16. Algebraic closures and splitting fields

16.1. **Uniqueness of algebraic closures.**

Notation: Let $\sigma : K \to L$ be a field embedding. Then σ naturally extends to a ring homomorphism $\sigma^* : K[x] \to L[x]$ given by

$$\sigma^*(a_n x^n + \ldots + a_0) = \sigma(a_n)x^n + \ldots + \sigma(a_0).$$

Lemma 16.1 (Simple Extension Lemma)**.** *Let $M(\alpha)/M$ be an algebraic extension. Suppose that $\sigma : M \to L$ is a field embedding such that the polynomial $\sigma^*(\mu_{\alpha,M})$ has a root $\beta \in L$. Then there exists a field embedding $\sigma' : M(\alpha) \to L$ s.t. $\sigma'_{|M} = \sigma$ and $\sigma'(\alpha) = \beta$.*

Proof. By Lemma 14.4 every element of $M(\alpha)$ is equal to $p(\alpha)$ for some $p(x) \in M[x]$. Define $\sigma' : M(\alpha) \to L$ by

$$\sigma'(p(\alpha)) = (\sigma^*(p))(\beta).$$

The map σ' is a field embedding as long as it is well defined. It is well defined since if $p(\alpha) = \widetilde{p}(\alpha)$ for some $p, \widetilde{p} \in M[x]$, then $\mu_{\alpha,M} \mid (\widetilde{p} - p)$, whence $\sigma^*(\mu_{\alpha,M}) \mid (\sigma^*(\widetilde{p}) - \sigma^*(p))$, and therefore $(\sigma^*(\widetilde{p}))(\beta) = (\sigma^*(p))(\beta)$ since β is a root of $\sigma^*(\mu_{\alpha,M})$. It is clear that $\sigma'(\alpha) = \beta$. Finally, $\sigma'_{|M} = \sigma$ since any element of M is represented by a constant polynomial $p \in M[x]$. $\square$

Definition. Let K/F and L/F be field extensions. A map $\iota : K \to L$ is called an <u>F-embedding</u> (resp. <u>F-isomorphism</u>) if ι is a field embedding (resp. isomorphism) and $\iota_{|F} = id_F$.

Lemma 16.2 (Main Extension Lemma)**.** *Let K/F and L/F be field extensions. Suppose that K/F is algebraic and L is algebraically closed. Then there exists an F-embedding $\sigma : K \to L$.*

Proof. Let Ω be the set of pairs (M, φ) where M is a field with $F \subseteq M \subseteq K$ and $\varphi : M \to L$ is an F-embedding. Define an order relation on Ω as follows:

$$(M, \varphi) \le (M', \varphi') \text{ if } M \subseteq M' \text{ and } \varphi'_{|M} = \varphi.$$

Note that Ω is non-empty since $(F, id) \in \Omega$.

Next we claim that any chain in Ω has an upper bound. Indeed, if $\{(M_i, \varphi_i)\}$ is a chain in Ω, let $M = \cup M_i$, and define $\varphi : M \to L$ as follows: given $\alpha \in M$, choose i s.t. $\alpha \in M_i$ and put $\varphi(\alpha) = \varphi_i(\alpha)$. Note that φ is well defined because of our order relation on Ω. It is clear that $(M, \varphi) \in \Omega$ is an upper bound for $\{(M_i, \varphi_i)\}$.

We can now apply Zorn lemma to deduce that Ω has a maximal element (M, σ). If we show that $M = K$, we will be done. Suppose not, and choose $\alpha \in K \setminus M$. By assumption, α is algebraic over F, hence also algebraic over M. Since L is algebraically closed, the polynomial $\sigma^*(\mu_{\alpha,M})$ has a root $\beta \in L$. Applying Lemma 16.1, we obtain an embedding $\sigma' : M(\alpha) \to L$ s.t. $\sigma'_{|M} = \sigma$. But then clearly, $(M, \sigma) < (M(\alpha), \sigma')$ in Ω, which contradicts maximality of (M, σ). □

We can now give the precise statement of the uniqueness theorem:

Theorem 16.3. *For any field F the algebraic closure is unique up to F-isomorphism, that is, if K and K' are two algebraic closures of F, then there exists an F-isomorphism $\varphi : K \to K'$.*

Proof. Left as an exercise. It is a fairly easy consequence of the Main Extension Lemma. □

Here is one more simple result that we shall be frequently used.

