

a. Show that for $a \in \mathbb{Z}$, where $a \not\equiv 0 \pmod{p}$, the congruence $x^2 \equiv a \pmod{p}$ has a solution in \mathbb{Z} if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. [Hint: Formulate an equivalent statement in the finite field \mathbb{Z}_p , and use the theory of cyclic groups.]

b. Using part (a), determine whether or not the polynomial $x^2 - 6$ is irreducible in $\mathbb{Z}_{17}[x]$.

15. Let F be an arbitrary field. We define the **derivative** of $p(x) = \sum_{k=0}^n a_k x^k \in F[x]$ to be $D(p(x)) = \sum_{k=1}^n (k \cdot (a_k x^{k-1}))$.

Let $p(x), q(x) \in F[x]$, and let n and m be nonnegative integers. Prove the following statements.

- a. $D(p(x) + q(x)) = D(p(x)) + D(q(x))$.
- b. $D(ap(x)) = aD(p(x))$ for any $a \in F$.
- c. $D(x^n x^m) = x^n D(x^m) + D(x^n) x^m$.
- d. $D(p(x)x^m) = p(x)D(x^m) + D(p(x))x^m$.
- e. $D(p(x)q(x)) = p(x)D(q(x)) + D(p(x))q(x)$.
- f. $(x - a)^2$ divides $p(x)$ if and only if a is a zero of both $p(x)$ and $D(p(x))$.
- g. Give a proof of Lemma 42.8 using part f.

Galois Theory

- Section 43** Introduction to Galois Theory
- Section 44** Splitting Fields
- Section 45** Separable Extensions
- Section 46** Galois Theory
- Section 47** Illustrations of Galois Theory
- Section 48** Cyclotomic Extensions
- Section 49** Insolvability of the Quintic

SECTION 43 INTRODUCTION TO GALOIS THEORY

An Example

We learned in high school that the quadratic formula provides zeros for polynomials of degree two. There are similar formulas for solutions to polynomials of degree three and four. These solutions all involve addition, subtraction, multiplication, division, and taking radicals. **Galois theory**, which provides an interesting connection between group theory and field theory, can be used to show that it is futile to seek a similar formula for polynomials of degree five or greater. Our main goal for the remainder of the book is to provide a proof of this fact.

43.1 Definition Let E be a field. An **automorphism** of E is a isomorphism of E onto itself. ■

43.2 Theorem The set of automorphisms of a field E is a group under function composition.

Proof The proof is Exercise 29. ◆

43.3 Example A field isomorphism $\phi : E \rightarrow K$ maps $1 \in E$ to $1 \in K$ and, it maps $0 \in E$ to $0 \in K$. Therefore, for any automorphism ϕ of \mathbb{Q} , $\phi(1) = 1$ and $\phi(0) = 0$. It follows by induction that $\phi(n) = n$ for any natural number n . Since $\phi(-x) = -\phi(x)$, for any integer n , $\phi(n) = n$. Every rational number is a ratio of integers, so $\phi(r) = r$ for every rational number r . Therefore the only automorphism of \mathbb{Q} is the identity map. ▲

43.4 Example Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. From Example 40.9, the degree of the extension K over \mathbb{Q} is 4 and a basis for the vector space K over the field \mathbb{Q} is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Thus $K = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$. We determine the automorphisms of K .

Let ϕ be any automorphism of K . Since $\phi(1) = 1$, ϕ maps every rational number to itself as shown in the previous example. Since ϕ is a field automorphism, $\phi(\sqrt{2}^2 - 2) = \phi(0) = 0$. But $\phi(\sqrt{2}^2 - 2) = \phi(\sqrt{2})^2 - 2$. Thus $\phi(\sqrt{2})$ is a zero of the polynomial $x^2 - 2$, which means that $\phi(\sqrt{2})$ is either $\sqrt{2}$ or $-\sqrt{2}$. Similarly, $\phi(\sqrt{3}) = \pm\sqrt{3}$. Given any $a, b, c, d \in \mathbb{Q}$, if

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in K,$$

then

$$\phi(\alpha) = a + b\phi(\sqrt{2}) + c\phi(\sqrt{3}) + d\phi(\sqrt{2})\phi(\sqrt{3}).$$

Once $\phi(\sqrt{2})$ and $\phi(\sqrt{3})$ are specified, there is at most one automorphism meeting these specifications. We have at most four automorphisms of K given by Table 43.5.

