

A BOOK OF ABSTRACT ALGEBRA

Second Edition

Charles C. Pinter
Professor of Mathematics
Bucknell University

Dover Publications, Inc., Mineola, New York

Copyright © 1982, 1990 by Charles C. Pinter
All rights reserved.

Bibliographical Note

This Dover edition, first published in 2010, is an unabridged republication of the 1990 second edition of the work originally published in 1982 by the McGraw-Hill Publishing Company, Inc., New York.

Library of Congress Cataloging-in-Publication Data

Pinter, Charles C, 1932–

A book of abstract algebra / Charles C. Pinter. — Dover ed.

p. cm.

Originally published: 2nd ed. New York : McGraw-Hill, 1990.

Includes bibliographical references and index.

ISBN-13: 978-0-486-47417-5

ISBN-10: 0-486-47417-8

1. Algebra, Abstract. I. Title.

QA162.P56 2010

512'.02—dc22

2009026228

Manufactured in the United States by Courier Corporation
47417803

www.doverpublications.com

Preface

- Chapter 1** Why Abstract Algebra?
History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.
- Chapter 2** Operations
Operations on a Set. Properties of Operations.
- Chapter 3** The Definition of Groups
Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables.
Theory of Coding: Maximum-Likelihood Decoding.
- Chapter 4** Elementary Properties of Groups
Uniqueness of Identity and Inverses. Properties of Inverses.
Direct Product of Groups.
- Chapter 5** Subgroups
Definition of Subgroup. Generators and Defining Relations.
Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.
- Chapter 6** Functions
Injective, Surjective, Bijective Function. Composite and Inverse of Functions.
Finite-State Machines. Automata and Their Semigroups.
- Chapter 7** Groups of Permutations
Symmetric Groups. Dihedral Groups.
An Application of Groups to Anthropology.
- Chapter 8** Permutations of a Finite Set
Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.
- Chapter 9** Isomorphism
The Concept of Isomorphism in Mathematics. Isomorphic and Nonisomorphic Groups. Cayley's Theorem.

Chapter 10 Order of Group Elements

Powers/Multiples of Group Elements. Laws of Exponents. Properties of the Order of Group Elements.

Chapter 11 Cyclic Groups

Finite and Infinite Cyclic Groups. Isomorphism of Cyclic Groups. Subgroups of Cyclic Groups.

Chapter 12 Partitions and Equivalence Relations

Chapter 13 Counting Cosets

Lagrange's Theorem and Elementary Consequences.

Survey of Groups of Order ≤ 10 .

Number of Conjugate Elements. Group Acting on a Set.

Chapter 14 Homomorphisms

Elementary Properties of Homomorphisms. Normal Subgroups. Kernel and Range.

Inner Direct Products. Conjugate Subgroups.

Chapter 15 Quotient Groups

Quotient Group Construction. Examples and Applications.

The Class Equation. Induction on the Order of a Group.

Chapter 16 The Fundamental Homomorphism Theorem

Fundamental Homomorphism Theorem and Some Consequences.

The Isomorphism Theorems. The Correspondence Theorem. Cauchy's Theorem. Sylow Subgroups. Sylow's Theorem. Decomposition Theorem for Finite Abelian Groups.

Chapter 17 Rings: Definitions and Elementary Properties

Commutative Rings. Unity. Invertibles and Zero-Divisors. Integral Domain. Field.

Chapter 18 Ideals and Homomorphisms

Chapter 19 Quotient Rings

Construction of Quotient Rings. Examples. Fundamental Homomorphism Theorem and Some Consequences. Properties of Prime and Maximal Ideals.

Chapter 20 Integral Domains

Characteristic of an Integral Domain. Properties of the Characteristic. Finite Fields. Construction of the Field of Quotients.

Chapter 21 The Integers

Ordered Integral Domains. Well-ordering. Characterization of $\mathbf{Z}$ Up to Isomorphism. Mathematical Induction. Division Algorithm.

Chapter 22 Factoring into Primes

Ideals of $\mathbb{Z}$. Properties of the GCD. Relatively Prime Integers. Primes. Euclid's Lemma. Unique Factorization.

Chapter 23 Elements of Number Theory (Optional)

Properties of Congruence. Theorems of Fermat and Euler. Solutions of Linear Congruences. Chinese Remainder Theorem.

Wilson's Theorem and Consequences. Quadratic Residues. The Legendre Symbol. Primitive Roots.

Chapter 24 Rings of Polynomials

Motivation and Definitions. Domain of Polynomials over a Field. Division Algorithm.

Polynomials in Several Variables. Fields of Polynomial Quotients.

Chapter 25 Factoring Polynomials

Ideals of $F[x]$. Properties of the GCD. Irreducible Polynomials. Unique factorization.

Euclidean Algorithm.

Chapter 26 Substitution in Polynomials

Roots and Factors. Polynomial Functions. Polynomials over $\mathbb{Q}$. Eisenstein's Irreducibility Criterion. Polynomials over the Reals. Polynomial Interpolation.

Chapter 27 Extensions of Fields

Algebraic and Transcendental Elements. The Minimum Polynomial. Basic Theorem on Field Extensions.

Chapter 28 Vector Spaces

Elementary Properties of Vector Spaces. Linear Independence. Basis. Dimension. Linear Transformations.

Chapter 29 Degrees of Field Extensions

Simple and Iterated Extensions. Degree of an Iterated Extension.

Fields of Algebraic Elements. Algebraic Numbers. Algebraic Closure.

Chapter 30 Ruler and Compass

Constructible Points and Numbers. Impossible Constructions.

Constructible Angles and Polygons.

Chapter 31 Galois Theory: Preamble

Multiple Roots. Root Field. Extension of a Field. Isomorphism.

Roots of Unity. Separable Polynomials. Normal Extensions.

Chapter 32 Galois Theory: The Heart of the Matter

Field Automorphisms. The Galois Group. The Galois Correspondence. Fundamental Theorem of Galois Theory.

Computing Galois Groups.

Chapter 33 Solving Equations by Radicals

Radical Extensions. Abelian Extensions. Solvable Groups. Insolubility of the Quintic.

Appendix A	Review of Set Theory
Appendix B	Review of the Integers
Appendix C	Review of Mathematical Induction
	Answers to Selected Exercises
	Index

* Italic headings indicate topics discussed in the exercise sections.

GALOIS THEORY: PREAMBLE

Field extensions were used in [Chapter 30](#) to settle some of the most puzzling questions of classical geometry. Now they will be used to solve a problem equally ancient and important: they will give us a definite and elegant theory of solutions of polynomial equations.

We will be concerned not so much with *finding* solutions (which is a problem of computation) as with the nature and properties of these solutions. As we shall discover, these properties turn out to depend less on the polynomials themselves than on the fields which contain their solutions. This fact should be kept in mind if we want to clearly understand the discussions in this chapter and [Chapter 32](#). We will be speaking of field extensions, but polynomials will always be lurking in the background. Every extension will be generated by roots of a polynomial, and every theorem about these extensions will actually be saying something about the polynomials.

Let us quickly review what we already know of field extensions, filling in a gap or two as we go along. Let F be a field; an element a (in an extension of F) is *algebraic over F* if a is a root of some polynomial with its coefficients in F . The *minimum polynomial* of a over F is the monic polynomial of lowest degree in $F[x]$ having a as a root; every other polynomial in $F[x]$ having a as a root is a multiple of the minimum polynomial.

The basic theorem of field extensions tells us that any polynomial of degree n in $F[x]$ has exactly n roots in a suitable extension of F . However, this does not necessarily mean n *distinct* roots. For example, in $\mathbb{R}[x]$ the polynomial $(x - 2)^5$ has five roots *all equal* to 2. Such roots are called *multiple roots*. It is perfectly obvious that we can come up with polynomials such as $(x - 2)^5$ having multiple roots; but are there any *irreducible* polynomials with multiple roots? Certainly the answer is not obvious. Here it is:

Theorem 1 *If F has characteristic 0, irreducible polynomials over F can never have multiple roots.*

PROOF: To prove this, we must define the *derivative* of the polynomial $a(x) = a_0 + a_1x + \cdots + a_nx^n$. It is $a'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. As in elementary calculus, it is easily checked that for any two polynomials $f(x)$ and $g(x)$,

$$(f + g)' = f' + g' \quad \text{and} \quad (fg)' = fg' + f'g$$

Now suppose $a(x)$ is irreducible in $F[x]$ and has a multiple root c : then in a suitable extension we can factor $a(x)$ as $a(x) = (x - c)^2 q(x)$, and therefore $a'(x) = 2(x - c)q(x) + (x - c)^2 q'(x)$. So $x - c$ is a factor of $a'(x)$, and therefore c is a root of $a'(x)$. Let $p(x)$ be the minimum polynomial of c over F ; since both $a(x)$ and $a'(x)$ have c as a root, they are both multiples of $p(x)$.

But $a(x)$ is irreducible: its only nonconstant divisor is itself; so $p(x)$ must be $a(x)$. However, $a(x)$ cannot divide $a'(x)$ unless $a'(x) = 0$ because $a'(x)$ is of *lower degree* than $a(x)$. So $a'(x) = 0$ and therefore its coefficient na_n is 0. Here is where characteristic 0 comes in: if $na_n = 0$ then $a_n = 0$, and this is impossible because a_n is the leading coefficient of $a(x)$. ■

In the remaining three chapters we will confine our attention to *fields of characteristic 0*. Thus, by [Theorem 1](#), any irreducible polynomial of degree n has n *distinct* roots.

Let us move on with our review. Let E be an extension of F . We call E a *finite extension* of F if E , as a vector space with scalars in F , has finite dimension. Specifically, if E has dimension n , we say that the degree of E over F is equal to n , and we symbolize this by writing $[E: F] = n$. If c is algebraic over F , the degree of $F(c)$ over F turns out to be equal to the degree of $p(x)$, the minimum polynomial of c over F .

$F(c)$, obtained by adjoining an algebraic element c to F , is called a *simple extension* of F . $F(c_1, \dots, c_n)$, obtained by adjoining n algebraic elements in succession to F , is called an *iterated extension* of F . Any iterated extension of F is finite, and, conversely, any finite extension of F is an iterated extension $F(c_1, \dots, c_n)$. In fact, even more is true; let F be of characteristic 0.

Theorem 2 *Every finite extension of F is a **simple** extension $F(c)$.*

PROOF: We already know that every finite extension is an iterated extension. We will now show that any extension $F(a, b)$ is equal to $F(c)$ for some c . Using this result several times in succession yields our theorem. (At each stage, we reduce by 1 the number of elements that must be adjoined to F in order to get the desired extension.)

Well, given $F(a, b)$, let $A(x)$ be the minimum polynomial of a over F , and let $B(x)$ be the minimum polynomial of b over F . Let K denote any extension of F which contains all the roots $a_1, \dots, a_n$ of $A(x)$ as well as all the roots $b_1, \dots, b_m$ of $B(x)$. Let a_1 be a and let b_1 be b .

Let t be any nonzero element of F such that

$$t \neq \frac{a_i - a}{b - b_j} \quad \text{for every } i \neq 1 \text{ and } j \neq 1$$

Cross multiplying and setting $c = a + tb$, it follows that $c \neq a_i + tb_j$, that is,

$$c - tb_j \neq a_i \quad \text{for all } i \neq 1 \text{ and } j \neq 1$$

$$c - tb_j \neq a_i \quad \text{for all } i \neq 1 \text{ and } j \neq 1$$

Define $h(x)$ by letting $h(x) = A(c - tx)$; then

$$h(b) = A(\underbrace{c - tb}_{=a}) = 0$$

while for every $j \neq 1$,

$$h(b_j) = A(\underbrace{c - tb_j}_{\neq \text{any } a_i}) \neq 0$$

Thus, b is the *only common root* of $h(x)$ and $B(x)$.

