Thus

$$|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot 5.$$

Cauchy's Theorem 14.20 says that $G(K/\mathbb{Q})$ has a subgroup of order 5 and therefore an element of order 5. So $G(K/\mathbb{Q})$ has an element that permutes the zeros of $f(x)$ in a 5-cycle, since the only elements in S_5 that have order 5 are the 5-cycles. Also, complex conjugation is an element in $G(K/\mathbb{Q})$ that fixes each real zero of $f(x)$ and switches the two complex zeros. Thus an element of $G(K/\mathbb{Q})$ permutes the zeros of $f(x)$ by a 2-cycle. By Theorem 49.5, $G(K/\mathbb{Q})$ is isomorphic with S_5.

49.6 Theorem There is a polynomial in $\mathbb{Q}[x]$ that is not solvable by radicals.

Proof As we just discovered, $f(x) = 2x^5 - 5x^4 + 5$ is one such polynomial since its splitting field over $\mathbb{Q}$ has Galois group isomorphic with S_5, which is not a solvable group. ◆

There are many other polynomials that are not solvable by radicals. In the proof given above, we need a few key properties for the polynomial $f(x)$ to have Galois group S_5. First we require that $f(x)$ be an irreducible polynomial over $\mathbb{Q}$ with degree 5. We then exploit the fact that $f(x)$ has three real zeros and two complex zeros. As long as a polynomial meets these conditions, the polynomial is not solvable by radicals. The set of polynomials with these properties is infinite as shown in Exercise 8.

Exercise 9 gives a different approach to constructing polynomials in $F[x]$ whose Galois group over F is S_5, where F is a subfield of $\mathbb{R}$. This approach also shows that there are an infinite number of polynomials that are not solvable by radicals, although the polynomials do not have rational coefficients. While Exercises 8 and 9 both produce an infinite number of polynomials that are not solvable by radicals, in Exercise 8 the number is countable while in Exercise 9 the number is uncountable.

EXERCISES 49

Concepts

1. Can the splitting field K of $x^2 + x + 1$ over $\mathbb{Z}_2$ be obtained by adjoining a square root to $\mathbb{Z}_2$ of an element in $\mathbb{Z}_2$? Is K an extension of $\mathbb{Z}_2$ by radicals?
2. Is every polynomial in $F[x]$ of the form $ax^8 + bx^6 + cx^4 + dx^2 + e$, where $a \neq 0$, solvable by radicals over F, if $F \leq \mathbb{R}$? Why or why not?
3. Determine whether each of the following is true or false.
   a. Let F be a field of characteristic 0. A polynomial in $F[x]$ is solvable by radicals if and only if its splitting field in $\bar{F}$ is contained in an extension of F by radicals.
   b. Let F be a field of characteristic 0. A polynomial in $F[x]$ is solvable by radicals if and only if its splitting field in $\bar{F}$ has a solvable Galois group over F.
   c. The splitting field of $x^{17} - 5$ over $\mathbb{Q}$ has a solvable Galois group.
   d. If $f(x) \in \mathbb{Q}[x]$ is any polynomial of degree five having three real zeros and two complex zeros, then $f(x)$ is not solvable by radicals.
   e. The Galois group of a finite extension of a finite field is solvable.
   f. No quintic polynomial is solvable by radicals over any field.
   g. Every 4th degree polynomial over a field $F \leq \mathbb{R}$ is solvable by radicals.
   h. The zeros of a cubic polynomial over a field $F \leq \mathbb{R}$ can always be attained by means of a finite sequence of operations of addition, subtraction, multiplication, division, and taking square roots starting with elements in F.

i. The zeros of a cubic polynomial over a field F of characteristic 0 can never be attained by means of a finite sequence of operations of addition, subtraction, multiplication, division, and taking square roots, starting with elements in F.

j. The theory of subnormal series of groups plays an important role in applications of Galois theory.

Theory

4. Let F be a field, and let $f(x) = ax^2 + bx + c$ be in $F[x]$, where $a \neq 0$. Show that if the characteristic of F is not 2, the splitting field of $f(x)$ over F is $F(\sqrt{b^2 - 4ac})$. [*Hint:* Complete the square, just as in your high school work, to derive the "quadratic formula."]

5. Show that if F is a field of characteristic different from 2 and

$$f(x) = ax^4 + bx^2 + c,$$

where $a \neq 0$, then $f(x)$ is solvable by radicals over F.

6. Show that for a finite group, every refinement of a subnormal series with abelian quotients also has abelian quotients, thus completing the proof of Lemma 49.3. [*Hint:* Use Theorem 16.8.]

7. Show that for a finite group, a subnormal series with solvable quotient groups can be refined to a composition series with abelian quotients, thus completing the proof of Theorem 49.4. [*Hint:* Use Theorem 16.8.]

8. Let p be a prime number and $f(x) = x^5 - p^2x + p \in \mathbb{Q}[x]$. Prove that $f(x)$ is not solvable by radicals. [Hint: Mimic the proof that $2x^5 - 5x^4 + 5$ is not solvable by radicals.]

