Lecture 26: Automorphisms of normal extensions

Tuesday, March 6, 2018 1:56 PM

In the previous lectures we proved:

① Any embedding of $E \to \overline{F}$ can be extended to an automor. of $\overline{F}$ where $F \subseteq E \subseteq \overline{F}$.

② The following are equivalent:

(a) $\forall \sigma \in \mathrm{Aut}(\overline{F}/F)$, $\sigma(E) = E$.

(b) $\forall \alpha \in E, \exists \alpha_i \in E$, $m_{\alpha,F}(x) = \prod (x - \alpha_i)$

(c) E is a splitting field of a non-empty subset $\mathcal{F} \subseteq F[x] \setminus F$.

(d) $\exists \{E_i\}_{i\in I}$ s.t.

(d-1) E_i is a splitting field of $f_i(x)$ over F $(E_i \subseteq \overline{F})$.

(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 <u>normal extension</u> if the above statements hold.)

<u>Remark.</u> (d-3) implies a finite extension E/F is normal $\Leftrightarrow$ E is a splitting field of $f(x)$ over F.

Lecture 26: Automorphisms of normal extensions

Saturday, March 3, 2018 11:00 AM

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 $$\mathrm{Aut}(\overline{F}/F) \xrightarrow{r_{E_2}} \mathrm{Aut}(E_2/F) \xrightarrow{r_{E_2/E_1}} \mathrm{Aut}(E_1/F), \qquad \mathrm{Aut}(\overline{F}/F) \xrightarrow{r_{E_1}} \mathrm{Aut}(E_1/F)$$

given by restrictions are well-defined group homomorphisms.

② $$\mathrm{Aut}(\overline{F}/F) \longrightarrow \Big\{ (\phi_E) \in \prod_{\substack{E/F \\ E:\text{ finite normal} \\ E \subseteq \overline{F}}} \mathrm{Aut}(E/F) \;\Big|\; \phi_{E_2}\big|_{E_1} = \phi_{E_1},\ \substack{E_i/F:\text{ finite, normal} \\ E_1 \subseteq E_2 \subseteq \overline{F}} \Big\}$$

$$\phi \longmapsto (\phi|_E)$$

is an isomorphism.

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

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

For any $\theta \in \mathrm{Aut}(E_i/F)$, $\exists\, \tilde{\theta}: \overline{F} \xrightarrow{\sim} \overline{F}$ s.t. $\tilde{\theta}|_{E_i} = \theta$. 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 $(\phi_E) \in \prod_{E/F:\text{ finite normal}} \mathrm{Aut}(E/F)$ and $\forall \underset{E_i/F:\text{ finite normal}}{E_1 \subseteq E_2 \subseteq \overline{F}}$, $\phi_{E_2}\big|_{E_1} = \phi_{E_1}$;

We know that $\overline{F} = \bigcup_{\substack{E \subseteq \overline{F} \\ E/F \\ \text{finite normal}}} E$; we "glue" ϕ_E s:

$\phi: \overline{F} \to \overline{F}$, $\phi(\alpha) = \phi_E(\alpha)$ if $\alpha \in E$.

Since ϕ_E s are compatible, ϕ is well-defined. One can easily check that $\phi \in \mathrm{Aut}(\overline{F}/F)$; And the claim follows. ∎

<u>Def.</u> The group given in RHS of part <u>2</u> is called the inverse limit of $\mathrm{Aut}(E/F)$'s; and it is denoted by $\varprojlim_{\substack{E/F:\text{finite} \\ \text{normal}}} \mathrm{Aut}(E/F)$.

So we proved $\mathrm{Aut}(\overline{F}/F) \simeq \varprojlim_{\substack{E/F: \\ \text{finite normal}}} \mathrm{Aut}(E/F)$.

Moreover the above proof implies:

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

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

$$\mathrm{Aut}(E_2/F)/\mathrm{Aut}(E_2/E_1) \simeq \mathrm{Aut}(E_1/F).$$

Lecture 26: Topology on group of Automorphisms of normal extensions

Tuesday, March 6, 2018 2:05 PM

Pf. We have seen $\sigma \longmapsto \sigma|_{E_1}$ is an onto group hom

$\mathrm{Aut}(E_2/F) \twoheadrightarrow \mathrm{Aut}(E_1/F)$. Its kernel is precisely $\mathrm{Aut}(E_2/E_1)$.

And so by the 1st isomorphism theorem, we are done. ∎

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

Hence $\varprojlim \mathrm{Aut}(E/F)$ is a closed subset of $\prod_{\substack{E/F:\text{ finite}\\ \text{normal}}} \mathrm{Aut}(E/F)$.

Therefore $\varprojlim \mathrm{Aut}(E/F)$ is a compact group.

(Called Krull topology)

If $F \subseteq K \subseteq L \subseteq \overline{F}$ and L/F and K/F are normal, then

$$\begin{array}{ccc}
\mathrm{Aut}(L/F) & \twoheadrightarrow & \mathrm{Aut}(K/F) \\
\wr\wr & \circlearrowleft & \wr\wr \\
\varprojlim\limits_{\substack{E\subseteq L\\ E/F:\text{ finite}\\ \text{normal}}} \mathrm{Aut}(E/F) & \twoheadrightarrow & \varprojlim\limits_{\substack{E\subseteq K\\ E/F:\text{ finite}\\ \text{normal}}} \mathrm{Aut}(E/F)
\end{array}$$

$\boxed{\mathrm{Aut}(L/K) \text{ is a closed normal subgp of } \mathrm{Aut}(L/F)}$

projection to those components $\} \Rightarrow$ and so it is continuous.

