Chapter 3

Splitting Fields and Normal Extensions

The purpose of this chapter is to show how we can use the methods of Chapter 2 to construct, given a polynomial $f(X)$ over some base field, an extension in which the polynomial $f(X)$ can be factorized as a product of linear (that is, degree 1) factors.

Splitting fields

Let F be a field and consider a polynomial $f(X)$ over the field F. Suppose that there is an extension L of F such that, when $f(X)$ is viewed as a polynomial over L, we can factorize it as a product of linear factors:

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n).$$

We shall then say that $f(X)$ *splits* over L. Necessarily, in such a situation, then the roots α_1, α_2, ..., α_n of $f(X)$ are elements of the field L. Note then that $f(X)$ might split in some such extension L, because it contains all the roots of $f(X)$, but not in some particular subfield of L because one or more of those roots do not belong to that subfield.

In this context, we make the following definition:

Definition 3.1 Let $f(X)$ be a polynomial over some field F. We say that a field K is a *splitting field* for $f(X)$ over F if K is an extension of F satisfying the following properties:

(i) $f(X)$ splits into a product of linear factors over K, and

(ii) if $F \subseteq L \subseteq K$ and $f(X)$ splits over L, then $L = K$.

Thus, a splitting field for a polynomial $f(X)$ over a field F is an extension K of F in which $f(X)$ splits over K but such that $f(X)$ does not split over any proper subfield of K; that is, K is a minimal field over which $f(X)$ splits.

The form of a splitting field is quite naturally expressed using the roots of our polynomial:

Lemma 3.2 *Let $f(X)$ be a polynomial over a field F and suppose there is some extension L of F such that $f(X)$ splits over L with roots α_1, α_2, ..., α_n. Then*

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

is a splitting field for $f(X)$ over F.

In particular, in the case of a polynomial $f(X)$ over $F = \mathbb{Q}$, we know that $L = \mathbb{C}$ is a suitable extension to use in the lemma since we know from the Fundamental Theorem of Algebra (proved in *Complex Analysis*) that every polynomial over $\mathbb{Q}$ has roots in $\mathbb{C}$ and hence splits over $\mathbb{C}$. We then obtain a splitting field for $f(X)$ over $\mathbb{Q}$ as $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ where α_1, α_2, …, α_n are the roots of $f(X)$ in $\mathbb{C}$.

We now prove the lemma:

Proof: By assumption, over the field L, we can factorize $f(X)$ as

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n). \tag{3.1}$$

where $c \in F$ (since it is a coefficient of the original polynomial $f(X)$). Write

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n),$$

the smallest subfield of L containing α_1, α_2, …, α_n. Certainly $f(X)$ splits over the field K.

Suppose $F \subseteq K' \subseteq K$ such that $f(X)$ splits over K'. This means that we have a decomposition of $f(X)$ as a product of linear factors with coefficients from K', say

$$f(X) = c(X - \beta_1)(X - \beta_2) \dots (X - \beta_n)$$

where $\beta_1, \beta_2, \dots, \beta_n \in K'$. As $K' \subseteq K$, we now have two factorizations in $K[X]$ for $f(X)$ as a product of linear factors. Since the polynomial ring $K[X]$ is a unique factorization domain, these factorizations into irreducible polynomials must be the same; that is, the α_i and the β_i are the same. We conclude that $\alpha_1, \alpha_2, \dots, \alpha_n \in K'$ and the definition of $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ as the smallest field containing F and the α_i, then forces $K' = K$.

This establishes that K is indeed a splitting field for F. □

We now apply the method of Lemma 3.2 to find some splitting fields of relatively straightforward polynomials.

Example 3.3 Find splitting fields for the following polynomials over Q:

(i) $f(X) = X^2 - 2$;

(ii) $g(X) = X^3 - 1$;

(iii) $h(X) = X^3 - 2$.

Solution: (i) The factorization of $f(X)$ over $\mathbb{C}$ is

$$f(X) = (X - \sqrt{2})(X + \sqrt{2}).$$

Hence a splitting field for $f(X)$ over $\mathbb{Q}$ is, by our argument above,

$$K = \mathbb{Q}(\sqrt{2}).$$

(Note that $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, as the latter is a field, so closed under subtraction.)