9. This is an alternate method of finding a polynomial with coefficients in a field F, a subfield of $\mathbb{R}$, whose Galois group over F is S_5.

a. Suppose that $F \leq \mathbb{R}$ is a countable field and x is an indeterminate. Show that $F[x]$, $F(x)$, and the set of real numbers that are algebraic over F are all countable sets.

b. Show that there is a sequence of real numbers $y_1, y_2, \cdots \in \mathbb{R}$, with y_1 transcendental over $\mathbb{Q}$, and for each $i > 1$, y_i is transcendental over $\mathbb{Q}(y_1, y_2, \ldots, y_{i-1})$.

c. Using the notation of part b), let $K = \mathbb{Q}(y_1, y_2, y_3, y_4, y_5)$ and

$$f(x) = \prod_{i=1}^{5}(x - y_i).$$

Let s_1, s_2, s_3, s_4, s_5 be the value of the elementary symmetric functions (as defined in Section 47) evaluated at y_1, y_2, y_3, y_4, y_5. Show that $f(x) \in F = \mathbb{Q}(s_1, s_2, s_3, s_4, s_5)$.

d. Show that K is the splitting field of $f(x)$ over F and $G(K/F)$ is isomorphic with S_5.

This page is intentionally left blank

Appendix: Matrix Algebra

We give a brief summary of matrix algebra here. Matrices appear in examples in some chapters of the text and also are involved in several exercises.

A **matrix** is a rectangular array of numbers. For example, the array

$$\begin{bmatrix} 2 & -1 & 4 \\ 3 & 1 & 2 \end{bmatrix} \tag{1}$$

is a matrix having two rows and three columns. A matrix having m rows and n columns is an $m \times n$ matrix, so Matrix (1) is a 2×3 matrix. If $m = n$, the matrix is **square**. Entries in a matrix may be any type of number—integer, rational, real, or complex. We let $M_{m\times n}(\mathbb{R})$ be the set of all $m \times n$ matrices with real number entries. If $m = n$, the notation is abbreviated to $M_n(\mathbb{R})$. We can similarly consider $M_n(\mathbb{Z}), M_{2\times 3}(\mathbb{C})$, etc.

Two matrices having the same number m of rows and the same number n of columns can be added in the obvious way: we add entries in corresponding positions.

A1 Example In $M_{2\times 3}(\mathbb{Z})$, we have

$$\begin{bmatrix} 2 & -1 & 4 \\ 3 & 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -3 \\ 2 & -7 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -1 & 1 \\ 5 & -6 & 3 \end{bmatrix}. \qquad \blacktriangle$$

We will use uppercase letters to denote matrices. If A, B, and C are $m \times n$ matrices, it is easily seen that $A + B = B + A$ and that $A + (B + C) = (A + B) + C$.

Matrix multiplication, AB, is defined only if the number of columns of A is equal to the number of rows of B. That is, if A is an $m \times n$ matrix, then B must be an $n \times s$ matrix for some integer s. We start by defining as follows the product AB where A is a $1 \times n$ matrix and B is an $n \times 1$ matrix:

$$AB = [a_1 \quad a_2 \quad \cdots \quad a_n] \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1b_1 + a_2b_2 + \cdots + a_nb_n. \tag{2}$$

Note that the result is a number. (We shall not distinguish between a number and the 1×1 matrix having that number as its sole entry.) You may recognize this product as the *dot product* of vectors. Matrices having only one *row* or only one *column* are **row vectors** or **column vectors**, respectively.

A2 Example We find that

$$\begin{bmatrix}3 & -7 & 2\end{bmatrix}\begin{bmatrix}1\\4\\5\end{bmatrix} = (3)(1)+(-7)(4)+(2)(5) = -15.$$

▲

Let A be an $m \times n$ matrix and let B be an $n \times s$ matrix. Note that the number n of entries in each row of A is the same as the number n of entries in each column of B. The product $C = AB$ is an $m \times s$ matrix. The entry in the ith row and jth column of AB is the product of the ith row of A times the jth column of B as defined by Eq. (2) and illustrated in Example A2.

A3 Example Compute

$$AB = \begin{bmatrix}2 & -1 & 3\\1 & 4 & 6\end{bmatrix}\begin{bmatrix}3 & 1 & 2 & 1\\1 & 4 & 1 & -1\\-1 & 0 & 2 & 1\end{bmatrix}.$$

Solution Note that A is 2×3 and B is 3×4. Thus AB will be 2×4. The entry in its second row and third column is

$$(\text{2nd row } A)(\text{3rd column } B) = \begin{bmatrix}1 & 4 & 6\end{bmatrix}\begin{bmatrix}2\\1\\2\end{bmatrix} = 2+4+12 = 18.$$

Computing all eight entries of AB in this fashion, we obtain

$$AB = \begin{bmatrix}2 & -2 & 9 & 6\\1 & 17 & 18 & 3\end{bmatrix}.$$

▲

A4 Example The product

$$\begin{bmatrix}2 & -1 & 3\\1 & 4 & 6\end{bmatrix}\begin{bmatrix}2 & 1\\5 & 4\end{bmatrix}$$

is not defined, since the number of entries in a row of the first matrix is not equal to the number of entries in a column of the second matrix. ▲

For square matrices of the same size, both addition and multiplication are always defined. Exercise 10 asks us to illustrate the fact that matrix multiplication is not commutative.

That is, AB need not equal BA even when both products are defined, as for $A, B \in M_2(\mathbb{Z})$. It can be shown that $A(BC) = (AB)C$ and $A(B+C) = AB + AC$ whenever all these expressions are defined.

We let I_n be the $n \times n$ matrix with entries 1 along the diagonal from the upper-left corner to the lower-right corner, and entries 0 elsewhere. For example,

$$I_3 = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}.$$

It is easy to see that if A is any $n \times s$ matrix and B is any $r \times n$ matrix, then $I_n A = A$ and $BI_n = B$. That is, the matrix I_n acts much as the number 1 does for multiplication when multiplication by I_n is defined.