Observation 16.4. *Let K/F be an algebraic extension and $\overline{K}$ an algebraic closure of K. Then $\overline{K}$ is also an algebraic closure of F.*

Proof. Follows directly from the fact that a tower of algebraic extensions is algebraic (Lemma 15.1). □

16.2. **Splitting fields.**

Definition. Let F be a field and $f(x) \in F[x]$. An extension field K of F is called a <u>splitting field for $f(x)$</u> (over F) if

(i) $f(x)$ splits over K, that is, $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$

(ii) K is generated by F and the roots of $f(x)$, that is, $K = F(\alpha_1, \ldots, \alpha_n)$.

Lemma 16.5. *Any polynomial $p(x) \in F[x]$ has a splitting field which is unique up to F-isomorphism. Moreover, if $\overline{F}$ is a fixed algebraic closure of F, there is a unique splitting field for $p(x)$ inside $\overline{F}$.*

Proof. Existence: Let $\overline{F}$ be an algebraic closure of F. Then $f(x)$ splits over $\overline{F}$: $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ for some $\alpha_i \in \overline{F}$. Let $K = F(\alpha_1, \ldots, \alpha_n)$. It is clear that K is the unique splitting field for F inside $\overline{F}$.

Uniqueness: Exercise – follows from Theorem 16.3 and Observation 16.4. □

<u>Example 16.1:</u> Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and let $K \subseteq \mathbb{C}$ be the splitting field of $f(x)$. Let us describe K (as well as we can).

Since $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, by definition we have $K = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$, but it is clear that $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Claim. $[K : \mathbb{Q}] = 6$.

Proof.

$$\begin{tikzcd} & \mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "c"] & \\ \mathbb{Q} \arrow[ur, dash, "a"] \arrow[dr, dash, "b"'] & & K \\ & \mathbb{Q}(\omega) \arrow[ur, dash, "d"'] & \end{tikzcd}$$

Let $a = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, $b = [\mathbb{Q}(\omega) : \mathbb{Q}]$, $c = [K : \mathbb{Q}(\sqrt[3]{2})]$ and $d = [K : \mathbb{Q}(\omega)]$. Then $[K : \mathbb{Q}] = ac = bd$.

Note that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ since it is irreducible (by Eisenstein) and vanishes at $\sqrt[3]{2}$. Therefore, $a = \deg_{\mathbb{Q}}(\sqrt[3]{2}) = \deg(x^3 - 2) = 3$. Similarly $x^2 + x + 1$ is the minimal polynomial of ω over $\mathbb{Q}$, whence $b = \deg_{\mathbb{Q}}(\omega) = 2$.

Also note that $c = \deg_{\mathbb{Q}(\sqrt[3]{2})}(\omega) \leq \deg_{\mathbb{Q}}(\omega) = 2$ and $d \leq \deg_{\mathbb{Q}}(\sqrt[3]{2}) = 3$. This implies that $[K : \mathbb{Q}] = ac \leq 6$. On the other hand, $[K : \mathbb{Q}]$ is a multiple of both $a = 3$ and $b = 2$, and thus we must have $[K : \mathbb{Q}] = 6$.

Alternatively, we could argue that $c \neq 1$ for otherwise we would have $\omega \in \mathbb{Q}(\sqrt[3]{2})$ which is impossible since ω is not even real. Thus, $c = 2$ and so $[K : \mathbb{Q}] = ac = 6$. $\square$