We start with an example of a non-separable extension.

**Example 18.1.** Let $\mathbb{F}_p$ be a finite field of order $p$, let $K = \mathbb{F}_p(\zeta)$ be the field of rational functions over $\mathbb{F}_p$ in a formal variable $\zeta$ and $F = \mathbb{F}_p(\zeta^p)$. Then it is easy to see that $[K : F] = p$ and $\mu_{\zeta,F}(x) = x^p - \zeta^p \in F[x]$. Thus $\mu'_{\zeta,F}(x) = 0$, so $\zeta$ is inseparable over $F$. Alternatively observe that $x^p - \zeta^p = (x - \zeta)^p$ has a repeated root.

**Definition.** A field $F$ is called perfect if either char $F = 0$ or char $F = p$ and $\mathbb{F}_p = F$ where $\mathbb{F}_p = \{x^p : x \in F\}$.

**Theorem 18.1** (see DF, 13.5). A field $F$ admits a non-separable extension if and only if $F$ is not perfect.

18.1. **Separable degree.**

**Definition.** Let $F$ be a field and $K$ and $E$ extensions of $F$. Denote by $\text{Emb}_F(K,E)$ the set of $F$-embeddings of $K$ into $E$.

We shall be mostly interested in the case $E = \overline{F}$, an algebraic closure of $F$.

**Definition.** Let $K/F$ be an algebraic extension. For each $\alpha \in K$ define

(i) degree of $\alpha$ over $F$ $\deg_F(\alpha) = \deg \mu_{\alpha,F}(x)$

(ii) separable degree of $\alpha$ over $F$ $\text{sdeg}_F(\alpha) = \text{the number of distinct roots of } \mu_{\alpha,F}(x) \text{ in } \overline{F}$.

**Note:** (1) $\text{sdeg}_F(\alpha)$ is independent of the choice of $\overline{F}$ (exercise).
(2) $\text{sdeg}_F(\alpha) \leq \deg_F(\alpha)$, and equality holds $\iff$ $\alpha$ is separable over $F$.

**Lemma 18.2.** Let $K/F$ be an algebraic extension and $\alpha \in K$.

(a) Assume that $K = F(\alpha)$. Then $|\text{Emb}_F(K,\overline{F})| = \text{sdeg}_F(\alpha)$.

(b) Assume that $F \subseteq L \subseteq K$ with $K = L(\alpha)$. Then $|\text{Emb}_F(K,\overline{F})| = |\text{Emb}_F(L,\overline{F})| \cdot \text{sdeg}_L(\alpha)$.

**Proof.** Note that (a) is a special case of (b) with $L = F$, so we will only prove (b).

Let $R : \text{Emb}_F(K,\overline{F}) \to \text{Emb}_F(L,\overline{F})$ be the natural restriction map. It is enough to show that for each $\sigma \in \text{Emb}_F(L,\overline{F})$ there are precisely $\text{sdeg}_L(\alpha)$ distinct ways to extend $\sigma$ to some $\sigma' \in \text{Emb}_F(K,\overline{F})$.  

Since \( K = L(\alpha) \), any such extension \( \sigma' \) is completely determined by \( \sigma'(\alpha) \), and possible values of \( \sigma'(\alpha) \) are \( \overline{F} \)-roots of \( \sigma^*(\mu_{\alpha,L}(x)) \). Conversely, by Lemma 16.1 for each \( \overline{F} \)-root \( \beta \) of \( \sigma^*(\mu_{\alpha,L}(x)) \) there is an extension \( \sigma' \) of \( \sigma \) s.t. \( \sigma'(\alpha) = \beta \). Thus, the number of ways to extend \( \sigma \) to \( \sigma' \) equals 
\[
\text{# of } \overline{F} \text{-roots of } \sigma^*(\mu_{\alpha,L}(x)) = \text{# of } \overline{F} \text{-roots of } \mu_{\alpha,L}(x) = \text{sdeg}_L(\alpha).
\]
\[\square\]

**Theorem 18.3.** Let \( K/F \) be a finite extension. Then
\[
|\text{Emb}_F(K,F)| \leq [K:F],
\]
and equality holds \(\iff\) \( K/F \) is separable.

