ABSTRACT ALGEBRA:

REVIEW PROBLEMS ON GROUPS AND GALOIS THEORY

John A. Beachy

Northern Illinois University

2006

This is a supplement to

Abstract Algebra, *Third Edition*
by John A. Beachy and William D. Blair

ISBN 1–57766–443–4, Copyright 2006

Waveland Press, Inc.
4180 IL Route 83, Suite 101
Long Grove, Illinois 60047-9580
847 / 634-0081
www.waveland.com

Formatted January 11, 2007, at which time the original was available at:
http://www.math.niu.edu/~beachy/abstract_algebra/

Contents

PREFACE

My goal is to provide some help in reviewing Chapters 7 and 8 of our book *Abstract Algebra*. I have included summaries of most of these sections, together with some general comments. The review problems are intended to have relatively short answers, and to be more typical of exam questions than of standard textbook exercises.

By assuming that this is a review, I have been able make some minor changes in the order of presentation. The first section covers various examples of groups. In presenting these examples, I have introduced some concepts that are not studied until later in the text. I think it is helpful to have the examples collected in one spot, so that you can refer to them as you review.

A complete list of the definitions and theorems in the text can be found on the web site `www.math.niu.edu/~beachy/aaol/` . This site also has some group multiplication tables that aren't in the text. I should note two minor changes in notation–I've used 1 to denote the identity element of a group (instead of e), and I've used the abbreviation "iff" for "if and only if".

Abstract Algebra begins at the undergraduate level, but Chapters 7–9 are written at a level that we consider appropriate for a student who has spent the better part of a year learning abstract algebra. Although it is more sharply focused than the standard graduate level textbooks, and does not go into as much generality, I hope that its features make it a good place to learn about groups and Galois theory, or to review the basic definitions and theorems.

Finally, I would like to gratefully acknowledge the support of Northern Illinois University while writing this review. As part of the recognition as a "Presidential Teaching Professor," I was given leave in Spring 2000 to work on projects related to teaching.

DeKalb, Illinois John A. Beachy
May 2000

In this new printing the references have been updated to the third edition of the text. Otherwise, the changes are relatively minor.

DeKalb, Illinois John A. Beachy
December 2006

Chapter 7

STRUCTURE OF GROUPS

The goal of a structure theory is to find the basic building blocks of the subject and then learn how they can be put together. In group theory the basic building blocks are usually taken to be the simple groups, and they fit together by "stacking" one on top of the other, using factor groups.

To be more precise about this, we need to preview Definition 7.6.9. Let G be a group. A chain of subgroups $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_k$ is called a *composition series* for G if

(i) N_i is a normal subgroup of N_{i-1} for $i = 1, 2, \ldots, k$,

(ii) N_{i-1}/N_i is simple for $i = 1, 2, \ldots, k$, and

(iii) $N_k = \langle 1 \rangle$

The factor groups N_{i-1}/N_i are called the *composition factors* of the series. The number n is called the *length* of the series.

We can always find a composition series for a finite group G, by choosing N_1 to be a maximal normal subgroup of G, then choosing N_2 to be a maximal normal subgroup of N_1, and so on. The Jordan-Hölder theorem (see Theorem 7.6.10) states that any two composition series for a finite group have the same length. Furthermore, there exists a one-to-one correspondence between composition factors of the two composition series, under which corresponding factors are isomorphic.

Unfortunately, the composition factors of a group G do not, by themselves, completely determine the group. We still need to know how to put them together. That is called the "extension problem": given a group G with a normal subgroup N such that N and G/N are simple groups, determine the possibilities for the structure of G. The most elementary possibility for G is that $G = N \times K$, for some normal subgroup K with $K \cong G/N$, but there are much more interesting ways to construct G that tie the groups N and G/N together more closely.

What is known as the Hölder program for classifying all finite groups is this: first classify all finite simple groups, then solve the extension problem to determine the ways in which finite groups can be built out of simple composition factors. This attack on the structure of finite groups was begun by Otto Hölder (1859–1937) in a series of papers published during the period 1892–1895.

The simple abelian groups are precisely the cyclic groups of prime order, and groups whose simple composition factors are abelian form the class of solvable groups, which plays an important role in Galois theory. Galois himself knew that the alternating groups A_n are simple, for $n \geq 5$, and Camille Jordan (1838–1922) discovered several classes of simple groups defined by matrices over $\mathbf{Z}_p$, where p is prime. Hölder made a search for simple nonabelian groups, and showed that for order 200 or less, the only ones are A_5, of order 60, and the group $\mathrm{GL}_3(\mathbf{Z}_2)$ of all invertible 3×3 matrices with entries in $\mathbf{Z}_2$, which has order 168.

7.0 Some Examples

Summary: It is impossible to overemphasize the importance of examples.

Since this is a review of material you have already covered, it makes sense to group together the examples you have worked with. It is important to use them to deepen your understanding of the definitions and theorems. They can also be used to help you generate ideas on how to solve specific exercises and exam questions.

