Lecture 25: Uniqueness of algebraic closure

Friday, March 2, 2018 12:39 PM

We were proving the following:

<u>Theorem.</u> Let F be a field, and E, E' be two algebraic closures of F. Suppose $\sigma_0 : F \to E'$ is an embedding. Then $\exists\, \tilde{\sigma} : E \xrightarrow{\sim} E'$, s.t. $\tilde{\sigma}|_F = \sigma_0$.

We considered the set $\Sigma := \{(K, \sigma) \mid F \subseteq K \subseteq E,\ \sigma : K \hookrightarrow E' \text{ s.t. } \sigma|_F = \sigma_0\}$

We said $(K_1, \sigma_1) \preccurlyeq (K_2, \sigma_2)$ if $K_1 \subseteq K_2$ and $\sigma_2|_{K_1} = \sigma_1$.

Using Zorn's lemma, we proved Σ has a maximal element.

Say (K, σ) is a maximal element of Σ. Then we claimed:

- $K = E$.

<u>Pf.</u> If not, $\exists\, \alpha \in E \setminus K$. Let $m_\alpha(x) \in F[x]$ be the minimal polynomial of α over F. Since E is algebraically closed, $\exists\, \alpha = \alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in E$ s.t. $m_\alpha(x) = (x-\alpha)(x-\alpha_1)\cdots(x-\alpha_{m-1})$. And so $K[\alpha, \alpha_1, \ldots, \alpha_{m-1}]$ is the splitting field of $m_\alpha(x)$ over K. Thus, by part (1),

$\exists\, \tilde{\sigma} : K[\alpha, \alpha_1, \ldots, \alpha_{m-1}] \hookrightarrow E'$, $\tilde{\sigma}|_K = \sigma$. Hence

$(K, \sigma) \underset{\neq}{\preccurlyeq} (K[\alpha, \ldots, \alpha_{m-1}], \tilde{\sigma})$, which is a contradiction.

Lecture 25: Uniqueness of algebraic closure

Thursday, March 1, 2018 10:03 PM

<u>Claim.</u> $\sigma: E \hookrightarrow E'$ is onto.

<u>Pf.</u> Let $K' := \sigma(E)$; and $\theta: K' \xrightarrow{\sim} E$, $\theta(a') = \sigma^{-1}(a')$.

Suppose $E' \neq K'$; and let $\alpha' \in E' \setminus K'$. As before, there is a subfield L' of E' which is the splitting field of the minimal poly. $m_{\alpha'}(x)$ of α' over K'. Then, by part (1), $\exists\, \tilde{\theta}: L' \hookrightarrow E$ s.t. $\tilde{\theta}|_{K'} = \theta$. This implies $\tilde{\theta}(\alpha') \in E = \theta(K') = \tilde{\theta}(K')$ which implies $\tilde{\theta}$ is not injective; and this is a contradiction. ■

A lot of mathematics is about understanding symmetries of an algebraic closure $\overline{F}$ of F.

<u>Def.</u> Let E/F be a field extension. Then

$$\mathrm{Aut}(E/F) := \{\sigma: E \xrightarrow{\sim} E \mid \sigma|_F = \mathrm{id}.\}.$$

Let's start with $\sigma \in \mathrm{Aut}(\overline{F}/F)$, and assume $F \subseteq E \subseteq \overline{F}$ is a subfield. Then $\sigma|_E$ gives us an embedding of E into $\overline{F}$.

$\boxed{Q}$ What can we say about $\sigma(E)$? Under what conditions $\sigma(E) = E$?

Lecture 25: Algebraic elements under an embedding

Friday, March 2, 2018 8:35 AM

The following is the key observation:

Lemma. Let $\overline{F}$ be an algebraic closure of F, $\sigma \in \mathrm{Aut}(\overline{F}/F)$, and $\alpha \in \overline{F}$. If $f(\alpha)=0$ for some $f(x) \in F[x]$, then $f(\sigma(\alpha))=0$.

(And so σ permutes zeros of any polynomial $f(x) \in F[x]\setminus F$.)

Pf is clear.

Lemma. Suppose $\overline{F}$ is an algebraic closure of F, and $E \subseteq \overline{F}$ is a splitting field of $f(x) \in F[x]\setminus F$. Then for any $\sigma \in \mathrm{Aut}(\overline{F}/F)$, $\sigma(E)=E$.