**Proof.** We use induction on \([K:F]\). Choose \( \alpha \in K \) and a subfield \( F \subseteq L \subseteq K \) with \( K = L(\alpha) \) and \( \alpha \notin L \). Thus, by Lemma 18.2 we have
\[
|\text{Emb}_F(K,F)| = |\text{Emb}_F(L,F)| \cdot \text{sdeg}_L(\alpha). \tag{***}
\]

1. Assume \( K/F \) is separable. Then clearly \( L/F \) is separable \(\Rightarrow\) by induction \( |\text{Emb}_F(L,F)| = [L:F] \). In addition, \( \alpha \) is separable over \( L \) (since \( \mu_{\alpha,L} \) divides \( \mu_{\alpha,F} \)), whence \( \text{sdeg}_L(\alpha) = \deg_L(\alpha) = [L(\alpha) : L] = [K:L] \). Hence (***) implies that \( |\text{Emb}_F(K,F)| = [L:F][K:L] = [K:F] \).

2. Now assume that \( K/F \) is not separable, and let \( \beta \in K \) be non-separable over \( F \). If \( K = F(\beta) \), then by Lemma 18.2(a) we have
\[
|\text{Emb}_F(K,F)| = \text{sdeg}_F(\beta) < \deg_F(\beta) = [K:F].
\]
If \( K \neq F(\beta) \), we can assume in the construction of \( L \) that \( \beta \in L \). Then \( L/F \) is also non-separable, whence by induction \( |\text{Emb}_F(L,F)| < [L:F] \). Since \( \text{sdeg}_L(\alpha) \leq \deg_L(\alpha) = [K:L] \), using (***) again we get
\[
|\text{Emb}_F(K,F)| < [L:F] \cdot [K:L] = [K:F].
\]
\[\square\]

18.2. **Primitive Element Theorem.**

**Theorem 18.4 (Primitive Element Theorem).** Let \( K/F \) be a finite separable extension. Then \( K = F(\gamma) \) for some \( \gamma \in K \).

**Proof.** First consider the case of finite \( F \). Then \( K \) is also finite, and we know from [Algebra I, Lecture 25] that the multiplicative group \( K^* \) is cyclic. If \( \alpha \) is any generator of \( K^* \), then trivially \( F(\alpha) = K \).

Now assume that \( F \) is infinite. We know that \( K = F(\alpha_1, \ldots, \alpha_n) \) for some \( \alpha_1, \ldots, \alpha_n \in K \). Since \( F(\alpha_1, \ldots, \alpha_{n-1})/F \) is also separable, it is enough to do the case \( n = 2 \).
So, assume that $K = F(\alpha, \beta)$ and let $n = [K : F]$. By Theorem 18.3 we have $|Emb_F(K, F)| = n$, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of $K$ into $F$.

**Claim.** There exists $c \in F$ s.t. the elements $\sigma_1(\alpha + c\beta), \ldots, \sigma_n(\alpha + c\beta)$ are all distinct.

**Proof of the Claim.** We will show that there are only finitely many $c \in F$ which do NOT satisfy the claim. Since $F$ is infinite, this will imply that some $c \in F$ will satisfy the claim.

If $c \in F$ does not satisfy the claim, there must exist $i \neq j$ s.t.

$$\sigma_i(\alpha + c\beta) = \sigma_j(\alpha + c\beta). \quad (*)$$

Since $c \in F$, we have

$$\sigma_i(\alpha) + c\sigma_i(\beta) = \sigma_j(\alpha) + c\sigma_j(\beta). \quad (**)$$

Note that if $\sigma_i(\beta) = \sigma_j(\beta)$, then $\sigma_i(\alpha) = \sigma_j(\alpha)$ by (**) , whence $\sigma_i = \sigma_j$ (since $K = F(\alpha, \beta)$), which is impossible. Hence $\sigma_i(\beta) \neq \sigma_j(\beta)$, whence

$$c = \frac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\sigma_j(\beta) - \sigma_i(\beta)}.$$ 

Since only $i$ and $j$ can vary, there are finitely many possibilities for $c$. □

We can now finish the proof of Primitive Element Theorem. If $c \in F$ is s.t. $\sigma_1(\alpha + c\beta), \ldots, \sigma_n(\alpha + c\beta)$ are distinct, then the restrictions of $\sigma_1, \ldots, \sigma_n$ to the subfield $F(\alpha + c\beta)$ are also distinct. Applying Theorem 18.3 to the field $F(\alpha + c\beta)$, we get

$$[F(\alpha + c\beta) : F] \geq |Emb_F(F(\alpha + c\beta), F)| \geq n = [K : F].$$

Therefore, $K = F(\alpha + c\beta)$. □

**Example 18.2:** Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. Let us show that $K = \mathbb{Q}(\sqrt[3]{2} + \omega)$.

