Math200b, lecture 19

Golsefidy

Algebraic closure.

In the previous lecture we proved:

Theorem 1 *Suppose F is a field. Then there is a field extension E/F such that E is algebraically closed.*

Today first we prove:

Proposition 2 *Suppose E/F is a field extension and E is algebraically closed. Let $L \subseteq E$ be the algebraic closure of F in E. Then L is algebraically closed.*

Proof. Suppose $p(x) \in L[x] \setminus L$. Since E is algebraically closed, there is $\alpha \in E$ such that $p(\alpha) = 0$. Hence α is algebraic over L;

and so $L[\alpha]/L$ is algebraic. Since L/F is algebraic, we deduce that $L[\alpha]/F$ is algebraic. Hence α is in the algebraic closure L of F in E, which implies that $\alpha \in L$. Therefore $p(x)$ has a zero in L, which implies that L is algebraically closed. ■

The following is an immediate corollary:

Theorem 3 *Suppose F is a field. Then there is an algebraic field extension E/F such that E is algebraically closed.*

E is called an algebraic closure of F if it satisfies properties of the previous theorem. Next we want to show that up to an isomorphism an algebraic closure is unique. We start with an important proposition.

Proposition 4 *Suppose F is a field, Ω is algebraically closed and $\sigma : F \to \Omega$ is an embedding. Suppose $f(x) \in F[x] \setminus F$ and E is a splitting field of $f(x)$ over F. Then there is $\widetilde{\sigma} : E \to \Omega$ such that $\widetilde{\sigma}|_F = \sigma$.*

Proof. Since Ω is algebraically closed, there are α_i's in Ω such that $\sigma(f) = \alpha_0 \prod_{i=1}^n (x - \alpha_i)$; notice that $\alpha_0 \in \sigma(F)$. Let $E' := \sigma(F)[\alpha_1, \ldots, \alpha_n] \subseteq \Omega$. Then it is easy to see that E' is a splitting field of $\sigma(f)$ over $\sigma(F)$. Hence by a theorem that we have proved earlier, there is a field isomorphism $\widetilde{\sigma} : E \to E'$ such that $\widetilde{\sigma}|_F = \sigma$; and claim follows. ■

Proposition 5 *Suppose* F *is a field,* $\overline{F}$ *is an algebraic closure of* F*,* Ω *is algebraically closed, and* $\sigma : F \to \Omega$ *is an embedding. Then there is* $\widetilde{\sigma} : \overline{F} \to \Omega$ *such that* $\widetilde{\sigma}|_F = \sigma$*.*

Proof. Let $\Sigma := \{(K, \theta) | \, F \subseteq K \subseteq \overline{F}, \theta : K \hookrightarrow \Omega, \theta|_F = \sigma\}$. We define a partial ordering on Σ: we say $(K_1, \theta_1) \preceq (K_2, \theta_2)$ if $K_1 \subseteq K_2$ and $\theta_2|_{K_1} = \theta_1$. It is easy to see that $(\Sigma, \preceq)$ is a POSet.

Claim. Σ has a maximal element.

Proof of Claim. By Zorn's lemma it is enough to show that any chain $\{(K_i, \theta_i)\}_{i\in I}$ in Σ has an upper bound. Let $K := \bigcup_{i\in I} K_i$ and $\theta : K \to \Omega, \theta(k) = \theta_i(k)$ if $k \in K_i$.

Step 1. K is a subfield of $\overline{F}$.

Proof of Step 1. For any $\alpha, \beta \in K \setminus \{0\}$, there are $i_0, j_0 \in I$ such that $\alpha \in K_{i_0}$ and $\beta \in K_{j_0}$. Since $\{(K_i, \theta_i)\}_{i\in I}$ is a chain, either $(K_{i_0}, \theta_{i_0}) \preceq (K_{j_0}, \theta_{j_0})$ or $(K_{j_0}, \theta_{j_0}) \preceq (K_{i_0}, \theta_{i_0})$. W.L.O.G. we can and will assume that $(K_{i_0}, \theta_{i_0}) \preceq (K_{j_0}, \theta_{j_0})$; and so $K_{i_0} \subseteq K_{j_0}$. Hence $\alpha, \beta \in K_{j_0}$; and so $\alpha \pm \beta, \alpha\beta^{\pm 1} \in K_{j_0}$. Therefore $\alpha \pm \beta, \alpha\beta^{\pm 1} \in K$; and so K is a subfield of $\overline{F}$.

Step 2. θ is well-defined.

Proof of Step 2. Suppose $k \in K_{i_0} \cap K_{j_0}$. Since Since $\{(K_i, \theta_i)\}_{i\in I}$ is a chain, either $(K_{i_0}, \theta_{i_0}) \preceq (K_{j_0}, \theta_{j_0})$ or $(K_{j_0}, \theta_{j_0}) \preceq (K_{i_0}, \theta_{i_0})$. W.L.O.G. we can and will assume that $(K_{i_0}, \theta_{i_0}) \preceq (K_{j_0}, \theta_{j_0})$; and so $K_{i_0} \subseteq K_{j_0}$ and $\theta_{j_0}|_{K_{i_0}} = \theta_{i_0}$. Therefore $\theta_{j_0}(k) = \theta_{i_0}(k)$; and so θ is well-defined.