We will prove that $b \in F(c)$, hence also $a = c - tb \in F(c)$, and therefore $F(a, b) \subseteq F(c)$. But $c \in F(a, b)$, so $F(c) \subseteq F(a, b)$. Thus $F(a, b) = F(c)$.

So, it remains only to prove that $b \in F(c)$. Let $p(x)$ be the minimum polynomial of b over $F(c)$. If the degree of $p(x)$ is 1, then $p(x)$ is $x - b$, so $b \in F(c)$, and we are done. Let us suppose $\deg p(x) \geq 2$ and get a contradiction: observe that $h(x)$ and $B(x)$ must both be multiples of $p(x)$ because both have b as a root, and $p(x)$ is the minimum polynomial of b . But if $h(x)$ and $B(x)$ have a common factor of degree ≥ 2 , they must have two or more roots in common, contrary to the fact that b is their only common root. Our proof is complete. ■

For example, we may apply this theorem directly to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Taking $t = 1$, we get $c = \sqrt{2} + \sqrt{3}$, hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

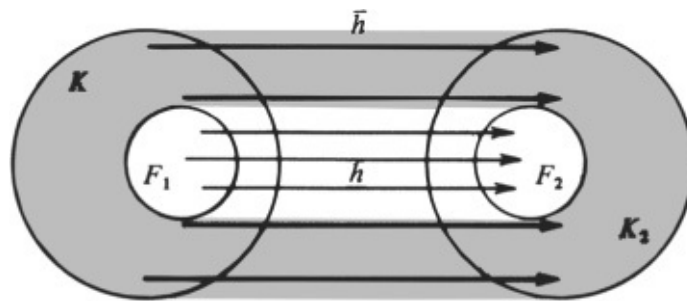
If $a(x)$ is a polynomial of degree n in $F[x]$, let its roots be $c_1, \dots, c_n$. Then $F(c_1, \dots, c_n)$ is clearly *the smallest extension of F containing all the roots of $a(x)$* . $F(c_1, \dots, c_n)$ is called the *root field of $a(x)$ over F* . We will have a great deal to say about root fields in this and subsequent chapters.

Isomorphisms were important when we were dealing with groups, and they are important also for fields. You will remember that if F_1 and F_2 are fields, an *isomorphism* from F_1 to F_2 is a bijective function $h: F_1 \rightarrow F_2$ satisfying

$$h(a + b) = h(a) + h(b) \quad \text{and} \quad h(ab) = h(a)h(b)$$

From these equations it follows that $h(0) = 0$, $h(1) = 1$, $h(-a) = -h(a)$, and $h(a^{-1}) = (h(a))^{-1}$.

Suppose F_1 and F_2 are fields, and $h: F_1 \rightarrow F_2$ is an isomorphism. Let K_1 and K_2 be extensions of F_1 and F_2 , and let $\bar{h}: K_1 \rightarrow K_2$ also be an isomorphism. We call $\bar{h}$ an *extension of h* if $\bar{h}(x) = h(x)$ for every x in F_1 that is, if h and $\bar{h}$ are the same on F_1 . ($\bar{h}$ is an extension of h in the plain sense that it is formed by “adding on” to h .)



As an example, given any isomorphism $h: F_1 \rightarrow F_2$, we can extend h to an isomorphism $\bar{h}: F_1[x] \rightarrow F_2[x]$. (Note that $F[x]$ is an extension of F when we think of the elements of F as constant polynomials; of course, $F[x]$ is not a field, simply an integral domain, but in the present example this fact is unimportant.) Now we ask: What is an obvious and natural way of extending h ? The answer, quite clearly, is to let $\bar{h}$ send the polynomial with coefficients $a_0, a_1, \dots, a_n$ to the polynomial with coefficients

$h(a_0), h(a_1), \dots, h(a_n)$:

$$\bar{h}(a_0 + a_1x + \dots + a_nx^n) = h(a_0) + h(a_1)x + \dots + h(a_n)x^n$$

It is child's play to verify formally that $\bar{h}$ is an isomorphism from $F_1[x]$ to $F_2[x]$. In the sequel, the polynomial $\bar{h}(a(x))$, obtained in this fashion, will be denoted simply by $ha(x)$. Because $\bar{h}$ is an isomorphism, $a(x)$ is irreducible iff $ha(x)$ is irreducible.

A very similar isomorphism extension is given in the next theorem.

Theorem 3 *Let $h: F_1 \rightarrow F_2$ be an isomorphism, and let $p(x)$ be irreducible in $F_1[x]$. Suppose a is a root of $p(x)$, and b a root of $hp(x)$. Then h can be extended to an isomorphism*

$$\bar{h}: F_1(a) \rightarrow F_2(b)$$

Furthermore, $\bar{h}(a) = b$.

PROOF: Remember that every element of $F_1(a)$ is of the form

$$c_0 + c_1a + \dots + c_na^n$$

where $c_0, \dots, c_n$ are in F_1 , and every element of $F_2(b)$ is of the form $d_0 + d_1b + \dots + d_nb^n$ where $d_0, \dots, d_n$ are in F_2 . Imitating what we did successfully in the preceding example, we let $\bar{h}$ send the expression with coefficients $c_0, \dots, c_n$ to the expression with coefficients $h(c_0), \dots, h(c_n)$:

$$\bar{h}(c_0 + c_1a + \dots + c_na^n) = h(c_0) + h(c_1)b + \dots + h(c_n)b^n$$

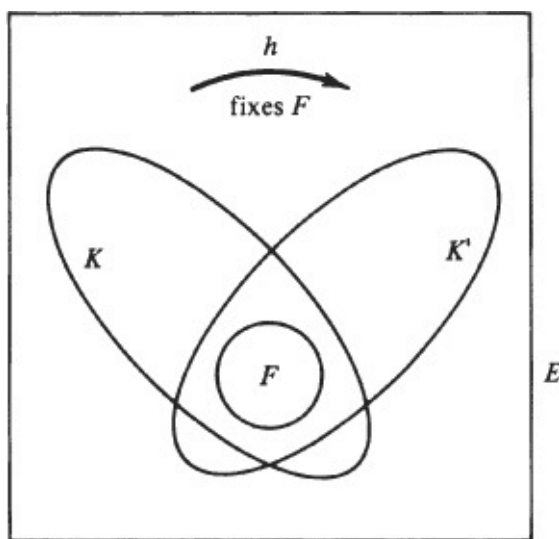
Again, it is routine to verify that $\bar{h}$ is an isomorphism. Details are laid out in [Exercise H](#) at the end of the chapter. ■

Most often we use [Theorem 3](#) in the special case where F_1 and F_2 are the same field—let us call it F —and h is the identity function $\varepsilon: F \rightarrow F$. [Remember that the identity function is $\varepsilon(x) = x$.] When we apply [Theorem 3](#) to the identity function $\varepsilon: F \rightarrow F$, we get

Theorem 4 *Suppose a and b are roots of the same irreducible polynomial $p(x)$ in $F[x]$. Then there is an isomorphism $g: F(a) \rightarrow F(b)$ such that $g(x) = x$ for every x in F , and $g(a) = b$.*

Now let us consider the following situation: K and K' are finite extensions of F , and K and K' have a common extension E . If $h: K \rightarrow K'$ is an isomorphism such that $h(x) = x$ for every x in F , we say that h fixes F . Let c be an element of K ; if h fixes F , and c is a root of some polynomial $a(x) = a_0 + \dots + a_nx^n$ in $F[x]$, $h(c)$ also is a root of $a(x)$. It is easy to see why: the coefficients of $a(x)$ are in F and are therefore not changed by h . So if $a(c) = 0$, then

$$\begin{aligned} a(h(c)) &= a_0 + a_1h(c) + \dots + a_nh(c)^n \\ &= h(a_0 + a_1c + \dots + a_nc^n) = h(0) = 0 \end{aligned}$$



What we have just shown may be expressed as follows:

(*) *Let $a(x)$ be any polynomial in $F[x]$. Any isomorphism which fixes F sends roots of $a(x)$ to roots of $a(x)$.*

If K happens to be the root field of $a(x)$ over F , the situation becomes even more interesting. Say $K = F(c_1, c_2, \dots, c_n)$, where $c_1, c_2, \dots, c_n$ are the roots of $a(x)$. If $h: K \rightarrow K'$ is any isomorphism which fixes F , then by (*), h permutes $c_1, c_2, \dots, c_n$. Now, by the brief discussion headed “For later reference” on page 296, every element of $F(c_1, \dots, c_n)$ is a sum of terms of the form

$$kc_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}$$

where the coefficient k is in F . Because h fixes F , $h(k) = k$. Furthermore, $c_1, c_2, \dots, c_n$ are the roots of $a(x)$, so by (*), the product $c_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}$ is transformed by h into another product of the same form. Thus, h sends every element of $F(c_1, c_2, \dots, c_n)$ to another element of $F(c_1, c_2, \dots, c_n)$.

The above comments are summarized in the next theorem.

Theorem 5 *Let K and K' be finite extensions of F . Assume K is the root field of some polynomial over F . If $h: K \rightarrow K'$ is an isomorphism which fixes F , then $K = K'$.*

PROOF: From Theorem 2, K and K' are simple extensions of F , say $K = F(a)$ and $K' = F(b)$. Then $E = F(a, b)$ is a common extension of K and K' . By the comments preceding this theorem, h maps every element of K to an element of K' ; hence $K' \subseteq K$. Since the same argument may be carried out for h^{-1} , we also have $K \subseteq K'$. ■

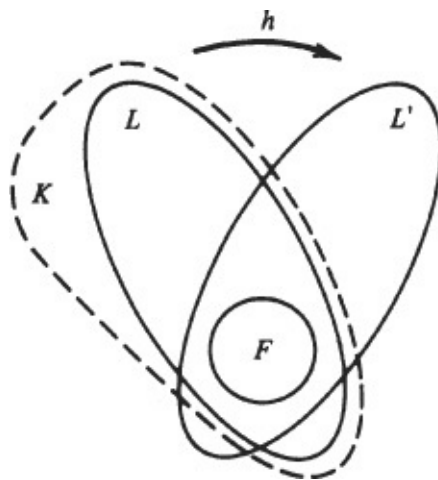
Theorem 5 is often used in tandem with the following (see the figure on the next page):

Theorem 6 *Let L and L' be finite extensions of F . Let K be an extension of L such that K is a root field over F . Any isomorphism $h: L \rightarrow L'$ which fixes F can be extended to an isomorphism $\bar{h}: K \rightarrow K$.*

PROOF: From Theorem 2, K is a simple extension of L , say $K = L(c)$. Now we can use Theorem 3 to extend the isomorphism $h: L \rightarrow L'$ to an isomorphism

$$\bar{h}: \underbrace{L(c)}_K \rightarrow \underbrace{L'(d)}_{K'}$$

By [Theorem 5](#) applied to $\bar{h}$, $K = K'$. ■



REMARK: It follows from the theorem that $L' \subseteq K$ since $\text{ran } h \subseteq \text{ran } \bar{h} = K$.

For later reference. The following results, which are of a somewhat technical nature, will be needed later. The first presents a surprisingly strong property of root fields.

Theorem 7 *Let K be the root field of some polynomial over F . For **every** irreducible polynomial $p(x)$ in $F[x]$, if $p(x)$ has one root in K , then $p(x)$ must have **all** of its roots in K .*

PROOF: Indeed, suppose $p(x)$ has a root a in K , and let b be any other root of $p(x)$. From [Theorem 4](#), there is an isomorphism $h : F(a) \rightarrow F(b)$ fixing F . But $F(a) \subseteq K$; so from [Theorem 6](#) and the remark following it $F(b) \subseteq K$; hence $b \in K$. ■

Theorem 8 *Suppose $I \subseteq E \subseteq K$, where E is a finite extension of I and K is a finite extension of E . If K is the root field of some polynomial over I , then K is also the root field of some polynomial over E .*

PROOF: Suppose K is a root field of some polynomial over I . Then K is a root field of the same polynomial over E . ■

EXERCISES

A. Examples of Root Fields over $\mathbb{Q}$

Example Find the root field of $a(x) = (x^2 - 3)(x^3 - 1)$ over $\mathbb{Q}$.

