq E \subseteq E_0 \) finite normal, \( \phi = (\phi_{E_0}) \mid \phi_{E_i} \mid_{E_i} \) is a closed subset.

Hence \( \lim \text{Aut}(E/F) \) is a closed subset of \( \prod_{E_i/F: \text{finite normal}} \text{Aut}(E_i/F) \). Therefore \( \lim \text{Aut}(E/F) \) is a compact group.

If \( F \subseteq K \subseteq L \subseteq F \) and \( L/F \) and \( K/F \) are normal, then

\[
\text{Aut}(L/F) \to \text{Aut}(K/F) \text{ normal subgp of } \text{Aut}(L/F)
\]

Now we focus on finite normal extensions.
Theorem. Let $\sigma : F \rightarrow F'$, and $f(x) = \prod_{i=1}^{m} f_i(x)$, where $f_i(x)$ are distinct irreducible elements of $F[x]$. Let $E$ be a splitting field of $f(x)$ over $F$, and $E'$ be a splitting field of $\sigma(f)(x)$ over $F'$. Then $|\{ \sigma : E \rightarrow E' \mid \sigma|_F = \sigma \}| \leq [E:F]$. Moreover, equality holds, if $f$ do not have multiple zeros.

Proof. We proceed by induction on $[E:F]$. If all the irreducible factors of $f$ are of degree 1, then $E=F$ and $E'=F'$; and so clearly equality holds.

Now suppose $f_1(x)$ is an irreducible factor of $f(x)$ that has degree $\geq 2$; and suppose $\alpha$ is a zero of $f_1(x)$. Then for any $\sigma : E \rightarrow E'$, $\sigma(\alpha)$ is a zero of $\sigma(f_1)(x)$.

Hence $\sigma|_{\text{Fix}_\sigma}$ has at most # of distinct zeros of $\sigma(f_1)$ possibilities. For any given such possibilities, by the strong induction hypothesis, there are at most $[E:F_{\text{Fix}}] - $ many possibilities of extension to an isomorphism from $E$ to $E'$. So
Lecture 26: Automorphisms of finite normal extensions

\[ |\mathcal{G} : E \rightarrow E'| G|_F = \sigma(G) \leq (\text{# of distinct zeros of } f) \]

\[ = \deg f \cdot [E:F] \]

Suppose \( f \) has no multiple zeros. Then \( f \) does not have multiple zeros, and \( f \) remains square-free over \( F[G] \) as it is square-free over \( F[G] \). And so by the strong induction hypothesis equality in the above inequality hold.

On the other hand, if equality holds, then all zeros of \( f \) are distinct. By a similar argument, all zeros of \( g \) are distinct. Since \( \text{gcd}(f_i, f_j) = 1 \) for \( i \neq j \), we deduce that all zeros of \( f \) are distinct; and the claim follows.

**Def.** A polynomial \( f(x) \in F[x] \setminus F \) is called **separable** if its irreducible factors do not have multiple roots.

**Corollary.** Suppose \( f(x) \in F[x] \setminus F \), and \( E \) is a splitting field of \( f(x) \) over \( F \). Then \( |\text{Aut}(E/F)| \leq [E:F] \). And equality holds exactly when \( f(x) \) is separable.
Lecture 26: Separable extensions

Def. An algebraic extension $E/F$ is called separable if $\forall \alpha \in E$, $m_{\alpha, F}(x)$ is separable.

Ex. $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ is NOT a separable extension. By Eisenstein’s criterion $x^p - t$ is irreducible in $\mathbb{F}_p(t)$, and so $m_{t^{1/p}, \mathbb{F}_p}(x) = x^p - t$.

But $x^3 - t = (x - t^p)$ has multiple zeros.

Another corollary of the previous argument is the following:

Theorem. Suppose $E/F$ is a finite extension. Then the following statements are equivalent:

1. $E$ is a splitting field of a separable polynomial $f(x)$ over $F$.

2. $|\text{Aut}(E/F)| = [E:F]$.

3. $E/F$ is a normal separable extension.

Proof. We have already proved $(1) \implies (2)$; next we show $(2) \implies (3)$. $\forall \alpha \in E$, as in the proof of previous theorem $|\text{Aut}(E/F)| \leq (# \text{ of distinct zeros of } m_{\alpha, F} \text{ in } E) [E:F[\alpha]]$.
And so 
\[
|\text{Aut}(E/F)| \leq \left( \text{# of dist. zeros of } m_\alpha \text{ in } E \right) [E:F] [\sigma_J]
\]
\[
\leq \deg m_\alpha \cdot [E:F[J = [F[J:F] [E:F[J] = [E:F[J]. \quad (\ast)
\]

Since by (2) equality holds, \# of dist. zeros of \( m_\alpha \) in \( E = \deg m_\alpha \)

And so all zeros are in \( E \) and are distinct \( \Rightarrow \) \( E/F \) is normal & \( \alpha \) separable.

(3) \( \Rightarrow \) (1) Since \( E/F \) is finite, \( \exists \alpha_1, \ldots, \alpha_n \in E \) st. \( E = F(\alpha_1, \ldots, \alpha_n) \).

Since \( E/F \) is (algebraic) normal, all zeros of \( m_{\alpha_i}(\alpha) \) are in \( E \).

And so \( E \) is a splitting field of \( \prod_{i=1}^{n} m_{\alpha_i}(\alpha) \) over \( F \). Since \( E/F \) is separable, \( \prod_{i=1}^{n} m_{\alpha_i}(\alpha) \) is a separable polynomial. \[ \square \]

Def. An algebraic extension \( E/F \) is called a Galois extension if \( E/F \) is a normal and separable extension. If \( E/F \) is Galois, we write \( \text{Gal}(E/F) \) instead of \( \text{Aut}(E/F) \).

So far we have seen that \( \text{Gal}(F/E) \) gives us \( [F:E] \) if \( F/E \) is a Galois extension. Next we will show having \( \text{Gal}(F/E) \) as a subgroup of \( \text{Aut}(F) \) uniquely determines \( E \). The following is the key technical lemma:
Lemma. Let $G$ be a finite subgroup of $\text{Aut}(E)$.

Suppose $0 \neq V \subseteq E^n$ is an $E$-subspace, and for any $\sigma \in G$ and $(e_1, \ldots, e_n) \in V$, we have $(\sigma(e_1), \ldots, \sigma(e_n)) \in V$.

Then $V^G := \{ (f_1, \ldots, f_n) \mid \forall \sigma \in G, \sigma(f_i) = f_i, f_i \neq 0 \}$.

Proof: Among all elements of $V$, take a non-zero vector with smallest possible non-zero components; say $(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0) \in V$ is such an element and $\alpha_i$'s are not zero. Hence $(1, \alpha'_1, \ldots, \alpha'_r, 0, \ldots, 0) \in V$.

$\Rightarrow \forall \sigma \in G, (1, \sigma(\alpha'_1), \ldots, \sigma(\alpha'_r), 0, \ldots, 0) \in V$

$\Rightarrow (0, \alpha'_1 - \sigma(\alpha'_1), \ldots, \alpha'_r - \sigma(\alpha'_r), 0, \ldots, 0) \in V$

Since these vectors have only at most $r-1$ non-zero components, they should be zero. Hence $(1, \alpha'_1, \ldots, \alpha'_r, 0, \ldots, 0) \in V^G$. $\blacksquare$