Advanced Algebra I

FIELD EXTENSIONS AND ALGEBRAIC CLOSURE

In this section, we are going to prove the existence and uniqueness of algebraic closure. As a consequence, we are able to show the existence and uniqueness of splitting fields.

Proposition 0.1. *Let F be a field. The following are equivalent:*

(1) *Every polynomial of $F[x]$ of degree ≥ 1 has a root in F.*
(2) *Every polynomial of $F[x]$ of degree ≥ 1 has all the roots in F.*
(3) *Every irreducible polynomial in $F[x]$ has degree ≤ 1*
(4) *If E is an algebraic extension over F, then $E = F$.*
(5) *There is a subfield $K \subset F$ such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.*

Definition 0.2. *A field F satisfying above conditions is said to be algebraically closed.*

Sketch of the proof of the Proposition. (1) $\Rightarrow$ (2) by induction on degree. And hence (1) $\Leftrightarrow$ (2) are equivalent. It's easy to see that (2) $\Leftrightarrow$ (3). We now look at (3) and (4). If E is an algebraic extension. Pick $u \in E$ algebraic over F with minimal polynomial $p(x)$. By (3), $p(x)$ has degree 1, hence $[E : F] = deg(p(x)) = 1$. In particular, $E = F$. Conversely, if there is an irreducible polynomial $p(x)$ of degree > 1, then $K[x]/(p(x))$ gives an algebraic extension of degree $deg(p(x))$. This leads to a contradiction, hence (4) implies (3).

Lastly, it's clear that (3) implies (5) by picking $K = F$. We now prove that (5) $\Rightarrow$ (4). Let E be an algebraic extension over F. For any $u \in E$, u is algebraic over K as well. Let $p_F(x), p_K(x)$ be the minimal polynomial of u over F, K respectively. By viewing $p_K(x)$ as a polynomial in F, then one has $p_F(x)|p_K(x) \in F[x]$. However, $p_K(x)$ splits in $F[x]$. It follows that $p_F(x)$ has degree 1. And hence $u \in F$. Thus $E = F$. □

We can also define the notion of algebraic closure.

Proposition 0.3. *Let F/K be an extension. The following are equivalent.*

(1) *F/K is algebraic, and F is algebraically closed.*
(2) *F/K is algebraic, and every polynomial in $K[x]$ splits in $F[x]$.*
(3) *F is a splitting field of all polynomials of K.*

Definition 0.4. *F is said to be an algebraical closure of K if F/K satisfies the above conditions.*

Proof. The proof is an easy consequence of the Prop. 0.1, we leave it to the readers. □

Theorem 0.5. *Algebraic closure exists.*

The following is due to M. Artin as it appeared in [Lang, Algebra].

Proof. Let K be a field.

Step 1. There is an extension E_1 over K such that every polynomial of degree ≥ 1 has a root in E_1.

To this end, let S be the set of all polynomials of degree ≥ 1. We consider $K[S]$ to be the polynomial ring with indeterminates x_f, for $f \in S$. Consider now an ideal $I =< f(x_f) >_{f \in S}$. We claim that $I \neq K[S]$, hence $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. The field $K[S]/\mathfrak{m}$ gives an extension E_1 over K. Now, for every $f(x) \in K[x]$, one sees that $f(\overline{x_f}) = \overline{f(x_f)} = 0 \in E$. Hence $f(x)$ has a root $\overline{x_f}$ in E_1.

It remains to show that $I \neq K[S]$. Suppose on the contrary that $I = K[S]$, in particular, $1 \in I$. We may write

$$1 = \sum_{i=1}^{r} g(X) f_i(x_{f_i}).$$

One can construct an algebraic extension F/K such that each f_i has a root u_i in F. Substitute x_{f_i} by u_i in F, one has

$$1 = \sum_{i=1}^{r} g(X) f_i(u_i) = 0 \in F,$$

which is the required contradiction.

Step 2. Inductively, one has $K = E_0 \subset E_1 \subset E_2 ....$ Let $E = \cup E_i$, then E is a field extension over K. And E is algebraically closed.

To see this, for any polynomial $f(x) = \sum a_i x^i \in E[x]$, $a_i \in E_{j_i}$ for some j_i. One can pick J maximal among j_i so that $a_i \in E_J$ for all i. Hence $f(x) \in E_J$. By construction, $f(x)$ has a root in E_{J+1}, and inductively, $f(x)$ has all its root in E_{J+d}, where $d = deg(f(x))$. Therefore, $f(x)$ has all its root in E.

Step 3. Let $E_a := \{u \in E | u \text{ is algebraic over } K\}$. Then E_a is an algebraic closure of K.