Cyclic groups

Cyclic groups are classified in Theorem 3.5.2: if G is infinite, then the powers of its generator are distinct, and G is isomorphic to the group $\mathbf{Z}$; if G is cyclic of order n, with generator a, then $a^m = a^k$ iff $k \equiv m \pmod{n}$, and G is isomorphic to $\mathbf{Z}_n$. Since every subgroup of a cyclic group is cyclic, the nonzero subgroups of $\mathbf{Z}$ correspond to the cyclic subgroups generated by the positive integers. The nonzero subgroups of $\mathbf{Z}_n$ correspond to the proper divisors of n. In multiplicative terminology, if G is cyclic of order n, with generator a, then the subgroup generated by a^m coincides with the subgroup generated by a^d, where $d = \gcd(m, n)$, and so this subgroup has order n/d. (This subgroup structure is described in Propositions 3.5.3 and 3.5.4.)

Figure 7.0.1

$$
\begin{tikzcd}
& \mathbf{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & & \\
\langle 3 \rangle \arrow[dr, dash] & & \langle 2 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
& \langle 6 \rangle \arrow[dr, dash] & & \langle 4 \rangle \arrow[dl, dash] \\
& & \langle 0 \rangle &
\end{tikzcd}
$$

Figure 7.0.1 gives the subgroups of $\mathbf{Z}_{12}$. Any path from $\mathbf{Z}_{12}$ to $\langle 0 \rangle$ produces a composition series for $\mathbf{Z}_{12}$. In fact, there are the following three choices.

$$\mathbf{Z}_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 0 \rangle$$

$$\mathbf{Z}_{12} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \langle 0 \rangle$$

$$\mathbf{Z}_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 0 \rangle$$

All composition series for $\mathbf{Z}_n$ can be determined from the prime factorization of n.

How can you recognize that a given group is cyclic? Of course, if you can actually produce a generator, that is conclusive. Another way is to compute the *exponent* of G, which is the smallest positive integer n such that $g^n = 1$, for all $g \in G$. Proposition 3.5.9 (b) states that a finite abelian group is cyclic if and only if its exponent is equal to its order. For example, in Theorem 6.5.10 this characterization of cyclic groups is used to prove that any finite subgroup of the multiplicative group of a field is cyclic.

Direct products

Recall that the *direct product* of two groups G_1 and G_2 is the set of all ordered pairs (x_1, x_2), where $x_1 \in G_1$ and $x_2 \in G_2$, with the componentwise operation $(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1, x_2y_2)$ (see Definition 3.3.3 and Proposition 3.3.4). This construction can be extended to any finite number of groups, and allows us to produce new examples from known groups. Note that when the groups involved are abelian, and are written additively, many authors use the notation $A_1 \oplus A_2$ instead of $A_1 \times A_2$.

The opposite of constructing a new group from known groups is to be able to recognize when a given group can be constructed from simpler known groups, using the direct product. In the case of the cyclic group $\mathbf{Z}_n$, we have the following result from Proposition 3.4.5. If the positive integer n has a factorization $n = km$, as a product of relatively prime positive integers, then $\mathbf{Z}_n \cong \mathbf{Z}_k \times \mathbf{Z}_m$.

This is proved by defining a group homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k \times \mathbf{Z}_m$ by setting $\phi([x]_n) = ([x]_k, [x]_m)$. Since the two sets have the same number of elements, it suffices to show either that ϕ is onto or that $\ker(\phi) = \{[0]_n\}$. The statement that ϕ is onto is precisely the statement of the Chinese remainder theorem (see Theorem 1.3.6 for the statement and proof). That the kernel is zero follows from elementary number theory: if $k \mid x$ and $m \mid x$, then $km \mid x$, since k and m are relatively prime.

The above result can be extended to show that any finite cyclic group is isomorphic to a direct product of cyclic groups of prime power order. (See Theorem 3.5.5, whose proof uses the prime factorization of $|G|$.) This is a special case of the structure theorem for finite abelian groups, and Figure 7.0.2 uses this approach to give another way to view the subgroups of the cyclic group $\mathbf{Z}_{12}$, and to find a composition series for it.

