Notes on Simple Extensions: The purpose of these notes is to re-write the proof in Herstein about simple roots.

Theorem 0.1 *Suppose F and K are fields of characteristic 0 with $F \subset K$. Suppose that $a, b \in K$ are algebraic over F. Then there exists an algebraic number $c \in F(a, b)$ such that $F(a, b) = F(c)$.*

Proof: Without loss of generality, assume that K contains all the roots of all the polynomials we consider and every element that we consider.

We're going to set $c = a + \lambda b$ for some $\lambda \in F - \{0\}$. This will guarantee that $c \in F(a, b)$ and $F(c) \subset F(a, b)$. The strategy is to show that there is a choice of λ which forces $b \in F(c)$. But then $a = c - \lambda b \in F(c)$ as well. This means that $F(c) = F(a, b)$.

Let f be the minimal polynomial for a and let g be the minimal polynomial for b. Call λ *bad* if there are roots a' of f and b' of g such that $a' \neq a$ and $b' \neq b$ and $a' + \lambda b' = a + \lambda b$. Otherwise call λ *good*. If λ is bad, we can solve for λ in terms of a, b, a', b'. Hence, there are only finitely many bad choices. Since F has characteristic 0, there are infinitely many possible choices of λ. So, we make a good choice of λ.

Consider the polynomial $h(x) = f(c - \lambda x)$. This polynomial is defined over $F(c)[x]$. Note that $a = c - \lambda b$. Since $h(b) = f(a) = 0$ the element b is a root of $h(x)$. Hence, the minimal polynomial of b in $F(c)[x]$ divides $h(x)$. Call this polynomial $m(x)$. Since b is a root of $g(x)$, we see that $m(x)$ also divides $g(x)$ in $F(c)[x]$.

Suppose we knew that $m(x)$ has degree 1. Then, since $m(b) = 0$, we would have $m(x) = x - b$. But the coefficients of $m(x)$ are in $F(c)$. This means that $b \in F(c)$.

We will suppose that $m(x)$ has degree greater than 1 and derive a contradiction. Since K has characteristic 0 and m has degree greater than 1 there is some other root $b' \neq b \in K$ of m. (See the lemma after this proof.)

Since $m(b') = 0$ we have $h(b') = 0$ and $g(b') = 0$. In particular,

$$h(b') = f(c - \lambda b') = 0.$$

But then $a' = c - \lambda b'$ is a root of f. But then $c = a' + \lambda b'$ where a' is a root of f and b' is a root of g and $a' \neq a$ and $b' \neq b$. This contradicts the goodness of λ. ♠

There is one missing ingredient, another result from the same section in Herstein. In the application, $E = F(c)$.

Lemma 0.2 *Suppose that $m(x)$ is an irreducible polynomial in $E[x]$ and E is a field of characteristic 0. Then m does not have multiple roots.*

Proof: Let $m'(x)$ denote the formal derivative of m. Since E has characteristic 0, the polynomial $m'(x)$ has degree at least 1. Let K be a splitting field for m. If we can write $m(x) = (x - b)^2 \ldots$ in $K[x]$ then $m'(b) = 0$. We can think of $m(x)$ and $m'(x)$ as polynomials over $E[x]$. Since $m(x)$ is irreducible in $E[x]$ and $m'(x)$ has lower degree, these two polynomials are relatively prime. That is, we can write

$$\lambda(x)m(x) + \mu(x)m'(x) = 1,$$

where all polynomials are defined in $E[x]$. Plugging in b we get $0 = 1$, a contradiction. ♠