Now we focus on finite normal extensions.

Lecture 26: Automorphisms of finite normal extensions

Saturday, March 3, 2018 11:52 PM

<u>Theorem</u>. Let $\sigma: F \xrightarrow{\sim} F'$, 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 $|\{\tilde{\sigma}: E \xrightarrow{\sim} E' \mid \tilde{\sigma}|_F = \sigma\}| \leq [E:F]$. Moreover equality holds, if f do not have multiple zeros.

<u>Pf.</u> We proceed by induction on $[E:F]$. If all the irred. 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 irredu. factor of $f(x)$ that has degree ≥ 2; and suppose α is a zero of $f_1(x)$. Then for any $\tilde{\sigma}: E \xrightarrow{\sim} E'$, $\tilde{\sigma}(\alpha)$ is a zero of $\sigma(f_1)(x)$.

Hence $\tilde{\sigma}|_{F[\alpha]}$ has at most # of distinct zeros of $\sigma(f_1)$ possibilities. For any given such possibilities, by the strong induction hypoth. there are at most $[E:F[\alpha]]$-many possibil. of extension to an isomorphism from E to E'. So

Lecture 26: Automorphisms of finite normal extensions

Sunday, March 4, 2018 12:13 AM

$$|\{\tilde{\sigma}: E \xrightarrow{\sim} E' \mid \tilde{\sigma}|_F = \sigma\}| \leq (\#\text{ of distinct zeros of } f_1)\,[E:F[\alpha]]$$

$$\leq \deg f_1\,[E:F[\alpha]]$$

$$= [F[\alpha]:F]\,[E:F[\alpha]] = [E:F[\alpha]].$$

Suppose f has no multiple zeros. Then f_1 does not have multiple zeros, and f remains square-free over $F[\alpha][x]$ as it is square-free over $\overline{F}[x]$. And so by the strong induction hypothesis equality in the above inequal. hold.

On the other hand, if equality holds, then all zeros of f_1 are distinct. By a similar argument, all zeros of f_i are distinct. Since $\gcd(f_i, f_j) = 1$ 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 $|\mathrm{Aut}(E/F)| \leq [E:F]$. And equality holds exactly when $f(x)$ is separable.

Lecture 26: Separable extensions

Saturday, March 3, 2018 11:27 PM

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 Eisenestein's criterion $x^p - t$ is irreducible in $\mathbb{F}_p(t)$, and so $m_{t^{1/p}}(x) = x^p - t$. But $x^p - t = (x - t^{1/p})^p$ 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) $|\mathrm{Aut}(E/F)| = [E:F]$.

(3) E/F is a normal separable extension.

Pf.. We have already proved $(1) \Longrightarrow (2)$;

Next we show $(2) \Rightarrow (3)$. $\forall \alpha \in E$, as in the proof of previous theorem

$|\mathrm{Aut}(E/F)| \leq (\#\text{ of distinct zeros of } m_{\alpha,F} \text{ in } E)\,[E:F[\alpha]]$

Lecture 26: Galois extensions

Sunday, March 4, 2018 1:21 PM

And so $|\mathrm{Aut}(E/F)| \leq$ (# of disti. zeros of m_α in E) $[E:F[\alpha]]$

$$\leq \deg m_\alpha \cdot [E:F[\alpha]] = [F[\alpha]:F][E:F[\alpha]]$$

$$= [E:F[\alpha]]. \qquad (*)$$

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

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

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

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

And so E is a splitting field of $\prod_{i=1}^{n} m_{\alpha_i}(x)$ over F. Since

E/F is separable, $\prod_{i=1}^{n} m_{\alpha_i}(x)$ is a separable polynomial. ■

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 $\mathrm{Gal}(E/F)$ instead of $\mathrm{Aut}(E/F)$.

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

Lecture 26: Non-zero set of fixed points

Sunday, March 4, 2018 9:49 PM

Lemma. Let G be a finite subgroup of $\mathrm{Aut}(E)$.

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

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

Pf. Among all elements of V, take a non-zero vector with smallest possible non-zero components; say $(\alpha_1, \dots, \alpha_r, 0, \dots, 0) \in V$ is such an element and α_i's are not zero. Hence $(1, \alpha_2', \dots, \alpha_r', 0, \dots, 0) \in V$.

$\Rightarrow \forall \sigma \in G, \ (1, \sigma(\alpha_2'), \dots, \sigma(\alpha_r'), 0, \dots, 0) \in V$

$\Rightarrow (0, \alpha_2' - \sigma(\alpha_2'), \dots, \alpha_r' - \sigma(\alpha_r'), 0, \dots, 0) \in V$

Since these vectors have only at most $r-1$ non-zero components, they should be zero. Hence $(1, \alpha_2', \dots, \alpha_r', 0, \dots, 0) \in V^G$. ■