Figure 7.0.2

$$\begin{tikzcd}
 & \mathbf{Z}_4 \times \mathbf{Z}_3 \arrow[dl, dash] \arrow[dr, dash] & & \\
\mathbf{Z}_4 \times \langle 0 \rangle \arrow[dr, dash] & & \langle 2 \rangle \times \mathbf{Z}_3 \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle 2 \rangle \times \langle 0 \rangle \arrow[dr, dash] & & \langle 0 \rangle \times \mathbf{Z}_3 \arrow[dl, dash] \\
 & & \langle (0,0) \rangle &
\end{tikzcd}$$

Using the decomposition $\mathbf{Z}_{12} \cong \mathbf{Z}_4 \times \mathbf{Z}_3$, we have the following composition series.

$$\mathbf{Z}_4 \times \mathbf{Z}_3 \supset \mathbf{Z}_4 \times \langle 0 \rangle \supset \langle 2 \rangle \times \langle 0 \rangle \supset \langle (0,0) \rangle$$

$$\mathbf{Z}_4 \times \mathbf{Z}_3 \supset \langle 2 \rangle \times \mathbf{Z}_3 \supset \langle 2 \rangle \times \langle 0 \rangle \supset \langle (0,0) \rangle$$

$$\mathbf{Z}_4 \times \mathbf{Z}_3 \supset \langle 2 \rangle \times \mathbf{Z}_3 \supset \langle 0 \rangle \times \mathbf{Z}_3 \supset \langle (0,0) \rangle$$

Theorem 7.1.3 gives one possible way to recognize a direct product. Let G be a group with normal subgroups H, K such that $HK = G$ and $H \cap K = \langle 1 \rangle$. Then $G \cong H \times K$. Note that the conditions of the theorem imply that any element of H must commute with any element of K.

With the above notation, it may happen that $H \cap K = \langle 1 \rangle$ and $HK = G$, even though only one of the subgroups is normal in G. This situation defines what is called the *semidirect product* of H and K, and provides an important tool in classifying finite groups. Unfortunately, the use of semidirect products is beyond the scope of our text. (They are covered in the supplement that is available on the book's web site.)

Finite abelian groups

The simplest way to approach the structure of a finite abelian group is to remember that it can be written as a direct product of cyclic groups. Just saying this much does not guarantee any uniqueness. There are two standard ways to do this decomposition in order to achieve a measure of uniqueness. The cyclic groups can each be broken apart as much as possible, yielding a decomposition into groups of prime power order. These cyclic groups are unique, but in the direct product they can be written in various orders. A second method arranges the cyclic groups into a direct product in which the order of each factor is a divisor of the order of the previous factor. This is illustrated by the following two decompositions of the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$, which has order $2^3 \cdot 3^3$.

$$\mathbf{Z}_{12} \times \mathbf{Z}_{18} \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_3 \cong \mathbf{Z}_{36} \times \mathbf{Z}_6$$

The symmetric groups S_n

The *symmetric group* S_n is defined as the set of all permutations of the set $\{1, \ldots, n\}$ (see Definition 3.1.5). These groups provided the original motivation for the development of group theory, and a great many of the general theorems on the structure of finite groups were first proved for symmetric groups. This class of groups is the most basic of all, in the sense that any group of order n is isomorphic to a subgroup of S_n. Recall that this is the statement of Cayley's theorem, which can be proved using the language of group actions, by simply letting the group act on itself via the given multiplication. (See Theorem 3.6.2.) One important fact to remember about S_n is that two permutations are conjugate in S_n iff they have the same number of cycles, of the same length.

The alternating groups A_n

Any permutation in S_n can be written as a product of transpositions, and although the expression is not unique, the *number* of transpositions *is* well-defined, modulo 2. In fact, if we define $\pi : S_n \to \mathbf{Z}^{\times}$ by setting $\pi(\sigma) = 1$ if σ is even and $\pi(\sigma) = -1$ if σ is odd, then π is a well-defined group homomorphism whose kernel is the *alternating group* A_n consisting of the even permutations in S_n.

For $n = 3$, the series $S_3 \supset A_3 \supset \langle 1 \rangle$ is a composition series. Theorem 7.7.4 shows that the alternating group A_n is simple if $n \geq 5$, so in this case we have the composition series $S_n \supset A_n \supset \langle 1 \rangle$. Problem 7.0.4 shows that S_4 has a normal subgroup $N_2 \subseteq A_4$ with $S_4/N_2 \cong S_3$ and $N_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$, and so it has a composition series

$$S_4 \quad \supset \quad A_4 \quad \supset \quad N_2 \quad \supset \quad N_3 \quad \supset \quad \langle 1 \rangle$$

with $A_4/N_2 \cong \mathbf{Z}_3$, $N_2/N_3 \cong \mathbf{Z}_2$, and $N_3 \cong \mathbf{Z}_2$.

It is also possible to give some information about the conjugacy classes of A_n. Let $\sigma \in A_n$, let $C_A(\sigma)$ be the centralizer of σ in A_n, and let $C_S(\sigma)$ be the centralizer of σ in S_n. If $C_S(\sigma) \subseteq A_n$, then $C_S(\sigma) = C_A(\sigma)$, and in this case σ has $|A_n|/|C_S(\sigma)|$ conjugates, representing half as many conjugates as it has in S_n. On the other hand, if $C_S(\sigma)$ contains an odd permutation, then $C_A(\sigma)$ has half as many elements as $C_S(\sigma)$, and so σ has the same conjugates in A_n as in S_n.

