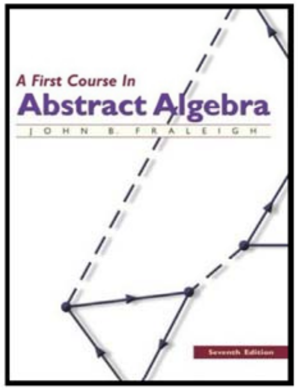
Introduction to Modern Algebra

Part X. Automorphisms and Galois Theory

X.50. Splitting Fields



Theorem 50.3.

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. ($\Rightarrow$) Let E be a splitting field over F in $\bar{F}$ of $\{f_i(x) \mid i \in I\}$. Let σ be an automorphism of $\bar{F}$ leaving F fixed. Let $\{\alpha_j \mid j \in J\}$ 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 α_j the field $F(\alpha_j)$ has as elements all expressions of the form

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

where n_j is the degree of $irr(\alpha_i, F)$ 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)

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) Since each element of S is in some finite extension of F, say $F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_r})$, then for any $s \in S$ $s \neq 0$, $s \in F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_r})$ we have $s^{-1} \in F(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_r})$ and $s^{-1} \in S$. So S is a subfield of E and S contains all α_j for $j \in J$. Since E is the splitting of $\{f_i(x) \mid i \in I\}$ over F, then E is the smallest subfield of $\bar{F}$ containing F and all α_j for $j \in J$ (by definition of "splitting field"), so it must be that $S = F$ since S is a subfield of E containing all α_j for $j \in J$.

Theorem 50.3. (Continued)

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) Since S consists of all finite sums of finite products of elements of the form $g(\alpha_j)$ for all $j \in J$ (where each g is a polynomial function with coefficients from F), then E also satisfies this — we ay that $\{\alpha_j \mid j \in J\}$ generates E over F (in the sense of taking finite sums and finite products, not in the sense of vector spaces discusses in the past). So for σ an automorphism of $\bar{F}$ which fixes F, the value of σ on E is determined by the value of $\sigma(\alpha_j)$ for $j \in J$. By Corollary 48.5, $\sigma(\alpha_j)$ must be the conjugate of α_j and so $\sigma(\alpha_j)$ must also be a zero of $irr(\alpha_j, F)$. By Theorem 29.13, the polynomial $irr(\alpha_j, F) \in F[x]$ divides $f_i(x)$ for which $f_i(\alpha_j) = 0$.

Theorem 50.3. (Continued)

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

Theorem 50.3.

Theorem 50.3. (Continued)

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) ($\Leftarrow$)

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 E 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 α in E. If β is any zero of f in $\bar{F}$ (that is, β is a conjugate of α), 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 τ of $\bar{F}$ into a subfield of $\bar{F}$ which fixes F. Now $\tau^{-1} : \tau[\bar{F}] \to \bar{F}$ (not necessarily onto) is an isomorphism of $\tau[\bar{F}]$ with a subfield of $\bar{F}$ which fixes F (and maps β to α) and by Theorem 49.3 (The Isomorphism Extension Theorem), τ^{-1} can be extended from $\tau[\bar{F}]$ to all of $\bar{F}$ and $\tau^{1-}[\bar{F}]$ is a subfield of $\bar{F}$.

Corollary 50.6.

Corollary 50.6. (Continued)

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 E splits in E.

Proof. (Continued) Since τ is defined on all of $\bar{F}$, then the range of τ^{-1} is all of $\bar{F}$. Hence, as in the proof of Theorem 50.3(a), $\tau[\tau^{-1}[\bar{F}]] = \bar{F}$ and so τ is an automorphism of $\bar{F}$ which fixes F. As commented earlier, by Theorem 50.3(a), τ induces an automorphism of E, and we have $\tau(\alpha) = \beta \in E$. Since β 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.

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. Every isomorphism σ mapping E onto a subfield of $\bar{F}$ leaving F fixed, can be extended to an isomrophism τ 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 τ^{-1}), we see that τ is onto $\bar{F}$ and so τ is an automorphism of $\bar{F}$. Since E is a splitting field over F (by hypothesis), then by Theorem 50.3, τ restricted to E (that is σ since τ is an extension of σ) is an automorphism of E. That is, σ 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. □