Theorem 44.8 says that it does not matter how you construct the splitting field for a fixed set of polynomials, you will always get the same field up to isomorphism fixing F. Because of this we will often speak of *the* splitting field of a set of polynomials instead of *a* splitting field.

44.9 Definition Let E be an extension field of F. A polynomial $f(x) \in F[x]$ **splits in** E if it factors into linear factors in $E[x]$. ■

44.10 Example The polynomial $x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ splits in the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ since

$$x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3}).$$

▲

44.11 Theorem Let E be a finite extension of the field F. Then E is the splitting field of some finite set of polynomials in $F[x]$ if and only if for every field extension K over E and for every isomorphism σ that fixes all the elements of F and maps E onto a subfield of K, σ is an automorphism of E.

Proof We first assume that E is the splitting field for some set of polynomials

$$P = \{f_1(x), f_2(x), \ldots, f_s(x)\}.$$

Let $\alpha_1, \ldots, \alpha_n$ be the zeros in E of the polynomials in P. Then $E = F(\alpha_1, \alpha_2, \ldots \alpha_n)$. Let K be a field extension of E. Since all the polynomials $f_i(x)$ split in $E[x]$, all the zeros of $f_i(x)$ in K are actually in E. Let σ be an isomorphism from E to a subfield of K that fixes elements of F. Since σ maps each α_k to a zero of $f_i(x)$, for some i, $\sigma(\alpha_k) \in E$. Thus σ maps E into E. Since σ is an isomorphism, isomorphisms preserve the degree of the extension, and the degree of E over F is finite, σ is an isomorphism mapping E onto E. Thus σ is an automorphism of E.

We next assume that for any field extension K over E and any isomorphism σ that fixes all the elements of F and maps E to a subfield of K, σ is an automorphism of E. Since E is a finite extension of F, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some elements $\alpha_k \in E$ that are algebraic over F. Let $f_k(x) = \text{irr}(\alpha_k, F)$ be the minimal polynomial for α_k over F and $P = \{f_k(x) \mid 1 \leq k \leq n\}$. We show that E is the splitting field of P over F. Suppose by way of contradiction that some $f_k(x)$ does not split in E. By reordering the α_k we can assume that $k = 1$. Let $\overline{E}$ be the algebraic closure of E. So $f_1(x)$ factors into linear factors in $\overline{E}$, which says that there is an element $\beta \in \overline{E}$, $\beta \notin E$, and β is a zero of $f_1(x) = \text{irr}(\alpha_1, F)$. Thus, α_1 and β are conjugates over F. By Theorem 43.18, there is an isomorphism

$$\psi_{\alpha_1,\beta} : F(\alpha_1) \to F(\beta)$$

that fixes all the elements of F and maps α_1 to β. Since $\overline{E}$ contains the splitting field of $\{(\psi_{\alpha_1,\beta})_x(\text{irr}(\alpha_k, F(\alpha_1))) \mid 1 \leq k \leq n\}$, by the Isomorphism Extension Theorem 44.6, $\psi_{\alpha_1,\beta}$ extends to an isomorphism σ mapping E onto a subfield of $\overline{E}$. But

$$\sigma(\alpha_1) = \psi_{\alpha_1,\beta}(\alpha_1) = \beta \notin E.$$

This gives a contradiction, which implies that each $f_k(x)$ splits in $E[x]$. Since each α_k is a zero of $f_k(x)$ and $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, E is the smallest subfield of E where each $f_k(x)$ splits. Thus E is a splitting field of P over F. ◆

The following corollary highlights one of the very strong properties of splitting fields.

44.12 Corollary If K is a finite splitting field over F and K contains one zero of an irreducible polynomial $f(x) \in F[x]$, then $f(x)$ splits in $K[x]$.