It's an easy exercise to check that E_a is a field extension over K. We leave it to the readers. It's also clear that E_a is algebraic over K. Hence, it suffices to check that E_a is algebraically closed.

To see this, one notices that every polynomial of $K[x]$ splits in E and it follows that every root of $K[x]$ is in E_a. Therefore, one has that every polynomial of $K[x]$ splits in E_a and we are done. □

Remark 0.6. *Let X be a set of indeterminantes and $K[X]$ be the polynomial ring. Let $\mathfrak{m}$ be a maximal ideal in $K[X]$. Then $K[X]/\mathfrak{m}$ is a field. There is a natural embedding $\sigma : K \to K[X]/\mathfrak{m}$ by $\sigma(k) = \bar{k}$.*

Ones might say that $K[X]/\mathfrak{m}$ is an "extension over K", which is not completely precise cause as a set $K \not\subset K[X]/\mathfrak{m}$. One can make sense of this by consider a field $E \cong K[X]/\mathfrak{m}$ and $K \subset E$.

The field E can be constructed as following: Let $K_c := K[X]/\mathfrak{m} - \sigma(K)$ and $E = K \cup K^c$. Define on E the addition and multiplication naturally then we are there.

We next work on the uniqueness of algebraic closure. The main ingredient is the following extension theorem.

Theorem 0.7 (Extension theorem)**.** *Let $\sigma : K \to L$ be an embedding to an algebraically closed field L. Let E/K be an algebraic extension. Then one can extend the embedding σ to an embedding $\bar{\sigma} : E \to L$. That is, there is an embedding $\bar{\sigma} : E \to L$ such that $\bar{\sigma}|_K = \sigma$.*

We remark that L is not necessarily an algebraic closure of K. For example, L could be something like $\overline{K(x)}$, an algebraic closure of $K(x)$.

In order to prove the uniqueness, we need the following useful Lemma.

Sketch of the proof. The staring point is an extension to a simple extension. More precisely, let $u \in E$ be algebraic over K with minimal polynomial $p(x)$. Then $p^\sigma(x)$ is an irreducible polynomial in $\sigma(K)[x]$. In L, Pick any root v of $\sigma(K)[x]$. This is possible since L is algebraically closed. One claims that there is an isomorphism (hence an embedding to L)

$$\bar{\sigma} : K(u) \to \sigma(K)(v) \subset L$$

extending σ. We leave the detail to the readers.

In order to work on the general case, we apply Zorn's Lemma to the non-empty P.O. set of fields

$$S := \{(F, \tau) | K \subset F \subset E, \tau : F \to L, \tau|_K = \sigma\}.$$

The ordering is given naturally as: $(F_1, \tau_1) \leq (F_2, \tau_2)$ if $F_1 \subset F_2$ and $\tau_1 = \tau_2|_{F_1}$.

By Zorn's Lemma, there is a maximal element, say E_m. It's easy to see that $E_m = E$. Otherwise, pick any $u \in E$, which is algebraic over K and hence over E_m. There is an extension to $E_m(u)$ as we have seen in the first paragraph. This is a contradiction to the maximality of E_m. Hence $E_m = E$. □

Lemma 0.8. *Let E/K be an algebraic extension and $\sigma : E \to E$ be an embedding such that $\sigma|_K = \mathbf{1}_K$. Then σ is an isomorphism.*

Proof. If E/K is finite, then injective implies isomorphic in the case of finite dimensional vector space.

In general, let's pick any $u \in E$. It suffices to show that u is in the image of σ. To see this, let $p(x)$ be the minimal polynomial of u over K and $u = u_1, u_2, ..., u_r$ be the roots of $p(x)$ in E. Let $E' := K(u_1, ..., u_r)$. It's clear that for each i, $\sigma(u_i) = u_j$ for some j. Hence $\sigma|_{E'}$ gives an homomorphism from E' to E'.

Now $\sigma|_{E'} : E' \to E'$ is an injective homomorphism of finite dimensional vector space E'/K. Therefore, $\sigma|_{E'}$ is an isomorphism. In particular, u is in the image of $\sigma|_{E'}$ and therefore in the image of σ. □

Corollary 0.9. *Algebraic closure of a field is unique up to isomorphism.*

Proof. Suppose that E, F are algebraic closure of K. By the extension theorem, there are embedding $\sigma : E \to F$ and $\tau : F \to E$ such that $\sigma|_K = \tau|_K = \mathbf{1}_K$.

Hence one has an embedding $\sigma \circ \tau : F \to F$, which is an isomorphism by the Lemma. Similarly, $\tau \circ \sigma$ is an isomorphism. Hence E and F are isomorphic. $\square$