Lecture 8 : Algebraic Closure of a Field

Objectives

(1) Existence and isomorphisms of algebraic closures.
(2) Isomorphism of splitting fields of a polynomial.

Key words and phrases: algebraically closed field, algebraic closure, splitting field.

In the previous section we showed that all complex polynomials of positive degree split in $\mathbb{C}[x]$ as products of linear polynomials in $\mathbb{C}[x]$. While working with polynomials with coefficients in a field F, it is desirable to have a field extension K/F so that all polynomials in $K[x]$ split as product of linear polynomials in $K[x]$.

Definition 8.1. *A field F is called an* **algebraically closed field** *if every polynomial $f(x) \in F[x]$ of positive degree has a root in F.*

It is easy to see that a field F is algebraically closed if and only if $f(x)$ is a product of linear factors in $F[x]$. The fundamental theorem of algebra asserts that $\mathbb{C}$ is an algebraically closed field. Let us show that any field is contained in an algebraically closed field.

Existence of algebraic closure

Theorem 8.2. *Let k be a field. Then there exists an algebraically closed field containing k.*

Proof. (**Artin**) We construct a field $K \supseteq k$ in which every polynomial of positive degree in $k[x]$ has a root. Let S be a set of indeterminates which is in $1-1$ correspondence with set of all polynomials in $k[x]$ of degree ≥ 1. Let x_f denote the indeterminate in S corresponding to f.

Let $I = (f(x_f) \mid \deg f \geq 1)$ be the ideal generated by all the polynomials $f(x_f) \in k[S]$. We claim that I is a proper ideal of $k[S]$. Suppose to the contrary, $I = k[S]$. Then

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) \tag{1}$$

for some $g_1, g_2, \ldots, g_n \in k[S]$. The polynomial $g_1, g_2, \ldots, g_n$ involve only finitely many variables. Put $x_{f_i} = x_i$ for $i = 1, 2, \ldots, n$ and let $x_{n+1}, \ldots, x_m$ be the remaining variables in $g_1, g_2, \ldots, g_n$. Then

$$\sum_{i=1}^{n} g_i(x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_m) f_i(x_i) = 1.$$

Let E/k be an extension field in which the polynomials $f_1(x_1), \ldots, f_n(x_n)$ have roots $\alpha_1, \ldots, \alpha_n$ respectively. Putting $x_{n+1} = \ldots = x_m = 0$ and $x_i = \alpha_i$ for all $i = 1, 2, \ldots, n$ in the equation 1 we get a contradiction. Hence I is a proper ideal of $k[S]$. Let $\mathfrak{m}$ be a maximal ideal of $k[S]$ containing I. Then $K_1 = k[S]/\mathfrak{m}$ is a field. We claim that $x_f + \mathfrak{m}$ is a root of $f(x)$. Indeed, $f(x_f + \mathfrak{m}) = f(x_f) + \mathfrak{m} = \mathfrak{m}$. Thus each polynomial in $k[x]$ has a root in K_1. Repeat the procedure on K_1 to get $K_2 \supset K_1$ which has roots of all monic polynomials in $K_1[x]$. Let $K = \cup_{i=1}^{\infty} K_i$. Then K is a field. If $f(x) \in K[x]$ then $f(x) \in K_n[x]$ for some n. Hence $f(x)$ has a root in $K_{n+1} \subseteq K$. Thus K is algebraically closed. $\square$

Corollary 8.3. *Let F be a Field. Then there exists a field $K \supset F$ such that K is algebraically closed and K is algebraic over F.*

Proof. Let $L \supset F$ be an algebraically closed field. Then the field

$$K = \{a \in L \mid a \text{ is algebraic over } F\}$$

is algebraically closed and it is algebraic over F. $\square$

Definition 8.4. *Let F be a field. An extension K/F is called an* **algebraic closure of** *F if K is algebraically closed and K/F is an algebraic extension.*

Isomorphism of algebraic closures

We now show that if E_1 and E_2 are algebraic closures of a field F then they are $F-$isomorphic. As a consequence we also prove that any two splitting fields of a polynomial $f(x) \in F[x]$ are $F-$isomorphic. Extensions of embeddings of fields is one of the main observations in various arguments in Galois theory. The next result prepares us for the theorem about isomorphism of algebraic closures of a field.