The dihedral groups D_n

The *dihedral group* D_n is defined for $n \geq 3$ in Definition 3.6.3 as the group of rigid motions of a regular n-gon. In terms of generators and relations, we can describe D_n as generated by an element a of order n, and an element b of order 2, subject to the relation $ba = a^{-1}b$. The elements can then be put in the standard form $a^i b^j$, where $0 \leq i < n$ and $0 \leq j < 2$. The important formula to remember is that $ba^i = a^{-i}b$. A composition series for D_n can be constructed by using the fact that $\langle a \rangle$ is a maximal normal subgroup with $\langle a \rangle \cong \mathbf{Z}_n$.

The conjugacy classes of D_n can be computed easily, and provide excellent examples of this crucial concept. Exercise 7.2.13 of the text shows that a^m is conjugate to itself and a^{-m}, while $a^m b$

is conjugate to $a^{m+2k}b$, for any $k \in \mathbf{Z}$. Thus if n is odd, the center of D_n is trivial, and if n is even, it contains 1 and $a^{n/2}$. In the first case the centralizer of b contains only b and 1, while in the second it contains the center as well. Thus in the second case b is conjugate to exactly half of the elements of the form $a^i b$.

The general linear groups $\mathrm{GL}_n(F)$

The general linear groups over finite fields provide the typical examples of finite groups. To be more specific, we start with a finite field F. The set of $n \times n$ invertible matrices with entries in F forms a group under multiplication that is denoted by $\mathrm{GL}_n(F)$. (You will find that other authors may use the notation $\mathrm{GL}(n, F)$.)

It is quite common to begin the study of nonabelian groups with the symmetric groups S_n. Of course, this class contains all finite groups as subgroups, but the size also quickly gets out of hand. On the other hand, Problem 7.0.1 shows that $\mathrm{GL}_n(F)$ also contains a copy of each group of order n, and working with matrices allows use of ideas from linear algebra, such as the determinant and the trace. Note that Exercise 7.7.11 in the text shows that $|\,\mathrm{GL}_n(F)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

The first step in constructing a composition series for $\mathrm{GL}_n(F)$ is to use the determinant function. Since the determinant preserves products, it defines a group homomorphism $\Delta : \mathrm{GL}_n(F) \to F^\times$ from $\mathrm{GL}_n(F)$ onto the multiplicative group of the field F. We use the notation $\mathrm{SL}_n(F)$ for the set of invertible matrices with determinant 1, so we have $\mathrm{SL}_n(F) = \ker(\Delta)$. The group $F^\times$ is cyclic, since F is finite, so $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong \mathbf{Z}_{q-1}$, where $|F| = q$.

We note two special cases. First, Example 3.4.5 shows that $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$, and it is obvious that $\mathrm{SL}_2(\mathbf{Z}_2) = \mathrm{GL}_2(\mathbf{Z}_2)$. Secondly, the group $\mathrm{GL}_2(\mathbf{Z}_3)$ has $(3^2 - 1)(3^2 - 3) = 48$ elements. The center of $\mathrm{GL}_2(\mathbf{Z}_3)$ consists of scalar matrices, and these all have determinant 1. This gives us a series of normal subgroups

$$\mathrm{GL}_2(\mathbf{Z}_3) \;\supset\; \mathrm{SL}_2(\mathbf{Z}_3) \;\supset\; Z(\mathrm{GL}_2(\mathbf{Z}_3))$$

in which $\mathrm{SL}_2(\mathbf{Z}_3)/Z(\mathrm{GL}_2(\mathbf{Z}_3))$ has 12 elements. Example 7.7.2 and Exercise 7.7.13 in the text show that this factor group is isomorphic to A_4, and with this knowledge it is possible to refine the above series to a composition series for $\mathrm{GL}_2(\mathbf{Z}_3)$.

The special linear groups $\mathrm{SL}_n(F)$

The group $\mathrm{SL}_n(F)$ is called the *special linear group* over F. Its center can be shown to be

$$Z(\mathrm{SL}_n(F)) = \mathrm{SL}_n(F) \cap Z(\mathrm{GL}_n(F)) \; .$$

The center may be trivial in certain cases, but in any event, $Z(\mathrm{SL}_n(F))$ is isomorphic to a subgroup of the additive group of the field, so it is an abelian group, and we can construct a composition series for it as before.

In constructing a composition series for $\mathrm{GL}_n(F)$, we have the following series,

$$\mathrm{GL}_n(F) \;\supset\; \mathrm{SL}_n(F) \;\supset\; Z(\mathrm{SL}_n(F)) \;\supset\; \langle 1 \rangle \; ,$$

in which the factors $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$ and $Z(\mathrm{SL}_n(F))$ are abelian. These two factors can be handled easily since they are abelian, so the real question is about $\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$, which is called the *projective special linear group*, and is denoted by $\mathrm{PSL}_n(F)$. The following theorem is beyond the scope of our text; we only prove the special case $n = 2$ (see Theorem 7.7.9). You can find the proof of the general case in Jacobson's *Basic Algebra I.*

Theorem. If F is a finite field, then $\mathrm{PSL}_n(F)$ is a simple group, except for the special cases $n = 2$ and $|F| = 2$ or $|F| = 3$.

