Thus a can be any rational number other than

$$\frac{\sqrt{2}-\sqrt{2}}{\sqrt{3}-(-\sqrt{3})}=0 \quad\text{and}\quad \frac{-\sqrt{2}-\sqrt{2}}{\sqrt{3}-(-\sqrt{3})}=-\frac{\sqrt{2}}{\sqrt{3}}.$$

Since $-\frac{\sqrt{2}}{\sqrt{3}}$ is not a rational number, we can take $a = 1, 2, 1/2, -17/42$, or any rational number other than 0. Using $a = 2$, we have that

$$\alpha = \beta + a\gamma = \sqrt{2} + 2\sqrt{3}.$$

Thus

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

and in general,

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

for any rational number a other than 0. ▲

45.15 Corollary If F is either a finite field or a field of characteristic 0, then every finite extension of F is a simple extension.

Proof This is an immediate consequence of Theorems 45.7 and 45.13. ◆

Normal Extensions

We have now investigated the essential conditions on a field extension $F \leq E$ that are required in order to apply Galois theory. The requirements are that E is a separable splitting field over F.

45.16 Definition A finite extension E of F is a **normal extension of** F if E is a separable splitting field over F. If E is a normal extension of F, then $G(E/F)$ is the **Galois group of** E **over** F. The Galois group is sometimes denoted by $\mathrm{Gal}(E/F)$. ■

Although one can define an infinite normal extension, for our purposes we will restrict our attention to finite extensions. In what follows, when we refer to a normal extension, it will be assumed that the extension is finite.

45.17 Theorem Let K be a normal extension of F and let E be an intermediate field of the extension, $F \leq E \leq K$. Then K is a normal extension of E and $|G(K/E)| = [K : E]$.

Proof Since K is a splitting field over F, there are polynomials $f_1(x), f_2(x), \ldots, f_r(x) \in F[x]$ with zeros $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and each f_i factors into linear factors in K. Then $K = E(\alpha_1, \alpha_2, \ldots, \alpha_k)$, also. Thus K is the splitting field of $\{f_1(x), f_2(x), \ldots, f_r(x)\}$ over E. Furthermore, Theorem 45.8 states that K is a separable extension of E, which implies that K is a normal extension of E.

Since K is a separable splitting field over E, Corollary 45.10 says that $|G(K/E)| = [K : E]$. ◆

45.18 Corollary If $F \leq E \leq K$ where K is a normal extension of F, then $G(K/E)$ is a subgroup of $G(K/F)$ with index $(G(K/F) : G(K/E)) = [E : F]$.

Proof Theorem 45.17 says that K is a normal extension of E. Each isomorphism $\sigma \in G(K/E)$ fixes all the elements of E and, therefore, σ fixes all the elements of F. Thus $\sigma \in G(K/F)$ and $G(K/E) \leq G(K/F)$.

We have

$$(G(K/F) : G(K/E)) = \frac{|G(K/F)|}{|G(K/E)|} = \frac{[K : F]}{[K : E]} = [E : F].$$ ◆

45.19 Example In Example 44.2 we saw that the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is

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

The degree of the extension of K over $\mathbb{Q}(\sqrt[3]{2})$ is

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

Also, the degree of the extension $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is

$$[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = \deg(\sqrt[3]{2}, \mathbb{Q}) = 3,$$

and

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}\sqrt[3]{2} : \mathbb{Q}] = 6.$$

Since $\mathbb{Q}$ is a perfect field, K is a separable and, therefore, a normal extension of $\mathbb{Q}$. Thus Corollary 45.18 applies and we have

$$|G(K/\mathbb{Q})| = 6, \quad |G(K/\mathbb{Q}(\sqrt[3]{2})| = 2, \quad \text{and} \quad (G(K/\mathbb{Q}) : G(K/\mathbb{Q}(\sqrt[3]{2}))) = 3.$$

Up to isomorphism, there are two groups of order 6, $\mathbb{Z}_6$ and S_3. We will see in Section 46 that $G(K/\mathbb{Q})$ is isomorphic with S_3. ▲

EXERCISES 45

Computations

In Exercises 1 through 4, find an α such that the given field is $\mathbb{Q}(\alpha)$. Show that your α is indeed in the given field. Verify by direct computation that the given generators for the extension of $\mathbb{Q}$ can indeed be expressed as formal polynomials in your α with coefficients in $\mathbb{Q}$.

1. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

2. $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$

3. $\mathbb{Q}(\sqrt{2}, \sqrt{5})$

4. $\mathbb{Q}(i, \sqrt[3]{2})$

Concepts

In Exercises 5 and 6, 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.

5. Let E be a splitting field over F. The *multiplicity of a zero* $\alpha \in E$ of a polynomial $f(x) \in F[x]$ is $\nu \in \mathbb{Z}^+$ if and only if $(x-\alpha)^\nu$ is a factor of $f(x)$ in $F[x]$.

6. Let E be an extension of a field F. An element α in E is *separable over* F if and only if α is a zero of multiplicity 1 of $\mathrm{irr}(\alpha, F)$.

7. Give an example of an $f(x) \in \mathbb{Q}[x]$ that has no zeros in $\mathbb{Q}$ but whose zeros in $\mathbb{C}$ are all of multiplicity 2. Explain how this is consistent with Theorem 45.7, which shows that $\mathbb{Q}$ is perfect.

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

a. Every finite extension of every field F is separable over F.

b. Every finite extension of every finite field F is separable over F.

c. Every field of characteristic 0 is perfect.
d. Every polynomial of degree n over every field F always has n distinct zeros in $\bar{F}$.
e. Every polynomial of degree n over every perfect field F always has n distinct zeros in $\bar{F}$.
f. Every irreducible polynomial of degree n over every perfect field F always has n distinct zeros in $\bar{F}$.
g. Every algebraically closed field is perfect.
h. Every field F has an algebraic extension E that is perfect.
i. If E is a finite separable splitting field extension of F, then $|G(E/F)| = [E : F]$.
j. If a field F is neither finite nor of characteristic 0, then F is not a perfect field.

Theory

9. Show that $\{1, y, \cdots, y^{p-1}\}$ is a basis for $\mathbb{Z}_p(y)$ over $\mathbb{Z}_p(y^p)$, where y is an indeterminate. Referring to Example 45.5, conclude by a degree argument that $x^p - t$ is irreducible over $\mathbb{Z}_p(t)$, where $t = y^p$.

10. Prove that if E is an algebraic extension of a perfect field F, then E is perfect.

11. Let E be a finite field of order p^n.

a. Show that the Frobenius automorphism σ_p, defined in Exercise 35 of Section 43, has order n.
b. Deduce from part (a) that $G(E/\mathbb{Z}_p)$ is cyclic of order n with generator σ_p. [*Hint:* Remember that

$$|G(E/F)| = [E : F]$$

for a normal field extension E over F.]

12. Let $f(x) \in F[x]$, and let $\alpha \in \bar{F}$ be a zero of $f(x)$ of multiplicity ν. Show that $\nu > 1$ if and only if α is also a zero of $f'(x)$, the derivative of $F(x)$. [*Hint:* Apply Exercise 15 is Section 42 to the factorization $f(x) = (x - \alpha)^\nu g(x)$ of $f(x)$ in the ring $\bar{F}[x]$.]

13. Show from Exercise 12 that every irreducible polynomial over a field F of characteristic 0 is separable.

14. Show from Exercise 12 that an irreducible polynomial $q(x)$ over a field F of characteristic $p \neq 0$ is not separable if and only if each exponent of each term of $q(x)$ is divisible by p.

15. Generalize Exercise 12, showing that $f(x) \in F[x]$ has no zero of multiplicity >1 if and only if $f(x)$ and $f'(x)$ have no common factor in $\bar{F}[x]$ of degree >0.

16. Working a bit harder than in Exercise 15, show that $f(x) \in F[x]$ has no zero of multiplicity >1 if and only if $f(x)$ and $f'(x)$ have no common nonconstant factor in $F[x]$. [*Hint:* Use Theorem 35.9 to show that if 1 is a gcd of $f(x)$ and $f'(x)$ in $F[x]$, it is a gcd of these polynomials in $E[x]$ for E any splitting field of F, also.]

