## The primitive element theorem.

We assume that $E$ and $F$ are subfields of an algebraic closed field $K$ on this handout.

**The primitive element theorem.** Suppose that $E$ is a field of characteristic zero and that $F$ is a finite extension of $E$. Then $F = E(\theta)$ for some element $\theta$ in $F$.

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

$$\theta = \alpha + e\beta$$

where $e \in E$. Since $char(E) = 0$, the field $E$ is infinite. We will actually prove that $F = E(\theta)$ for all but finitely many $e \in E$.

Let $f(x) \in E[x]$ be the minimal polynomial for $\alpha$ over $E$. Let $g(x) \in E[x]$ be the minimal polynomial for $\beta$ over $E$. Then $f(x)$ and $g(x)$ are both irreducible over $E$. We have

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

where $m = deg\big(f(x)\big)$, $\;n = deg\big(g(x)\big)$, $\;\alpha_1, ...\alpha_m$ are distinct elements of $K$, and $\beta_1, ..., \beta_n$ are distinct elements of $K$. This follows from the facts that $char(E) = 0$, $f(x)$ and $g(x)$ are irreducible over $E$, and therefore cannot have a multiple root in $K$.

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

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

holds for exactly one $e \in K$ and therefore for at most one $e \in E$. This is true because $\beta_j \neq \beta$ for $j \ge 2$. Since $E$ is infinite, we can therefore suppose from here on that $e$ is chosen so that none of the above equations hold. That is, we can assume that

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

Let $F' = E(\theta)$, a subfield of $F$. Consider the polynomial $h(x) = f(\theta - ex)$. Since $e, \theta \in F'$ and $f(x) \in E[x] \subseteq F'[x]$, it follows that $h(x) \in F'[x]$. Notice also that

$$F \;=\; E(\alpha, \beta) \;=\; E(\alpha, \beta, \alpha + e\beta) \;=\; E(\beta, \alpha + e\beta) \;=\; E(\theta, \beta) = F'(\beta)$$

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

Note that $\beta$ is a root of $g(x)$. Since $g(x) \in E[x] \subseteq F'[x]$, it follows that $p(x)|g(x)$ in $F'[x]$. Therefore, the set of roots of $p(x)$ in $K$ must be a subset of the set $\{\beta_1, ..., \beta_n\}$. However, $\beta$ is also root of $h(x)$ because

$$h(\beta) \;=\; f(\theta - e\beta) \;=\; f(\alpha + e\beta - e\beta) \;=\; f(\alpha) \;=\; 0_K \;,$$

using the fact that $\alpha$ is one of the roots of $f(x)$ in $K$. Hence, since $h(x) \in F'[x]$, we can also say that $p(x)|h(x)$ in $F'[x]$.

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

$$h(\beta_j) = 0_K \implies f(\theta - e\beta_j) = 0_K \implies \theta - e\beta_j = \alpha_i$$

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

In summary, every root of $p(x)$ in $K$ 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 $K$, namely $\beta_1 = \beta$. Since $p(x)$ has no multiple roots, we can conclude that $deg\big(p(x)\big) = 1$, as we wanted to prove. Therefore, $F = F' = E(\theta)$.

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

$$F \;=\; E(\gamma_1, ..., \gamma_k) \;=\; E(\gamma_1, \gamma_2)(\gamma_3, ..., \gamma_k) \;=\; E(\theta_1, \gamma_3, ..., \gamma_k) \;\;,$$

and so we do have a generating set $\{\theta_1, \gamma_3, ..., \gamma_k\}$ with just $k - 1$ elements. Continuing, we eventually find a generating set for $F/E$ with just one element. This proves the Primitive Element Theorem.