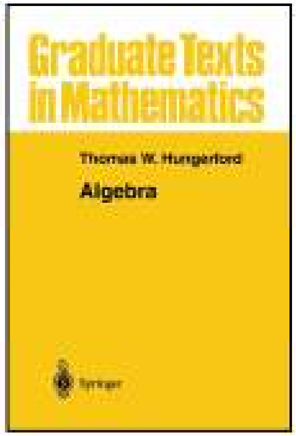
Modern Algebra

Chapter V. Fields and Galois Theory

V.3. Splitting Fields, Algebraic Closure, and Normality (Partial)—Proofs of Theorems



Theorem V.3.2

Theorem V.3.2. If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field F of f with dimension $[F : K] \leq n!$.

Proof. We prove this by induction on $n = \deg(f)$. For the base step, if $n = 1$ (or if f splits over K) then $F = K$ is a splitting field and $[F : K] = [F : F] = 1 \leq n!$.

If $n > 1$ and f does not split over K, let $g \in K[x]$ be an irreducible factor of f of degree greater than one. By Theorem V.1.10 (Kronecker's Theorem) there is a simple extension field $K(u)$ of K such that u is a root of g and $[K(u) : K] = \deg(g) > 1$. Then by Theorem III.6.6 (the Factor Theorem) we have $f(x) = (x - u)h(x)$ for some $h \in K(u)[x]$ of degree $n - 1$ (we have only used polynomial g in passing; notice $\deg(g) \leq n$). Repeating this process (and factoring f) we can produce (inductively) a splitting field F of $h \in K(u)[x]$ of degree at most $(n-1)!$. By Exercise V.3.3, F is a splitting field of f over K. By Theorem V.1.2, $[F : K] = [F : K(u)][K(u) : K] \leq (n-1)!\deg(g) \leq (n-1)!n = n!$. The result now follows by induction. □

Theorem V.3.8

Theorem V.3.8. Let $\sigma : K \to L$ be an isomorphism of fields, $S = \{f_i\}$ a set of polynomials (of positive degree) in $K[x]$, and $S' = \{\sigma f_i\}$ the corresponding set of polynomials in $L[x]$. If F is a splitting field of S over K and M is a splitting field of S' over L, then σ is extendible to an isomorphism $F \cong M$.

Proof for S a Finite Set. Suppose that S consists of a single polynomial $f \in K[x]$. Let F be a splitting field of f over K. Let $n = [F : K]$. We give an inductive proof on n. For the base case, if $n = 1$ then $F = K$ and f splits over K. So $S = \{\sigma f\}$ splits over $\sigma(K) = L$ and, since M is the splitting field of S', then $L = M$. So σ is in fact an isomorphism giving $F \cong M$ and the base case is established. If $n > 1$ then f must have an irreducible factor g of degree greater than 1 (or else F splits over K and $[F : K] = 1 \neq n$). Let u be a root of g in F. Since g is irreducible in $K[x]$ and $\sigma : K \to L$ is an isomorphism, then $\sigma g \in L[x]$ is irreducible.

Theorem V.3.8

Theorem V.3.8. Let $\sigma : K \to L$ be an isomorphism of fields, $S = \{f_i\}$ a set of polynomials (of positive degree) in $K[x]$, and $S' = \{\sigma f_i\}$ the corresponding set of polynomials in $L[x]$. If F is a splitting field of S over K and M is a splitting field of S' over L, then σ is extendible to an isomorphism $F \cong M$.

Proof for S a Finite Set (continued). If $v \in M$ is a root of σg, then by Theorem V.1.8(ii) σ extends to an isomorphism $\tau : K(u) \cong L(v)$ with $\tau(u) = v$. By Theorem V.1.6(iii) we have $[K(u) : K] = \deg(g) > 1$, we must have $n = [F : K] = [F : K(u)][K(u) : K]$ by Theorem V.1.2 and so $[F : K(u)] < n$. By Exercise V.3.2, F is a splitting field of f over (the intermediate field) $K(u)$ (here, $K \subset K(u) \subset F$) and similarly M is a splitting field of σf over (intermediate field) $L(v)$ (here, $L \subset L(v) \subset M$). So by the induction hypothesis (since $[F : K(u)] < n$) we have that τ extends to an isomorphism $F \cong M$. □

Corollary V.3.9

Corollary V.3.9. Let K be a field and S a set of polynomials (of positive degree) in $K[x]$. Then any two splitting fields of S over K are K-isomorphic. In particular, any two algebraic closures of K are K-isomorphic.