43.5 Table

	$\phi(\sqrt{2})$	$\phi(\sqrt{3})$	$\phi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$
ι	$\sqrt{2}$	$\sqrt{3}$	$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$
σ	$-\sqrt{2}$	$\sqrt{3}$	$a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$
τ	$\sqrt{2}$	$-\sqrt{3}$	$a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$
γ	$-\sqrt{2}$	$-\sqrt{3}$	$a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$

It is tedious, but not difficult, to check that each of these maps is a field automorphism. By Theorem 43.2, $G = \{\iota, \sigma, \tau, \gamma\}$ forms a group under function composition. Every group with exactly four elements is isomorphic with the Klein 4-group or the cyclic group of order four. Each element of G has order one or two, so G is isomorphic with the Klein 4-group. ▲

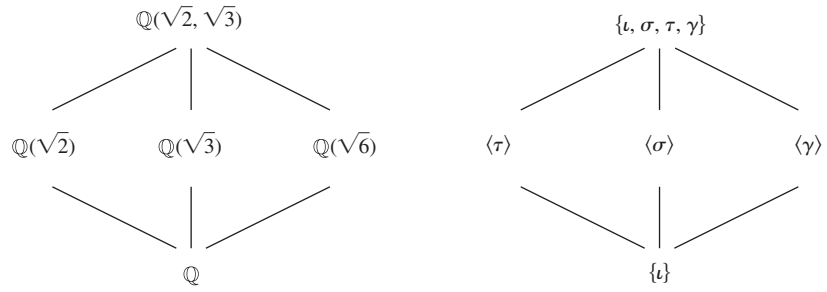
43.6 Definition If E and K are both field extensions of a field F and $\sigma : E \rightarrow K$ is a field isomorphism, then an element $\alpha \in E$ is **fixed by** σ if $\sigma(\alpha) = \alpha$. An element $\alpha \in E$ is **fixed by** a collection of isomorphisms if α is fixed by every isomorphism in the collection. A subset L of E is **fixed by** a collection of isomorphisms if every $\alpha \in L$ is fixed by the collection. Often we write **remains fixed** instead of simply fixed. ■

The discussion in Example 43.3 shows that for any field extensions E and K of \mathbb{Q} and isomorphism $\sigma : E \rightarrow K$, \mathbb{Q} remains fixed by σ .

43.7 Example We find the elements fixed by each of the four automorphisms of G in Example 43.4. From Table 43.5 we see that each element fixes a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, and from this we can determine the field fixed by each subgroup of G .

- Each element K is fixed by ι . In other words, K remains fixed by the trivial subgroup $\{\iota\}$.
- Each element of $\{a + c\sqrt{3} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$ is fixed by σ . This implies that $\mathbb{Q}(\sqrt{3})$ remains fixed by the subgroup $\langle \sigma \rangle \leq G$.
- Each element of $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$ is fixed by τ . So $\mathbb{Q}(\sqrt{2})$ remains fixed by the subgroup $\langle \tau \rangle$.
- Each element of $\{a + d\sqrt{6} \mid a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$ is fixed by γ . Therefore, $\mathbb{Q}(\sqrt{6})$ remains fixed by the subgroup $\langle \gamma \rangle$.
- The only elements that remain fixed by G are the elements of \mathbb{Q} .

Exercise 30 shows the five fields \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, are the only subfields of K . Furthermore, from group theory we know that G , $\langle \sigma \rangle$, $\langle \tau \rangle$, $\langle \gamma \rangle$, and $\{\iota\}$ are the only subgroups of G . We have established a one-to-one correspondence between the subfields of K containing \mathbb{Q} , and the subgroups of the automorphism group of K that fix elements of \mathbb{Q} . Figure 43.8 shows the subfield diagram for K and the subgroup diagram for G . Notice that relabeling the fields by their corresponding subgroups gives the subgroup diagram, except that it is inverted. The reason that the diagrams are flipped is that if $H_1 \leq H_2$ are both subgroups of the automorphism group of K , then every element of K fixed by all the automorphisms in H_2 is also fixed by all the elements of H_1 . So the set that remains fixed by H_2 is a subset of the set that remains fixed by H_1 . ▲



43.8 Figure

The fact that the subfield diagram and the subgroup diagram correspond by associating a subfield of K with a subgroup of G is no accident. In fact, this is the heart of Galois theory. Before we can give precise statements of the Galois theorems, we need a few definitions and some background lemmas and theorems. It is advisable to have Examples 43.4 and 43.7 well in mind when reading the next few sections.

Subfields and Subgroups

We now investigate the Galois correspondence between subfields and subgroups of the automorphism group of a field. In Example 43.7, K was an extension field of \mathbb{Q} . In general we will investigate the automorphisms of a field that fix elements of a subfield that is not necessarily the rational numbers.

43.9 Theorem Let σ be an automorphism of the field E . Then the set E_σ of all the elements $a \in E$ that remain fixed by σ forms a subfield of E .

Proof Suppose that $a, b \in E$ remain fixed by σ , that is, $\sigma(a) = a$ and $\sigma(b) = b$. Since σ is a field automorphism, we have

$$\begin{aligned}\sigma(a \pm b) &= \sigma(a) \pm \sigma(b) = a \pm b, \\ \sigma(ab) &= \sigma(a)\sigma(b) = ab, \\ \sigma(a/b) &= \sigma(a)/\sigma(b) = a/b \quad \text{if } b \neq 0, \\ \sigma(0) &= 0, \text{ and} \\ \sigma(1) &= 1.\end{aligned}$$

Thus $a \pm b, ab, 0, 1 \in E_\sigma$ and if $b \neq 0$, $a/b \in E_\sigma$, which imply that E_σ is a subfield of E . \blacklozenge

43.10 Corollary Let $\{\sigma_i \mid i \in I\}$ be a collection of automorphisms of a field E . Then the set $E_{\{\sigma_i\}}$, of all $a \in E$ that remain fixed by every σ_i , for $i \in I$, is a subfield of E .