17. Describe a feasible computational procedure for determining whether $f(x) \in F[x]$ has a zero of multiplicity >1, without actually finding the zeros of $f(x)$. [*Hint:* Use Exercise 16.]

18. Let $F \leq E \leq K$ be field extensions with K a normal extension of F. By Corollary 45.18, $G(K/E)$ is a subgroup of $G(K/F)$. For two automorphisms $\sigma, \tau \in G(K/F)$, show that they are in the same left cosets of $G(K/E) \leq G(K/F)$ if and only if $\sigma(\alpha) = \tau(\alpha)$ for all $\alpha \in E$.

19. Prove that Definition 45.3 does not depend on which splitting field over F is used.

SECTION 46 GALOIS THEORY

The Galois Theorems

In this section we present the main theorems of Galois theory. These theorems provide precise statements regarding the correspondence between intermediate fields of a normal field extension and subgroups of the Galois group. But first we state key definitions related to the correspondence.

46.1 Definition Let K be a normal extension of F, E an intermediate field of the extension, and H a subgroup of $G(K/F)$. The set of all $\alpha \in K$ such that each element of H fixes α is an intermediate field of the extension K over F, and it is called the **fixed field for** H. We write K_H to denote the fixed field for H.

We let $\lambda(E)$ be the set of all $\sigma \in G(K/F)$ that fix all the elements of E, that is, $\lambda(E) = G(K/E)$. We call $\lambda(E)$ the **group of** E.

If K is the splitting field of $f(x) \in F[x]$, then we say that $G(K/F)$ is the **group of the polynomial** $f(x)$. ■

46.2 Example Let K be the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$. As we saw in Example 45.19, K is a normal extension of $\mathbb{Q}$ and

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

The group of $f(x)$ is $G(K/\mathbb{Q})$. Also,

$$\lambda(\mathbb{Q}(\sqrt[3]{2})) = \{\sigma \in G(K/\mathbb{Q}) \mid \sigma(\sqrt[3]{2}) = \sqrt[3]{2}\} = G(K/\mathbb{Q}(\sqrt[3]{2})).$$

Both the identity, ι, and complex conjugation, $\sigma(a + bi) = a - bi$, fix $\sqrt[3]{2}$. Therefore,

$$\langle\sigma\rangle = \{\iota, \sigma\} \leq \lambda(\mathbb{Q}(\sqrt[3]{2}))$$

and

$$K_\sigma = \mathbb{Q}(\sqrt[3]{2}).$$

At this point, we can only say $\langle\sigma\rangle$ is a subgroup of $\lambda(\mathbb{Q}(\sqrt[3]{2}))$ since it is conceivable that there could be other automorphisms of $G(K/\mathbb{Q})$ that fix $\mathbb{Q}(\sqrt[3]{2})$. As we will soon see, this cannot be the case, and the two subgroups are equal. ▲

We now present a series of related theorems that together make up the essence of Galois Theory.

46.3 Theorem Let K be a normal extension of a field F and E an intermediate field. The fixed field for the set of all automorphisms of K that fix E is exactly E. That is,

$$E = K_{\lambda(E)}.$$

Proof Clearly $E \subseteq K_{\lambda(E)}$. We show that $K_{\lambda(E)} \subseteq E$. Let α be an element of K that is not in E. The minimal polynomial for α over E has degree at least two and therefore α has a conjugate $\beta \in K$, with $\beta \neq \alpha$, by Corollary 44.12 and the fact that K is a separable extension of F. Theorem 43.18, the Conjugation Isomorphism Theorem, says there is an isomorphism

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

that maps α to β and fixes all the elements of E. The map $\psi_{\alpha,\beta}$ can be extended to an automorphism $\sigma : K \to K$ by the Isomorphism Extension Theorem, Theorem 44.6. Thus $\sigma \in \lambda(E)$, and σ does not fix α. We have shown that if $\alpha \notin E$, then $\lambda(E)$ does not fix α; or equivalently, $K_{\lambda(E)} \subseteq E$, which completes the proof. ◆

