Since $G(E/F)$ is a subgroup of the automorphisms of E, we naturally call $G(E/F)$ the **group of automorphisms of** E **that fix** F. More briefly, we say that $G(E/F)$ is the **group of** E **over** F.

Beware! The symbol "/" in $G(E/F)$ does not refer to a fraction or a quotient space. The symbol "/" is used since we read $G(E/F)$ as the group of E *over* F and in the subfield diagram, E is written above F.

Since $G(E/F)$ is a subgroup of the automorphisms of E, we naturally call $G(E/F)$ the **group of automorphisms of** E **that fix** F. More briefly, we say that $G(E/F)$ is the **group of** E **over** F.

Beware! The symbol "/" in $G(E/F)$ does not refer to a fraction or a quotient space. The symbol "/" is used since we read $G(E/F)$ as the group of E *over* F and in the subfield diagram, E is written above F.

Conjugation Isomorphisms

In our ongoing example of $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we noticed that for any automorphism σ of K, $\sigma(\sqrt{2}) = \pm\sqrt{2}$ since the image of a zero of $x^2 - 2$ must also be a zero of $x^2 - 2$. This observation can be used for any polynomial and it is the basis for the Conjugation Theorem.

43.16 Definition Let E be an algebraic extension of the field F. Two elements α and β in E are **conjugates over** F, if both have the same minimal polynomial over F. That is, $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$. ■

43.17 Example The definition of conjugates over F is consistent with our familiar use of the term complex conjugates in the setting of complex numbers. For $a, b \in \mathbb{R}$, the numbers $a + bi$ and $a - bi$ are complex conjugates. Both are zeros of the polynomial $f(x) = x^2 - 2ax + a^2 + b^2$ and, as long as $b \neq 0$, $f(x)$ is irreducible over $\mathbb{R}$. Thus for $b \neq 0$, $a + bi$ and $a - bi$ have the same minimal polynomial and they are conjugates over $\mathbb{R}$ in the sense of Definition 43.16. ▲

43.18 Theorem **(The Conjugation Isomorphism)** Let F be a field, K an extension field of F, and $\alpha, \beta \in K$ algebraic over F with $\deg(\alpha, F) = n$. The map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ defined by

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{n-1}\beta^{n-1},$$

for $c_i \in F$, is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F.

Proof We first assume that $\psi_{\alpha,\beta}$ is an isomorphism. Since $\deg(\alpha, F) = n$, $\text{irr}(\alpha, F) = x^n + g(x)$, for some polynomial $g(x) \in F[x]$, where the degree of $g(x)$ is less than n. Therefore

$$\alpha^n = -g(\alpha).$$

Since $\psi_{\alpha,\beta}$ is an isomorphism,

$$\psi_{\alpha,\beta}(\alpha^n) = (\psi_{\alpha,\beta}(\alpha))^n = \beta^n.$$

On the other hand,

$$\psi_{\alpha,\beta}(g(\alpha)) = g(\beta).$$

Thus

$$\beta^n = \psi_{\alpha,\beta}(\alpha^n) = \psi_{\alpha,\beta}(-g(\alpha)) = -g(\beta).$$

So β is a zero of the polynomial $x^n + g(x) = \text{irr}(\alpha, F)$, which is irreducible over F. By the definition of the minimal polynomial, $\text{irr}(\beta, F) = x^n + g(x) = \text{irr}(\alpha, F)$.