(ii) The factorization of $g(X)$ over $\mathbb{Q}$ is

$$g(X) = (X - 1)(X^2 + X + 1).$$

We can further factorize it over $\mathbb{Q}$ as

$$g(X) = (X - 1)(X - \omega)(X - \omega^2)$$

where $\omega = \mathrm{e}^{2\pi i/3}$ (and note $\omega^2 = \mathrm{e}^{4\pi i/3}$ is the other cube root of 1 in $\mathbb{C}$). Hence a splitting field for $g(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\omega).$$

(iii) The factorization of $h(X)$ over $\mathbb{C}$ is

$$h(X) = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2})$$

where $\omega = \mathrm{e}^{2\pi i/3}$. Our method tells us a splitting field for $h(X)$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}).$$

However, note that ω belongs to this field K, since K is closed under division, and we now observe that this field K equals

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

The latter description would be helpful if we wished to use the methods of Chapter 2 to determine the degree of K over $\mathbb{Q}$ and even to find a basis for this splitting field over the base field $\mathbb{Q}$. □

Existence of splitting fields

Using the method described above relied upon us being able to find some extension L in which $f(X)$ splits and then finding a splitting field inside it. Over the rational numbers $\mathbb{Q}$, this is no problem since we can use the complex numbers $\mathbb{C}$, but even then it gives little restriction upon the degree of the splitting extension. In fact, using the theory developed in Chapter 2 we can construct a splitting field for a polynomial $f(X)$ irrespective of what the base field is and to also obtain decent bounds on the degree of the extension in terms of the polynomial.

Theorem 3.4 (Existence of Spitting Fields) *Let $f(X)$ be a polynomial of degree n over a field F. Then there is a splitting field K for $f(X)$ over F with degree $|K : F|$ dividing $n!$.*

Proof: We proceed by induction on n. If $n = 1$, then $f(X)$ is already a linear polynomial, so F itself is a splitting field for $f(X)$ over F and, of course, $|F : F| = 1$.

We now assume that the claimed result holds for all polynomials of degree less than n. We consider two cases:

Case 1: $f(X)$ is irreducible over F.

Let us apply Theorem 2.13 to adjoin a root α of $f(X)$ to F. Then $|F(\alpha) : F| = n$, by Theorem 2.14 and we can write

$$f(X) = (X - \alpha)\, g(X)$$

for some polynomial $g(X)$ of degree $n-1$ with coefficients in $F(\alpha)$. Now by induction, $g(X)$ has a splitting field K over $F(\alpha)$ and the degree $|K : F(\alpha)|$ divides $(n-1)!$. Note that $K = F(\alpha, \alpha_2, \dots, \alpha_n)$ where α_2, …, α_n are the roots of $g(X)$; that is, K is obtained by adjoining the roots of $f(X)$ to F. Hence, using Lemma 3.2, K is a splitting field for $f(X)$ over F and, by the Tower Law (Theorem 2.4),

$$|K : F| = |K : F(\alpha)| \cdot |F(\alpha) : F| = |K : F(\alpha)|\, n,$$

which divides $n!$.

Case 2: $f(X)$ is reducible over F.

We can then write $f(X) = g(X)\,h(X)$ where $g(X)$ and $h(X)$ are polynomials over F of degree k and $n-k$, respectively (where $1 \leqslant k \leqslant n-1$). By induction, there is a splitting field

$$L = F(\beta_1, \dots, \beta_k)$$

for $g(X)$ over F where $|L:F|$ divides $k!$ and $\beta_1, \dots, \beta_k$ are the roots of $g(X)$ in L. Equally, there is a splitting field

$$K = L(\gamma_{k+1}, \dots, \gamma_n)$$

for $h(X)$ over L where $|K:L|$ divides $(n-k)!$ and $\gamma_{k+1}, \dots, \gamma_n$ are the roots of $h(X)$ in K.