SOLUTION The complex roots of $a(x)$ are $\pm\sqrt{3}, 1, \frac{1}{2}(-1 \pm \sqrt{3}i)$, so the root field is $\mathbb{Q}(\pm\sqrt{3}, 1, \frac{1}{2}(-1 \pm \sqrt{3}i))$. The same field can be written more simply as $\mathbb{Q}(\sqrt{3}, i)$.

1 Show that $\mathbb{Q}(\sqrt{3}, i)$ is the root field of $(x^2 - 2x - 2)(x^2 + 1)$ over $\mathbb{Q}$.

Comparing part 1 with the example, we note that different polynomials may have the same root field. This is true even if the polynomials are irreducible.

2 Prove that $x^2 - 3$ and $x^2 - 2x - 2$ are both irreducible over $\mathbb{Q}$. Then find their root fields over $\mathbb{Q}$ and show they are the same.

3 Find the root field of $x^4 - 2$, first over $\mathbb{Q}$, then over $\mathbb{R}$.

4 Explain: $\mathbb{Q}(i, \sqrt{2})$ is the root field of $x^4 - 2x^2 + 9$ over $\mathbb{Q}$, and is the root field of $x^2 - 2\sqrt{2}x + 3$ over

$\mathbb{Q}(\sqrt{2})$.

5 Find irreducible polynomials $a(x)$ over $\mathbb{Q}$, and $b(x)$ over $\mathbb{Q}(i)$, such that $\mathbb{Q}(i, \sqrt{3})$ is the root field of $a(x)$ over $\mathbb{Q}$, and is the root field of $b(x)$ over $\mathbb{Q}(i)$. Then do the same for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

6 Which of the following extensions are root fields over $\mathbb{Q}$? Justify your answer: $\mathbb{Q}(i)$; $\mathbb{Q}(\sqrt{2})$; $\mathbb{Q}(\sqrt[3]{2})$, where $\sqrt[3]{2}$ is the *real* cube root of 2; $\mathbb{Q}(2 + \sqrt{5})$; $\mathbb{Q}(i + \sqrt{3})$; $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$.

B. Examples of Root Fields over $\mathbb{Z}_p$

Example Find the root field of $x^2 + 1$ over $\mathbb{Z}_3$.

SOLUTION By the basic theorem of field extensions,

$$\frac{\mathbb{Z}_3[x]}{\langle x^2 + 1 \rangle} \cong \mathbb{Z}_3(u)$$

where u is a root of $x^2 + 1$. In $\mathbb{Z}_3(u)$, $x^2 + 1 = (x + u)(x - u)$, because $u^2 + 1 = 0$. Since $\mathbb{Z}_3(u)$ contains $\pm u$, it is the root field of $x^2 + 1$ over $\mathbb{Z}_3$. Note that $\mathbb{Z}_3(u)$ has nine elements, and its addition and multiplication tables are easy to construct. (See [Chapter 27, Exercise C4](#)).

1 Show that, in any extension of $\mathbb{Z}_3$ which contains a root u of

$$a(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$$

it happens that $u + 1$ and $u + 2$ are the remaining two roots of $a(x)$. Use this fact to find the root field of $x^3 + 2x + 1$ over $\mathbb{Z}_3$. List the elements of the root field.

2 Find the root field of $x^2 + x + 2$ over $\mathbb{Z}_3$, and write its addition and multiplication tables.

3 Find the root field of $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ over $\mathbb{Z}_2$. Write its addition and multiplication tables.

4 Find the root field over $\mathbb{Z}_2$ of $x^3 + x + 1 \in \mathbb{Z}_2[x]$. (CAUTION: This will prove to be a little more difficult than part 3.)

5 Find the root field of $x^3 + x^2 + x + 2$ over $\mathbb{Z}_3$. Find a basis for this root field over $\mathbb{Z}_3$.

C. Short Questions Relating to Root Field

Prove each of the following

1 Every extension of degree 2 is a root field.

2 If $F \subseteq I \subseteq K$ and K is a root field of $a(x)$ over F , then K is a root field of $a(x)$ over I .

3 The root field over $\mathbb{R}$ of any polynomial in $\mathbb{R}[x]$ is $\mathbb{R}$ or $\mathbb{C}$.

4 If c is a complex root of a cubic $a(x) \in \mathbb{Q}[x]$, then $\mathbb{Q}(c)$ is the root field of $a(x)$ over $\mathbb{Q}$.

5 If $p(x) = x^4 + ax^2 + b$ is irreducible in $F[x]$, then $F[x]/\langle p(x) \rangle$ is the root field of $p(x)$ over F .

6 If $K = F(a)$ and K is the root field of some polynomial over F , then K is the root field of the minimum polynomial of a over F .

7 Every root field over F is the root field of some *irreducible* polynomial over F . (HINT: Use part 6 and [Theorem 2](#).)

8 Suppose $[K : F] = n$, where K is a root field over F . Then K is the root field over F of *every* irreducible

polynomial of degree n in $F[x]$ having a root in K .

9 If $a(x)$ is a polynomial of degree n in $F[x]$, and K is the root field of $a(x)$ over F , then $[K: F]$ divides $n!$

D. Reducing Iterated Extensions to Simple Extensions

1 Find c such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(c)$. Do the same for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

2 Let a be a root of $x^3 - x + 1$, and b a root of $x^2 - 2x - 1$. Find c such that $\mathbb{Q}(a, b) = \mathbb{Q}(c)$. (HINT: Use calculus to show that $x^3 - x + 1$ has one real and two complex roots, and explain why no two of these may differ by a real number.)

3 Find c such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(c)$.

4 Find an *irreducible polynomial* $p(x)$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the root field of $p(x)$ over $\mathbb{Q}$. (HINT: Use Exercise C6.)

5 Do the same as in part 4 for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

De Moivre's theorem provides an explicit formula to write the n complex n th roots of 1. (See Chapter 16, Exercise H.) By de Moivre's formula, the n th roots of unity consist of $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$ and its first n powers, namely, $1, \omega, \omega^2, \dots, \omega^{n-1}$. We call ω a *primitive* n th root of unity, because all the other n th roots of unity are powers of ω . Clearly, every n th root of unity (except 1) is a root of

† E. Roots of Unity and Radical Extensions

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + x + 1$$

This polynomial is irreducible if n is a prime (see Chapter 26, Exercise D3). Prove parts 1–3, where ω denotes a primitive n th root of unity.

1 $\mathbb{Q}(\omega)$ is the root field of $x^{n-1} + \dots + x + 1$ over $\mathbb{Q}$.

2 If n is a prime, $[\mathbb{Q}(\omega): \mathbb{Q}] = n - 1$.

3 If n is a prime, ω^{n-1} is equal to a linear combination of $1, \omega, \dots, \omega^{n-2}$ with rational coefficients.

4 Find $[\mathbb{Q}(\omega): \mathbb{Q}]$, where ω is a primitive n th root of unity, for $n = 6, 7$, and 8 .

5 Prove that for any $r \in \{1, 2, \dots, n-1\}$, $\sqrt[n]{a}\omega^r$ is an n th root of a . Conclude that $\sqrt[n]{a}, \sqrt[n]{a}\omega, \dots, \sqrt[n]{a}\omega^{n-1}$ are the n complex n th roots of a .

6 Prove that $\mathbb{Q}(\omega, \sqrt[n]{a})$ is the root field of $x^n - a$ over $\mathbb{Q}$.

7 Find the degree of $\mathbb{Q}(\omega, \sqrt[3]{2})$ over $\mathbb{Q}$, where ω is a primitive cube root of 1. Also show that $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ (HINT: Compute ω .)

8 Prove that if K is the root field of any polynomial over $\mathbb{Q}$, and K contains an n th root of *any* number a , then K contains all the n th roots of unity.

† F. Separable and Inseparable Polynomials

Let F be a field. An irreducible polynomial $p(x)$ in $F[x]$ is said to be *separable* over F if it has no multiple roots in any extension of F . If $p(x)$ does have a multiple root in some extension, it is *inseparable* over F .

1 Prove that if F has characteristic 0, every irreducible polynomial in $F[x]$ is separable.

Thus, for characteristic 0, there is no question whether an irreducible polynomial is separable or not. However, for characteristic $p \neq 0$, it is different. This case is treated next. In the following problems, let F be a field of characteristic $p \neq 0$.

2 If $a'(x) = 0$, prove that the only nonzero terms of $a(x)$ are of the form $a_{mp}x^{mp}$ for some m . [In other words, $a(x)$ is a polynomial in powers of x^p .]

3 Prove that if an irreducible polynomial $a(x)$ is inseparable over F , then $a(x)$ is a polynomial in powers of x^p . (HINT: Use part 2, and reason as in the proof of [Theorem 1](#).)

4 Use [Chapter 27, Exercise J](#) (especially the conclusion following J6) to prove the converse of part 3.

Thus, if F is a field of characteristic $p \neq 0$, an irreducible polynomial $a(x) \in F[x]$ is inseparable iff $a(x)$ is a polynomial in powers of x^p . For finite fields, we can say even more:

5 Prove that if F is any field of characteristic $p \neq 0$, then in $F[x]$,

$$(a_0 + a_1x + \cdots + a_nx^n)^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np}$$

(HINT: See [Chapter 24, Exercise D6](#).)

6 If F is a finite field of characteristic $p \neq 0$, prove that, in $F[x]$, every polynomial $a(x^p)$ is equal to $[b(x)]^p$ for some $b(x)$. [HINT: Use part 5 and the fact that in a finite field of characteristic p , every element has a p th root (see [Chapter 20, Exercise F](#)).]

7 Use parts 3 and 6 to prove: In any finite field, every irreducible polynomial is separable.

Thus, fields of characteristic 0 and finite fields share the property that *irreducible polynomials have no multiple roots*. The only remaining case is that of infinite fields with finite characteristic. It is treated in the next exercise set.

† G. Multiple Roots over Infinite Fields of Nonzero Characteristic

If $\mathbf{z}_p[y]$ is the domain of polynomials (in the letter y) over $\mathbf{z}_p$, let $E = \mathbf{z}_p(y)$ be the field of quotients of $\mathbf{z}_p[y]$. Let K denote the subfield $\mathbf{z}_p(y^p)$ of $\mathbf{z}_p(y)$.

1 Explain why $\mathbf{z}_p(y)$ and $\mathbf{z}_p(y^p)$ are infinite fields of characteristic p .

2 Prove that $a(x) = x^p - y^p$ has the factorization $x^p - y^p = (x - y)^p$ in $E[x]$, but is irreducible in $K[x]$. Conclude that there is an irreducible polynomial $a(x)$ in $K[x]$ with a root whose multiplicity is p .

Thus, over an infinite field of nonzero characteristic, an irreducible polynomial may have multiple roots. Even these fields, however, have a remarkable property: *all the roots of any irreducible polynomial have the same multiplicity*. The details follow: Let F be any field, $p(x)$ irreducible in $F[x]$, a and b two distinct roots of $p(x)$, and K the root field of $p(x)$ over F . Let $i: K \rightarrow i(K) = K'$ be the isomorphism of [Theorem 4](#), and $\bar{i}: K[x] \rightarrow K'[x]$ the isomorphism described immediately preceding [Theorem 3](#).