We next assume that α and β are conjugates over F with minimal polynomial $p(x) = \text{irr}(\alpha, F) = \text{irr}(\beta, F)$. By Corollary 39.14, the ideal $\langle p(x)\rangle \subseteq F[x]$ is the kernel of the evaluation homomorphism $\phi_\alpha : F[x] \to F(\alpha)$, which is onto. By the Fundamental Homomorphism Theorem 30.17, there is an isomorphism $\psi_\alpha : F[x]/\langle p(x)\rangle \to F(\alpha)$ with $\psi_\alpha(a + \langle p(x)\rangle) = a$ for all $a \in F$ and $\psi_\alpha(x + \langle p(x)\rangle) = \alpha$. Similarly, there is an isomorphism $\psi_\beta : F[x]/\langle p(x)\rangle \to F(\beta)$ with $\psi_\beta(a + \langle p(x)\rangle) = a$ for all $a \in F$, and $\psi_\beta(x + \langle p(x)\rangle) = \beta$. Since ψ_α and ψ_β are both isomorphisms, $\psi_\alpha^{-1} : F(\alpha) \to F[x]/\langle p(x)\rangle$ is an isomorphism and $\psi_{\alpha,\beta} = \psi_\beta \circ \psi_\alpha^{-1} : F(\alpha) \to F(\beta)$ is also an isomorphism. We have

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

We also note that for $c \in F$, $\psi_{\alpha,\beta}(c) = c$. Let $c_0, c_1, \ldots, c_{n-1} \in F$ since $\psi_{\alpha,\beta}$ is an isomorphism,

$$\begin{aligned}&\psi_{\alpha,\beta}(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) \\ &\qquad = \psi_{\alpha,\beta}(c_0) + \psi_{\alpha,\beta}(c_1)\psi_{\alpha,\beta}(\alpha) + \cdots + \psi_{\alpha,\beta}(c_{n-1})\psi_{\alpha,\beta}(\alpha^{n-1}) \\ &\qquad = c_0 + c_1\psi_{\alpha,\beta}(\alpha) + \cdots + c_{n-1}\psi_{\alpha,\beta}(\alpha)^{n-1} \\ &\qquad = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}.\end{aligned}$$

◆

43.19 Corollary Let K be a field extension of F with $\alpha \in K$ algebraic over F. Suppose that ψ is an isomorphism of $F(\alpha)$ onto a subfield of K, with the property that every element of F is fixed by ψ. Then ψ maps α to a conjugate over F of α. Conversely, if $\beta \in K$ is conjugate over F with α, then there is a unique isomorphism $\psi_{\alpha,\beta}$ mapping $F(\alpha)$ onto a subfield of K with the properties that each $a \in F$ is fixed by σ and $\sigma(\alpha) = \beta$.

Proof Let ψ be an isomorphism from $F(\alpha)$ onto a subfield of K with the property that every element of F is fixed by ψ. Let $\text{irr}(\alpha, F) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Then

$$a_0 + a_1\alpha + \ldots a_{n-1}\alpha^{n-1} = 0$$

and

$$0 = \psi(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\psi(\alpha) + \cdots + a_{n-1}\psi(\alpha)^{n-1}.$$

Thus $\beta = \psi(\alpha)$ has minimal polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ over F, which says that α and β are conjugates over F.

Now we let $\beta \in K$ be a conjugate of α over F. Theorem 43.18 provides an isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ with the desired properties. Uniqueness follows since any isomorphism from $F(\alpha)$ to any field is completely determined by its values on elements of F and its value on α. ◆

Theorem 43.9 and Corollary 43.19 formalize ideas used in Examples 43.7 and 43.14. Any automorphism σ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ when restricted to the subfield $\mathbb{Q}(\sqrt{2})$ is an isomorphism onto a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Corollary 43.19 states that the automorphism maps $\sqrt{2}$ to $\pm\sqrt{2}$. Similarly $\sqrt{3}$ maps to $\pm\sqrt{3}$, making a total of at most four automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Looking back at Example 43.14, any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ maps $\sqrt[3]{2}$ to a conjugate over $\mathbb{Q}$ and fixes elements of $\mathbb{Q}$. But $\sqrt[3]{2}$ has no conjugates in $\mathbb{Q}(\sqrt[3]{2})$ other than itself, so the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$ is the identity map. Corollary 43.19 is essential for the rest of our study of Galois theory.

We now give a familiar corollary of Theorem 43.18 concerning complex number zeros of polynomials with real coefficients. Corollary 43.20 states that complex zeros of polynomials with real coefficients occur in conjugate pairs.