Now in the field K, $f(X)$ splits as a product of linear factors with roots β_1, …, β_k, γ_{k+1}, …, γ_n. We conclude that

$$K = F(\beta_1, \dots, \beta_k, \gamma_{k+1}, \dots, \gamma_n)$$

is a splitting field for $f(X)$ over F and the degree

$$|K:F| = |K:L| \cdot |L:F|$$

divides $k!\,(n-k)!$, and hence divides $n!$ (since the binomial coefficient $\binom{n}{k}$ is an integer). □

Uniqueness of splitting fields and related isomorphisms

We now know that splitting fields always exist, have some constraint about their degree over the base field, and have a method to construct them in a nice case (for example, splitting fields over any subfield of $\mathbb{C}$). We now turn to establishing that splitting fields are unique and in doing so will also develop some key tools for the main theorem of the course.

We begin with the following first step.

Lemma 3.5 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be an irreducible polynomial in $F_1[X]$ and write $f^{\phi}(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let α be a root of $f(X)$ and β be a root of $f^{\phi}(X)$ in some extensions of F_1 and F_2, respectively. Then there exists an isomorphism $\psi\colon F_1(\alpha) \to F_2(\beta)$ which extends ϕ and maps α to β.*

To say that ψ *extends* ϕ means that $a\psi = a\phi$ for all $a \in F_1$; that is, the restriction $\psi|_{F_1}$ of ψ to F_1 is the isomorphism ϕ we started with.

Proof: First note that the isomorphism $\phi\colon F_1 \to F_2$ induces an isomorphism $\phi^*\colon F_1[X] \to F_2[X]$ between the corresponding polynomial rings, namely

$$\phi^*\colon a_0 + a_1X + \dots + a_mX^m \mapsto (a_0\phi) + (a_1\phi)X + \dots + (a_m\phi)X^m.$$

So, in this notation, $f^{\phi}(X) = f(X)\phi^*$. This map ϕ^* is indeed an isomorphism of rings because addition and multiplication is determined by operations on the coefficients within polynomials and ϕ preserves these operations. Since $f(X)$ is irreducible in $F_1[X]$, we conclude that $f^{\phi}(X) = f(X)\phi^*$ is irreducible in $F_2[X]$. The isomorphism ϕ^* maps the ideal $\bigl(f(X)\bigr)$ to the ideal $\bigl(f^{\phi}(X)\bigr)$ and hence we have an induced isomorphism

$$\bar{\phi}\colon \frac{F_1[X]}{\bigl(f(X)\bigr)} \to \frac{F_2[X]}{\bigl(f^{\phi}(X)\bigr)}$$

given by

$$\bar{\phi}\colon \bigl(f(X)\bigr) + g(X) \mapsto \bigl(f^{\phi}(X)\bigr) + g(X)\phi^*.$$

In particular,

$$\big((f(X)) + X\big)\,\bar{\phi} = \big(f^{\phi}(X)\big) + X \qquad \text{and} \qquad \big((f(X)) + a\big)\,\bar{\phi} = \big(f^{\phi}(X)\big) + a\phi$$

for $a \in F_1$.

We link these quotients to the field extensions $F_1(\alpha)$ and $F_2(\beta)$. Recall from Theorem 2.14 that these field extensions are isomorphic to the quotient rings appearing above. To be specific, there are isomorphisms

$$\psi_1\colon \frac{F_1[X]}{(f(X))} \to F_1(\alpha)$$

$$\psi_2\colon \frac{F_2[X]}{(f^{\phi}(X))} \to F_2(\beta)$$

and these satisfy

$$\big((f(X)) + a\big)\,\psi_1 = a \qquad\qquad \big((f(X)) + X\big)\,\psi_1 = \alpha$$

$$\Big(\big(f^{\phi}(X)\big) + b\Big)\,\psi_2 = b \qquad\qquad \Big(\big(f^{\phi}(X)\big) + X\Big)\,\psi_2 = \beta$$

for any $a \in F_1$ and $b \in F_2$. We now compose these isomorphisms: $\psi_1^{-1}\bar{\phi}\psi_2$ is an isomorphism from $F_1(\alpha)$ to $F_2(\beta)$ satisfying

$$a\,\psi_1^{-1}\bar{\phi}\psi_2 = \big((f(X)) + a\big)\,\bar{\phi}\psi_2 = \Big(\big(f^{\phi}(X)\big) + a\phi\Big)\,\psi_2 = a\phi,$$

for all $a \in F_1$, and

$$\alpha\,\psi_1^{-1}\bar{\phi}\psi_2 = \big((f(X)) + X\big)\,\bar{\phi}\psi_2 = \Big(\big(f^{\phi}(X)\big) + X\Big)\,\psi_2 = \beta.$$