Proof. With $\sigma : K \to K$ as $\sigma = 1_K$ (the identity on K) in Theorem V.3.8, we have that if L and M are splitting fields for K (so $K \subset L$, $K \subset M$) then σ extends to an isomorphism $\tau : L \to M$ and the two splitting fields are isomorphic.

For the "in particular" claim, we need to consider the set S of all polynomials in $K[x]$. By Theorem V.3.4, the splitting field of S is the algebraic closure of K. Again, Theorem V.3.8 with $\sigma = 1_K$ yields the result. (This is also shown in Theorem V.3.6.) □

Theorem V.3.11

Theorem V.3.11. If F is an extension field of K, then the following statements are equivalent.

(i) F is algebraic and Galois over K.

(ii) F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Proof. (i) $\Rightarrow$ (ii) and (iii) If $u \in F$ has irreducible polynomial f, then as in the proof of Lemma V.2.13 (up to the "Consequently, all the roots of f are distinct and lie in E" part) f splits in $F[x]$ into a product of distinct linear factors. Hence (by definition) u is separable over K. Let $\{v_i \mid i \in I\}$ be a basis of F over K and for each $i \in I$ let $f_i \in K[x]$ be the irreducible polynomial of v_i. As just argued, each f_i is separable and splits in $F[x]$ (and also, each v_i is separable over K, by definition). Therefore F is a splitting field over K of $S = \{f_i \mid i \in I\}$ and (ii) and (iii) follow.

Theorem V.3.11 (continued 1)

Theorem V.3.11. If F is an extension field of K, then the following statements are equivalent.

(ii) F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Proof. (ii) $\Rightarrow$ (iii) [Here we need to "move" the hypothesis of separable extension to the conclusion of separable polynomials.] Let $f \in S$ where F is a splitting field over K of set S of polynomials. Let $g \in K[x]$ be a monic irreducible factor of f. Since by hypothesis f splits over K, then (by definition of "splits") f is a product of linear factors in K, and so g is the irreducible polynomial in $K[x]$ of some $u \in F$. Since by hypothesis F is separable over K, then u is separable over K (definition of separable extension) and so g is separable over K (definition of separable element $u \in F$).

Theorem V.3.11 (continued 2)

Theorem V.3.11. If F is an extension field of K, then the following statements are equivalent.

(ii) F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Proof (continued). (ii) $\Rightarrow$ (iii) So define set T to be the set of all monic irreducible factors in $K[x]$ of polynomials in set S. We have just argued that set T consists of separable polynomials in $K[x]$. By Exercise V.3.4 ("If F is a splitting field over K of [set S of polynomials in $K[x]$] then F is also a splitting field over K of the set T of all irreducible factors of polynomials in S.") F is a splitting field of set T.

Theorem V.3.11 (continued 3)

Theorem V.3.11. If F is an extension field of K, then the following statements are equivalent.

(i) F is algebraic and Galois over K.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Proof. (iii) $\Rightarrow$ (i) F is algebraic over K since any splitting field over K is (by definition of splitting field, Definition V.3.1) an algebraic extension of K. Let X be the set of all roots of polynomials in K. Then by the definition of splitting field, $F = K(X)$. Let $u \in F \setminus K'$. By Theorem V.1.3(vii) there is finite set $\{v_1, v_2, \ldots, v_n\} \subset X$ (so each v_i is a root of some $f_j \in T$) such that $u \in K(v_1, v_2, \ldots, v_n)$. Now consider the $f_1, f_2, \ldots, f_n$ which have $v_1, v_2, \ldots, v_n$ as roots (respectively). Let $u_1, u_2, \ldots, u_r$ be the set of *all* roots (in F) of $f_1, f_2, \ldots, f_n$. Thus $u \in K(v_1, v_2, \ldots, v_n) \subset K(u_1, u_2, \ldots, u_r) = E$. By Theorem V.1.12, F is a finite dimensional extension of K; that is, $[E : K]$ is finite.

