33. Let E be an algebraic extension of a field F, and let σ be an automorphism of E leaving F fixed. Let $\alpha \in E$. Show that σ induces a permutation of the set of all zeros of $\text{irr}(\alpha, F)$ that are in E.

34. Let E be an algebraic extension of a field F. Let $S = \{\sigma_i \mid i \in I\}$ be a collection of automorphisms of E such that every σ_i leaves each element of F fixed. Show that if S generates the subgroup H of $G(E/F)$, then $E_S = E_H$.

35. Let F be a finite field with characteristic p. Prove that the map $\phi : F \to F$ defined by $\phi(\alpha) = \alpha^p$ is a field automorphism. This automorphism is called the **Frobenius automorphism**.

36. Referring to Exercise 35, let F be a finite field of characteristic p, and let ϕ be the Frobenius automorphism on F. Prove that the fixed field $F_{\{\phi\}}$ is isomorphic with $\mathbb{Z}_p$.

37. Referring to Exercise 35, show that the finite assumption is necessary by finding an example of a field F with characteristic p, such that the map $\phi : F \to F$ given by $\phi(\alpha) = \alpha^p$ is not an automorphism.

38. We saw in Corollary 28.18 that the cyclotomic polynomial

$$\Phi_p(x) = \frac{x^{p-1}}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$ for every prime p. Let ζ be a zero of $\Phi_p(x)$, and consider the field $\mathbb{Q}(\zeta)$.

a. Show that $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ are distinct zeros of $\Phi_p(x)$, and conclude that they are all the zeros of $\Phi_p(x)$.

b. Deduce from Corollary 43.19 and part (a) of this exercise that $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian of order $p - 1$.

c. Show that the fixed field of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is $\mathbb{Q}$. [*Hint:* Show that

$$\{\zeta, \zeta^2, \cdots, \zeta^{p-1}\}$$

is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, and consider which linear combinations of $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ are fixed by all elements of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$.

39. Theorem 43.18 described conjugation isomorphisms for the case where α and β were conjugate algebraic elements over F. Is there a similar isomorphism of $F(\alpha)$ with $F(\beta)$ in the case that α and β are both transcendental over F?

40. Let F be a field, and let x be an indeterminate over F. Determine all automorphisms of $F(x)$ leaving F fixed, by describing their values on x.

41. Prove the following sequence of theorems.

a. An automorphism of a field E carries elements that are squares of elements in E onto elements that are squares of elements of E.

b. An automorphism of the field $\mathbb{R}$ of real numbers carries positive numbers onto positive numbers.

c. If σ is an automorphism of $\mathbb{R}$ and $a < b$, where $a, b \in \mathbb{R}$, then $\sigma(a) < \sigma(b)$.

d. The only automorphism of $\mathbb{R}$ is the identity automorphism.

SECTION 44 SPLITTING FIELDS

In Example 43.4, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ included all the zeros of the minimal polynomials for $\sqrt{2}$ and $\sqrt{3}$ over $\mathbb{Q}$. This is a key requirement in order to have the Galois correspondence between subgroups of the automorphism group of a field extension and intermediate fields. We saw in Example 43.14 that the correspondence failed due to the fact that the polynomial $x^3 - 2$ had only one zero in $\mathbb{Q}(\sqrt[3]{2})$. Definition 44.1 formalizes this idea.

44.1 Definition Let F be a field and $P = \{f_1(x), f_2(x), \ldots, f_s(x)\}$ be a finite set of polynomials in $F[x]$. An extension field K of F is a **splitting field of** P **over** F if every polynomial $f_k(x) \in P$ factors into linear factors in $K[x]$ and for any intermediate field E, $F \leq E < K$, at least one polynomial $f_j(x) \in P$ does not factor into linear factors in $E[x]$. A field K is a **splitting field for** F if E is a splitting field for some finite set of polynomials. ■

44.2 Example The field $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(-1+\sqrt{3}i)/2)$ is a splitting field of $\{x^3 - 2\}$ over $\mathbb{Q}$. The zeros of $x^3 - 2$ are

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\frac{-1+\sqrt{3}i}{2}, \quad \text{and} \quad \sqrt[3]{2}\frac{-1-\sqrt{3}i}{2};$$

and each is an element of E. Also, any proper subfield of E would either not contain $\sqrt[3]{2}$ or not contain $\sqrt[3]{2}(-1+\sqrt{3}i)/2$. ▲

Before using splitting fields, we need to verify that they actually exist! Here we give a proof based on the existence of an algebraic closure. Exercise 31 gives an alternative way of proving the existence without relying on an algebraic closure.

44.3 Theorem Let F be a field and $P = \{f_1, f_2, \ldots, f_s\}$ a finite set of polynomials in $F[x]$. Then there is a splitting field K of P over F. Furthermore K is a finite extension of F.