This establishes the result. □

We use this as the base step in an induction to establish the uniqueness of splitting fields. The most important theorem in this chapter is the following:

Theorem 3.6 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be any polynomial in $F_1[X]$ and write $f^{\phi}(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let K_1 be a splitting field for $f(X)$ over F_1 and K_2 be a splitting field for $f^{\phi}(X)$ over F_2. Then there exists an isomorphism $\theta\colon K_1 \to K_2$ which extends ϕ.*

To establish uniqueness of splitting fields, we take $F_1 = F_2$ and ϕ to be the identity map in the above theorem. This tells us that two splitting fields for a polynomial over F_1 are isomorphic via an isomorphism that restricts to the identity on F_1.

We accordingly make the following definition:

Definition 3.7 Let F be a field and let K_1 and K_2 be extensions of F. An *F-isomorphism* from K_1 to K_2 is a field isomorphism $\psi\colon K_1 \to K_2$ such that

$$a\psi = a \qquad \text{for all } a \in F.$$

We then say K_1 and K_2 are *F-isomorphic.*

Thus taking $F_1 = F_2 = F$ in Theorem 3.6 and ϕ to be the identity, we conclude:

Corollary 3.8 (Uniqueness of Splitting Fields) *Let $f(X)$ be a polynomial over a field F. Any two splitting fields for $f(X)$ over F are F-isomorphic.* □

It remains then to establish the above theorem.

Proof of Theorem 3.6: Let $n = \deg f(X)$ and proceed by induction on n. If $n = 1$, then $K_1 = F_1$ and $K_2 = F_2$, so we may take $\theta = \phi$.

Now we assume the result holds for all polynomials of degree smaller than n. We shall consider two cases:

Case 1: $f(X)$ is irreducible over F_1.

Let α be any root of $f(X)$ in the field K_1 and β be any root of $f^{\phi}(X)$ in K_2. (We know these exist because K_1 and K_2 are splitting fields for $f(X)$ and $f^{\phi}(X)$ over F_1 and F_2 respectively.) By Lemma 3.5, there is an isomorphism $\psi\colon F_1(\alpha) \to F_2(\beta)$ such that $\psi|_{F_1} = \phi$ and $\alpha\psi = \beta$. Now

$$f(X) = (X - \alpha)\, g(X),$$

for some polynomial $g(X)$ with coefficients from $F_1(\alpha)$, and, applying ψ to the coefficients, we observe

$$f^{\phi}(X) = (X - \beta)\, g^{\psi}(X)$$

(where $g^{\psi}(X)$ is the polynomial with coefficients in $F_2(\beta)$ obtained by applying ψ to the coefficients of $g(X)$). Now K_1 is a splitting field for $g_1(X)$ over $F_1(\alpha)$ (since K_1 is obtained by adjoining α and all the roots of $g(X)$ to F) and K_2 is a splitting field for $g^{\psi}(X)$ over $F_2(\beta)$. Hence, by induction, there is an isomorphism $\theta\colon K_1 \to K_2$ such that $\theta|_{F_1(\alpha)} = \psi$. In particular,

$$\theta|_{F_1} = \psi|_{F_1} = \phi,$$

as required.

Case 2: $f(X)$ is reducible over F_1.

Let us write $f(X) = g(X)\, h(X)$ in $F_1[X]$ where $g(X)$ and $h(X)$ are non-constant polynomials. Applying ϕ to the coefficients, we obtain

$$f^{\phi}(X) = g^{\phi}(X)\, h^{\phi}(X)$$

in $F_2[X]$ (using the notation introduced in the statement of the Theorem). Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be the roots of $g(X)$ in K_1 and $\beta_1, \beta_2, \dots, \beta_k$ be the roots of $g^{\phi}(X)$ in K_2. Put

$$L_1 = F_1(\alpha_1, \alpha_2, \dots, \alpha_k) \qquad \text{and} \qquad L_2 = F_2(\beta_1, \beta_2, \dots, \beta_k).$$

Then L_1 is a splitting field for $g(X)$ over F_1 and L_2 is a splitting field for $g^{\phi}(X)$ over F_2. By induction, there is an isomorphism $\psi\colon L_1 \to L_2$ such that $\psi|_{F_1} = \phi$.