REVIEW PROBLEMS: SECTION 7.0

1. Prove that if G is a group of order n, and F is any field, then $\mathrm{GL}_n(F)$ contains a subgroup isomorphic to G.

2. What is the largest order of an element in $\mathbf{Z}_{200}^{\times}$?

3. Let G be a finite group, and suppose that for any two subgroups H and K either $H \subseteq K$ or $K \subseteq H$. Prove that G is cyclic of prime power order.

4. Let $G = S_4$ and $N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Prove that N is normal, and that $G/N \cong S_3$.

5. Problem 4 can be used to construct a composition series $S_4 \supset N_1 \supset N_2 \supset N_3 \supset \langle 1 \rangle$ in which $N_1 = A_4$ and $N_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Show that there is no composition series in which $N_2 \cong \mathbf{Z}_4$.

6. Find the center of the alternating group A_n.

7. In a group G, any element of the form $xyx^{-1}y^{-1}$, with $x, y \in G$, is called a *commutator* of G.

   (a) Find all commutators in the dihedral group D_n. Using the standard description of D_n via generators and relations, consider the cases $x = a^i$ or $x = a^i b$ and $y = a^j$ or $y = a^j b$.

   (b) Show that the commutators of D_n form a normal subgroup N of D_n, and that D_n/N is abelian.

8. Prove that $\mathrm{SL}_2(\mathbf{Z}_2) \cong S_3$.

9. Find $|\,\mathrm{PSL}_3(\mathbf{Z}_2)|$ and $|\,\mathrm{PSL}_3(\mathbf{Z}_3)|$.

10. For a commutative ring R with identity, define $\mathrm{GL}_2(R)$ to be the set of invertible 2×2 matrices with entries in R. Prove that $\mathrm{GL}_2(R)$ is a group.

11. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{Z}_4)$ defined by the set $\left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \right\}$ such that $b \in \mathbf{Z}_4$ and $m = \pm 1$. Show that G is isomorphic to a known group of order 8.

    Hint: The answer is either D_4 or the quaternion group (see Example 3.3.7).

12. Let G be the subgroup of $\mathrm{GL}_3(\mathbf{Z}_2)$ defined by the set $\left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$ such that $a, b, c \in \mathbf{Z}_2$.

    Show that G is isomorphic to a known group of order 8.

7.1 Isomorphism theorems

Summary: This section investigates some useful applications of the fundamental homomorphism theorem.

The first step is to review the definition of a factor group, given in Section 3.8. Let H be a subgroup of the group G, and let $a \in G$. The set $aH = \{ah \mid h \in H\}$ is called the *left coset* of H in G determined by a. The *right coset* of H in G determined by a is defined similarly as Ha. The number of left cosets of H in G is called the *index* of H in G, and is denoted by $[G : H]$.

The subgroup N of G is called *normal* if $gxg^{-1} \in N$, for all $g \in G$ and all $x \in N$. The subgroup N is normal iff its left and right cosets coincide, and in this case the set of cosets of N forms a group under the coset multiplication given by $aNbN = abN$, for all $a, b \in G$. The group of left cosets of N in G is called the *factor group* of G determined by N, and is denoted by G/N. The *natural projection* mapping $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a group homomorphism, with $\ker(\pi) = N$.

Here are some elementary facts about normal subgroups (you should prove any that raise questions in your mind).

(i) Any intersection of normal subgroups is again normal.
(ii) If N is normal in G and H is a subgroup of G, then $N \cap H$ is normal in H.
(iii) If N is normal in H and H is normal in G, we can't, in general, say that N is normal in G.
(iv) The *center* $Z(G) = \{x \in G \mid gx = xg \ \forall g \in G\}$ of G is a normal subgroup.

Let G be a group with normal subgroup N. The next list of statements contains some good problems on which to test your understanding of factor groups.

(i) If $a \in G$ has finite order, then the order of the coset aN in G/N is a divisor of the order of a.
(ii) The factor group G/N is abelian iff $aba^{-1}b^{-1} \in N$, for all $a, b \in G$.
(iii) If N is a subgroup of $Z(G)$, and G/N is cyclic, then G must be abelian.

At this stage, the right way to think of normal subgroups is to view them as kernels of group homomorphisms. If $N = \ker(\phi)$, for the group homomorphism $\phi : G_1 \to G_2$, then for any $y \in G_2$ the solutions in G_1 of the equation $\phi(x) = y$ form the coset x_1N, where x_1 is any particular solution, with $\phi(x_1) = y$. The elements of each left coset aN can be put in a one-to-one correspondence with N. This shows how neatly the algebraic properties of ϕ set up a one-to-one correspondence between elements of the image $\phi(G_1)$ and cosets of $\ker(\phi)$. (The one-to-one correspondence $\overline{\phi}$ is defined by setting $\overline{\phi}(aN) = \phi(a)$.) The fundamental homomorphism theorem shows that $\overline{\phi}$ preserves the group multiplications that are defined respectively on the elements of the image of ϕ and on the cosets of $\ker(\phi)$. The formal statement is given next.