Step 3. $\theta : K \longrightarrow \Omega$ is a ring homomorphism.

Proof of Step 3. Suppose $\alpha, \beta \in K\backslash\{0\}$. By a similar argument as in Step 1, there is $i_0 \in I$ such that $\alpha, \beta \in K_{i_0}$. And so $\alpha \pm \beta, \alpha\beta^{\pm 1} \in K_{i_0}$. Hence $\theta(\alpha) = \theta_{i_0}(\alpha)$, $\theta(\beta) = \theta_{i_0}(\beta)$, $\theta(\alpha \pm \beta) = \theta_{i_0}(\alpha \pm \beta)$, and $\theta(\alpha\beta^{\pm 1}) = \theta_{i_0}(\alpha\beta^{\pm})$. Since θ_{i_0} is a ring homomorphism, we can deduce claim of Step 3.

Step 4. Finishing proof of Claim.

It is clear that $(K_i, \theta_i) \preceq (K, \theta)$ for any $i \in I$; and so $(K, \theta) \in \Sigma$ is an upper bound for the chain $\{(K_i, \theta_i)\}_{i\in I}$; and claim follows.□

Suppose (K, θ) is a maximal element. Next we prove that $K = \overline{F}$. Suppose to the contrary that $\alpha \in \overline{F} \setminus K$. Then α is a zero of $f(x) \in F[x] \setminus F$. Let E be the splitting field of $f(x)$ over K. By the previous proposition, there is $\theta' : E \longrightarrow \Omega$ such that

$\theta'|_K = \theta$; and so $(K, \theta) \preceq (E, \theta')$ and $K \subsetneq E$, which contradicts maximality of (K, θ); and claim follows. ∎

Proposition 6 *Suppose E is an algebraic closure of F, E' is an algebraic closure of F', and $\sigma : E \hookrightarrow E'$ is an embedding such that $\sigma(F) = F'$. Then σ is surjective.*

Proof. Suppose to the contrary that there is $\alpha \in E' \setminus \sigma(E)$. Then α is algebraic over $F' \subseteq \sigma(E)$. Let $K \subseteq E'$ be a splitting field of the minimal polynomial of α over $\sigma(E)$. Then by a result that we have proved earlier, there is an embedding $\theta : K \to E$ such that $\theta|_{\sigma(E)} = \sigma^{-1}$. Then $\theta(\alpha) \in E = \theta(\sigma(E))$. Since θ is injective, we deduce that $\alpha \in \sigma(E)$, which is a contradiction. ∎

Theorem 7 *Suppose $\sigma : F \to F'$ is a field isomorphism, E is an algebraic closure of F, and E' is an algebraic closure F'. Then there is a field isomorphism $\widetilde{\sigma} : E \to E'$ such that $\widetilde{\sigma}|_F = \sigma$.*

Proof. By Proposition 5, there is $\widetilde{\sigma} : E \hookrightarrow E'$ such that $\widetilde{\sigma}|_F = \sigma$. By Proposition 6, $\widetilde{\sigma}$ is surjective and so it is an isomorphism; and claim follows. ∎

Normal extensions.

A lot of mathematics is about understanding symmetries of the field extension $\overline{F}/F$ where $\overline{F}$ is an algebraic closure of F. For a field extension E/F, we let

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

The following observation is the key in understanding $\mathrm{Aut}(\overline{F}/F)$.

Lemma 8 *Suppose* $\sigma \in \mathrm{Aut}(\overline{F}/F)$ *and* $\alpha \in \overline{F}$ *is a zero of* $f(x) \in F[x] \setminus F$. *Then* $\sigma(\alpha)$ *is a zero of* $f(x)$*; and so* σ *permutes zeros of* $f(x)$.

Proof. Suppose $f(x) = \sum_{i=0}^{n} f_i x^i$. Since α is a zero f, we have $\sum_{i=0}^{n} f_i \alpha^i = 0$; and so $\sigma(\sum_{i=0}^{n} f_i \alpha^i) = 0$. Therefore

$$0 = \sum_{i=0}^{n} \sigma(f_i)\sigma(\alpha)^i = \sum_{i=0}^{n} f_i \sigma(\alpha)^i,$$

which means that $\sigma(\alpha)$ is a zero of $f(x)$. So σ sends zeros of f to zeros of f; and as σ is injective and the set of zeros of f is a finite set, we deduce that σ permutes zeros of f. ■

An immediate corollary of this observation is the following:

Lemma 9 *Suppose* $\overline{F}$ *is an algebraic closure of* F *and* $f(x) \in F[x] \setminus F$. *Suppose* $E \subseteq \overline{F}$ *is a splitting field of* $f(x)$ *over* F. *Then for any* $\sigma \in \mathrm{Aut}(\overline{F}/F)$ *we have* $\sigma(E) = E$.

