The Primitive Element Theorem.

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

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

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

where $f \in F$. We will assume in the rest of this proof that θ has this specific form. Note that $\theta \in K$ since $f \in F$ and $\alpha, \beta \in K$. Since F is a subfield of $\mathbf{C}$, F contains $\mathbf{Q}$, and is therefore infinite. Assuming that θ 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 α and β are algebraic over F. Let $g(x)$ be the minimal polynomial for α over F. Let $h(x)$ be the minimal polynomial for β over F. Then both $g(x)$ and $h(x)$ are in $F[x]$ and are irreducible over F. We have

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

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

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

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

holds for exactly one $f \in \mathbf{C}$ and therefore for at most one $f \in F$. This is true because $\beta_j \neq \beta$ for $j \ge 2$. 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

$$\theta \;\neq\; \alpha_i + f\beta_j \;\; for\ all\ i, j\ satisfying \;\; 1 \le i \le m, \;\; 2 \le j \le n \quad .$$

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

$$K \;=\; F(\alpha, \beta) \;=\; F(\alpha, \beta, \alpha + f\beta) \;=\; F(\beta, \alpha + f\beta) \;=\; F(\theta, \beta) = E(\beta) \quad .$$

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

By definition, β 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 $\mathbf{C}$ must be a subset of the set $\{\beta_1, ..., \beta_n\}$. However, β is also root of $k(x)$ because

$$k(\beta) \;=\; g(\theta - f\beta) \;=\; g(\alpha + f\beta - f\beta) \;=\; g(\alpha) \;=\; 0\;,$$

using the fact that α is one of the roots of $g(x)$ in $\mathbf{C}$. 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 β over E.

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

$$k(\beta_j) = 0 \quad\Longrightarrow\quad g(\theta - f\beta_j) = 0 \quad\Longrightarrow\quad \theta - f\beta_j = \alpha_i$$

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

In summary, we have proved that every root of $p(x)$ in $\mathbf{C}$ must be contained in the set $\{\beta_1, ..., \beta_n\}$, but the elements $\beta_2, ..., \beta_n$ of that set are actually not roots of $p(x)$. Therefore, $p(x)$ has exactly one root in $\mathbf{C}$, namely $\beta_1 = \beta$. Since $p(x)$ is irreducible over E, a subfield of $\mathbf{C}$, $p(x)$ cannot have multiple roots. We can therefore conclude that $deg\big(p(x)\big) = 1$, 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 $\{\gamma_1, ..., \gamma_t\}$ of K so that $K = F(\gamma_1, ..., \gamma_t)$. We will refer to such a set $\{\gamma_1, ..., \gamma_t\}$ as a *"generating set"* for the extension K/F. For example, we could simply take $\{\gamma_1, ..., \gamma_t\}$ to be a basis for K as a vector space over F. Suppose that $\{\gamma_1, ..., \gamma_t\}$ 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 θ_1 in K. If $t = 2$, we are done. If $t > 2$, then we have

$$K \;=\; F(\gamma_1, ..., \gamma_t) \;=\; F(\gamma_1, \gamma_2)(\gamma_3, ..., \gamma_t) \;=\; F(\theta_1)(\gamma_3, ..., \gamma_t) \;\; = F(\theta_1, \gamma_3, ..., \gamma_t),$$

and so we do have a generating set $\{\theta_1, \gamma_3, ..., \gamma_t\}$ 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.