Proof Let $\overline{F}$ be an algebraic closure of F and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{F}$ be a list of all the zeros of all the polynomials in P. Let $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Since $\overline{F}$ is algebraically closed, each polynomial f_k factors into linear factors in $\overline{F}[x]$ and, therefore, in $K[x]$. Furthermore, for any proper subfield E of K that contains F, E does not contain at least one α_j, which says that at least one f_k does not factor into linear factors in $E[x]$. Thus K is a splitting field of P over F. The fact that K is a finite extension of F follows from Corollary 40.6, the fact that each α_k is algebraic, and there are only a finite number of α_k. ◆

We only defined splitting fields using a finite collection of polynomials. It is also possible to use infinite sets of polynomials, but for our purposes finite sets of polynomials will do. We restrict out attention to splitting fields that are finite algebraic extensions.

In the proof of Theorem 44.3 we attached all the roots of all the polynomials in order to construct a splitting field. We will use the fact that a splitting field K of P over F has the property that $K = F(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the zeros of the polynomials in P in an algebraic closure of F. Explicitly attaching some of the roots may be unnecessary. We saw in Example 44.2 that the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(-1+\sqrt{3}i)/2)$. It is unnecessary to attach $\sqrt[3]{2}(-1-\sqrt{3}i)/2$, the third zero of $x^3 - 2$, since it is already an element of $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(-1+\sqrt{3}i)/2)$, that is,

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(-1+\sqrt{3}i)/2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}(-1+\sqrt{3}i)/2, \sqrt[3]{2}(-1-\sqrt{3}i)/2).$$

The Isomorphism Extension Theorem

Now that we know splitting fields exist, it is natural to ask if they are unique up to isomorphism. To answer the question we need the Isomorphism Extension Theorem. We first give a definition that makes the theorem easier to state.

44.4 Definition Let $\sigma : F \to F'$ be a field isomorphism; then $\sigma_x : F[x] \to F'[x]$, defined by

$$\sigma_x(a_0 + a_1 x + \cdots + a_n x^n) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n,$$

is the **polynomial extension of** σ. ■

The image $\sigma_x(f(x))$ is simply the polynomial in $F'[x]$ that corresponds to the polynomial $f(x)$ in $F[x]$ obtained by relabeling the coefficients via the isomorphism σ. It is intuitively clear that if $\sigma : F \to F'$ is an isomorphism, then $\sigma_x : F[x] \to F'[x]$ is also an isomorphism. You are asked to verify the details of the proof in Exercise 32 .

44.5 Lemma Let $K = F(\alpha)$, where α is algebraic over F, and let $\sigma : F \to F'$ be a field isomorphism. If K' is an extension field of F' and $\beta \in K'$ is a zero of $\sigma_x(\operatorname{irr}(\alpha, F))$, then there is a unique isomorphism $\phi : F(\alpha) \to F'(\beta)$ with $\sigma(a) = \phi(a)$ for all $a \in F$ and $\phi(\alpha) = \beta$.

Proof Let $p(x) = \operatorname{irr}(\alpha, F)$ be the minimal polynomial for α over F. Then $p'(x) = \sigma_x(p(x))$ is an irreducible polynomial over F' since any factorization of $p'(x)$ in $F'[x]$ would give a factorization of $p(x)$ in $F[x]$. Since $p'(x)$ is irreducible over F' and β is a zero of $p'(x)$, $p'(x) = \operatorname{irr}(\beta, F')$.

As in the proof of Kronecker's Theorem 39.3, we have an isomorphism $\psi_\alpha : F[x]/\langle p(x)\rangle \to F(\alpha)$, which is defined by the formula:

$$\psi_\alpha(f(x) + \langle p(x)\rangle) = f(\alpha)$$

for any $f(x) \in F[x]$.

We also have an isomorphism $\psi_\beta : F'[x]/\langle p'(x)\rangle \to F(\beta)$ defined by

$$\psi_\beta(g(x) + \langle p'(x)\rangle) = g(\beta)$$

for any $g(x) \in F'[x]$.

A third isomorphism is $\theta : F[x]/\langle p(x)\rangle \to F'[x]/\langle p'(x)\rangle$ defined by

$$\theta(f(x) + \langle p(x)\rangle) = \sigma_x(f(x)) + \langle p'(x)\rangle$$

for any $f(x) \in F[x]$. The fact that θ is a homomorphism is Exercise 28 in Section 30. Also, using the homomorphism $\sigma_x^{-1} : F'[x] \to F[x]$, Exercise 28 in Section 30 shows that θ^{-1} is well defined. Therefore, θ is a one-to-one homomorphism mapping onto $F'[x]/\langle p'(x)\rangle$, or an isomorphism. The fact that θ is an isomorphism is intuitively clear since σ is an isomorphism between F and F' and the polynomial $p(x) \in F[x]$ corresponds to the polynomial $p'(x)$ by way of the isomorphism σ_x.