Theorem 3.8.9 (Fundamental homomorphism theorem) If $\phi : G_1 \to G_2$ is a group homomorphism with $K = \ker(\phi)$, then the factor group G_1/K is isomorphic to the image $\phi(G_1)$ of ϕ.

The accompanying diagram, in Figure 7.1.0, shows how ϕ can be written as $\phi = i\,\overline{\phi}\,\pi$, where π is an onto homomorphism, $\overline{\phi}$ is an isomorphism, and i is a one-to-one homomorphism. This diagram is often given without the inclusion mapping i, so the figure shows both versions.

Figure 7.1.0

$$\begin{tikzcd}
G_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & G_2 \\
G_1/K \arrow[r, "\overline{\phi}"] & \phi(G_1) \arrow[u, "i"']
\end{tikzcd}
\qquad
\begin{tikzcd}
G_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & G_2 \\
G_1/K \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

Proposition 3.8.7 (b) states that if N is a normal subgroup of G, then there is a one-to-one correspondence between subgroups of G/N and subgroups H of G with $H \supseteq N$. Under this correspondence, normal subgroups correspond to normal subgroups.

It is very important to understand this proposition. The function that determines the correspondence between subgroups that contain N and subgroups of G/N is the one that maps a subgroup $H \supseteq N$ to its image $\pi(H)$, where $\pi : G \to G/N$ is the natural projection. In more concrete terms, the function just maps an element $a \in H$ to the corresponding coset aN. The inverse function assigns to a subgroup of cosets the union of all of the elements that belong to the cosets. It is particularly important to understand this relationship in the case $G = \mathbf{Z}$ and $N = n\mathbf{Z}$.

The second isomorphism theorem shows that any factor group of G/N can actually be realized as a factor group of G. Any normal subgroup of G/N has the form H/N, where H is a normal subgroup of G that contains N. Factoring out H/N can then be shown to be equivalent to G/H.

Theorem 7.1.2 (Second isomorphism theorem) Let G be a group with normal subgroups N and H such that $N \subseteq H$. Then H/N is a normal subgroup of G/N, and $(G/N)\,/\,(H/N) \cong G/H$.

The proof of the second isomorphism theorem makes use of the fundamental homomorphism theorem. We need to define a homomorphism ϕ from G/N onto G/H, in such a way that $\ker(\phi) = H/N$. We can use the natural mapping defined by $\phi(aN) = aH$ for all $a \in G$, and this gives the isomorphism $\overline{\phi}$ (see Figure 7.1.1.).

Figure 7.1.1

$$\begin{tikzcd}
G/N \arrow[r, "\phi"] \arrow[d, "\pi"'] & G/H \\
(G/N)\,/\,(H/N) \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

The first isomorphism theorem also deals with the relationship between subgroups of G and subgroups of G/N, where N is a normal subgroup of G. If H is any subgroup of G, then the image of H under the natural projection $\pi : G \to G/N$ is $\pi(H) = HN/N$. To see this, note that the set $\pi(H)$ consists of all cosets of N of the form aN, for some $a \in H$. The corresponding subgroup of G is HN (under the correspondence given in Theorem 3.8.7 (b)), and then the one-to-one correspondence shows that $\pi(H) = HN/N$.

Theorem 7.1.1 (First isomorphism theorem) Let G be a group, let N be a normal subgroup of G, and let H be any subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and $(HN)\,/\,N \cong H\,/\,(H \cap N)$.

Figure 7.1.2

$$\begin{tikzcd}
 & G \arrow[d, dash] & \\
 & HN \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & N \arrow[dl, dash] \\
 & H \cap N \arrow[d, dash] & \\
 & \langle 1 \rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}
H \arrow[r, "i"] \arrow[d] & G \arrow[r, "\pi"] & G/N \\
H/(H \cap N) \arrow[rr, "\overline{\pi\, i}"] & & HN/N \arrow[u]
\end{tikzcd}$$

The proof of the first isomorphism theorem also uses the fundamental homomorphism theorem. Let $i : H \to G$ be the inclusion, and let $\pi : G \to G/N$ be the natural projection (see Figure 7.1.2.). The composition of these mappings is a homomorphism whose image is HN/N, and whose kernel is $H \cap N$. Therefore $H/(H \cap N) \cong (HN)/N$.