Theorem V.3.11 (continued 4)

Proof (continued). (iii) $\Rightarrow$ (i) Since each $f_i \in T$ splits in F by hypothesis, E is a splitting field over K of the finite set of polynomials $\{f_1, f_2, \ldots, f_n\}$ (or equivalently, of the single polynomial $f = f_1 f_2 \cdots f_n$). "Assume for now" that the theorem (i.e., (iii)$\Rightarrow$(i)) holds in the finite dimensional case ($[F : K]$ is finite). Under this assumption, then E is Galois over K; that is, the fixed field of $\mathrm{Aut}_K E$ is E itself (Definition V.2.4). Since $u \in E \setminus K$ (we are replacing field F with finite extension field E in the current discussion), then for some $\tau \in \mathrm{Aut}_K E$ we have $\tau(u) \neq u$. By Exercise V.3.2 ("If F is a splitting field of S over K and E is an intermediate field, then F is a splitting field of S over E.") F is a splitting field of T over E. So by Theorem V.3.8 with $\tau : E \to E$ (τ is an automorphism of E and hence an isomorphism of E with itself) we have that τ can be extended to isomorphism $\sigma : F \to F$ (and so σ is an automorphism of F) where $\sigma \in \mathrm{Aut}_K F$ and $\sigma = \tau$ on E. So $\sigma(u) = \tau(u) \neq u$.

Theorem V.3.11 (continued 5)

Proof (continued). (iii) $\Rightarrow$ (i) Since u was an arbitrary element of $F \setminus K$ at the very beginning of this proof, and there exists $\sigma \in \mathrm{Aut}_K F$ such that $\sigma(u) \neq u$, then the fixed field of $\mathrm{Aut}_K F$ must be K. That is (by definition), F is Galois over K. So the theorem holds in general *if* it holds when $[F : K]$ is finite.

We now prove that the theorem holds for $[F : K]$ is finite, hence completing the proof. With $[F : K]$ finite, there exists a finite number of polynomials $g_1, g_2, \ldots, g_t \in T$ such that F is a splitting field of $\{g_1, g_2, \ldots, g_t\}$ over K. Furthermore $\mathrm{Aut}_K F$ must be a finite group by Lemma V.2.8. If K_0 is the fixed field of $\mathrm{Aut}_K F$, then F is a Galois extension of K_0 by Artin's Theorem (Theorem V.2.15). By the Fundamental Theorem (Theorem V.2.5(i)) $[F : K_0] = |\mathrm{Aut}_{K_0} F|$. Since K_0 is the fixed field of $\mathrm{Aut}_K F$ then we have $\mathrm{Aut}_{K_0} F = \mathrm{Aut}_K F$ (this is a remark on page 245). So $[F : K_0] = |\mathrm{Aut}_K F|$. Now we have $K \subset K_0 \subset F$, and so by Theorem V.1.2 we have $[F : K] = [F : K_0][K_0 : K]$.

Theorem V.3.11 (continued 6)

Proof (continued). (iii) $\Rightarrow$ (i) So if we show that $[F : K] = |\mathrm{Aut}_K F|$ then we will have that $[K_0 : K] = 1$ and so $K_0 = K$, which implies the fixed field of $\mathrm{Aut}_K F$ is $K_0 = K$; that is, F is a Galois extension of K.

We proceed by induction on $n = [F : K]$, with the case $n = 1$ being trivial (since this implies that $F = K$ and $\mathrm{Aut}_K F$ consists only of the identity on F). If $n > 1$, then one of th eg_i, say g_1, has degree $s > 1$ (otherwise all the roots of the g_i lie in K an d$F = K$). Let $u \in F$ be a root of g_1; then $[K(u) : K] = \deg(g_1) = s$ by Theorem V.1.6(iii) (we need g_1 irreducible here to apply Theorem V.1.6) and the number of distinct roots of g_1 is s since g_1 is separable in F by hypothesis.

Theorem V.3.11 (continued 7)

Proof (continued). (iii) ⇒ (i) By the second paragraph of the proof of Lemma V.2.8 (with $L = k$, $M = K(u)$ and $f = g_1$) we have that there is an injective map from the set of all left cosets of $H = \text{Aut}_{K(u)}F$ (this is set S in Lemma V.2.8; and $M' = H = \text{Aut}_{K(u)}F$ in $\text{Aut}_K F$ (in Lemma V.2.8, with $L' = \text{Aut}_L F$) to the set of all roots of g_1 in F (set T in Lemma V.2.8), given by $\sigma H \mapsto \sigma(u)$ (in Lemma V.2.8, the mapping is $\tau M' \mapsto \tau(u)$ so the $\tau \in L' = \text{Aut}_L F$ of Lemma V.2.8 equals the $\sigma \in \text{Aut}_K F = K'$ here). Therefore since the mapping is injective (one to one) then the number of left cosets of $H = \text{Aut}_{K(u)}F$ in $\text{Aut}_K F$ is less than or equal to the number of roots of g_1; that is, $[\text{Aut}_K F : H] \le s$. Now if $v \in F$ is any other root of g_1 (which exists since $\deg(g_1) = s > 1$), there is an isomorphism $\tau : K(u) \cong K(v)$ with $\tau(u) - v$ and $\tau|_K = 1_K$ by Corollary V.1.9. Since F is a splitting field of $\{g_1, g_2, \ldots, g_t\}$ over $K(u)$ and over $K(v)$ (by Exercise V.3.2 since $K(u)$ and $K(v)$ are intermediate fields between K and splitting field F), then τ extends to an automorphism $\sigma \in \text{Aut}_K F$ with $\sigma(u) = v$ by Theorem V.3.8.

