The Primitive Element Theorem.

**The Primitive Element Theorem.** Assume that $F$ and $K$ are subfields of $\mathbb{C}$ and that $K/F$ is a finite extension. Then $K = F(\theta)$ for some element $\theta$ in $K$.

**Proof.** The key step is to prove that if $K = F(\alpha, \beta)$, then $K = F(\theta)$ for some element $\theta$ in $K$. We will find such a $\theta$ of the following form:

$$\theta = \alpha + f \beta,$$

where $f \in F$. We will assume in the rest of this proof that $\theta$ has this specific form. Note that $\theta \in K$ since $f \in F$ and $\alpha, \beta \in K$. Since $F$ is a subfield of $\mathbb{C}$, $F$ contains $\mathbb{Q}$, and is therefore infinite. Assuming that $\theta$ has the above form, we will actually prove that $K = F(\theta)$ for all but finitely many choices of $f \in F$.

Note that $\alpha, \beta \in K$, a finite extension of $F$, and hence $\alpha$ and $\beta$ are algebraic over $F$. Let $g(x)$ be the minimal polynomial for $\alpha$ over $F$. Let $h(x)$ be the minimal polynomial for $\beta$ over $F$. Then both $g(x)$ and $h(x)$ are in $F[x]$ and are irreducible over $F$. We have

$$g(x) = \prod_{i=1}^{m} (x - \alpha_i), \quad h(x) = \prod_{j=1}^{n} (x - \beta_j),$$

where $m = \deg(g(x))$, $n = \deg(h(x))$, $\alpha_1, ..., \alpha_m$ are distinct elements of $\mathbb{C}$, and $\beta_1, ..., \beta_n$ are distinct elements of $\mathbb{C}$. This follows from a result proved in class: An irreducible polynomial over a subfield of $\mathbb{C}$ cannot have multiple roots in $\mathbb{C}$.

We assume that the indexing is such that $\alpha = \alpha_1$ and $\beta = \beta_1$. For any specific subscripts $i, j$ satisfying $1 \leq i \leq m$ and $2 \leq j \leq n$, the equation

$$\alpha_i + f \beta_j = \alpha + f \beta$$

holds for exactly one $f \in \mathbb{C}$ and therefore for at most one $f \in F$. This is true because $\beta_j \neq \beta$ for $j \geq 2$. Since $F$ is infinite, we can therefore suppose from here on that $f$ is chosen so that none of the above equations hold. That is, since $\theta = \alpha + f \beta$, we can assume that

$$\theta \neq \alpha_i + f \beta_j \text{ for all } i, j \text{ satisfying } 1 \leq i \leq m, \ 2 \leq j \leq n.$$

Let $E = F(\theta)$. Since $\theta \in K$, $E$ is a subfield of $K$. Consider the polynomial $k(x) = g(\theta - f x)$. One can use the binomial theorem to write $k(x)$ as a polynomial. Its coefficients will be in $\mathbb{C}$. More precisely, since $g(x) \in F[x]$, $f$ and $\theta$ are in the field $E$, and $F[x] \subseteq E[x]$, it follows that $k(x) \in E[x]$. Notice also that

$$K = F(\alpha, \beta) = F(\alpha, \beta, \alpha + f \beta) = F(\beta, \alpha + f \beta) = F(\theta, \beta) = E(\beta).$$
We will prove that \( K = E \) by showing that \([K : E] = 1\). Let \( p(x) \) denote the minimal polynomial for \( \beta \) over \( E \). Since \( K = E(\beta) \), we can say that \([K : E] = \deg(p(x))\). Hence we must show that \( \deg(p(x)) = 1 \).

By definition, \( \beta \) is a root of \( h(x) \). Since \( h(x) \in F[x] \subseteq E[x] \), it follows that \( p(x)|h(x) \) in \( E[x] \).

Therefore, the set of roots of \( p(x) \) in \( C \) must be a subset of the set \( \{\beta_1, \ldots, \beta_n\} \). However, \( \beta \) is also a root of \( k(x) \) because

\[
k(\beta) = g(\theta - f\beta) = g(\alpha + f\beta - f\beta) = g(\alpha) = 0,
\]

using the fact that \( \alpha \) is one of the roots of \( g(x) \) in \( C \). Hence, since \( k(x) \in E[x] \), we can also say that \( p(x)|k(x) \) in \( E[x] \). We are again using the fact that \( p(x) \) is the minimal polynomial for \( \beta \) over \( E \).

Suppose that \( 2 \leq j \leq n \). We will show that \( \beta_j \) is not a root of \( k(x) \). To see this, note that \( k(\beta_j) = g(\theta - f\beta_j) \). Thus,

\[
k(\beta_j) = 0 \iff g(\theta - f\beta_j) = 0 \iff \theta - f\beta_j = \alpha_i
\]

for some index \( i \), \( 1 \leq i \leq m \). This is because the roots of \( g(x) \) in \( C \) are \( \alpha_1, \ldots, \alpha_m \). But then we would have \( \theta = \alpha_i + f\beta_j \), contrary to the way that we chose \( f \) before. It follows that, if \( 2 \leq j \leq n \), then \( \beta_j \) is not a root of \( p(x) \).

In summary, we have proved that every root of \( p(x) \) in \( C \) must be contained in the set \( \{\beta_1, \ldots, \beta_n\} \), but the elements \( \beta_2, \ldots, \beta_n \) of that set are actually not roots of \( p(x) \). Therefore, \( p(x) \) has exactly one root in \( C \), namely \( \beta_1 = \beta \). Since \( p(x) \) is irreducible over \( E \), a subfield of \( C \), \( p(x) \) cannot have multiple roots. We can therefore conclude that \( \deg(p(x)) = 1 \), as we wanted to prove. Therefore, we have proved that \( K = E = F(\theta) \).

To finish the proof of the primitive element theorem, it is clear that we can find a finite subset \( \{\gamma_1, \ldots, \gamma_t\} \) of \( K \) so that \( K = F(\gamma_1, \ldots, \gamma_t) \). We will refer to such a set \( \{\gamma_1, \ldots, \gamma_t\} \) as a “generating set” for the extension \( K/F \). For example, we could simply take \( \{\gamma_1, \ldots, \gamma_1\} \) to be a basis for \( K \) as a vector space over \( F \). Suppose that \( \{\gamma_1, \ldots, \gamma_t\} \) is a generating set for the extension \( K/F \) and that \( t > 1 \). We will show that we can find another generating set for \( K/F \) which has only \( t - 1 \) elements. Consider the field \( F(\gamma_1, \gamma_2) \), which is a subfield of \( K \) and therefore a finite extension of \( F \). Taking \( \alpha = \gamma_1 \) and \( \beta = \gamma_2 \), the result proved above shows that we have \( F(\gamma_1, \gamma_2) = F(\theta_1) \) for some suitably chosen element \( \theta_1 \) in \( K \). If \( t = 2 \), we are done. If \( t > 2 \), then we have

\[
K = F(\gamma_1, \ldots, \gamma_t) = F(\gamma_1, \gamma_2)(\gamma_3, \ldots, \gamma_t) = F(\theta_1)(\gamma_3, \ldots, \gamma_t) = F(\theta_1, \gamma_3, \ldots, \gamma_t),
\]

and so we do have a generating set \( \{\theta_1, \gamma_3, \ldots, \gamma_t\} \) for \( K \) over \( F \) with just \( t - 1 \) elements. Continuing, we eventually find a generating set for \( K/F \) with just one element. This proves the Primitive Element Theorem.