Proposition 8.5. *Let $\sigma : k \to L$ be an embedding of fields where L is algebraically closed. Let α be algebraic over k and $p(x) = irr(\alpha, k)$. Let $p(x) = \sum a_i x^i \in k[x]$ and $p^\sigma(x) = \sum \sigma(a_i)x^i$. Then $\tau \to \tau(\alpha)$ is a bijection between the sets*

$$\{\tau : k(\alpha) \to L \mid \tau \text{ is an embedding and } \tau|_k = \sigma\} \longleftrightarrow \{\beta \in L \mid p^\sigma(\beta) = 0\}.$$

Proof. Let $\tau : k(\alpha) \to L$ be an embedding extending σ. Then

$$\tau(p(\alpha)) = p^\sigma(\tau(\alpha)) = 0.$$

Hence $\tau(\alpha)$ is a root of $p^\sigma(x)$. Conversely let $\beta \in L$ and $p^\sigma(\beta) = 0$. Define $\tau : k(\alpha) \to L$ by $\tau(f(\alpha)) = f^\sigma(\beta)$. We show that τ is well defined.

Suppose $f(\alpha) = g(\alpha)$. Then $(f - g)(\alpha) = 0$, so $p(x) \mid (f(x) - g(x))$. Hence $p^\sigma(x) \mid (f - g)^\sigma(x)$. Thus $p^\sigma(\beta) = (f^\sigma(\beta) - g^\sigma(\beta) = 0$. Hence $f^\sigma(\beta) = \tau(f(\alpha)) = g^\sigma(\beta) = \tau(g(\alpha))$. Thus τ is well-defined. Suppose that $f^\sigma(\beta) = \tau(f(\alpha)) = 0$. Then $p^\sigma(x) \mid f^\sigma(x)$. Since σ is an embedding, $p(x) \mid f(x)$. Thus $f(\alpha) = 0$.

□

Proposition 8.6. *Let $\sigma : k \to L$ be an embedding of fields where L is algebraically closed. Let E be an algebraic extension of k. Then there exists an embedding $\tau : E \to L$ extending σ. If E is an algebraic closure of k and L is an algebraic closure of $\sigma(k)$ then τ is an isomorphism extending σ.*

Proof. Consider the set

$$S = \{(F, \tau) \mid k \subseteq F \subseteq E \text{ are fields and } \tau : F \to L \text{ such that } \tau|_k = \sigma\}.$$

Since $(k, \sigma) \in S$, it is nonempty. Let (F, τ) and $(F', \tau') \in S$. Define

$$(F, \tau) \leq (F', \tau') \text{ if and only if } F \subseteq F' \text{ and } \tau'|_F = \tau.$$

Then S is a partially ordered inductive set. Indeed, if $\{(F_\alpha, \tau_\alpha)\}_{\alpha \in I}$ is a chain in S then $F = \cup_{\alpha \in I} F_\alpha$ is a subfield of E. Define $\tau : F \to L$ as $\tau(x) = \tau_\alpha(x)$ if $x \in F_\alpha$. Then τ is well-defined.

By Zorn's Lemma there exists a maximal element $(F, \tau) \in S$. We claim that $F = E$. Suppose there exists $\alpha \in E \setminus F$. Since α is algebraic over $F, \tau : F \to L$ can be extended to $F(\alpha) \to L$. This contradicts maximality of (F, τ). Thus $E = F$. Hence σ can be extended to an embedding of E into L.

Now suppose E is an algebraic closure of k and L is an algebraic closure of $\sigma(k)$. Since $\tau(E)$ is algebraically closed and L is algebraic over $\tau(E), L = \tau(E)$. Thus $\tau : E \to L$ is an isomorphism. $\square$

Theorem 8.7. *If E_1 and E_2 are algebraic closures of a field k then they are $k-$isomorphic.*

Proof. The identity map $k \to E_2$ can be extended to $\tau : E_1 \to E_2$ by the above proposition, τ is a $k-$isomorphism. $\square$

Theorem 8.8. *Let E and F be splitting fields of polynomial $f(x) \in k[x]$ where k is a field. Then they are k-isomorphic.*

Proof. Let F^a be an algebraic closure of F. Then it is also an algebraic closure of k. Thus there exists an embedding $\tau : E \to k^a$ extending $id_k : k \to k^a$. Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ be a factorization of $f(x)$ in $E[x]$. Then

$$f^\tau(x) = (x - \tau(\alpha_1)) \cdots (x - \tau(\alpha_n)) \in F^a[x].$$

Thus $F = k(\tau(\alpha_1), \ldots, \tau(\alpha_n)) = \tau(E)$ as k^a contains a unique splitting field of any polynomial in $k[x]$. $\square$