3 Prove that $\bar{i}$ leaves $p(x)$ fixed.

4 Prove that $\bar{i}((x - a)^m) = (x - b)^m$.

5 Prove that a and b have the same multiplicity.

† H. An Isomorphism Extension Theorem (Proof of [Theorem 3](#))

Let $F_1, F_2, h, p(x), a, b$, and $\bar{h}$ be as in the statement of [Theorem 3](#). To prove that $\bar{h}$ is an isomorphism, it must first be shown that it is properly defined: that is, if $c(a) = d(a)$ in $F_1(a)$, then $\bar{h}(c(a)) = \bar{h}(d(a))$.

1 If $c(a) = d(a)$, prove that $c(x) - d(x)$ is a multiple of $p(x)$. Deduce from this that $hc(x) - hd(x)$ is a multiple of $hp(x)$.

2 Use part 1 to prove that $\bar{h}(c(a)) = \bar{h}(d(a))$.

3 Reversing the steps of the preceding argument, show that $\bar{h}$ is injective.

4 Show that $\bar{h}$ is surjective.

5 Show that $\bar{h}$ is a homomorphism.

† I. Uniqueness of the Root Field

Let $h: F_1 \rightarrow F_2$ be an isomorphism. If $a(x) \in F_1[x]$, let K_1 be the root field of $a(x)$ over F_1 , and K_2 the root field of $ha(x)$ over F_2 .

1 Prove: If $p(x)$ is an irreducible factor of $a(x)$, $u \in K_1$ is a root of $p(x)$, and $v \in K_2$ is a root of $hp(x)$, then $F_1(u) \cong F_2(v)$.

2 $F_1(u) = K_1$ iff $F_2(v) = K_2$.

3 Use parts 1 and 2 to form an inductive proof that $K_1 \cong K_2$.

4 Draw the following conclusion: The root field of a polynomial $a(x)$ over a field F is unique up to isomorphism.

† J. Extending Isomorphism

In the following, let F be a subfield of $\mathbb{C}$. An injective homomorphism $h: F \rightarrow \mathbb{C}$ is called a *monomorphism*; it is obviously an isomorphism $F \rightarrow h(F)$.

1 Let ω be a complex p th root of unity (where p is a prime), and let $h: \mathbb{Q}(\omega) \rightarrow \mathbb{C}$ be a monomorphism fixing $\mathbb{Q}$. Explain why h is completely determined by the value of $h(\omega)$. Then prove that there exist exactly $p - 1$ monomorphisms $\mathbb{Q}(\omega) \rightarrow \mathbb{C}$ which fix $\mathbb{Q}$.

2 Let $p(x)$ be irreducible in $F[x]$, and c a complex root of $p(x)$. Let $h: F \rightarrow \mathbb{C}$ be a monomorphism. If $\deg p(x) = n$, prove that there are exactly n monomorphisms $F(c) \rightarrow \mathbb{C}$ which are extensions of h .

3 Let $F \subseteq K \subseteq \mathbb{C}$, with $[K: F] = n$. If $h: F \rightarrow \mathbb{C}$ is a monomorphism, prove that there are exactly n monomorphisms $K \rightarrow \mathbb{C}$ which are extensions of h .

4 Prove: The only possible monomorphism $h: \mathbb{Q} \rightarrow \mathbb{C}$ is $h(x) = x$. Thus, any monomorphism $h: \mathbb{Q}(a) \rightarrow \mathbb{C}$ necessarily fixes $\mathbb{Q}$.

5 Prove: There are exactly three monomorphisms $\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{C}$, and they are determined by the conditions: $\sqrt[3]{2} \rightarrow \sqrt[3]{2}; \sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega; \sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega^2$, where ω is a primitive cube root of unity.

K. Normal Extensions

If K is the root field of some polynomial $a(x)$ over F , K is also called a *normal extension* of F . There are other possible ways of defining normal extensions, which are equivalent to the above. We consider the two most common ones here: they are precisely the properties expressed in theorems 7 and 6. Let K be a finite extension of F .

1 Suppose that for every irreducible polynomial $p(x)$ in $F[x]$, if $p(x)$ has one root in K , then $p(x)$ must

have all its roots in K . Prove that K is a normal extension of F .

2 Suppose that, if h is any isomorphism with domain K which fixes F , then $h(K) \subseteq K$. Prove that K is a normal extension of F .

GALOIS THEORY: THE HEART OF THE MATTER

If K is a field and h is an isomorphism from K to K , we call h an *automorphism* of K (automorphism = “self-isomorphism”).

We begin this chapter by restating [Theorems 5 and 6 of Chapter 31](#):

Let K be the root field of some polynomial over F ; suppose $a \in K$:

- (i) *Any isomorphism with domain K which fixes F is an automorphism of K .*
- (ii) *If a and b are roots of an irreducible polynomial $p(x)$ in $F[x]$, there is an automorphism of K fixing F and sending a to b .*

Rule (i) is merely a restatement of [Theorem 5 of Chapter 31](#), using the notion of automorphism. Rule (ii) is a result of combining [Theorem 4 of Chapter 31](#) [which asserts that there exists an F -fixing isomorphism from $L = F(a)$ to $L' = F(b)$] with [Theorem 6](#) of the same chapter.

Let K be the root field of a polynomial $a(x)$ in $F[x]$. If $c_1, c_2, \dots, c_n$ are the roots of $a(x)$, then $K = F(c_1, c_2, \dots, c_n)$, and, by (*) on page 316, any automorphism h of K which fixes F *permutes* $c_1, c_2, \dots, c_n$. On the other hand, remember that every element a in $F(c_1, c_2, \dots, c_n)$ is a sum of terms of the form

$$kc_1^{i_1}c_2^{i_2}\cdots c_n^{i_n}$$

where the coefficient k of each term is in F . If h is an automorphism which fixes F , h does not change the coefficients, so $h(a)$ is completely determined once we know $h(c_1), \dots, h(c_n)$. Thus, *every automorphism of K fixing F is completely determined by a permutation of the roots of $a(x)$.*

This is *very* important!

What it means is that we may identify the automorphisms of K which fix F with permutations of the roots of $a(x)$.

It must be pointed out here that, just as the symmetries of geometric figures determine their geometric properties, so the symmetries of equations (that is, permutations of their roots) give us all the vital information needed to analyze their solutions. Thus, if K is the root field of our polynomial $a(x)$ over F , we will now pay very close attention to the automorphisms of K which fix F .

To begin with, how many such automorphisms are there? The answer is a classic example of mathematical elegance and simplicity.

Theorem 1 Let K be the root field of some polynomial over F . The number of automorphisms of K fixing F is equal to the degree of K over F .

PROOF: Let $[K : F] = n$, and let us show that K has exactly n automorphisms fixing F . By Theorem 2 of Chapter 31, $K = F(a)$ for some $a \in K$. Let $p(x)$ be the minimum polynomial of a over F ; if b is any root of $p(x)$, then by (ii) on the previous page, there is an automorphism of K fixing F and sending a to b . Since $p(x)$ has n roots, there are exactly n choices of b , and therefore n automorphisms of K fixing F .

[Remember that every automorphism h which fixes F permutes the roots of $p(x)$ and therefore sends a to *some* root of $p(x)$; and h is completely determined once we have chosen $h(a)$.] ■

For example, we have already seen that $\mathbb{Q}(\sqrt{2})$ is of degree 2 over $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2})$ is the root field of $x^2 - 2$ over $\mathbb{Q}$ because $\mathbb{Q}(\sqrt{2})$ contains both roots of $x^2 - 2$, namely $\pm\sqrt{2}$. By Theorem 1, there are exactly two automorphisms of $\mathbb{Q}(\sqrt{2})$ fixing $\mathbb{Q}$: one sends $\sqrt{2}$ to $\sqrt{2}$; it is the identity function. The other sends $\sqrt{2}$ to $-\sqrt{2}$, and is therefore the function $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$.

Similarly, we saw that $\mathbb{C} = \mathbb{R}(i)$, and $\mathbb{C}$ is of degree 2 over $\mathbb{R}$. The two automorphisms of $\mathbb{C}$ which fix $\mathbb{R}$ are the identity function and the function $a + bi \rightarrow a - bi$ which sends every complex number to its complex conjugate.

As a final example, we have seen that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension of degree 4 over $\mathbb{Q}$, so by Theorem 1, there are four automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which fix $\mathbb{Q}$: Now, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the root field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ for it contains the roots of this polynomial, and any extension of $\mathbb{Q}$ containing the roots of $(x^2 - 2)(x^2 - 3)$ certainly contains $\sqrt{2}$ and $\sqrt{3}$. Thus, by (*) on page 316, each of the four automorphisms which fix $\mathbb{Q}$ sends roots of $x^2 - 2$ to roots of $x^2 - 2$, and roots of $x^2 - 3$ to roots of $x^2 - 3$. But there are only four possible ways of doing this, namely,

$$\begin{array}{cc} \left\{ \begin{array}{l} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{array} \right\} & \left\{ \begin{array}{l} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{array} \right\} \\ \left\{ \begin{array}{l} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{array} \right\} & \text{and} \quad \left\{ \begin{array}{l} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{array} \right\} \end{array}$$

Since every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, these four automorphisms (we shall call them $\varepsilon, \alpha, \beta,$ and γ) are the following:

$$\begin{array}{lcl} a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} & \xrightarrow{\varepsilon} & a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} & \xrightarrow{\alpha} & a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} & \xrightarrow{\beta} & a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} & \xrightarrow{\gamma} & a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \end{array}$$

If K is an extension of F , the automorphisms of K which fix F form a group. (The operation, of course, is composition.) This is perfectly obvious: for if g and h fix F , then for every x in F ,

$$x \xrightarrow{h} x \quad \text{and} \quad x \xrightarrow{g} x \quad \text{so} \quad x \xrightarrow{h} x \xrightarrow{g} x$$

that is, $g \circ h$ fixes F . Furthermore, if

$$x \xrightarrow{h} x \quad \text{then} \quad x \xrightarrow{h^{-1}} x$$

that is, if h fixes F so does h^{-1}

This fact is perfectly obvious, but nonetheless of great importance, for it means that we can now use all of our accumulated knowledge about groups to help us analyze the solutions of polynomial equations. And that is precisely what Galois theory is all about.

If K is the root field of a polynomial $a(x)$ in $F[x]$, *the group of all the automorphisms of K which fix F is called the Galois group of $a(x)$* . We also call it the *Galois group of K over F* , and designate it by the symbol

$$\text{Gal}(K : F)$$

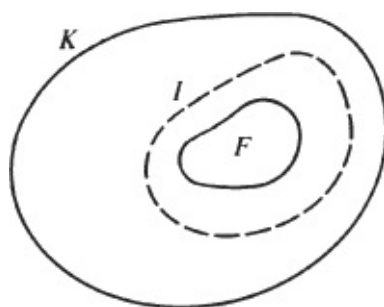
In our last example we saw that there are four automorphisms of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ which fix $\mathbf{Q}$. We called them $\varepsilon, \alpha, \beta$, and γ . Thus, the Galois group of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$ is $\text{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}) = \{\varepsilon, \alpha, \beta, \gamma\}$; the operation is composition, giving us the table

$\circ$	ε	α	β	γ
ε	ε	α	β	γ
α	α	ε	γ	β
β	β	γ	ε	α
γ	γ	β	α	ε

As one can see, this is an abelian group in which every element is its own inverse; almost at a glance one can verify that it is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Let K be the root field of $a(x)$, where $a(x)$ is in $F[x]$. In our earlier discussion we saw that every automorphism of K fixing F [that is, every member of the Galois group of $a(x)$] may be identified with a permutation of the roots of $a(x)$. However, it is important to note that *not every permutation of the roots of $a(x)$ need be in the Galois group of $a(x)$* , even when $a(x)$ is irreducible. For example, we saw that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$, where $\sqrt{2} + \sqrt{3}$ is a root of the irreducible polynomial $x^4 - 10x^2 + 1$ over $\mathbf{Q}$. Since $x^4 - 10x^2 + 1$ has four roots, there are $4! = 24$ permutations of its roots, only four of which are in its Galois group. This is because only four of the permutations are genuine symmetries of $x^4 - 10x^2 + 1$, in the sense that they determine automorphisms of the root field.