Pf. By definition, $E = F(\alpha_1,\ldots,\alpha_n)$ and $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for some $\alpha_1,\ldots,\alpha_n \in \overline{F}$. By the previous lemma σ induces a permutation on $\{\alpha_1,\ldots,\alpha_n\}$. Hence
$$\sigma(E) = F(\sigma(\alpha_1),\ldots,\sigma(\alpha_n)) = F(\alpha_1,\ldots,\alpha_n) = E. \quad \blacksquare$$

In order to get a kind of converse statement, we need the following definition:

Def. Let $\mathcal{F} \subseteq F[x]\setminus F$ be a set consisting of monic polynomials.

Lecture 25: Normal extensions

Thursday, March 1, 2018 10:41 PM

We say E is a <u>splitting field of $\mathcal{F}$ over F</u> if

(1) $\forall f \in \mathcal{F}$, $\exists\, \alpha_{i,f} \in E$ s.t. $f(x) = \prod_i (x - \alpha_{i,f})$

(2) E is generated by F and $\alpha_{i,f}$'s as a field.

<u>Theorem.</u> Let F be a field, $\overline{F}$ be an algebraic closure of F, and $F \subseteq E \subseteq \overline{F}$ be a subfield. Then the following statements are equivalent:

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

(b) $\forall \alpha \in E$, $\exists\, \alpha_1, \ldots, \alpha_{n-1} \in E$ s.t. $m_{\alpha,F}(x) = (x-\alpha)(x-\alpha_1)\cdots(x-\alpha_{n-1})$.

(c) E is a splitting field of a set $\mathcal{F} \subseteq F[x] \setminus F$ of monic polynomials.

(d) There are $F \subseteq E_i \subseteq \overline{F}$ s.t.

(1) E_i is a splitting field of $f_i(x) \in F[x] \setminus F$. (in particular, $[E_i : F] < \infty$).

(2) $\forall\, i, j$, $\exists\, k$ s.t. $E_i \cup E_j \subseteq E_k$.

(3) $E = \bigcup_{i \in I} E_i$.

<u>Pf.</u> (a) $\Rightarrow$ (b) Let $\alpha' \in \overline{F}$ be another zero of $m_{\alpha,F}(x)$. Then $\exists\, \theta : F[\alpha] \xrightarrow{\sim} F[\alpha'] \subseteq \overline{F}$, $\theta(\alpha) = \alpha'$. Then by the previous theorem $\exists\, \tilde{\theta} \in \operatorname{Aut}(\overline{F}/F)$, $\tilde{\theta}|_{F[\alpha]} = \theta$. Since $\tilde{\theta}(E) = E$, we deduce that $\tilde{\theta}(\alpha) = \theta(\alpha) = \alpha' \in E$; and the claim follows.

Lecture 25: Normal extensions

Saturday, March 3, 2018 10:43 AM

(b) $\Rightarrow$ (c). Let $\mathcal{F} := \{m_{\alpha,F}(x) \mid \alpha \in E\}$. Then E is a splitting field of $\mathcal{F}$ over F, by definition.

(c) $\Rightarrow$ (d). Let I be the set of all the finite subsets of $\mathcal{F}$. And, for any $i \in I$, let $f_i(x) := \prod_{p \in i} p(x)$. Let E_i be the splitting field of $f_i(x)$ over F. Then, $E_i \subseteq E$; and for any i, j, if $k = i \cup j$, then $E_k \supseteq E_i \cup E_j$. Using this one can check that $\bigcup_{i \in I} E_i$ is a field. Since E is generated by zeros of $f(x) \in \mathcal{F}$, we get $E \subseteq \bigcup_{i \in I} E_i$. And so

$$E = \bigcup_{i \in I} E_i.$$

(d) $\Rightarrow$ (a) For any $\sigma \in \mathrm{Aut}(\overline{F}/F)$, we have seen that $\sigma(E_i) = E_i$. Therefore $\sigma(E) = \sigma(\bigcup_{i \in I} E_i) = \bigcup_{i \in I} \sigma(E_i) = \bigcup_{i \in I} E_i = E$; and $\bigcup_{i \in I} E_i$ is a field. $\blacksquare$

Def. We say an extension E/F is a normal extension if $E \subseteq \overline{F}$ (algebraic) and the statements of the previous theorem hold.