Content:

Theorem	$F \lhd E \Leftrightarrow E$ is a splitting field for a separable polynomial over F.
Question	If $F \lhd E$ and $F \subseteq K \subseteq E$, is $K \lhd E$? Yes. Is $F \lhd K$? Conditionally.
Theorem	Let $F \lhd E$. Then there is a 1 – 1 correspondence between intermediate fields of F and E (inclusive) and subgroups of Gal(E/F).
Corollary	If $F \lhd E$, then there are only finitely many intermediate fields.

Theorem $F \lhd E \Leftrightarrow E$ is a splitting field for a separable polynomial over F.

Proof:

Assume $F \lhd E$. Then $[E:F] = n < \infty$. Let $B = \{\gamma_1, \ldots, \gamma_n\}$ be a basis for E over F.

Since $[E:F]$ is finite, E is an algebraic extension.
In particular, γ_i is algebraic for each i.
Let $p_i(x) \in F[x]$ such that p_i is irreducible and $p_i(\gamma_i) = 0$.
Since $F \lhd E$ and E contains a root of $p_i(x)$ we know $p_i(x)$ is separable. Let $f(x) = p_1(x) \cdots p_n(x)$. Then f is separable.
Since E contains all roots, F splits over E.
Suppose K is a splitting field for $f(x)$ and $K \subsetneq E$.

Then there is a proper subset of B that would form a basis for K over F, a contradiction as we would lose a root.
So E is a splitting field for f.

Conversely, let $f \in F[x]$ such that f is separable. Assume E is a splitting field for f. Let $f = p_1(x) \cdots p_n(x)$ be an irreducible factorization in $F[x]$.
Since f is separable, each $p_i(x)$ have distinct roots.
Let $a_1, \ldots, a_n$ be the distinct roots of f.
Since E is a splitting field for f, $E = F(a_1, \ldots, a_n)$.
Since $a_1, \ldots, a_n$ are algebraic over F, $[F(a_1, \ldots, a_n):F] < \infty$.

We'll prove the result by induction on $[E:F]$.
If $[E:F] = 1$, then $E = F$, so $F \lhd E$.
Let $[E:F] = m > 1$ and assume that if E is a splitting field for some polynomial in $K[x]$ and $[E:K] < m$, then $K \lhd E$.
Since $[E:F] > 1$, $\exists\ a_i \in E - F$. Without loss of generality, say $a_1 \in E - F$.
Let $K = F(a)$. So $[K:F] > 1$. Thus $[E:K] < [E:F] = m$.
E is a splitting field for $f \in F[x]$, so E is a slitting field for f in $K[x]$.
Thus, by our induction hypothesis, $K \lhd E$. So then $E^{\mathrm{Gal}(E/K)} = K$.
We want to show $E^{\mathrm{Gal}(E/K)} = F$. Clearly $F \subseteq E^{\mathrm{Gal}(E/K)}$. Let $\gamma \in E^{\mathrm{Gal}(E/K)}$.
Since $F \subseteq K$, then $\mathrm{Gal}(E/K) \subseteq \mathrm{Gal}(E/F)$. So $E^{\mathrm{Gal}(E/F)} \subseteq E^{\mathrm{Gal}(E/K)} = K$.
So $\gamma \in K = F(a)$. Let deg $p_1(x) = t$.
Then since $K = F(a_1)$, $\gamma = b_0 + b_1 a + \cdots + b_{t-1}a^{t-1}$ for some $b_i \in F$.
$p_1(x)$ has distinct roots and after reordering, say $a_1, \ldots, a_t$ are the roots of $p_1(x)$.
Thus, for each a_j, $1 \le j \le t$, $\exists\ \sigma_j \in \mathrm{Gal}(E/F)$ such that $\sigma_j(a_1) = a_j$.
$\sigma_j(\gamma) = b_0 + b_1 a_j + \cdots + b_j a_j^{t-1} = \gamma$ since $\gamma \in E^{\mathrm{Gal}(E/K)}$.
Define $g(x) = (b_0 - \gamma) + b_1 x + \cdots + b_{t-1}x^{t-1} \in K[x]$. $g(a_j) = (b_0 - \gamma) + \gamma - b_0 = 0$.
Thus $g(x)$ has at least t roots or $g(x) = 0$. Since deg $g(x) \le t - 1$, $g(x) = 0$.
Thus $\gamma = b_0$ and $b_0 \in F$ so $\gamma \in F$.
$\therefore\ E^{\mathrm{Gal}(E/F)} = F$. Hence $F \lhd E$.