43.20 Corollary Let $f(x) \in \mathbb{R}[x]$. If $a, b \in \mathbb{R}$ and $f(a+bi) = 0$, then $f(a-bi) = 0$.

Proof As a field $\mathbb{C} = \mathbb{R}(i)$. Both i and $-i$ have minimal polynomial x^2+1 over $\mathbb{R}$, so they are conjugate over R. Theorem 43.18 assures us that there is an automorphism $\psi_{i,-i} : \mathbb{R}(i) = \mathbb{C} \to \mathbb{C}$ given by $\psi_{i,-i}(a+ib) = a - bi$. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

and assume that $a + bi$ is a zero of $f(x)$. Then

$$0 = f(a+bi) = a_0 + a_1(a+bi) + a_2(a+bi)^2 + \cdots + a_n(a+bi)^n,$$

so

$$0 = \psi_{i,-i}(f(a+bi)) = a_0 + a_1(a-bi) + a_2(a-bi)^2 + \cdots + a_n(a-bi)^n = f(a-bi).$$

Thus $f(a-bi) = 0$. ◆

In order to pursue the Galois connection between subgroups of $G(K/F)$ and intermediate fields $F \leq E \leq K$, we need a technical condition to be sure that K has enough conjugate elements so Theorem 43.18 and its Corollary 43.19 can be evoked as often as needed. When the technical condition on E is satisfied, then E is called a **splitting field**. We investigate splitting fields in Section 44.

There is one other technical condition that we will need in order to establish the Galois correspondence. That condition says that for each $\alpha \in K$, irr(α, F) has deg(α, F) distinct zeros in the algebraic closure of K. If the field extension E over F satisfies this condition, then the extension is said to be **separable**. As we will see, essentially all of our applications and examples, as well as most field extensions with which we are familiar, are separable. But we are getting ahead of ourselves, as properties of separable extensions are the focus of Section 45.

EXERCISES 43

Computations

In Exercises 1 through 8, find all conjugates in $\mathbb{C}$ of the given number over the given field.

1. $\sqrt{2}$ over $\mathbb{Q}$

2. $\sqrt{2}$ over $\mathbb{R}$

3. $3 + \sqrt{2}$ over $\mathbb{Q}$

4. $\sqrt{2} - \sqrt{3}$ over $\mathbb{Q}$

5. $\sqrt{2} + i$ over $\mathbb{Q}$

6. $\sqrt{2} + i$ over $\mathbb{R}$

7. $\sqrt{1 + \sqrt{2}}$ over $\mathbb{Q}$

8. $\sqrt{1 + \sqrt{2}}$ over $\mathbb{Q}(\sqrt{2})$

In Exercises 9 through 15, we consider the field $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. It can be shown that $[E : \mathbb{Q}] = 8$. In the notation of Theorem 43.18, we have the following conjugation isomorphisms (which are here automorphisms of E):

$$\psi_{\sqrt{2},-\sqrt{2}} : (\mathbb{Q}(\sqrt{3}, \sqrt{5}))(\sqrt{2}) \to (\mathbb{Q}(\sqrt{3}, \sqrt{5}))(-\sqrt{2}),$$
$$\psi_{\sqrt{3},-\sqrt{3}} : (\mathbb{Q}(\sqrt{2}, \sqrt{5}))(\sqrt{3}) \to (\mathbb{Q}(\sqrt{2}, \sqrt{5}))(-\sqrt{3}),$$
$$\psi_{\sqrt{5},-\sqrt{5}} : (\mathbb{Q}(\sqrt{2}, \sqrt{3}))(\sqrt{5}) \to (\mathbb{Q}(\sqrt{2}, \sqrt{3}))(-\sqrt{5}).$$

For shorter notation, let $\tau_2 = \psi_{\sqrt{2},-\sqrt{2}}$, $\tau_3 = \psi_{\sqrt{3},-\sqrt{3}}$, and $\tau_5 = \psi_{\sqrt{5},-\sqrt{5}}$. Compute the indicated element of E.