In the discussion throughout the remainder of this chapter, let F and K remain fixed. F is an arbitrary field and K is the root field of some polynomial $a(x)$ in $F[x]$. The thread of our reasoning will lead us to speak about fields I where $F \subseteq I \subseteq K$, that is, fields “between” F and K . We will



refer to them as *intermediate fields*. Since K is the root field of $a(x)$ over F , it is also the root field of $a(x)$ over I for every intermediate field I .

The letter $\mathbf{G}$ will denote the Galois group of K over F . With each intermediate field I , we associate the group

$$I^* = \text{Gal}(K : I)$$

that is, the group of all the automorphisms of K which fix I . It is obviously a subgroup of $\mathbf{G}$. We will call I^* the *fixer* of I .

Conversely, with each subgroup H of $\mathbf{G}$ we associate the subfield of K containing all the a in K which are not changed by any $\pi \in H$. That is,

$$\{a \in K : \pi(a) = a \text{ for every } \pi \in H\}$$

One verifies in a trice that this is a subfield of K . It obviously contains F , and is therefore one of the intermediate fields. It is called the *fixed field* of H . For brevity and euphony we call it the *fixfield* of H .

Let us recapitulate: Every subgroup H of $\mathbf{G}$ fixes an intermediate field I , called the *fixfield* of H . Every intermediate field I is fixed by a subgroup H of $\mathbf{G}$, called the *fixer* of I . This suggests very strongly that there is a one-to-one correspondence between the subgroups of $\mathbf{G}$ and the fields intermediate between F and K . Indeed, this is correct. This one-to-one correspondence is at the very heart of Galois theory, because it provides the tie-in between properties of field extensions and properties of subgroups.

Just as, in [Chapter 29](#), we were able to use vector algebra to prove new things about field extensions, now we will be able to use group theory to explore field extensions. The vector-space connection was a relative lightweight. The connection with group theory, on the other hand, gives us a tool of tremendous power to study field extensions.

We have not yet proved that the connection between subgroups of $\mathbf{G}$ and intermediate fields is a one-to-one correspondence. The next two theorems will do that.

Theorem 2 *If H is the fixer of I , then I is the fixfield of H .*

PROOF: Let H be the fixer of I , and I' be the fixfield of H . It follows from the definitions of *fixer* and *fixfield* that $I \subseteq I'$, so we must now show that $I' \subseteq I$. We will do this by proving that $a \notin I$ implies $a \notin I'$. Well, if a is an element of K which is not in I , the minimum polynomial $p(x)$ of a over I must have degree ≥ 2 (for otherwise, $a \in I$). Thus, $p(x)$ has another root b . By Rule (ii) given at the beginning of this chapter, there is an automorphism of K fixing I and sending a to b . This automorphism moves a , so $a \notin I'$. ■

Lemma *Let H be a subgroup of $\mathbf{G}$, and I the fixfield of H . The number of elements in H is equal to $[K : I]$.*

PROOF: Let H have r elements, namely, $h_1, \dots, h_r$. Let $K = I(a)$. Much of our proof will revolve around the following polynomial:

$$b(x) = [x - h_1(a)][x - h_2(a)] \cdots [x - h_r(a)]$$

Since one of the h_i is the identity function, one factor of $b(x)$ is $(x - a)$, and therefore a is a root of $b(x)$. In the next paragraph we will see that all the coefficients of $b(x)$ are in I , so $b(x) \in I[x]$. It follows that $b(x)$ is a multiple of the minimum polynomial of a over I , whose degree is exactly $[K : I]$. Since $b(x)$ is of degree r , this means that $r \geq [K : I]$, which is half our theorem.

Well, let us show that all the coefficients of $b(x)$ are in I . We saw on page 314 that every isomorphism $h_i : K \rightarrow K$ can be extended to an isomorphism $\bar{h}_i : K[x] \rightarrow K[x]$. Because $\bar{h}_i$ is an

isomorphism of polynomials, we get

$$\begin{aligned}\bar{h}_i(b(x)) &= \bar{h}_i(x - h_1(a))\bar{h}_i(x - h_2(a)) \cdots \bar{h}_i(x - h_r(a)) \\ &= (x - h_i \circ h_1(a)) \cdots (x - h_i \circ h_r(a))\end{aligned}$$

But $h_i \circ h_1, h_i \circ h_2, \dots, h_i \circ h_r$ are r distinct elements of H , and H has exactly r elements, so they are all the elements of H (that is, they are $h_1, \dots, h_r$, possibly in a different order). So the factors of $\bar{h}_i(b(x))$ are the same as the factors of $b(x)$, merely in a different order, and therefore $\bar{h}_i(b(x)) = b(x)$. Since equal polynomials have equal coefficients, h_i leaves the coefficients of $b(x)$ invariant. Thus, every coefficient of $b(x)$ is in the fixfield of H , that is, in I .

We have just shown that $[K : I] \leq r$. For the opposite inequality, remember that by [Theorem 1](#), $[K : I]$ is equal to the number of I -fixing automorphisms of K . But there are at least r such automorphisms, namely $h_1, \dots, h_r$. Thus, $[K : I] \geq r$, and we are done. ■

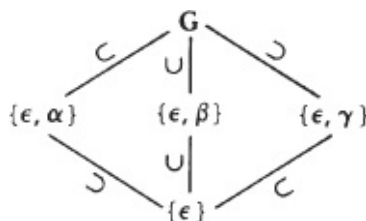
Theorem 3 *If I is the fixfield of H , then H is the fixer of I .*

PROOF: Let I be the fixfield of H , and I^* the fixer of I . It follows from the definitions of fixer and fixfield that $H \subseteq I^*$. We will prove equality by showing that there are as many elements in H as in I^* . By the lemma, the order of H is equal to $[K : I]$. By [Theorem 2](#), I is the fixfield of I^* , so by the lemma again, the order of I^* is also equal to $[K : I]$. ■

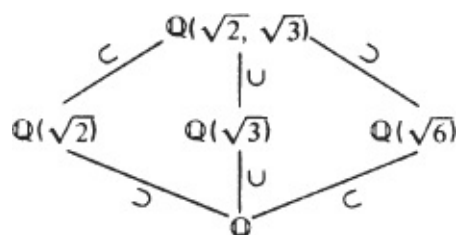
It follows immediately from [Theorems 2](#) and [3](#) that *there is a one-to-one correspondence between the subgroups of $\text{Gal}(K : F)$ and the intermediate fields between K and F* . This correspondence, which matches every subgroup with its fixfield (or, equivalently, matches every intermediate field with its fixer) is called a *Galois correspondence*. It is worth observing that larger subfields correspond to smaller subgroups; that is,

$$I_1 \subseteq I_2 \quad \text{iff} \quad I_2^* \subseteq I_1^*$$

As an example, we have seen that the Galois group of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$ is $\mathbf{G} = \{\epsilon, \alpha, \beta, \gamma\}$ with the table given on page 325. This group has exactly five subgroups—namely, $\{\epsilon\}$, $\{\epsilon, \alpha\}$, $\{\epsilon, \beta\}$, $\{\epsilon, \gamma\}$, and the whole group $\mathbf{G}$. They may be represented in the “inclusion diagram”:



On the other hand, there are exactly five fields intermediate between $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, which may be represented in the inclusion diagram:



- 3 List the elements of $\text{Gal}(\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q})$ and exhibit its table.
- 4 Write the inclusion diagram for the subgroups of $\text{Gal}(\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q})$, and the inclusion diagram for the fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(i, \sqrt{2})$. Indicate the Galois correspondence.

† B. Computing a Galois Group of Eight Elements

- 1 Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the root field of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$.
- 2 Show that the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ is 8.
- 3 List the eight elements of $G = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q})$ and write its table.
- 4 List the subgroups of G . (By Lagrange's theorem, any proper subgroup of G has either two or four elements.)
- 5 For each subgroup of G , find its fixfield.
- 6 Indicate the Galois correspondence by means of a diagram like the one on page 329.

† C. A Galois Group Equal to S_3

- 1 Show that $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is the root field of $x^3 - 2$ over $\mathbb{Q}$, where $\sqrt[3]{2}$ designates the *real* cube root of 2. (HINT: Compute the complex cube roots of unity.)
- 2 Show that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
- 3 Explain why $x^2 + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, then show that $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Conclude that $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$.
- 4 Use part 3 to explain why $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q})$ has six elements. Then use the discussion following Rule (ii) on page 323 to explain why every element of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q})$ may be identified with a permutation of the three cube roots of 2.
- 5 Use part 4 to prove that $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}) \cong S_3$.

† D. A Galois Group Equal to D_4

If $\alpha = \sqrt[4]{2}$ is a real fourth root of 2, then the four fourth roots of 2 are $\pm\alpha$ and $\pm i\alpha$. Explain parts 1–6, briefly but carefully:

- # 1 $\mathbb{Q}(\alpha, i)$ is the root field of $x^4 - 2$ over $\mathbb{Q}$.
- 2 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- 3 $i \notin \mathbb{Q}(\alpha)$; hence $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$.
- 4 $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$.
- 5 $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$ is a basis for $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}$.
- 6 Any $\mathbb{Q}$ -fixing automorphism h of $\mathbb{Q}(\alpha, i)$ is determined by its effect on the elements in the basis. These, in turn, are determined by $h(\alpha)$ and $h(i)$.
- 7 Explain: $h(\alpha)$ must be a fourth root of 2 and $h(i)$ must be equal to $\pm i$. Combining the four possibilities for $h(\alpha)$ with the two possibilities for $h(i)$ gives eight possible automorphisms. List them in the format

$$\left\{ \begin{array}{l} \alpha \rightarrow \alpha \\ i \rightarrow i \end{array} \right\}, \quad \left\{ \begin{array}{l} \alpha \rightarrow -\alpha \\ i \rightarrow i \end{array} \right\}, \dots$$

- 8 Compute the table of the group $\text{Gal}(\mathbb{Q}(\alpha, i) : \mathbb{Q})$ and show that it is isomorphic to D_4 , the group of

symmetries of the square.

† E. A Cyclic Galois Group

1 Describe the root field K of $x^7 - 1$ over $\mathbb{Q}$. Explain why $[K : \mathbb{Q}] = 6$.

2 Explain: If α is a primitive seventh root of unity, any $h \in \text{Gal}(K : \mathbb{Q})$ must send α to a seventh root of unity. In fact, h is determined by $h(\alpha)$.

3 Use part 2 to list explicitly the six elements of $\text{Gal}(K : \mathbb{Q})$. Then write the table of $\text{Gal}(K : \mathbb{Q})$ and show that it is cyclic.

4 List all the subgroups of $\text{Gal}(K : \mathbb{Q})$, with their fixfields. Exhibit the Galois correspondence.

5 Describe the root field L of $x^6 - 1$ over $\mathbb{Q}$, and show that $[L : \mathbb{Q}] = 2$. Explain why it follows that there are no intermediate fields between $\mathbb{Q}$ and L (except for $\mathbb{Q}$ and L themselves).

6 Let L be the root field of $x^6 - 2$ over $\mathbb{Q}$. List the elements of $\text{Gal}(L : \mathbb{Q})$ and write its table.

† F. A Galois Group Isomorphic to S_5

Let $a(x) = x^5 - 4x^4 + 2x + 2 \in \mathbb{Q}[x]$, and let $r_1, \dots, r_5$ be the roots of $a(x)$ in $\mathbb{C}$. Let $K = \mathbb{Q}(r_1, \dots, r_5)$ be the root field of $a(x)$ over $\mathbb{Q}$.