46.4 Theorem Let K be a normal extension of a field F and E an intermediate field. The degree of the extension K over E is the order of the group $\lambda(E)$:

$$[K : E] = |\lambda(E)| = |G(K/E)|.$$

Furthermore, the number of left cosets of $\lambda(E)$ in $G(K/F)$ is the degree of the extension of E over F. That is,

$$(G(K/F) : \lambda(E)) = [E : F].$$

Proof Since $\lambda(E) = G(K/E)$, this theorem is simply a restatement of Corollary 45.18. ◆

46.5 Example Continuing Example 46.2, $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. We saw that if σ is complex conjugation, then $\langle\sigma\rangle \leq \lambda(\mathbb{Q}(\sqrt[3]{2}))$. The degree of the extension K over $\mathbb{Q}(\sqrt[3]{2})$ is two since $\alpha = \sqrt{3}i \notin K$, but α is a zero of the degree 2 polynomial $x^2 + 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$. By Theorem 46.4,

$$2 = [K : \mathbb{Q}(\sqrt[3]{2})] = |\lambda(\mathbb{Q}(\sqrt[3]{2}))|.$$

Since $\langle\sigma\rangle \leq \lambda(\mathbb{Q}(\sqrt[3]{2}))$ and both finite groups have the same number of elements,

$$\langle\sigma\rangle = \lambda(\mathbb{Q}(\sqrt[3]{2})).$$ ▲

46.6 Theorem Let K be a normal extension of a field F and H a subgroup of the Galois group $G(K/F)$. The subgroup of $G(K/F)$ that fixes all the elements fixed by K_H is exactly H. That is,

$$\lambda(K_H) = H.$$

Proof It is clear that H is a subgroup of $\lambda(K_H)$. We will verify that the two groups are equal by checking that they have the same number of elements. Let $k = |H|$.

By Theorem 45.13, the field extension K over F has a primitive element, α, so $K = F(\alpha)$. Let $E = K_H$, the subfield of K that is fixed by every element in H. Then $K = E(\alpha)$ and $[K : E] = \deg(\alpha, E)$. We let $n = [K : E]$. We next let

$$f(x) = \prod_{\sigma \in H}(x - \sigma(\alpha)) \in K[x].$$

The degree of f is $k = |H|$. Let $\tau \in H$, so τ is an isomorphism from K onto K. Since H is a group, multiplying all the elements of H by τ on the left simply permutes the elements of H. That is,

$$H = \{\sigma_1, \sigma_2, \ldots, \sigma_k\} = \{\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_k\}.$$

By Exercise 32 in Section 44, the map $\tau_x : K[x] \to K[x]$ is an isomorphism and

$$\tau_x(f(x)) = \prod_{\sigma \in H}(x - \tau\sigma(\alpha)) = \prod_{\sigma \in H}(x - \sigma(\alpha)) = f(x).$$

Writing $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$,

$$\tau_x(f(x)) = \tau(a_0) + \tau(a_1)x + \tau(a_2)x^2 + \cdots + \tau(a_k)x^k.$$

Equating coefficients in $\tau_x(f(x)) = f(x)$, we see that for any $\tau \in H$, and for any i, $a_i = \tau(a_i)$. But the only elements of K that are fixed by every element in H are the elements of $E = K_H$, which implies that each a_i is in E. Therefore, $f(x) \in E[x]$. Since the identity map is in H, α is a zero of $f(x)$. Thus $\mathrm{irr}(\alpha, E)$ divides $f(x)$ and

$$k = \deg(f(x)) \geq \deg(\mathrm{irr}(\alpha, E)) = \deg(\alpha, E) = n.$$

Since H is a subgroup of $\lambda(K_H)$,

$$k = |H| \leq |\lambda(K_H)| = [K : E] = n.$$

Thus we have $k = n$ and $\lambda(K_H) = H$. ◆

Theorems 46.3 and 46.6 together imply that for normal extensions, the map λ, which maps the intermediate fields of the extension K over F to subgroups of $G(K/F)$, is both one-to-one and onto. Furthermore the inverse map λ^{-1} is simply the map that sends a subgroup $H \leq G(K/E)$ to the intermediate field $K_H = G(K/E)$.

46.7 Example Let $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ over $\mathbb{Q}$. In Example 45.19, we determined that $|G(K/\mathbb{Q})| = 6$. In this example, we take an alternate route to arrive at the same conclusion. In