Theorem 12.2.9: Let $F \subseteq E$ with $G = \text{Gal}(E/F)$.

$\text{FAE}$

1) $EG = F$, i.e., $F$ is the largest subfield of $E$ fixed by $G$.

2) Each irreducible $f(x) \in F[x]$ with a zero in $E$ is separable and has all of its zeros in $E$.

3) $E$ is the splitting of a separable $f(x) \in F[x]$. 

finite extension
A life ban on logic. If n statements $P_1, P_2, \ldots, P_n$ are said to be equivalent, it suffices to prove

$$P_1 \implies P_2 \implies \cdots \implies P_n \implies P_1$$

Proof that (1) $\implies$ (2): Let $p(x) \in \mathbb{F}[x]$

be a separable irreducible polynomial with a zero $\alpha_1 \in E_1$. Let

$$G_1(x) = \{ x(x_1) : \alpha \in \mathbb{C}_1 \} = \{ \alpha_1, x_2, \ldots, x_n \}$$

Let $h(x) = \prod_{i=1}^{n} (x - x_i) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}[x]$
$h(x)$ is fixed by $G$, so $a_i \in E_G = F$.
so $h(x) \in F[x]$. Each $a_i$ is a zero of $f(x)$
so $h(x) | f(x)$, hence $h(x) = c f(x)$

Hence all zeros of $f(x)$ are in $E$.

Proof that 2) $\implies$ 3). Assume 2) and that
$E \neq F$. Let $x_1 \in E$ with $x_1 \notin F$, and let
$f_1(x)$ be its minimal polynomial. Since
$E[x_1]$ is a zero, all of its zeros are in $E$.
Let $E_1$ be the splitting of $f_1(x)$. If $E = E_1$,
we are done. If not, let $x_2 \in E$ with
$x_2 \notin E_1$. Let $f_2(x)$ be its minimal poly.
All of its roots are in \( E \), so \( E \) contains the splitting field \( E_2 \) of \( \phi_1(x) \phi_2(x) \).

If \( E_2 \neq E \), choose an \( \alpha_3 \in E \setminus E_2 \) and repeat. Let \( E_3 \) be the splitting field for \( \phi_1(x) \phi_2(x) \phi_3(x) \). After finitely many steps like this, we find that \( E \) is a splitting field.

Proof that 3) \( \Rightarrow \) 1): Assume \( E \) is the splitting field for a separable \( f(x) \in \mathbb{F}_2[x] \).

It is also the splitting field of
If \( \Omega(x) \in E \), \[ \text{F \subset C \subset E} \]

By Thm 12.1.24
\[ [E : F] = |\text{Gal} (E/F)| = |G| \]
and \[ [E : E_G] = |\text{Gal} (E/E_G)| = |G| \]

These 2 Kolchin gaps are the same, so
\[ [E : F] = [E : E_G] \text{ so } F = E_G. \]

Q.E.D.

Cor 12.2.12 Let \( F \subset K \subset E \)
with \( E \) a Galois extension of \( F \). Then \( E \) is a Galois extension of \( K \).
If $E$ is the splitting field of $f(x) \in \mathbb{F}[x]$
with $f(x)$ separable,

since $f(x) \in K[x]$, the extension $K \subseteq E$ is a splitting field and hence

Hence, $\text{Gal}(E/K) = \{1, \sigma\}$

Example (first day of class)

$F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt[3]{2}), \quad E = \mathbb{Q}(\sqrt[3]{2}, -\sqrt[3]{2})$

$[K:F] = 3, \quad [E:K] = 2$

$G = \text{Gal}(E/F) = S_3$

$\Rightarrow$ splitting field for $x^3 = 2$. 
$K$ is not a Galois extension of $A$
$	ext{Gal}(K/A)$ is trivial,
$E$ is a Galois extension of $K$ with
$	ext{Gal}(E/K) = C_2$
$	ext{Gal}(E/F) = S_3$
$C_2$ is not a normal subgroup of $S_3$.
Con 12.2.12 Let $F \subset K \subset E$

with $E$ a Galois extension of $F$,
$E$ is a Galois extension of $K$.

Let $G = \text{Gal}(E/F)$ and $H = \text{Gal}(E/K)$

Then $H \triangleleft G$ and $E^H = K$ and $E^G = F$.

There is a 1-1 correspondence between
subgroups $H \subset G$ and intermediate
fields $K$ as above.
We will see later that $K$ is a Galois extension of $F$. If $H$ is a normal subgroup of $G$, this is part of the Fundamental Theorem of Galois Theory, coming soon.

**Def 12.1.29** An extension $F < E$ is simple if $E = F(\alpha)$. Such an $\alpha$ is primitive.
Thm 12.1.30 If the extension $F \subseteq E$ is finite and separable, then it is a simple, primitive element one.

Proof \ Suppose $F$ is finite. Then $E^*$ is cyclic. Let $\alpha$ be a generator of it. Then $E = F(\alpha)$.

Assume then that $F$ is infinite. $E = F(\mu_1, \mu_2, \ldots, \mu_n)$. We need
only consider the case $k = 2$
$E = F(\alpha, \beta)$. Let $p(x)$ and $q(y)$ be their minimal polynomials. They have zeros
$\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_n$
Let $K$ be the splitting field over $F$
$p(x), q(y)$. Then $\alpha_i, \beta_j \in K$.
$F \subset K \subset E$. 
Consider the quotients
\[ K \geq \frac{x_i - x_1}{\beta_i - \beta_1} \quad \text{for} \quad 1 \leq i \leq m. \]
Choose a \( 0 \neq u \in K \) not equal to any of the above.
Let \( X = x_1 + u \beta_1 = x + u \beta \in E \)
Claim \( E = F(X) \). It suffices to show \( x, \beta \in F(X) = K \).
Let \( h(x) \) be the minimal polynomial of \( \beta \) over \( K \). Want to show it has degree 1.

Will \( h(\beta) \neq 0 \) for all \( \beta \).

Let \( h(x) = p(x - u\beta) \in K[x] \).

\( h(\beta) = h(\beta) = p(x - u\beta) = p(x) = 0 \).

Hence \( h(x) \) divides \( k(x) \).
For $j > 1$, \( r(B_j) = \beta (x - \mu B_j) \).

Suppose this is 0. This means:
\[
x - \mu B_j = \alpha_i \quad \text{for some } i
\]

\[
m = \frac{x - x_i'}{x_i'} - \frac{\alpha_i + \mu B_j - x_i'}{B_i'}
\]

\[
\Rightarrow m = \alpha_i' - \alpha_i
\]

But $m$ was
chosen not be this.

Hence \( k(\beta_i) \neq 0 \).

CONCLUSION

\[ \begin{align*}
\kappa(\beta_i) & \neq 0 \quad \text{for } j \geq k \\
\kappa(\beta_i) & = 0 \\
\kappa(x) & = \rho(x - ux) \quad \text{is divisible by } \kappa(x) \quad \text{(the min}
Any root $\beta$ over $K$.

The only zero of $h(x)$ is $\beta$, so $h(x) = x - \beta$. Thus $\beta = \beta_1 \in K$.

$K = F(\alpha)$ and $\alpha = x - mb$

so $\alpha \in K$. Hence $F(\beta) = F(\alpha, \beta) = K$. 

\( \phi \) is our primitive element

\( \square \)