Prove: parts 1–3:

1 $a(x)$ is irreducible in $\mathbb{Q}[x]$.

2 $a(x)$ has three real and two complex roots. [HINT: Use calculus to sketch the graph of $y = a(x)$, and show that it crosses the x axis three times.]

3 If r_1 denotes a real root of $a(x)$, $[\mathbb{Q}(r_1) : \mathbb{Q}] = 5$. Use this to prove that $[K : \mathbb{Q}]$ is a multiple of 5.

4 Use part 3 and Cauchy's theorem (Chapter 13, Exercise E) to prove that there is an element α of order 5 in $\text{Gal}(K : \mathbb{Q})$. Since α may be identified with a permutation of $\{r_1, \dots, r_5\}$, explain why it must be a cycle of length 5. (HINT: Any product of disjoint cycles on $\{r_1, \dots, r_5\}$ has order $\neq 5$.)

5 Explain why there is a transposition in $\text{Gal}(K : \mathbb{Q})$. [It permutes the conjugate pair of complex roots of $a(x)$.]

6 Prove: Any subgroup of S_5 which contains a cycle of length 5 and a transposition must contain all possible transpositions in S_5 , hence all of S_5 . Thus, $\text{Gal}(K : \mathbb{Q}) = S_5$.

G. Shorter Questions Relating to Automorphisms and Galois Groups

Let F be a field, and K a finite extension of F . Suppose $a, b \in K$. Prove parts 1–3:

1 If an automorphism h of K fixes F and a , then h fixes $F(a)$.

2 $F(a, b)^* = F(a)^* \cap F(b)^*$.

3 Aside from the identity function, there are no $\mathbb{Q}$ -fixing automorphisms of $\mathbb{Q}(\sqrt[3]{2})$. [HINT: Note that $\mathbb{Q}(\sqrt[3]{2})$ contains only real numbers.]

4 Explain why the conclusion of part 3 does not contradict Theorem 1.

In the next three parts, let ω be a primitive p th root of unity, where p is a prime.

5 Prove: If $h \in \text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$, then $h(\omega) = \omega^k$ for some k where $1 \leq k \leq p - 1$.

6 Use part 5 to prove that $\text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is an abelian group.

7 Use part 5 to prove that $\text{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is a cyclic group.

† H. The Group of Automorphisms of $\mathbb{C}$

1 Prove: The only automorphism of $\mathbb{Q}$ is the identity function. [HINT: If h is an automorphism, $h(1) = 1$; hence $h(2) = 2$, and so on.]

2 Prove: Any automorphism of $\mathbb{R}$ sends squares of numbers to squares of numbers, hence positive numbers to positive numbers.

3 Using part 2, prove that if h is any automorphism of $\mathbb{R}$, $a < b$ implies $h(a) < h(b)$.

4 Use parts 1 and 3 to prove that the only automorphism of $\mathbb{R}$ is the identity function.

5 List the elements of $\text{Gal}(\mathbb{C} : \mathbb{Q})$.

6 Prove that the identity function and the function $a + bi \rightarrow a - bi$ are the only automorphisms of $\mathbb{C}$ which fix $\mathbb{Q}$.

I. Further Questions Relating to Galois Groups

Throughout this set of questions, let K be a root field over F , let $\mathbf{G} = \text{Gal}(K : F)$, and let I be any intermediate field. Prove the following:

1 $I^* = \text{Gal}(K : I)$ is a subgroup of $\mathbf{G}$.

2 If H is a subgroup of $\mathbf{G}$ and $H^\circ = \{a \in K : \pi(a) = a \text{ for every } \pi \in H\}$, then H° is a subfield of K , and $F \subseteq H^\circ$.

3 Let H be the fixer of I , and I' the fixfield of H . Then $I \subseteq I'$. Let I be the fixfield of H , and I^* the fixer of I . Then $H \subseteq I^*$.

4 Let I be a normal extension of F (that is, a root field of some polynomial over F). If $\mathbf{G}$ is abelian, then $\text{Gal}(K : I)$ and $\text{Gal}(I : F)$ are abelian. (HINT: Use [Theorem 4](#).)

5 Let I be a normal extension of F . If $\mathbf{G}$ is a cyclic group, then $\text{Gal}(K : I)$ and $\text{Gal}(I : F)$ are cyclic groups.

6 If $\mathbf{G}$ is a cyclic group, there exists exactly one intermediate field I of degree k , for each integer k dividing $[K : F]$.

† J. Normal Extensions and Normal Subgroups

Suppose $F \subseteq K$, where K is a normal extension of F . (This means simply that K is the root field of some polynomial in $F[x]$: see [Chapter 31](#), [Exercise K](#).) Let $I_1 \subseteq I_2$ be intermediate fields.

1 Deduce from [Theorem 4](#) that, if I_2 is a normal extension of I_1 , then I_2^* is a normal subgroup of I_1^* .

2 Prove the following for any intermediate field I : Let $h \in \text{Gal}(K : F)$, $g \in I^*$, $a \in I$, and $b = h(a)$. Then $[h \circ g \circ h^{-1}](b) = b$. Conclude that

$$hI^*h^{-1} \subseteq h(I)^*$$

3 Use part 2 to prove that $hI^*h^{-1} = h(I)^*$.

Two intermediate fields I_1 and I_2 are called *conjugate* iff there is an automorphism [i.e., an element $i \in \text{Gal}(K : F)$] such that $i(I_1) = I_2$.

4 Use part 3 to prove that I_1 and I_2 are conjugate iff I_1^* and I_2^* are conjugate subgroups in the Galois group.

5 Use part 4 to prove that for any intermediate fields I_1 and I_2 : iff I_2^* is a normal subgroup of I_1^* , then I_2 is a normal extension of I_1 .

Combining parts 1 and 5 we have: I_2 is a normal extension of I_1 iff I_2^* is a normal subgroup of I_1^* . (Historically, this result is the origin of the word “normal” in the term “normal subgroup.”)

CHAPTER THIRTY-THREE

SOLVING EQUATIONS BY RADICALS

In this final chapter, Galois theory will be used explicitly to answer practical questions about solving equations.

In the introduction to this book we saw that classical algebra was devoted largely to finding methods for solving polynomial equations. The quadratic formula yields the solutions of every equation of degree 2, and similar formulas have been found for polynomials of degrees 3 and 4. But every attempt to find explicit formulas, of the same kind as the quadratic formula, which would solve a general equation of degree 5 or higher ended in failure. The reason for this was finally discovered by the young Galois, who showed that an equation is solvable by the kind of explicit formula we have in mind if and only if its group of symmetries has certain properties. The group of symmetries is, of course, the Galois group which we have already defined, and the required group properties will be formulated in the next few pages.

Galois showed that the groups of symmetries of all equations of degree ≤ 4 have the properties needed for solvability, whereas equations of degree 5 or more do not always have them. Thus, not only is the classical quest for radical formulas to solve all equations of degree > 4 shown to be futile, but a criterion is made available to test any equation and determine if it has solutions given by a radical formula. All this will be made clear in the following pages.

Every quadratic equation $ax^2 + bx + c = 0$ has its roots given by the formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Equations of degree 3 and 4 can be solved by similar formulas. For example, the cubic equation $x^3 + ax + b = 0$ has a solution given by

$$\sqrt[3]{\frac{-b}{2} + \sqrt{D}} + \sqrt[3]{\frac{-b}{2} - \sqrt{D}} \quad \text{where } D = \frac{a^3}{27} + \frac{b^2}{4} \quad (1)$$

Such expressions are built up from the coefficients of the given polynomials by repeated addition,

subtraction, multiplication, division, *and taking roots*. Because of their use of radicals, they are called *radical expressions* or *radical formulas*. A polynomial $a(x)$ is *solvable by radicals* if there is a radical expression giving its roots in terms of its coefficients.

Let us return to the example of $x^3 + ax + b = 0$, where a and b are rational, and look again at [Formula \(1\)](#). We may interpret this formula to assert that if we start with the field of coefficients $\mathbf{Q}$, adjoin the square root $\sqrt{D}$, then adjoin the cube roots $\sqrt[3]{-b/2 \pm \sqrt{D}}$, we reach a field in which $x^3 + ax + b = 0$ has its roots.

In general, to say that the roots of $a(x)$ are given by a radical expression is the same as saying that we can extend the field of coefficients of $a(x)$ by successively adjoining n th roots (for various n), and in this way obtain a field which contains the roots of $a(x)$. We will express this notion formally now, in the language of field theory.

$F(c_1, \dots, c_n)$ is called a *radical extension* of F if, for each i , some power of c_i is in $F(c_1, \dots, c_{i-1})$. In other words, $F(c_1, \dots, c_n)$ is an iterated extension of F obtained by successively adjoining n th roots, for various n . We say that a polynomial $a(x)$ in $F[x]$ is *solvable by radicals* if there is a radical extension of F containing all the roots of $a(x)$, that is, containing the root field of $a(x)$.

To deal effectively with n th roots we must know a little about them. To begin with, the n th roots of 1, called *n th roots of unity*, are, of course, the solutions of $x^n - 1 = 0$. Thus, for each n , there are exactly n n th roots of unity. As we shall see, everything we need to know about roots will follow from properties of the roots of unity.

In $\mathbf{C}$ the n th roots of unity are obtained by de Moivre's theorem. They consist of a number ω and its first n powers: $1 = \omega^0, \omega, \omega^2, \dots, \omega^{n-1}$. We will not review de Moivre's theorem here because, remarkably, the main facts about roots of unity are true in *every* field of characteristic zero. Everything we need to know emerges from the following theorem:

Theorem 1 *Any finite group of nonzero elements in a field is a cyclic group. (The operation in the group is the field's multiplication.)*

PROOF: If F^* denotes the set of nonzero elements of F , suppose that $G \subseteq F^*$, and that G , with the field's "multiply" operation, is a group of n elements. We will compare G with $\mathbf{Z}_n$ and show that G , like $\mathbf{Z}_n$, has an element of order n and is therefore cyclic.

For any integer k , let $g(k)$ be the number of elements of order k in G , and let $z(k)$ be the number of elements of order k in $\mathbf{Z}_n$. For every positive integer k which is a factor of n , the equation $x^k = 1$ has *at most* k solutions in F ; thus,

(*) *G contains at most k elements whose order is a factor of k .*

If G has an element a of order k , then $\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}$ are *all* the distinct elements of G whose order is a factor of k . [By (*), there cannot be any others.] In $\mathbf{Z}_n$, the subgroup

$$\langle n/k \rangle = \left\{ 0, \frac{n}{k}, 2 \frac{n}{k}, \dots, (k-1) \frac{n}{k} \right\}$$

contains all the elements of $\mathbf{Z}_n$ whose order is a factor of k .

Since $\langle a \rangle$ and $\langle n/k \rangle$ are cyclic groups with the same number of elements, they are isomorphic; thus, the number of elements of order k in $\langle a \rangle$ is the same as the number of elements of order k in $\langle n/k \rangle$.

Thus, $g(k) = z(k)$.

Let us recapitulate: if G has an element of order k , then $g(k) = z(k)$; but if G has *no* such elements, then $g(k) = 0$. Thus, for each positive integer k which is a factor of n , the number of elements of order k in G is less than (or equal to) the number of elements of order k in $\mathbf{z}_n$.