Theorem V.3.11 (continued 8)

Proof (continued). (iii) ⇒ (i) Now the mapping of cosets takes σH to $\sigma(u) = v$ and so every root of g_1 is the image of some coset of H in $\text{Aut}_K F$; that is, the mapping is onto and so $[\text{Aut}_K F : H] = s$. Furthermore, F is a splitting field over $K(u)$ of the set of all irreducible factors h_j (in $K(u)[x]$) of the polynomials g_i (by Exercise V.3.4). Each h_j is clearly separable since it divides some g_i (the g_i are separable by the hypotheses of (iii)). Now by Theorem V.1.2, $n = [F : K] = [F : K(u)][K(u) : K] = [F : K(u)]s$, or $[F : K(u)] = n/s < n$ and so by the induction hypothesis we have that F is Galois over $K(u)$ and so the fixed field of $\text{Aut}_{K(u)}F$ is $K(u)$ and by the Fundamental Theorem (Theorem V.2.5(i)) $[F : K(u)] = |\text{Aut}_{K(u)}F| = |H|$.

Theorem V.3.11 (continued 9)

Proof (continued). (iii) ⇒ (i) Therefore

$$\begin{aligned}
[F : K] &= [F : K(u)][K(u) : K] \text{ by Theorem V.2.1} \\
&= |H|s \text{ since } [K(u) : K] = s \text{ and } H = \text{Aut}_{K(u)}F \\
&= |H|[\text{Aut}_K F : H] \text{ since } [\text{Aut}_K F : H] = s \\
&= |\text{Aut}_K F|
\end{aligned}$$

with the last equality holding because $[\text{Aut}_K F : H]$ is the number of cosets of H in $\text{Aut}_K F$, so $[\text{Aut}_K F : H] = |\text{Aut}_K F|/|H|$. We have now established what is required (namely, $[F : K] = |\text{Aut}_K F|$) for the previous paragraph to imply that F is Galois over K whenever $[F : K]$ is finite. In turn, this result can be used in the paragraph before that to show that F is Galois over K for $[F : K]$ not finite. □

Theorem V.3.14

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(i) F is normal over K.

(ii) F is a splitting field over K of some set of polynomials in $K[x]$.

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Proof. (i)⇒(ii) F is a splitting field over K of $\{f_i \in K[x] \mid i \in I\}$ where f_i is the irreducible polynomial in $K[x]$ for some $u_i \in F$, where $\{u_i \mid i \in I\}$ is a basis of F over K (every vector space has a basis, so the set of u_i's exists and since F is normal over K we have the splitting requirement; also, since the u_i form a basis we know that this covers every element in F).

Theorem V.3.14 (continued 1)

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(ii) F is a splitting field over K of some set of polynomials in $K[x]$.

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Proof. (ii)⇒(iii) Let F be a splitting field of $\{f_i \mid i \in I\}$ over K and $\sigma : F \to \overline{K}$ a K-monomorphism of fields. If $u \in F$ is a root of f_j then so is $\sigma(u)$ (as shown in the two-line proof of Theorem V.2.2). By hypothesis f_j splits in F, say $f_j = c(x - u_1)(x - u_2) \cdots (x - u_n)$ (where $u_i \in F$, $c \in K$).

Theorem V.3.14 (continued 2)

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(ii) F is a splitting field over K of some set of polynomials in $K[x]$.

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Proof (continued). (ii)⇒(iii) Since $\overline{K}[x]$ is a unique factorization domain by Corollary III.6.4 and $\sigma(u_i)$ is a root of f_j for all i, then by the Factor Theorem (Theorem III.6.6), $x - \sigma(u_i)$ must be a factor of f_j and so $\sigma(u_i)$ must be one of $u_1, u_2, \ldots, u_n$ for every i. Since σ is one to one, it must simply permute the u_i. But F is generated over K by all the roots of all the f_i. It follows from Theorem V.1.3(vi) that $\sigma(F) = F$ and hence $\sigma \in \text{Aut}_K F$ (so σ is a "K-automorphism of F").