Finally, note that K_1 is obtained from F_1 by adjoining all the roots of $f(X)$, so it is obtained from L_1 by adjoining all the roots of $h(X)$; that is, K_1 is a splitting field for $h(X)$ over L_1. Similarly K_2 is a splitting field for $h^{\phi}(X) = h^{\psi}(X)$ over L_2. Hence, by induction, there is an isomorphism $\theta\colon K_1 \to K_2$ such that $\theta|_{L_1} = \psi$. In particular,

$$\theta|_{F_1} = \psi|_{F_1} = \phi.$$

This completes the inductive step and establishes the theorem. □

Before turning to the final topic of this chapter, we shall give an example illustrating how the results established so far will appear within the later theory.

Definition 3.9 (i) An *automorphism* of a field F is an isomorphism from F to itself.

(ii) Let K be an extension of the field F. An F-*automorphism* of K is an F-isomorphism from K to itself.

Thus an F-automorphism of the extension K is an isomorphism $\phi\colon K \to K$ such that $a\phi = a$ for all a in the base field F.

Example 3.10 *Determine all $\mathbb{Q}$-automorphisms of the simple extension $\mathbb{Q}(i)$.*

To fit this example in context, note that the roots of the polynomial $X^2 + 1$ in $\mathbb{C}$ are $\pm i$. Hence $\mathbb{Q}(i)$ is the splitting field for $X^2 + 1$ over $\mathbb{Q}$. (In view of the uniqueness in Corollary 3.8, we are also now justified in referring to "the splitting field" rather than "a splitting field" of a polynomial.)

Solution: As noted, i is a root of the polynomial $X^2 + 1$. The latter polynomial is irreducible over $\mathbb{Q}$, so it is the minimum polynomial of i over $\mathbb{Q}$, the degree $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ and $\{1, i\}$ is a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$. Let ψ be a $\mathbb{Q}$-automorphism of $\mathbb{Q}(i)$. Then

$$(a + bi)\psi = a + b(i\psi),$$

for $a, b \in \mathbb{Q}$, and we conclude that ψ is determined by its effect on i. Now $i^2 + 1 = 0$, so applying the automorphism ψ we see that

$$(i\psi)^2 + 1 = 0.$$

Hence ψ must map i to a root of $X^2 + 1$; that is, $i\psi = \pm i$. Thus, there are at most two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$.

Conversely, if β is any root of $X^2 + 1$, applying Lemma 3.5 (taking $F_1 = F_2 = \mathbb{Q}$ and ϕ to be the identity map), there is a $\mathbb{Q}$-isomorphism $\mathbb{Q}(i) \to \mathbb{Q}(\beta)$ which maps i to β. However, $\beta = \pm i$, so $\mathbb{Q}(\beta) = \mathbb{Q}(i)$ and ψ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(i)$.

We conclude that there are precisely two $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i)$. □

Normal Extensions

Definition 3.11 An extension K of a field F is a *normal extension* if every irreducible polynomial over F that has at least one zero in K splits over K.

Note that having normal extension only tells us about irreducible polynomials that have a root in the larger field. It tells us nothing about reducible polynomials nor does it guarantee that a particular polynomial has any roots in the larger field.

Example 3.12 (i) The field $\mathbb{C}$ of complex numbers is a normal extension of $\mathbb{R}$, since every polynomial over $\mathbb{R}$ splits over $\mathbb{C}$.

(ii) Consider the simple extension $\mathbb{Q}(\sqrt[3]{2})$ obtained by adjoining the cube root of 2 to $\mathbb{Q}$. This is *not* a normal extension of $\mathbb{Q}$ since the irreducible polynomial $X^3 - 2$ (over $\mathbb{Q}$) has a root in $\mathbb{Q}(\sqrt[3]{2})$ but does not split over this field as the other two roots are complex numbers.

It would seem on the face of it rather complicated to show that an extension is normal. The definition asks us to show check that every irreducible polynomial with a root in the bigger field actually splits. The following theorem characterizes finite normal extensions (and hence gives essentially all examples) as the splitting fields of polynomials.