We now consider the isomorphism $\tau = \psi_\beta \circ \theta \circ \psi_\alpha^{-1}$. Let $a \in F$. We need to verify that $\tau(a) = \sigma(a)$. In the following calculation, we are thinking of a as a constant polynomial in $F[x]$, so $\sigma_x(a) = \sigma(a)$ and $\psi_\beta(\sigma_x(a) + \langle p'(x)\rangle) = \sigma(a)$. We have

$$\begin{aligned}
\tau(a) &= \psi_\beta \circ \theta \circ \psi_\alpha^{-1}(a) \\
&= \psi_\beta(\theta(a + \langle p(x)\rangle)) \\
&= \psi_\beta(\sigma_x(a) + \langle p'(x)\rangle) \\
&= \psi_\beta(\sigma(a) + \langle p'(x)\rangle) \\
&= \sigma(a).
\end{aligned}$$

Also,

$$\begin{aligned}
\tau(\alpha) &= \psi_\beta \circ \theta \circ \psi_\alpha^{-1}(\alpha) \\
&= \psi_\beta(\theta(x + \langle p(x)\rangle) \\
&= \psi_\beta(x + \langle p'(x)\rangle) \\
&= \beta.
\end{aligned}$$

Uniqueness follows since an isomorphism $\rho : F(\alpha) \to F'(\beta)$ is completely determined by the values of $\rho(a)$ for $a \in F$ and $\rho(\alpha)$. ◆

44.6 Theorem **(Isomorphism Extension Theorem)** Let $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a finite extension field of F, and let $\sigma : F \to F'$ be a field isomorphism. If K' contains a splitting field of $P = \{\sigma_x(\operatorname{irr}(\alpha_k, F)) \mid 1 \le k \le n\}$ over F', then σ can be extended to an isomorphism τ mapping K onto a subfield of K'.

Proof We first show that σ can be extended to an isomorphism mapping $F(\alpha_1)$ onto a subfield of K'. Since K' is the splitting field of P over F, there is a $\beta \in K'$ that is a zero of $\sigma_x(\text{irr}(\alpha_1, F))$. By Lemma 44.5, there is an isomorphism τ with the required properties.

We proceed by induction. Suppose τ is an isomorphism from $F(\alpha_1, \ldots, \alpha_k)$ to some subfield of K' such that $\tau(\alpha) = \sigma(\alpha)$ for all $\alpha \in F$. We need to extend τ to an isomorphism from $F(\alpha_1, \ldots, \alpha_k, \alpha_{k+1})$ to K'. There is a $\beta \in K'$ that is a zero of $g(x) = \tau_x(\text{irr}(\alpha_{k+1}, F(\alpha_1, \ldots, \alpha_k)))$ since $g(x)$ is a factor of

$$\tau_x(\text{irr}(\alpha_{k+1}, F)) = \sigma_x(\text{irr}(\alpha_{k+1}, F)),$$

which factors into linear factors in K'. By Lemma 44.5, there is an isomorphism τ' mapping $F(\alpha_1, \ldots, \alpha_{k+1})$ to a subfield of K' that extends τ. So by induction, σ can be extended to an isomorphism that maps K onto a subfield of K'. ◆

44.7 Example We consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. The map

$$\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$

defined by

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$$

is an isomorphism. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $x^2 - 3$ over $\mathbb{Q}(\sqrt{2})$, σ can be extended to an isomorphism $\tau : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ by Theorem 44.6. The proof of the theorem actually tells us more. We can choose τ to map to either zero of $x^2 - 3$, so we have two different choices for τ. In the notation of Example 43.4, these are the automorphisms σ and γ.

We could have used the identity map from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{2})$ instead of σ for the isomorphism. Extending the identity isomorphism to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ gives the automorphisms labeled ι and τ in Example 43.4. The Isomorphism Extension Theorem provides us with a simple way to show the existence of automorphisms that would otherwise be tedious to verify. ▲

Properties of Splitting Fields

We now show that given a finite set of polynomials, $P \subseteq F[x]$, a splitting field of P over F is unique up to isomorphism.

44.8 Theorem Let F be a field, $P = \{f_1, f_2, \ldots, f_s\} \subseteq F[x]$ a finite set of polynomials, and both K and K' splitting fields of P over F. Then there is an isomorphism $\sigma : K \to K'$, which is the identity map on F.

Proof Let K and K' both be splitting fields of P over F. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the zeros of the polynomials of P in K and $\beta_1, \beta_2, \ldots, \beta_m$ the zeros of the polynomials of P in K'. Then

$$K = F(\alpha_1, \ldots, \alpha_n) \quad \text{and} \quad K' = F(\beta_1, \ldots, \beta_m).$$

The extensions K and K' are finite over F since the α_i and β_j are algebraic. The extension K' over F is a splitting field of P, so it is also a splitting field of P', the set of all irreducible factors over F of the polynomials in P. By Theorem 44.6, there is an isomorphism τ mapping K onto a subfield of K' that fixes the field F. Furthermore, since τ preserves the degree of the extension over F, the degree of the extension K' over F is greater than or equal to the degree of the extension K over F. Similarly, there is an isomorphism mapping K' onto a subfield of K, and the degree of the extension K over F is greater than or equal to the degree of the extension K' over F. Thus K and K' have the same degree as extensions of F. Since $\tau(K) \leq K'$, and each has the same degree as an extension over F, τ is an isomorphism mapping K onto K'. ◆