Let G be a group. An isomorphism from G onto G is called an *automorphism* of G. An automorphism of G of the form i_a, for some $a \in G$, where $i_a(x) = axa^{-1}$ for all $x \in G$, is called an *inner automorphism* of G. The set of all automorphisms of G will be denoted by $\mathrm{Aut}(G)$ and the set of all inner automorphisms of G will be denoted by $\mathrm{Inn}(G)$.

Proposition 7.1.4 justifies part of the definition, showing that if G is a group, then for any $a \in G$ the function $i_a : G \to G$ defined by $i_a(x) = axa^{-1}$ for all $x \in G$ is an automorphism. Propositions 7.1.6 and 7.1.8 show that $\mathrm{Aut}(G)$ is a group under composition of functions, and $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, with $\mathrm{Inn}(G) \cong G/Z(G)$. The automorphisms of a group play an important role in studying its structure.

In the case of a cyclic group, it is possible to give a good description of the automorphism group. The automorphism group $\mathrm{Aut}(\mathbf{Z}_n)$ of the cyclic group on n elements is isomorphic to the multiplicative group $\mathbf{Z}_n^\times$. To show this, first note that every element $\alpha \in \mathrm{Aut}(\mathbf{Z}_n)$ must have the form $\alpha([m]) = [\alpha(1) \cdot m]$, for all $[m] \in \mathbf{Z}_n$. Then $\alpha(1)$ must be relatively prime to n, and it can be verified that $\mathrm{Aut}(\mathbf{Z}_n) \cong \mathbf{Z}_n^\times$.

REVIEW PROBLEMS: SECTION 7.1

16. Let G_1 and G_2 be groups of order 24 and 30, respectively. Let G_3 be a nonabelian group that is a homomorphic image of both G_1 and G_2. Describe G_3, up to isomorphism.

17. Prove that a finite group whose only automorphism is the identity map must have order at most two.

18. Let H be a nontrivial subgroup of S_n. Show that either $H \subseteq A_n$, or exactly half of the permutations in H are odd.

19. Let p be a prime number, and let A be a finite abelian group in which every element has order p. Show that $\mathrm{Aut}(A)$ is isomorphic to a group of matrices over $\mathbf{Z}_p$.

20. Let G be a group and let N be a normal subgroup of G of finite index. Suppose that H is a finite subgroup of G and that the order of H is relatively prime to the index of N in G. Prove that H is contained in N.

21. Let G be a finite group and let K be a normal subgroup of G such that $\gcd(|K|, [G : K]) = 1$. Prove that K is a characteristic subgroup of G.

    Note: Recall the definition given in Exercise 7.6.8 of the text. The subgroup K is a *characteristic subgroup* of G if $\phi(K) \subseteq K$ for all $\phi \in \mathrm{Aut}(G)$. In this case we say that K is *invariant* under all automorphisms of G.

22. Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and $|G|$ is odd. Prove that N is contained in the center of G.

7.2 Conjugacy

Summary: Counting the elements of a finite group via its conjugacy classes leads to the class equation and provides a surprising amount of information about the group.

Let G be a group, and let N be a subgroup of G. By definition, N is normal in G if $axa^{-1} \in N$, for all $x \in N$ and all $a \in G$. In Definition 7.2.1, an element $y \in G$ is said to be conjugate *conjugate* to the element $x \in G$ if there exists $a \in G$ with $y = axa^{-1}$. This defines an equivalence relation on G (Proposition 7.2.2), whose equivalence classes are called the *conjugacy classes* of G. It follows immediately from the definition of a normal subgroup that a subgroup N is normal in G iff it is a union of conjugacy classes, since if $x \in N$ then all conjugates of x must also belong to N.

At this point we switch to a somewhat more sophisticated point of view. Since looking at elements of the form axa^{-1} is so important, a deeper analysis shows that we should work with the inner automorphisms of G. By Proposition 7.1.8, for any group G, we have $\mathrm{Inn}(G) \cong G/Z(G)$. To understand this isomorphism, simply assign to each element $a \in G$ the inner automorphism i_a. Then $i_a \circ i_b = i_{ab}$, and the kernel of the mapping is the center $Z(G)$, since i_a is the identity function iff $axa^{-1} = x$ for all $x \in G$, or equivalently, iff $ax = xa$ for all $x \in G$. We also need the definition of the *centralizer* of x in G, denoted by $C(x) = \{g \in G \mid gxg^{-1} = x\}$. Proposition 7.2.4 shows that $C(x)$ is a subgroup of G.

Proposition 7.2.5 gives us an important connection. If x is an element of the group G, and $a \in C(x)$, then conjugating x by a does not produce a different element. In general, the conjugate axa^{-1} produced by a depends of the left coset of $C(x)$ to which a belongs. In fact, the elements of the conjugacy class of x are in one-to-one correspondence with the left cosets of the centralizer $C(x)$ of x in G. Since any conjugate of x is the image of x under an isomorphism, we can expect the conjugates of x to have properties similar to of x.