Theorem V.3.14 (continued 3)

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(i) F is normal over K.

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Proof. (iii)⇒(i) Let $\overline{K}$ be an algebraic closure of F. Then $\overline{K}$ is algebraic over K by Theorem V.1.13 (since $K \subset F \subset \overline{K}$). Therefore $\overline{K}$ contains K and is algebraically closed and contains F. Let $F \in K[x]$ be irreducible with a root $u \in F$. By construction, $\overline{K}$ contains all roots of f. To show that F is normal over K we must show that f splits in F. If $v \in \overline{K}$ is any root of f then there is a K-isomorphism of fields $\sigma : K(u) \cong K(v)$ with $\sigma(u) = v$ by Corollary V.1.19.

Theorem V.3.14 (continued 4)

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(i) F is normal over K.

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Proof (continued). (iii)⇒(i) By Theorems V.3.4 and V.3.8 and Exercise V.3.2, σ extends to a K-automorphism of $\overline{K}$. Now $\sigma|_F$ is a monomorphism (one to one, since σ is hypothesized to be a monomorphism) mapping $F \to \overline{K}$ and, since by hypothesis $\text{Im}(\sigma) = F$, we have $\sigma(F) = F$. Therefore $v = \sigma(u) \in F$ which implies that all roots of f are in F; that is, f splits in F. So F is normal over K. □

Theorem V.3.16

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(i) F is normal over K;

(ii) No proper subfield of F containing E is normal over K;

(iii) If E is separable over K, then F is Galois over K;

(iv) $[F : K]$ is finite if and only if $[E : K]$ is finite.

The field F is uniquely determined up to an E-isomorphism.

Proof. (i) Let $X = \{u_i \mid i \in I\}$ be a basis of E over K and let $f_i \in K[x]$ be the irreducible polynomial of u_i. If F is a splitting field of $S = \{f_i \mid i \in I\}$ over E, then F is also a splitting field of S over K by Exercise V.3.3. Whence F is normal over K by Theorem V.3.14 (the (ii)$\Rightarrow$(i) part).

Theorem V.3.16 (continued 1)

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(iii) If E is separable over K, then F is Galois over K;

(iv) $[F : K]$ is finite if and only if $[E : K]$ is finite.

The field F is uniquely determined up to an E-isomorphism.

Proof. (iii) If E is separable over K, then each f_i above is separable over F (since $K \subset E \subset F$). As explained above, F is a splitting field of $S = \{f_i \mid i \in I\}$ (and S consists of separable polynomials in $K[x]$), so by Theorem V.3.11 (the (iii)$\Rightarrow$(i) part), F is Galois over K.
(iv) If $[E : K]$ is finite, then so is X (since X is a basis for E over K) and hence S is finite. Since F is a splitting field of S over K, then $F = K(X)$ since X is the set of all roots of polynomials in S, then by Theorem V.1.12 F is algebraic over K and finite dimensional since X is finite. That is, $[F : K]$ is finite. The converse follows from Theorem V.1.2.

Theorem V.3.16 (continued 2)

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(ii) No proper subfield of F containing E is normal over K.

The field F is uniquely determined up to an E-isomorphism.

Proof. (ii) If F_0 is a subfield of F that contains E, then F_0 necessarily contains the root u_i of $f_i \in S$ for every i (since E contains each u_i). If F_0 is normal over K (so that each f_i splits in F_0 by definition) then $F \subset F_0$ and hence $F = F_0$ and subfield F_0 of F is not proper.

Uniqueness. Let F_1 be another extension field of E (in addition to F) with properties (i) and (ii). Since F_1 is normal over K by (i) and contains each u_i (since E contains each u_i and we have $K \subset E \subset F_1$), then (by the definition of normal) each polynomial in S splits in F_1. So F_1 must contain a splitting field F_2 of S over K with $E \subset F_2$. F_2 is normal over K (by Theorem V.3.14, the (ii)$\Rightarrow$(i) part), whence $F_2 = F_1$ by (ii).

Theorem V.3.16 (continued 3)

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(i) F is normal over K;

(ii) No proper subfield of F containing E is normal over K;

(iii) If E is separable over K, then F is Galois over K;

(iv) $[F : K]$ is finite if and only if $[E : K]$ is finite.

The field F is uniquely determined up to an E-isomorphism.

Proof (continued). (Uniqueness) Therefore both F and F_1 are splitting fields of S over K and hence (by Exercise V.3.2) are splitting fields of S over E. By Theorem V.3.8, the identity on E extends to an E-isomorphism $F \cong F_1$. □