Theorem 3.13 *A finite extension K of a field F is a normal extensions if and only if K is the splitting field of some polynomial over F.*

So we know that an extension is normal if we can recognize it as a splitting field of some polynomial (which does not need to be an irreducible polynomial). On the other hand, to show an extension is not normal, we should find an irreducible polynomial over the base field which has a root but does not split in the larger field and then by definition the extension is not normal.

Proof: Suppose K is a finite normal extension of F. By Theorem 2.17, we know that K is an algebraic extension of F of the form

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_m)$$

for some $\alpha_1, \alpha_2, \dots, \alpha_m \in K$. Let $f_i(X)$ be the minimum polynomial of α_i over F and let

$$g(X) = f_1(X)\, f_2(X) \dots f_m(X) \in F[X].$$

Now $f_i(X)$ is an irreducible polynomial over F and has a root α_i in K, Hence, by normality, $f_i(X)$ splits over K. It follows that $g(X)$ splits over K. On the other hand, K is constructed from F by adjoining (some of) the roots of $g(X)$, so K is the splitting field of $g(X)$ over F.

Conversely, suppose K is the splitting field of some polynomial $g(X)$ over F. Let $f(X)$ be any irreducible polynomial over F and suppose that $f(X)$ has some root α in K. We must show that $f(X)$ splits over K. First let L be the splitting field for $f(X)$ over K. (Our goal is essentially to show, in fact, that $L = K$.) Let β be any root of $f(X)$ in L and consider the following diagram (where an upward sloping line indicates inclusion):

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[dr, equal] \arrow[dd, dash] & & K(\beta) \arrow[dl, dash] \arrow[dd, dash] \\
 & K \arrow[dd, dash] & \\
F(\alpha) \arrow[dr, dash] & & F(\beta) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

We shall show that $K(\beta) = K$ to conclude $\beta \in K$. It will then follow that all the roots of $f(X)$ in L actually belong to K.

By the Tower Law (Theorem 2.4):

$$\begin{aligned}
|K(\beta) : K| \cdot |K : F| = |K(\beta) : F| = |K(\beta) : F(\beta)| \cdot |F(\beta) : F| \\
|K(\alpha) : K| \cdot |K : F| = |K(\alpha) : F| = |K(\alpha) : F(\alpha)| \cdot |F(\alpha) : F|
\end{aligned} \tag{3.2}$$

Since $f(X)$ is irreducible over F and α and β are roots of $f(X)$ in some extension, we know

$$|F(\alpha) : F| = |F(\beta) : F| = \deg f(X)$$

and

$$F(\alpha) \cong \frac{F[X]}{\big(f(X)\big)} \cong F(\beta)$$

by Theorem 2.14. Let $\phi\colon F(\alpha) \to F(\beta)$ be this isomorphism. Note, from the form of the isomorphism from $F[X]/\big(f(X)\big)$ to $F(\alpha)$ and $F(\beta)$ in Theorem 2.14, that ϕ is an F-isomorphism (that is, $a\phi = a$ for all $a \in F$).

Observe that $K(\alpha)$ can be obtained from $F(\alpha)$ by adjoining the roots of $g(X)$ to $F(\alpha)$, since we build K from F by adjoining these roots, and hence $K(\alpha)$ is the splitting field for $g(X)$

over $F(\alpha)$. Similarly, $K(\beta)$ is the splitting field for $g(X)$ over $F(\beta)$. We now make use of Theorem 3.6 to produce an isomorphism $\theta\colon K(\alpha) \to K(\beta)$ such that $\theta|_{F(\alpha)} = \phi$. This isomorphism then maps the subfield $F(\alpha)$ to the subfield $F(\beta)$. Therefore

$$|K(\alpha) : F(\alpha)| = |K(\beta) : F(\beta)|.$$

From this we conclude that the right-hand sides appearing in the Equations 3.2 are equal, and therefore the left-hand sides are equal. Hence

$$|K(\alpha) : K| = |K(\beta) : K|.$$

However, $\alpha \in K$, so we conclude $|K(\beta) : K| = 1$; that is, $\beta \in K$.

We have now shown that every root of $f(X)$ does indeed belong to K and hence $f(X)$ splits over K. It follows that K is indeed a normal extension of F. □