Proof The set $E_{\{\sigma_i\}} = \bigcap_{i \in I} E_{\{\sigma_i\}}$ is an intersection of subfields of E , so by Exercise 51 in Section 22, $E_{\{\sigma_i\}}$ is a subfield of E . \blacklozenge

We will continue to use the notation E_σ to denote the subfield of E that remains fixed by the automorphism σ and $E_{\{\sigma_i\}}$ to denote the subfield of E that remains fixed by σ_i for every $i \in I$.

43.11 Example Continuing Example 43.7, $\mathbb{Q}(\sqrt{2}, \sqrt{3})_{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})_{\langle \gamma \rangle} = \mathbb{Q}(\sqrt{6})$. \blacktriangle

In the above discussion we started with a set of automorphisms of a field K and saw that the elements fixed by the automorphisms form a subfield of K . This provides a way

to assign subfields of K to subgroups of the group of automorphisms. We now turn our attention to subfields $F \leq K$ and ask if there is a subgroup of the automorphism group of K that has exactly the set F as a fixed set.

43.12 Definition Let $F \leq K$ be a field extension. The set $G(K/F)$ is the set of all automorphisms of the field K that fix every element of the field F . ■

43.13 Example We see from Examples 43.4 and 43.7 that

$$\begin{aligned} G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) &= \{\iota, \sigma, \tau, \gamma\} \\ G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})) &= \{\iota, \sigma\} = \langle \sigma \rangle \\ G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) &= \{\iota, \tau\} = \langle \tau \rangle \\ G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{6})) &= \{\iota, \gamma\} = \langle \gamma \rangle \\ G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}, \sqrt{3})) &= \{\iota\}. \end{aligned}$$

▲

If K is an extension field of F and $F \leq E \leq K$, then we will refer to E as an **intermediate field** of the extension. In Examples 43.11 and 43.13, we saw that for every intermediate field E of the extension $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, there was a subgroup H of the automorphism group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that fixes every element of E and furthermore, $\mathbb{Q}(\sqrt{2}, \sqrt{3})_H = E$. This one-to-one correspondence between subgroups of the automorphism group and intermediate fields is the essence of Galois theory. There are field extensions where the correspondence fails, as shown by the next example. In order to have this one-to-one correspondence, a few technical conditions on the field extension need to be satisfied.

43.14 Example Let $K = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$. Then $G(K/\mathbb{Q})$ consists of all automorphisms of K that fix all the rational numbers. In $\mathbb{Q}(\sqrt[3]{2})$ there is only one zero of the polynomial $x^3 - 2$ since the other two zeros, $\sqrt[3]{2}(-1 \pm \sqrt{3}i)/2$, are complex numbers and $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the real numbers. For any automorphism $\sigma \in G(K/\mathbb{Q})$,

$$\begin{aligned} 0 &= \sigma(0) = \sigma(\sqrt[3]{2}^3 - 2) \\ &= (\sigma(\sqrt[3]{2}))^3 - 2. \end{aligned}$$

Thus $\sigma(\sqrt[3]{2})$ is a zero of $x^3 - 2$, which implies that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore any field automorphism of K fixes all elements of \mathbb{Q} and $\sqrt[3]{2}$, which implies that the only automorphism of K is the identity automorphism ι . Thus $G(K/\mathbb{Q}) = \{\iota\}$ and $K_{G(K/\mathbb{Q})} = K_{\{\iota\}} = K$. In this case, there is no subgroup $H \leq G(K/\mathbb{Q})$ with $K_H = \mathbb{Q}$. ▲

In the next two sections, we will investigate conditions on field extensions $F \leq K$ where there is a one-to-one correspondence between the intermediate fields and the subgroups of $G(K/F)$.

43.15 Theorem Let E be a field and let F be a subfield of E . Then the set $G(E/F)$ of all automorphisms that fix all the elements of F is a subgroup of the automorphism group of E . Furthermore, F is a subfield of $E_{G(E/F)}$.

Proof For $\sigma, \tau \in G(E/F)$ and $a \in F$,

$$(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = a,$$

so $\sigma\tau \in G(E/F)$. Furthermore, $G(E/F)$ contains the identity map and $\sigma^{-1}(a) = a$. Thus $G(E/F)$ is a subgroup of the automorphisms of E .

Finally, since every automorphism in $G(E/F)$ fixes all the elements of F , F is a subset and, therefore, a subfield of $E_{G(E/F)}$. ♦