Question If $F \lhd E$ and $F \subseteq K \subseteq E$, is $K \lhd E$? Yes. Is $F \lhd K$? Conditionally.

Proof:
$K \lhd E$ by homework.
If $F \lhd E$, then F is a splitting field for a separable polynomial, f, over F.
Since $F \subseteq K \subseteq E$, then f is separable over K. Thus $K \lhd E$.

Theorem$(*)$ Let $F \lhd E$. Then there is a 1 – 1 correspondence between intermediate fields of F and E (inclusive) and subgroups of $\mathrm{Gal}(E/F)$.

Proof:
Let $S = \{K | K \text{ is a field}, F \subseteq K \subseteq E\}$
Let $T = \{H | H \leq \mathrm{Gal}(E/F)\}$
Define $\Phi: S \to T$ by $\Phi(K) = \mathrm{Gal}(E/K)$.
Define $\psi: T \to S$ by $\psi(H) = E^H$.
We'll show $\Phi\psi = \mathrm{Id}$ and $\psi\Phi = \mathrm{Id}$.
Let $K \in S$. $\psi\Phi(K) = \psi(\mathrm{Gal}(E/K)) = E^{\mathrm{Gal}(E/K)}$.
We want to show $E^{\mathrm{Gal}(E/K)} = K$.
Since $F \lhd E$ and $F \subseteq K \subseteq E$, then $K \lhd E$ (by HW).
$\therefore E^{\mathrm{Gal}(E/K)} = K$. Hence $\psi\Phi = \mathrm{Id}$.

Let $H \in T$.
Then $\Phi\psi(H) = \Phi(E^H) = \mathrm{Gal}(E/E^H)$.
We want to show $\mathrm{Gal}(E/E^H) = H$.
By definition, $H \subseteq \mathrm{Gal}(E/E^H)$.
Now we have $F \subseteq E^H \subseteq E$ and $F \lhd E$. So $E^H \lhd E$.
Thus $[E:E^H] < \infty$ and $E^{\mathrm{Gal}(E/E^H)} = E^H$.
Claim: $\mathrm{Gal}(E/E^H)$ is finite.
$F \lhd E \Rightarrow |\mathrm{Gal}(E/F)| = [E:F] < \infty$.
Since $\mathrm{Gal}(E/E^H) \leq \mathrm{Gal}(E/F)$, then $\mathrm{Gal}(E/E^H)$ is finite.
Claim: $|H| = |\mathrm{Gal}(E/E^H)|$
$|H| = [E:E^H] = [E: E^{\mathrm{Gal}(E/E^H)}] = |\mathrm{Gal}(E/E^H)|$.
$\therefore H \subseteq \mathrm{Gal}(E/E^H)$ and $|H| = |\mathrm{Gal}(E/E^H)| < \infty$. Thus, $H = \mathrm{Gal}(E/E^H)$.
$\therefore \Phi\psi = \mathrm{Id}$. Hence Φ is a bijection.

Corollary If $F \lhd E$, then there are only finitely many intermediate fields.

Proof:
Any intermediate field corresponds uniquely to a subgroup of $\mathrm{Gal}(E/F)$. Thus we need only show there are only finitely many subgroups of $\mathrm{Gal}(E/F)$.
Since $F \lhd E$, $\mathrm{Gal}(E/F)$ is finite, hence only finitely many subgroups.