Proof. By definition, there are $c \in F^{\times}$ and $\alpha_i \in E \subseteq \overline{F}$ such that $f(x) = c \prod_{i=1}^{n}(x - \alpha_i)$ and $E = F[\alpha_1, \ldots, \alpha_n]$. By the previous lemma, for any $\sigma \in \mathrm{Aut}(\overline{F}/F)$, we have that

$$\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\}.$$

And so $\sigma(E) = \sigma(F)[\sigma(\alpha_1), \ldots, \sigma(\alpha_n)] = F[\alpha_1, \ldots, \alpha_n] = E$. ■

In order to get a kind of converse of the above Lemma, we need to consider more general splitting fields:

suppose $\mathcal{F} \subseteq F[x] \setminus F$ is a non-empty subset. We say E is a splitting field of $\mathcal{F}$ over F if there are $\alpha_{p,i} \in E$ for any $p \in \mathcal{F}$ such that

(a) $p(x) = c_p \prod_i (x - \alpha_{p,i})$ for some $c_p \in F^{\times}$, and

(b) $E = F[\alpha_{p,i} | \, p \in \mathcal{F}]$.

Theorem 10 *Suppose* F *is a field,* $\overline{F}$ *is an algebraic closure of* F, *and* $F \subseteq E \subseteq \overline{F}$ *is a subfield. Then the following statements are equivalent.*

1. *For any* $\sigma \in \mathrm{Aut}(\overline{F}/F)$, $\sigma(E) = E$.

2. *For any* $\alpha \in E$, *there are* $\alpha_i \in E$ *such that*

$$m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

3. *There is a non-empty subset* $\mathcal{F}$ *of* $F[x] \setminus F$ *such that* E *is a splitting field of* $\mathcal{F}$ *over* F.

4. *There is a family* $\{E_i\}_{i\in I}$ *of subfields of* $\overline{F}$, *and a family of polynomials* $\{p_i\}_{i\in I} \subseteq F[x] \setminus F$ *such that*

   (a) $E_i \subseteq \overline{F}$ *is a splitting field of* $p_i(x)$.

   (b) *For any* $i, j \in I$, *there is* $k \in I$ *such that* $E_i \cup E_j \subseteq E_k$.

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

Proof. (1)⇒(2). Suppose $\alpha' \in \overline{F}$ is a zero of $m_{\alpha,F}(x)$. Then there is an isomorphism $\sigma : F[\alpha] \to F[\alpha']$ such that $\sigma|_F = \mathrm{id}_F$ and $\sigma(\alpha) = \alpha'$. Notice that $\overline{F}$ is an algebraic closure of $F[\alpha]$ and also an algebraic closure of $F[\alpha']$. Hence by Theorem 7 there is an isomorphism $\widetilde{\sigma} : \overline{F} \to \overline{F}$ such that $\widetilde{\sigma}|_{F[\alpha]} = \sigma$; in particular, $\sigma|_F = \mathrm{id}_F$. This implies that $\widetilde{\sigma} \in \mathrm{Aut}(\overline{F}/F)$. Therefore by our assumption $\widetilde{\sigma}(E) = E$. Since $\alpha \in E$, we deduce that $\widetilde{\sigma}(\alpha) \in E$; and so $\alpha' = \sigma(\alpha) = \widetilde{\sigma}(\alpha) \in E$. Thus all the zeros of $m_{\alpha,F}(x)$ are in E; and claim follows.

(2)$\Rightarrow$ (3). Let $\mathcal{F} := \{m_{\alpha,F}(x) | \alpha \in E\}$. Then by our assumption, E is a splitting field of $\mathcal{F}$.

(3)$\Rightarrow$ (4). Let I be the set of all the finite subsets of $\mathcal{F}$. For $i \in I$, let $p_i(x) = \prod_{p \in i} p$, and $E_i \subseteq \overline{F}$ be a splitting field of $p_i(x)$ over F. For $i, j \in I$, $k := i \cup j$ is also a finite subset of $\mathcal{F}$; and it is easy to see that $E_i \cup E_j \subseteq E_k$. Let $E' := \bigcup_{i \in I} E_i$.

Claim. E' is a subfield of $\overline{F}$.

Proof of claim. For $\alpha, \beta \in E' \setminus \{0\}$, there are $i, j \in I$ such that $\alpha \in E_i$ and $\beta \in E_j$. We know that there is $k \in I$ such that $E_i \cup E_j \subseteq E_k$. Hence $\alpha, \beta \in E_k$. Therefore $\alpha \pm \beta, \alpha\beta^{\pm 1} \in E_k$; and so $\alpha \pm \beta, \alpha\beta^{\pm 1} \in E$. And claim follows. $\square$

It is clear that $E' \subseteq E$. On the other hand, E is generated by F and all the zeros of polynomials in $\mathcal{F}$; and E' contains F as a subfield and all the zeros of polynomials in $\mathcal{F}$. Hence $E \subseteq E'$. Altogether we deduce that $E' = E$.

(4)$\Rightarrow$ (1) will be proved in the next lecture. $\blacksquare$

We say E/F is a normal extension if, for some algebraic closure $\overline{F}$ of F, $E \subseteq \overline{F}$ satisfies the above properties (in particular E/F is an algebraic extension).