Theorem 50.3. A field $E$, where $F \leq E \leq \bar{F}$, is a splitting field over $F$ if and only if every automorphism of $\bar{F}$ leaving $F$ fixed maps $E$ onto itself (and this induces an automorphism of $E$ leaving $F$ fixed).

Proof. (⇒) Let $E$ be a splitting field over $F$ in $\bar{F}$ of $\{ f_i(x) | i \in I \}$. Let $\sigma$ be an automorphism of $\bar{F}$ leaving $F$ fixed. Let $\{ \alpha_j | j \in J \}$ be the set of all zeros in $\bar{F}$ of all the polynomials $f_i(x)$ for $i \in I$. By Theorem 29.18, for a given $\alpha_j$ the field $F(\alpha_j)$ has as elements all expressions of the form

$$ g(\alpha_j) = a_0 + a_1 \alpha_j + a_2 \alpha_j^2 + \ldots + a_{n_j-1} \alpha_j^{n_j-1} $$

where $n_j$ is the degree of $\text{irr}(\alpha_j, F)$ and each $a_k \in F$. Consider the set $S$ of all finite sums and finite products of elements of the form $g(\alpha_j)$ where $j \in J$. Then $S \subseteq E$ is closed under addition and multiplication, it contains 0,1, and is closed under the process of taking additive inverses (just replace the coefficients of $g(\alpha_j)$ with their additive inverses).

Theorem 50.3. (Continued)

Proof. (Continued) Since each element of $S$ is in some finite extension of $F$, say $F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_k})$, then for any $s \in S$, $s \neq 0$, $s \in F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_k})$ we have $s^{-1} \in F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_k})$ and $s^{-1} \in S$. So $S$ is a subfield of $E$ and $S$ contains all $\alpha_j$ for $j \in J$. Since $E$ is the splitting of $\{ f_i(x) | i \in I \}$ over $F$, then $E$ is the smallest subfield of $\bar{F}$ containing $F$ and all $\alpha_j$ for $j \in J$ (by definition of "splitting field"), so it must be that $S = F$ since $S$ is a subfield of $F$ containing all $\alpha_j$ for $j \in I$.
Theorem 50.3. A field $E$, where $F \leq E \leq \bar{F}$, is a splitting field over $F$ if and only if every automorphism of $\bar{F}$ leaving $F$ fixed maps $E$ onto itself (and this induces an automorphism of $E$ leaving $F$ fixed).

Proof. (Continued) So $f_i(\sigma(a_j)) = 0$ also and hence $\sigma(a_j) \in E$. [Here, we see that automorphism of $\bar{F}$ which fixes $F$ is mapping the zeros of $\text{irr}(a_j, F)$ to themselves — that is, $\sigma$ is permuting the zeros of $\text{irr}(a_j, F)$—] So $\sigma[E]$ is some subfield of $E$ (as an automorphism of $\bar{F}$, we know that $\sigma$ is one to one and has the homomorphism property with respect to $+$ and $\cdot$, but we do not know that $\sigma$ is onto when restricted to $E$). We can replace $\sigma$ with $\sigma^{-1}$ above ($\sigma^{-1}$ is also an automorphism of $\bar{F}$ which fixes $F$) to conclude that $\sigma^{-1}[E]$ is also a subfield of $E$. Let $e \in E$. Then $\sigma^{-1}(e) \in E$ and so $\sigma(\sigma^{-1}(e)) = e$. So $\sigma$ maps $E$ onto $E$ and $\sigma[E] = E$. Hence $\sigma$ is an automorphism of $E$ which leaves $F$ fixed.

Corollary 50.6.

Corollary 50.6. If $E \leq \bar{F}$ is a splitting field over $F$, then every irreducible polynomial in $F[x]$ having a zero in $\bar{F}$ splits in $E$.

Proof. If $E$ is a splitting field over $F$ in $\bar{F}$, then by Theorem 50.3a (the part for which we have given a proof), every automorphism of $\bar{F}$ induces an automorphism of $E$. Let $f(x) \in F[x]$ be irreducible and let $f(x)$ have a zero $\alpha$ in $E$. If $\beta$ is any zero of $f$ in $\bar{F}$ (that is, $\beta$ is a conjugate of $\alpha$), then by Theorem 48.3 (The Conjugation Isomorphisms Theorem), there is a conjugation isomorphism $\Psi_{\alpha, \beta}$ of $F(\alpha)$ onto $F(\beta)$ which fixes $F$. By Theorem 49.3 (The Isomorphism Extension Theorem — we are really using Corollary 49.4), $\Psi_{\alpha, \beta}$ can be extended to an isomorphism $\tau$ of $\bar{F}$ into a subfield of $\bar{F}$ which fixes $F$. Now $\tau^{-1}: \tau[\bar{F}] \rightarrow \bar{F}$ (not necessarily onto) is an isomorphism of $\tau[\bar{F}]$ with a subfield of $\bar{F}$ which fixes $F$ (and maps $\beta$ to $\alpha$) and by Theorem 49.3 (The Isomorphism Extension Theorem), $\tau^{-1}$ can be extended from $\tau[\bar{F}]$ to all of $\bar{F}$ and $\tau^{-1}[\bar{F}]$ is a subfield of $\bar{F}$. Since $\tau(\alpha) = \beta \in E$. Since $\beta$ is an arbitrary zero of $f(x)$, then all zeroes of $f(x)$ are in $E$. That is, $E$ splits $f(x)$. □
Corollary 50.7. If $E \leq \bar{F}$ is a splitting field over $F$, then every isomorphic mapping of $E$ onto a subfield of $\bar{F}$ leaving $F$ fixed is actually and automorphism of $F$. In particular, if $F$ is a splitting field of finite degree over $F$, then $\{E : F\} = |G(E/F)|$, where $G(E/F)$ is the group of automorphisms of $E$ leaving $F$ fixed.

**Proof.** Every isomorphism $\sigma$ mapping $E$ onto a subfield of $\bar{F}$ leaving $F$ fixed, can be extended to an isomorphism $\tau$ of $\bar{F}$ with a subfield of $\bar{F}$ by Theorem 49.3 (The Isomorphism Extension Theorem). By the argument in the proof of Corollary 50.6 (and considering $\tau^{-1}$), we see that $\tau$ is onto $\bar{F}$ and so $\tau$ is an automorphism of $\bar{F}$. Since $E$ is a splitting field over $F$ (by hypothesis), then by Theorem 50.3, $\tau$ restricted to $E$ (that is $\sigma$ since $\tau$ is an extension of $\sigma$) is an automorphism of $E$. That is, $\sigma$ is an automorphism of $E$ and the first claim holds.

---

Corollary 50.7. (Continued)

Corollary 50.7. If $E \leq \bar{F}$ is a splitting field over $F$, then every isomorphic mapping of $E$ onto a subfield of $\bar{F}$ leaving $F$ fixed is actually and automorphism of $E$. In particular, if $E$ is a splitting field of finite degree over $F$, then $\{E : F\} = |G(E/F)|$, where $G(E/F)$ is the group of automorphisms of $E$ leaving $F$ fixed.

**Proof. (Continued)** Since $\{E : F\}$ is by definition, the number of different isomorphic mappings of $E$ onto a subfield of $\bar{F}$ leaving $F$ fixed, as shown above, such isomorphic mappings are all automorphisms of $E$ (and of course an automorphism of $E$ leaving $F$ fixed is such a mapping). Since $G(E/F)$ is the group of automorphisms of $E$ leaving $F$ fixed, the result follows.