Now, every element of G (as well as every element of $\mathbf{z}_n$) has a well-defined order, which is a divisor of n . Imagine the elements of both groups to be partitioned into classes according to their order, and compare the classes in G with the corresponding classes in $\mathbf{z}_n$. For each k , G has as many *or fewer* elements of order k than $\mathbf{z}_n$ does. So if G had no elements of order n (while $\mathbf{z}_n$ *does* have one), this would mean that G has fewer elements than $\mathbf{z}_n$, which is false. Thus, G *must* have an element of order n , and therefore G is cyclic. ■

The n th roots of unity (which are contained in F or a suitable extension of F) obviously form a group with respect to multiplication. By [Theorem 1](#), it is a cyclic group. Any generator of this group is called a *primitive n th root of unity*. Thus, if ω is a primitive n th root of unity, the set of all the n th roots of unity is

$$1, \omega, \omega^2, \dots, \omega^{n-1}$$

If ω is a primitive n th root of unity, $F(\omega)$ is an *abelian extension of F* in the sense that $g \circ h = h \circ g$ for any two F -fixing automorphisms g and h of $F(\omega)$). Indeed, any automorphism must obviously send n th roots of unity to n th roots of unity. So if $g(\omega) = \omega^r$ and $h(\omega) = \omega^s$, then $g \circ h(\omega) = g(\omega^s) = \omega^{rs}$ and analogously, $h \circ g(\omega) = \omega^{rs}$. Thus, $g \circ h(\omega) = h \circ g(\omega)$. Since g and h fix F , and every element of $F(\omega)$ is a linear combination of powers of ω with coefficients in F , $g \circ h = h \circ g$.

Now, let F contain a primitive n th root of unity, and therefore all the n th roots of unity. Suppose $a \in F$, and a has an n th root b in F . It follows, then, that *all the n th roots of a are in F , for they are $b, b\omega, b\omega^2, \dots, b\omega^{n-1}$* . Indeed, if c is any other n th root of a , then clearly c/b is an n th root of 1, say ω^r ; hence $c = b\omega^r$. We may infer from the above that *if F contains a primitive n th root of unity, and b is an n th root of a , then $F(b)$ is the root field of $x^n - a$ over F* .

In particular, $F(b)$ is an *abelian extension of F* . Indeed, any F -fixing automorphism of $F(b)$ must send n th roots of a to n th roots of a : for if c is any n th root of a and g is an F -fixing automorphism, then $g(c)^n = g(c^n) = g(a) = a$; hence $g(c)$ is an n th root of a . So if $g(b) = b\omega^r$ and $h(b) = b\omega^s$, then

$$g \circ h(b) = g(b\omega^s) = b\omega^r\omega^s = b\omega^{r+s}$$

and

$$h \circ g(b) = h(b\omega^r) = b\omega^s\omega^r = b\omega^{r+s}$$

hence $g \circ h(b) = h \circ g(b)$. Since g and h fix F , and every element in $F(b)$ is a linear combination of powers of b with coefficients in F , it follows that $g \circ h = h \circ g$.

If $a(x)$ is in $F[x]$, remember that $a(x)$ is solvable by radicals just as long as there exists *some* radical extension of F containing the roots of $a(x)$. [Any radical extension of F containing the roots of $a(x)$ will do.] Thus, we may as well assume that any radical extension used here begins by adjoining to F the appropriate roots of unity; *henceforth we will make this assumption*. Thus, if $K = F(c_1, \dots, c_n)$ is a radical extension of F , then

$$\underbrace{F}_{I_0} \subseteq \underbrace{F(c_1)}_{I_1} \subseteq \underbrace{F(c_1, c_2)}_{I_2} \subseteq \cdots \subseteq \underbrace{F(c_1, \dots, c_n)}_{I_m = K} \quad (2)$$

is a sequence of simple *abelian* extensions. (The extensions are all *abelian* by the comments in the preceding three paragraphs.)

Still, this is not quite enough for our purposes: In order to use the machinery which was set up in the previous chapter, we must be able to say that each field in (2) *is a root field over F*. This may be accomplished as follows: Suppose we have already constructed the extensions $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_q$ in (2) so that I_q is a root field over F . We must extend I_q to I_{q+1} , so I_{q+1} is a root field over F . Also, I_{q+1} must include the element c_{q+1} , which is the n th root of some element $a \in I_q$.

Let $H = \{h_1, \dots, h_r\}$ be the group of all the F -fixing automorphisms of I_q , and consider the polynomial

$$b(x) = [x^n - h_1(a)][x^n - h_2(a)] \cdots [x^n - h_r(a)]$$

By the proof of the lemma on page 327, one factor of $b(x)$ is $(x^n - a)$; hence c_{q+1} is a root of $b(x)$. Moreover, by the same lemma, every coefficient of $b(x)$ is in the fixfield of H , that is, in F . We now define I_{q+1} to be the root field of $b(x)$ over F . Since all the roots of $b(x)$ are n th roots of elements in I_q , it follows that I_{q+1} is a radical extension of I_q . The roots may be adjoined one by one, yielding a succession of *abelian* extensions, as discussed previously. To conclude, we may assume in (2) that K is a root field over F .

If $\mathbf{G}$ denotes the Galois group of K over F , each of these fields I_k has a fixer which is a subgroup of $\mathbf{G}$. These fixers form a sequence

$$\underbrace{K^*}_{=\{e\}} \subseteq I_{m-1}^* \subseteq \cdots \subseteq I_1^* \subseteq \underbrace{F^*}_{=\mathbf{G}}$$

For each k , by [Theorem 4 of Chapter 32](#), I_k^* is a normal subgroup of I_{k+1}^* , and $I_{k+1}^*/I_k^* \cong \text{Gal}(I_{k+1}: I_k)$ which is abelian because is an abelian extension of I_k . The following definition was invented precisely to account for this situation.

*A group G is called **solvable** if it has a sequence of subgroups $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m = G$ such that for each k , G_k is a normal subgroup of G_{k+1} and G_{k+1}/G_k is abelian.*

We have shown that *if K is a radical extension of F , then $\text{Gal}(K: F)$ is a solvable group*. We wish to go further and prove that if $a(x)$ is any polynomial which is solvable by radicals, its Galois group is solvable. To do so, we must first prove that any homomorphic image of a solvable group is solvable. A key ingredient of our proof is the following simple fact, which was explained on page 152: G/H is abelian iff H contains all the products $xyx^{-1}y^{-1}$ for all x and y in G . (The products $xyx^{-1}y^{-1}$ are called “commutators” of G .)

Theorem 2 *Any homomorphic image of a solvable group is a solvable group.*

PROOF: Let G be a solvable group, with a sequence of subgroups

$$\{e\} \subseteq H_1 \subseteq \cdots \subseteq H_m = G$$

as specified in the definition. Let $f: G \rightarrow X$ be a homomorphism from G onto a group X . Then $f(H_0), f(H_1), \dots, f(H_m)$ are subgroups of X , and clearly $\{e\} \subseteq f(H_0) \subseteq f(H_1) \subseteq \dots \subseteq f(H_m) = X$. For each i we have the following: if $f(a) \in f(H_i)$ and $f(x) \in f(H_{i+1})$, then $a \in H_i$ and $x \in H_{i+1}$; hence $xax^{-1} \in H_i$ and therefore $f(x)f(a)f(x)^{-1} \in f(H_i)$. So $f(H_i)$ is a normal subgroup of $f(H_{i+1})$. Finally, since H_{i+1}/H_i is abelian, every commutator $xyx^{-1}y^{-1}$ (for all x and y in H_{i+1}) is in H_i ; hence every $f(x)f(y)f(x)^{-1}f(y)^{-1}$ is in $f(H_i)$. Thus, $f(H_{i+1})/f(H_i)$ is abelian. ■

Now we can prove the main result of this chapter:

Theorem 3 *Let $a(x)$ be a polynomial over a field F . If $a(x)$ is solvable by radicals, its Galois group is a solvable group.*

PROOF: By definition, if K is the root field of $a(x)$, there is an extension by radicals $F(c_1, \dots, c_n)$ such that $F \subseteq K \subseteq F(c_1, \dots, c_n)$. It follows by Theorem 4 of Chapter 32 that $Gal(F(c_1, \dots, c_n): F)/Gal(F(c_1, \dots, c_n): K) \cong Gal(K: F)$; hence by that theorem, $Gal(K: F)$ is a homomorphic image of $Gal(F(c_1, \dots, c_n): F)$ which we know to be solvable. Thus, by Theorem 2 $Gal(K: F)$ is solvable. ■

Actually, the converse of Theorem 3 is true also. All we need to show is that, if K is an extension of F whose Galois group over F is solvable, then K may be further extended to a radical extension of F . The details are not too difficult and are assigned as Exercise E at the end of this chapter.

Theorem 3 together with its converse say that a polynomial $a(x)$ is solvable by radicals iff its Galois group is solvable.

We bring this chapter to a close by showing that there exist groups which are not solvable, and there exist polynomials having such groups as their Galois group. In other words, *there are unsolvable polynomials*. First, here is an unsolvable group:

Theorem 4 *The symmetric group S_5 is not a solvable group.*

PROOF: Suppose S_5 has a sequence of subgroups

$$\{e\} = H_0 \subseteq H_1 \subseteq \dots \subseteq H_m = S_5$$

as in the definition of solvable group. Consider the subset of S_5 containing all the cycles (ijk) of length 3. We will show that if H_i contains all the cycles of length 3, so does the next smaller group H_{i-1} . It would follow in m steps that $H_0 = \{e\}$ contains all the cycles of length 3, which is absurd.

So let H_i contain all the cycles of length 3 in S_5 . Remember that if α and β are in H_i , then their commutator $\alpha\beta\alpha^{-1}\beta^{-1}$ is in H_{i-1} . But any cycle (ijk) is equal to the commutator

$$(ilj)(jkm)(ilj)^{-1}(jkm)^{-1} = (ilj)(jkm)(jli)(mkj) = (ijk)$$

hence every (ijk) is in H_{i-1} , as claimed. ■

Before drawing our argument toward a close, we need to know one more fact about groups; it is contained in the following classical result of group theory:

Cauchy's theorem *Let G be a finite group of n elements. If p is any prime number which divides n , then G has an element of order p .*

For example, if G is a group of 30 elements, it has elements of orders 2, 3, and 5. To give our proof a trimmer appearance, we will prove Cauchy's theorem specifically for $p = 5$ (the only case we will use here, anyway). However, the same argument works for any value of p .

PROOF: Consider all possible 5-tuples (a, b, c, d, k) of elements of G whose product $abcdk = e$. How many distinct 5-tuples of this kind are there? Well, if we select a, b, c , and d at random, there is a unique $k = d^{-1}c^{-1}b^{-1}a^{-1}$ in G making $abcdk = e$. Thus, there are n^4 such 5-tuples.

Call two 5-tuples *equivalent* if one is merely a cyclic permutation of the other. Thus, (a, b, c, d, k) is equivalent to exactly five distinct 5-tuples, namely, (a, b, c, d, k) , (b, c, d, k, a) , (c, d, k, a, b) , (d, k, a, b, c) and (k, a, b, c, d) . The only exception occurs when a 5-tuple is of the form (a, a, a, a, a) with all its components equal; it is equivalent only to itself. Thus, the equivalence class of any 5-tuple of the form (a, a, a, a, a) has a single member, while all the other equivalence classes have five members.

Are there any equivalence classes, other than $\{(e, e, e, e, e)\}$, with a single member? *If not*, then $5 | (n^4 - 1)$ [for there are n^4 5-tuples under consideration, less (e, e, e, e, e)]; hence $n^4 \equiv 1 \pmod{5}$. But we are assuming that $5 | n$; hence $n^4 \equiv 0 \pmod{5}$, which is a contradiction.