9. $\tau_2(\sqrt{3})$

10. $\tau_2(\sqrt{2} + \sqrt{5})$

11. $(\tau_3\tau_2)(\sqrt{2} + 3\sqrt{5})$

12. $(\tau_5\tau_3)\left(\dfrac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}\right)$

13. $(\tau_5{}^2\tau_3\tau_2)(\sqrt{2} + \sqrt{45})$

14. $\tau_3[\tau_5(\sqrt{2} - \sqrt{3} + (\tau_2\tau_5)(\sqrt{30}))]$

15. $\tau_3\tau_5\tau_3^{-1}(\sqrt{3}-\sqrt{5})$

In Exercises 16 through 21, refer to the directions for Exercises 9 through 15 and find the fixed field of the automorphism or set of automorphisms of E.

16. τ_3 **17.** τ_3^2 **18.** $\{\tau_2, \tau_3\}$

19. $\tau_5\tau_2$ **20.** $\tau_5\tau_3\tau_2$ **21.** $\{\tau_2, \tau_3, \tau_5\}$

22. Refer to the directions for Exercises 9 through 15 for this exercise.

a. Show that each of the automorphisms τ_2, τ_3, and τ_5 is of order 2 in $G(E/\mathbb{Q})$. (Remember what is meant by the *order* of an element of a group.)

b. Find the subgroup H of $G(E/\mathbb{Q})$ generated by the elements τ_2, τ_3, and τ_5, and give the group table. [*Hint:* There are eight elements.]

c. Just as was done in Example 43.4, argue that the group H of part (b) is the full group $G(E/\mathbb{Q})$.

Concepts

In Exercises 23 and 24, 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.

23. Two elements, α and β, of an algebraic extension E of a field F are *conjugate over* F if and only if they are both zeros of the same polynomial $f(x)$ in $F[x]$.

24. Two elements, α and β, of an algebraic extension E of a field F are *conjugate over* F if and only if the evaluation homomorphisms $\phi_\alpha : F[x] \to E$ and $\phi_\beta : F[x] \to E$ have the same kernel.

25. The fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(3+\sqrt{2})$ are the same, of course. Let $\alpha = 3+\sqrt{2}$.

a. Find a conjugate $\beta \neq \alpha$ of α over $\mathbb{Q}$.

b. Referring to part (a), compare the conjugation automorphism $\psi_{\sqrt{2},-\sqrt{2}}$ of $\mathbb{Q}(\sqrt{2})$ with the conjugation automorphism $\psi_{\alpha,\beta}$.

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

a. For all $\alpha, \beta \in E$, there is always an automorphism of E mapping α onto β.

b. For α, β algebraic over a field F, there is always an isomorphism of $F(\alpha)$ onto $F(\beta)$.

c. For α, β algebraic and conjugate over a field F, there is always an isomorphism of $F(\alpha)$ onto $F(\beta)$.

d. Every automorphism of every field E fixes every element of the prime subfield of E.

e. Every automorphism of every field E fixes an infinite number of elements of E.

f. Every automorphism of every field E fixes at least two elements of E.

g. Every automorphism of every field E of characteristic 0 fixes an infinite number of elements of E.

h. All automorphisms of a field E form a group under function composition.

i. The set of all elements of a field E fixed by a single automorphism of E forms a subfield of E.

j. For fields $F \leq E \leq K, G(K/E) \leq G(K/F)$.

Proof Synopsis

27. Give a one-sentence synopsis of the "if" part of Theorem 43.18.

28. Give a one-sentence synopsis of the "only if" part of Theorem 43.18.

Theory

29. Prove Theorem 43.2.

30. Show that the only subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. [Hint: Show that a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that is a degree 2 extension of $\mathbb{Q}$ must be of the form $\mathbb{Q}(\sqrt{s})$ for some rational number s.]

31. Let α be algebraic of degree n over F. Show that there are at most n different isomorphisms of $F(\alpha)$ onto a subfield of $\overline{F}$ and leaving F fixed.

32. Let $F(\alpha_1, \cdots, \alpha_n)$ be an extension field of F. Show that any automorphism σ of $F(\alpha_1, \cdots, \alpha_n)$ leaving F fixed is completely determined by the n values $\sigma(\alpha_i)$.