Proof Suppose by way of contradiction that $f(x)$ is irreducible over F, $f(x)$ has a zero α in $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, and $f(x)$ does not split in K. Let $\overline{K}$ be the algebraic closure of K. By our assumption, there is a $\beta \in \overline{K}$ that is a zero of $f(x)$ and $\beta \notin K$. Theorem 43.18, the Conjugation Isomorphism Theorem, says there is an isomorphism

$$\psi_{\alpha,\beta} : F(\alpha) \to F(\beta).$$

Since $\overline{K}$ is algebraically closed, it contains the splitting field of

$$\{(\psi_{\alpha,\beta})_x(\mathrm{irr}(\alpha_k, F(\alpha))) \mid 1 \leq k \leq n\}$$

over $F(\beta)$. The Isomorphism Extension Theorem allows us to extend $\psi_{\alpha,\beta}$ to an isomorphism σ mapping K onto a subfield of $\overline{K}$ with $\sigma(\alpha) = \beta \notin K$, which contradicts Theorem 44.11. Thus $f(x)$ splits in $K[x]$. ◆

Corollary 44.12 tells us that if K is a splitting field of P over F and the irreducible polynomial $f(x) \in F[x]$ has a zero in K, then K contains the splitting field of $f(x)$ over F. It is surprising at first glance that a multiple of $f(x)$ need not be in the set P.

44.13 Example As we have seen, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $\{x^2 - 2, x^2 - 3\}$ over $\mathbb{Q}$. We have $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and, as can easily be checked, α is a zero of

$$(x^2 - 5)^2 - 24 = x^4 - 10x^2 + 1.$$

With some effort, it can also be checked that $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$. Thus $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 10x^2 + 1$. By Corollary 44.12, $x^4 - 10x^2 + 1$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contains a splitting field K of $x^4 - 10x + 1$ over $\mathbb{Q}$. Since

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \leq K \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

and the two end fields have the same degree, 4, over $\mathbb{Q}$,

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

We have two interesting results. First, the splitting field of $x^4 - 10x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, and second, although $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ does not appear to be a simple extension of $\mathbb{Q}$, it is. In the next section we will find that under mild conditions, every finite extension is a simple extension.

A challenging high school exercise is to use the quadratic formula to find all the zeros of $x^4 - 10x^2 + 1$ and rewrite them to see that they are all in both $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. ▲

Theorem 44.11 gives a condition on a finite field extension $F \leq E$ that is equivalent to E being a splitting field. The condition involves looking at all possible extensions of E. Corollary 44.14 simplifies the condition significantly. Instead of looking at all extensions of E, Corollary 44.14 only requires looking at any one splitting field over F that contains E.

44.14 Corollary Let $F \leq E \leq K$ be fields with K a finite splitting field over F. Then E is a splitting field over F if and only if every isomorphism σ that fixes F and maps E to a subfield of K is an automorphism of E.

Proof Theorem 44.11 says that if E is a splitting field over F, then every isomorphism σ mapping E to a subfield of K that fixes F is an automorphism of E. This proves the only if direction.

We next assume that every isomorphism σ mapping E to a subfield of K that fixes F is an automorphism of E. Let $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $f_k(x) = \mathrm{irr}(\alpha_k, F)$ and $P = \{f_k(x) \mid 1 \leq k \leq n\}$. We first show that in the algebraic closure, $\overline{K}$, of K, every conjugate over F of every α_k is actually in E. By Theorems 43.18 and 44.6, for any conjugate $\beta \in \overline{K}$ of α_k over F, there is an isomorphism σ that fixes F, maps E onto a subfield of the algebraic closure $\overline{K}$, and maps α_k to β. Now $\sigma(\alpha_i)$ is a conjugate of α_j over F for each $1 \leq j \leq n$. That is, both α_j and $\sigma(\alpha_j)$ are zeros of $f_j(x)$. By Corollary 44.12, $f_j(x)$ splits in K, so $\sigma(\alpha_j) \in K$ for each j. Thus

$$\sigma(E) = \sigma(F(\alpha_1, \alpha_2, \ldots, \alpha_n)) \leq K.$$

By our assumption, σ is an automorphism of E, so in particular, $\beta \in E$. We have shown that E contains all the conjugates of $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$ over F. Since each $f_k(x)$ splits in the algebraically closed field $\overline{K}$, each $f_k(x)$ also splits in $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Since the splitting field of P over F contains E, E is the splitting field of P over F. ◆