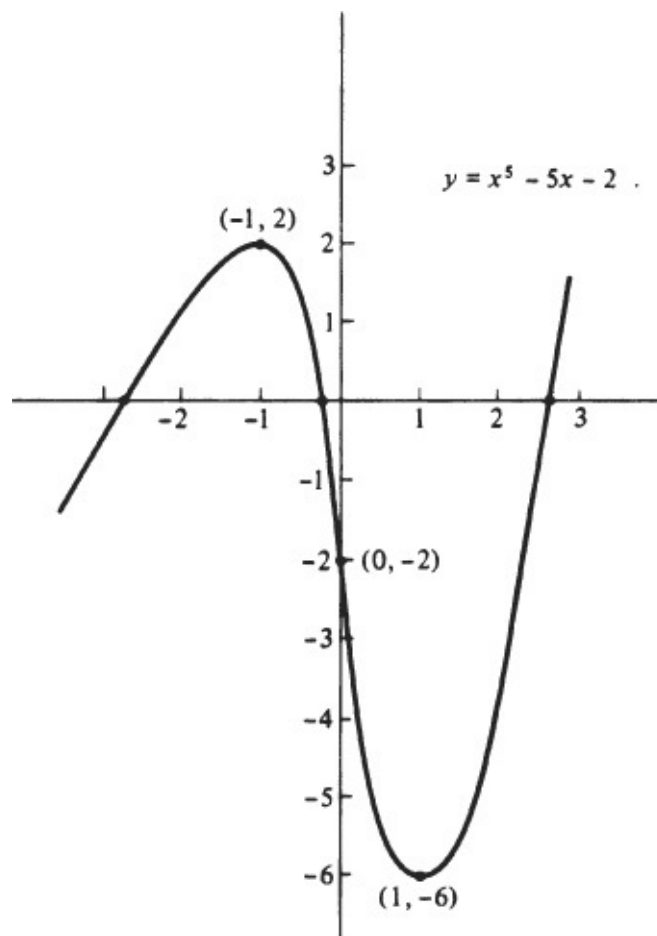
This contradiction shows that there must be a 5-tuple $(a, a, a, a, a) \neq (e, e, e, e, e)$ such that $aaaaa = a^5 = e$. Thus, there is an element $a \in G$ of order 5. ■

We will now exhibit a polynomial in $\mathbb{Q}[x]$ having S_5 as its Galois group (remember that S_5 is *not* a solvable group).

Let $a(x) = x^5 - 5x - 2$. By Eisenstein's criterion, $a(x + 2)$ is irreducible over $\mathbb{Q}$; hence $a(x)$ also is irreducible over $\mathbb{Q}$. By elementary calculus, $a(x)$ has a single maximum at $(-1, 2)$, a single minimum at $(1, -6)$, and a single point of inflection at $(0, -2)$. Thus (see figure), its graph intersects the x axis exactly three times. This means that $a(x)$ has three real roots, r_1, r_2 , and r_3 , and therefore two complex roots, r_4 and r_5 , which must be complex conjugates of each other.

Let K denote the root field of $a(x)$ over $\mathbb{Q}$, and $\mathbf{G}$ the Galois group of $a(x)$. As we have already noted, every element of $\mathbf{G}$ may be identified with a permutation of the roots r_1, r_2, r_3, r_4, r_5 of $a(x)$, so $\mathbf{G}$ may be viewed as a subgroup of S_5 . We will show that $\mathbf{G}$ is all of S_5 .

Now, $[\mathbb{Q}(r_1) : \mathbb{Q}] = 5$ because r_1 is a root of an irreducible polynomial of degree 5 over $\mathbb{Q}$. Since $[K : \mathbb{Q}] = [K : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}]$, it follows that 5 is a factor of $[K : \mathbb{Q}]$. Then, by Cauchy's theorem, $\mathbf{G}$ contains an element of order 5. This element must be a cycle of length 5: for by [Chapter 8](#), every other element of S_5 is a product of two or more disjoint cycles of length < 5 , and such products cannot have order 5. (Try the typical cases.) Thus, $\mathbf{G}$ contains a cycle of length 5.



Furthermore, $\mathbf{G}$ contains a transposition because complex conjugation $a + bi \rightarrow a - bi$ is obviously a $\mathbf{Q}$ -fixing automorphism of K ; it interchanges the complex roots r_4 and r_5 while leaving r_1 , r_2 , and r_3 fixed.

Any subgroup $G \subseteq S_5$ which contains a transposition τ and a cycle σ of length 5 necessarily contains all the transpositions. (They are $\sigma\tau\sigma^{-1}$, $\sigma^2\tau\sigma^{-2}$, $\sigma^3\tau\sigma^{-3}$, $\sigma^4\tau\sigma^{-4}$, and their products; check this by direct computation!) Finally, if G contains all the transpositions, it contains everything else: for every member of S_5 is a product of transpositions. Thus, $\mathbf{G} = S_5$.

We have just given an example of a polynomial $a(x)$ of degree 5 over $\mathbf{Q}$ whose Galois group S_5 is not solvable. Thus, $a(x)$ is an example of a polynomial of degree 5 which cannot be solved by radicals. In particular, there cannot be a radical formula (on the model of the quadratic formula) to solve all polynomial equations of degree 5, since this would imply that every polynomial equation of degree 5 has a radical solution, and we have just exhibited one which does not have such a solution.

In [Exercise B](#) it is shown that S_3 , S_4 , and all their subgroups are solvable; hence every polynomial of degree ≤ 4 is solvable by radicals.

EXERCISES

A. Finding Radical Extensions

1 Find radical extensions of $\mathbf{Q}$ containing the following complex numbers:

- (a) $(\sqrt{5} - \sqrt[5]{2})/(\sqrt[4]{3} + \sqrt[3]{4})$
- (b) $\sqrt{(1 - \sqrt[9]{2})/\sqrt[3]{1 - \sqrt{5}}}$
- (c) $\sqrt[3]{(\sqrt{3} - 2i)^3/(i - \sqrt{11})}$

2 Show that the following polynomials in $\mathbb{Q}[x]$ are not solvable by radicals:

(a) $2x^5 - 5x^4 + 5$

(b) $x^5 - 4x^2 + 2$

(c) $x^5 - 4x^4 + 2x + 2$

3 Show that $a(x) = x^5 - 10x^4 + 40x^3 - 80x^2 + 79x - 30$ is solvable by radicals over $\mathbb{Q}$, and give its root field. [HINT: Compute $(x - 2)^5 - (x - 2)$.]

4 Show that $ax^8 + bx^6 + cx^4 + dx^2 + e$ is solvable by radicals over any field. (HINT: Let $y = x^2$; use the fact that every fourth-degree polynomial is solvable by radicals.)

5 Explain why parts 3 and 4 do not contradict the principal finding of this chapter: that polynomial equations of degree $n \geq 5$ do not have a general solution by radicals.

† B. Solvable Groups

Let G be a group. The symbol $H \triangleleft G$ is commonly used as an abbreviation of “ H is a *normal* subgroup of G .” A *normal series* of G is a finite sequence $H_0, H_1, \dots, H_n$ of subgroups of G such that

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$$

Such a series is called a *solvable series* if each quotient group H_{i+1}/H_i is abelian. G is called a *solvable group* if it has a solvable series.

1 Explain why every abelian group is, trivially, a solvable group.

2 Let G be a solvable group, with a solvable series $H_0, \dots, H_n$. Let K be a subgroup of G . Show that $J_0 = K \cap H_0, \dots, J_n = K \cap H_n$ is a normal series of K .

3 Use the remark immediately preceding [Theorem 2](#) to prove that $J_0, \dots, J_n$ is a solvable series of K .

4 Use parts 2 and 3 to prove: Every subgroup of a solvable group is solvable.

5 Verify that $\{\varepsilon\} \subseteq \{\varepsilon, \beta, \delta\} \subseteq S_3$ is a solvable series for S_3 . Conclude that S_3 , and all of its subgroups, are solvable.

6 In S_4 , let A_4 be the group of all the even permutations, and let

$$B = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$$

Show that $\{\varepsilon\} \subseteq B \subseteq A_4 \subseteq S_4$ is a solvable series for S_4 . Conclude that S_4 and all its subgroups are solvable.

The next three sets of exercises are devoted to proving the converse of [Theorem 3](#): If the Galois group of $a(x)$ is solvable, then $a(x)$ is solvable by radicals.

† C. p th Roots of Elements in a Field

Let p be a prime number, and ω a primitive p th root of unity in the field F .

1 If d is any root of $x^p - a \in F[x]$, show that $F(\omega, d)$ is a root field of $x^p - a$. Suppose $x^p - a$ is *not* irreducible in $F[x]$.

2 Explain why $x^p - a$ factors in $F[x]$ as $x^p - a = p(x)f(x)$, where both factors have degree ≤ 2 .

3 If $\deg p(x) = m$, explain why the constant term of $p(x)$ (let us call it b) is equal to the product of m pth roots of a . Conclude that $b = \omega^k a^m$ for some k .

4 Use part 3 to prove that $b^p = a^m$.

5 Explain why m and p are relatively prime. Explain why it follows that there are integers s and t such that $sm + tp = 1$.

6 Explain why $b^{sp} = a^{sm}$. Use this to show that $(b^s a^t)^p = a$.

7 Conclude: If $x^p - a$ is *not* irreducible in $F[x]$, it has a root (namely, $b^s a^t$) in F .

We have proved: $x^p - a$ either has a root in F or is irreducible over F .

† D. Another Way of Defining Solvable Groups

Let G be a group. The symbol $H \triangleleft G$ should be read, “ H is a normal subgroup of G .” A *maximal* normal subgroup of G is an $H \triangleleft G$ such that, if $H \triangleleft J \triangleleft G$, then necessarily $J = H$ or $J = G$. Prove the following:

1 If G is a *finite* group, every normal subgroup of G is contained in a maximal normal subgroup.

2 Let $f: G \rightarrow H$ be a homomorphism. If $J \triangleleft H$, then $f^{-1}(J) \triangleleft G$.

3 Let $K \triangleleft G$. If $\mathcal{J}$ is a subgroup of G/K , let $\hat{\mathcal{J}}$ denote the union of all the cosets which are members of $\mathcal{J}$. If $\mathcal{J} \triangleleft G/K$, then $\hat{\mathcal{J}} \triangleleft G$. (Use part 2.)

4 If K is a maximal normal subgroup of G , then G/K has no nontrivial normal subgroups. (Use part 3.)

5 If an abelian group G has no nontrivial subgroups, G must be a cyclic group of prime order. (Otherwise, choose some $a \in G$ such that $\langle a \rangle$ is a proper subgroup of G .)

6 If $H \triangleleft K \triangleleft G$, then G/K is a homomorphic image of G/H .

7 Let $H \triangleleft G$, where G/H is abelian. Then G has subgroups $H_0, \dots, H_q$ such that $H = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_q = G$, where each quotient group H_{i+1}/H_i is cyclic of prime order.

It follows from part 7 that if G is a solvable group, then, by “filling in gaps,” G has a normal series in which all the quotient groups are cyclic of prime order. Solvable groups are often defined in this fashion.

E. If $\text{Gal}(K: F)$ Is Solvable, K Is a Radical Extension of F

Let K be a finite extension of F , where K is a root field over F , with $G = \text{Gal}(K: F)$ a solvable group. As remarked in the text, we will assume that F contains the required roots of unity. By [Exercise D](#), let $H_0, \dots, H_n$ be a solvable series for G in which every quotient H_{i+1}/H_i is cyclic of prime order. For any $i = 1, \dots, n$, let F_i and F_{i+1} be the fixfields of H_i and H_{i+1} .

1 Prove: F_i is a normal extension of F_{i+1} , and $[F_i: F_{i+1}]$ is a prime p .

2 Let π be a generator of $\text{Gal}(F_i: F_{i+1})$, ω a pth root of unity in F_{i+1} , and $b \in F_i$. Set

$$c = b + \omega\pi^{-1}(b) + \omega^2\pi^{-2}(b) + \dots + \omega^{p-1}\pi^{-(p-1)}(b)$$

Show that $\pi(c) = \omega c$.

3 Use part 2 to prove that $\pi^k(c^p) = c^p$ for every k , and deduce from this that $c^p \in F_{i+1}$

4 Prove that F_i is the root field of $x^p - c^p$ over F_{i+1} .

5 Conclude that K is a radical extension of F .