**Proof.** We have seen earlier that $[K : \mathbb{Q}] = 6$. Any $\mathbb{Q}$-embedding $\sigma : K \rightarrow \overline{\mathbb{Q}}$ is determined by the images of $\sqrt[3]{2}$ and $\omega$, and each element must map to an element with the same minimal polynomial. Thus, $\sqrt[3]{2}$ can map to $\sqrt[3]{2}$, $\omega \sqrt[3]{2}$ or $\omega^2 \sqrt[3]{2}$, and $\omega$ can map to $\omega$ or $\omega^2$. Overall, there are $3 \cdot 2 = 6$ possibilities.

On the other hand, the extension $K/\mathbb{Q}$ is separable since $\text{char} \mathbb{Q} = 0$. Thus by Theorem 18.3 there are $6 = [K : \mathbb{Q}]$ distinct $\mathbb{Q}$-embeddings of $K$ into $\overline{\mathbb{Q}}$, so each of the above 6 possibilities extends to a true embedding.

The proof of Theorem 18.4 shows that $K = \mathbb{Q}(\gamma)$ for any $\gamma$ which has 6 distinct images under the 6 distinct $\mathbb{Q}$-embeddings of $K$ into $\overline{\mathbb{Q}}$. Let $\gamma = \sqrt[3]{2} + \omega$. From our description the images of $\gamma$ under these embeddings
are \( \{ \omega^i \sqrt{2} + \omega^j : 0 \leq i \leq 2, \ 1 \leq j \leq 2 \} \). These 6 elements are easily seen to be distinct, and thus \( K = \mathbb{Q}(\gamma) \), as desired. \( \square \)

18.3. Transitivity of separability.

**Theorem 18.5.** Let \( K/F \) be a finite extension. The following are equivalent:

(a) \( K/F \) is separable

(b) \( K = F(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_1, \ldots, \alpha_n \) are separable over \( F \)

(c) There exist subfields \( F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K \) s.t. \( K_i = K_{i+1}(\alpha_i) \) where \( \alpha_i \) is separable over \( K_{i-1} \) for each \( i \).

**Proof.** “(a) \( \Rightarrow \) (b)” is clear

“(b) \( \Rightarrow \) (c)” is also clear: if \( \alpha_i \) is separable over \( F \), then \( \alpha_i \) is also separable over \( K_{i-1} \) (since \( \mu_{\alpha,K_i} \) divides \( \mu_{\alpha,F} \)).

“(c) \( \Rightarrow \) (a)” Applying Lemma 18.2(b) several times, we get

\[
|\text{Emb}_F(K,F)| = \prod_{i=1}^{n} \text{sdeg}_{K_{i-1}}(\alpha_i) = \prod_{i=1}^{n} \text{deg}_{K_{i-1}}(\alpha_i) = \prod_{i=1}^{n} [K_i : K_{i-1}] = [K_n : K_0] = [K : F].
\]

Hence by Theorem 18.3 \( K/F \) is separable. \( \square \)

**Corollary 18.6.** Let \( K/F \) be an algebraic extension, and suppose that \( K = F(A) \) where each \( \alpha \in A \) is separable over \( F \). Then \( K/F \) is separable.

**Proof.** If \( A \) is finite, the assertion follows directly from Theorem 18.5(b) \( \Rightarrow \) (a). The general case follows from this special case and the fact that any \( \gamma \in K \) lies in a subfield of the form \( F(B) \) where \( B \) is a finite subset of \( A \). \( \square \)

**Corollary 18.7.** Let \( K/L/F \) be a tower of algebraic extensions. Then \( K/F \) is separable \( \iff \) \( K/L \) and \( L/F \) are separable.

**Proof.** “\( \Rightarrow \)” is easy. “\( \Leftarrow \)” in the case when \( K/F \) is finite follows from the equivalence of (a) and (c) in Theorem 18.5. Finally, to prove “\( \Leftarrow \)” in the general case one can use the same trick as in the proof of Lemma 15.1 (this is left as an exercise). \( \square \)