44.15 Example We let $E = \mathbb{Q}(\sqrt[3]{2})$ and let K be the splitting field of the irreducible polynomial $x^3 - 2$ over $\mathbb{Q}$. The field K contains $\sqrt[3]{2}$, one zero of $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, but it does not contain the other two zeros, $\sqrt[3]{2}(-1 \pm \sqrt{3}i)/2$. We can see that E is not the splitting field of any set of polynomials over $\mathbb{Q}$ from Corollary 44.12. Alternatively, we can use the conjugation isomorphism theorem to show there is an isomorphism mapping $\mathbb{Q}(\sqrt[3]{2})$ to $\mathbb{Q}(\sqrt[3]{2}(-1 + \sqrt{3}i)/2) \leq K$. By Corollary 44.14, again we see that E is not a splitting field over $\mathbb{Q}$. ▲

EXERCISES 44

Computations

In Exercises 1 through 6, find the degree over $\mathbb{Q}$ of the splitting field over $\mathbb{Q}$ of the given polynomial in $\mathbb{Q}[x]$.

1. $x^2 + 3$
2. $x^4 - 1$
3. $(x^2 - 2)(x^2 - 3)$
4. $x^3 - 3$
5. $x^3 - 1$
6. $(x^2 - 2)(x^3 - 2)$

Refer to Example 44.2 for Exercises 7 through 9.

7. What is the order of $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$?

8. What is the order of $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})$?

9. What is the order of $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))$?

10. Let α be a zero of $x^3 + x^2 + 1$ over $\mathbb{Z}_2$. Show that $x^3 + x^2 + 1$ splits in $\mathbb{Z}_2(\alpha)$. [*Hint:* There are eight elements in $\mathbb{Z}_2(\alpha)$. Exhibit two more zeros of $x^3 + x^2 + 1$, in addition to α, among these eight elements. Alternatively, use the results of Section 42.]

Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. It can be shown that $[E : \mathbb{Q}] = 8$. In Exercises 11 through 13, for the given isomorphic mappings of a subfield of E, give all extensions of the mapping to an isomorphic mapping of E onto a subfield of $\mathbb{C}$. Describe the extensions by giving values on the generating set $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$ for E over $\mathbb{Q}$.

11. $\iota : \mathbb{Q}(\sqrt{2}, \sqrt{15}) \to \mathbb{Q}(\sqrt{2}, \sqrt{15})$, where ι is the identity map.

12. $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{15}) \to \mathbb{Q}(\sqrt{2}, \sqrt{15})$, where $\sigma(\sqrt{2}) = \sqrt{2}$ and $\sigma(\sqrt{15}) = -\sqrt{15}$.

13. $\Psi_{\sqrt{30}, -\sqrt{30}} : \mathbb{Q}(\sqrt{30}) \to \mathbb{Q}(\sqrt{30})$

In Exercises 14 through 16, let

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \sqrt[3]{2}\frac{-1 + \sqrt{3}i}{2}, \quad \text{and} \quad \alpha_3 = \sqrt[3]{2}\frac{-1 - \sqrt{3}i}{2},$$

where $\sqrt[3]{2}$ is the real number whose cube is 2. The zeros of $x^3 - 2$ are α_1, α_2, and α_3.

14. Describe all extensions of the identity map on $\mathbb{Q}$ to an isomorphism mapping $\mathbb{Q}(\sqrt[3]{2})$ onto a subfield of $\mathbb{C}$.

15. Describe all extensions of the identity map on $\mathbb{Q}$ to an isomorphism mapping $\mathbb{Q}(\sqrt{3}i, \sqrt[3]{2})$ onto a subfield of $\mathbb{C}$.

16. Describe all extensions of the automorphism $\Psi_{\sqrt{3}i,-\sqrt{3}i}$ on $\mathbb{Q}(\sqrt{3}i)$ to an isomorphism mapping $\mathbb{Q}(\sqrt{3}i, \sqrt[3]{2})$ onto a subfield of $\mathbb{C}$.

17. Let σ be an automorphism of $\mathbb{Q}(\pi)$ that maps π onto $-\pi$.

a. Describe the fixed field of σ.
b. Describe all extensions of σ to an isomorphism mapping the field $\mathbb{Q}(\sqrt{\pi})$ onto a subfield of the splitting field of $x^2 + \pi$ over $\mathbb{Q}(\pi)$.

Concepts

In Exercise 18, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

18. A polynomial $f(x)$ in $F[x]$ *splits in an extension field* E of F if and only if it factors in $E[x]$ into a product of polynomials of lower degree.

19. Let $f(x)$ be a polynomial in $F[x]$ of degree n. Let E be a splitting field of $f(x)$ over F. What bounds can be put on $[E : F]$?

20. Determine whether each of the following is true or false.

a. Let $\alpha, \beta \in E$, where E is a splitting field over F. Then there exists an automorphism of E leaving F fixed and mapping α onto β if and only if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.
b. If $f(x) \neq g(x)$ are polynomials in $\mathbb{Q}[x]$, F is the splitting field of $f(x)$ over $\mathbb{Q}$, and K is the splitting field of $g(x)$ over $\mathbb{Q}$, then $F \neq K$.
c. $\mathbb{R}$ is a splitting field over $\mathbb{R}$.
d. $\mathbb{C}$ is a splitting field over $\mathbb{R}$.
e. $\mathbb{Q}(i)$ is a splitting field over $\mathbb{Q}$.
f. $\mathbb{Q}(\pi)$ is a splitting field over $\mathbb{Q}(\pi^2)$.
g. For every splitting field E over F, every isomorphic mapping of E is an automorphism of E.
h. For every splitting field E over F, where $E \leq K$, every isomorphism mapping E onto a subfield of K is an automorphism of E.
i. For every splitting field E over F, where $E \leq K$, every isomorphism mapping E onto a subfield of K and leaving F fixed is an automorphism of E.
j. If E is a splitting field over F and $\alpha \in E$, then $\deg(\alpha, F)$ divides $[E : F]$.

21. Show by an example that Corollary 44.12 is no longer true if the word *irreducible* is deleted.

22. Is $|G(E/F)|$ multiplicative for finite towers of finite extensions, that is, is

$$|G(K/F)| = |G(K/E)||G(E/F)| \qquad \text{for} \qquad F \leq E \leq K?$$

Why or why not? [*Hint:* Use Exercises 7 through 9.]

Theory

23. Show that if a finite extension E of a field F is a splitting field over F, then E is a splitting field of one polynomial in $F[x]$.

24. Show that if $[E : F] = 2$, then E is a splitting field over F.

25. Show that for $F \leq E \leq \bar{F}$, E is a splitting field over F if and only if E contains all conjugates over F in $\bar{F}$ for each of its elements.

26. Show that the splitting field K of $\{x^2 - 2, x^2 - 5\}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2} + \sqrt{5})$.

27. Show that

$$G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3})) \simeq \langle \mathbb{Z}_3, + \rangle.$$

28. **a.** Show that an automorphism leaving F fixed of a splitting field E over F of a polynomial $f(x) \in F[x]$ permutes the zeros of $f(x)$ in E.
b. Show that an automorphism leaving F fixed of a splitting field E over F of a polynomial $f(x) \in F[x]$ is completely determined by the permutation of the zeros of $f(x)$ in E given in part (a).