The concept of conjugacy is nicely illustrated in S_n. Example 7.2.3 shows that two permutations in the symmetric group S_n, are conjugate iff they have the same cycle structure. That is, iff they have the same number of disjoint cycles, of the same lengths. The crucial argument is that if σ is a cycle in S_n, then $\tau\sigma\tau^{-1}(\tau(i)) = \tau(\sigma(i))$ for all i, and thus $\tau\sigma\tau^{-1}$ is the cycle constructed by applying τ to the entries of σ. The result is a cycle of the same length.

The next theorem provides the main tool in this section.

Theorem 7.2.6 (Class Equation) If G is a finite group, then the conjugacy class equation is stated as follows:

$$|G| = |Z(G)| + \sum [G : C(x)]$$

where the sum ranges over one element x from each nontrivial conjugacy class.

Recall that a group of order p^n, with p a prime number and $n \geq 1$, is called a *p-group.* The class equation has important applications to these groups. Burnside's theorem (Theorem 7.2.8) states that the center of any p-group is nontrivial (p is prime). It can then be shown that any group of order p^2 is abelian (p is prime). As another consequence of the conjugacy class equation, Cauchy's theorem (Theorem 7.2.10) states that if G is a finite group and p is a prime divisor of the order of G, then G contains an element of order p.

REVIEW PROBLEMS: SECTION 7.2

19. Prove that if the center of the group G has index n, then every conjugacy class of G has at most n elements.

20. Let G be a group with center $Z(G)$. Prove that $G/Z(G)$ is abelian iff for each element $x \notin Z(G)$ the conjugacy class of x is contained in the coset $Z(G)x$.

21. Find all finite groups that have exactly two conjugacy classes.

22. Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. Let $H = \{1, a^3, b, a^3b\}$. Find the normalizer of H in G and find the subgroups of G that are conjugate to H.

23. Write out the class equation for the dihedral group D_n. Note that you will need two cases: one when n is even, and one when n is odd.

24. Show that for all $n \geq 4$, the centralizer of the element $(1, 2)(3, 4)$ in S_n has order $8 \cdot (n - 4)!$. Determine the elements in $C_{S_n}((1, 2)(3, 4))$ explicitly.

7.3 Group actions

Summary: This section introduces the notion of a group action, and shows that a generalized class equation holds. Clever choices of group actions allow this class equation to be mined for information.

One possible approach in studying the structure of a given group is to find ways to "represent" it via a "concrete" group of permutations. To be more precise, given the group G we would like to find an associated set S and a group homomorphism $\phi : G \to \mathrm{Sym}(S)$, where $\mathrm{Sym}(S)$ is the group of all permutations on the set S. If we can find a homomorphism like this, note that for any $g \in G$ the value $\phi(g)$ is a permutation of S, so it acts as a function on S. We will use the shorthand notation $[\phi(g)](x) = g \cdot x$, for $g \in G$ and $x \in S$. This shorthand notation can really simplify things if $\phi(g)$ has a complicated definition.

For example, for any group G we have the homomorphism $\phi : G \to \mathrm{Aut}(G)$ defined by $\phi(a) = i_a$, where i_a is the inner automorphism defined by a, given by $i_a(x) = axa^{-1}$, for all $x \in G$. The shorthand notation in this case is to define $a \cdot x = axa^{-1}$. Then we use $Gx = \{a \cdot x \mid a \in G\}$ to denote the conjugacy class of x, since Gx consists of all elements of the form axa^{-1}, for $a \in G$. Note that since $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$, we actually have $\phi : G \to \mathrm{Sym}(G)$.

This idea leads to the notion of a group "acting" on a set (Definition 7.3.1). Let G be a group and let S be a set. A multiplication of elements of S by elements of G (defined by a function from $G \times S \to S$) is called a *group action* of G on S provided for each $x \in S$: (i) $a(bx) = (ab)x$ for all $a, b \in G$, and (ii) $1 \cdot x = x$ for the identity element 1 of G.

It is interesting to see when $ax = bx$, for some $a, b \in G$ and $x \in S$. If $b = ah$ for some $h \in G$ such that $hx = x$, then $bx = (ah)x = a(hx) = ax$. Actually, this is the only way in which $ax = bx$, since if this equation holds, then $x = (a^{-1}b)x$, and $b = ah$ for $h = a^{-1}b$. This can be expressed in much more impressive language, using the concepts of "orbit" and "stabilizer".

We need to look at a couple of examples. First, if G is a subgroup of a group S, then G acts in a natural way on S by just using the group multiplication in S. Secondly, if G is the multiplicative group of nonzero elements of a field, and V is any vector space over the field, then the scalar multiplication on V defines an action of G on V.

There is a close connection between group actions and certain group homomorphisms, as shown by Proposition 7.3.2. Let G be a group and let S be a set. Any group homomorphism from G into the group $\mathrm{Sym}(S)$ of all permutations of S defines an action of G on S. Conversely, every action of G on S arises in this way.

Definition 7.3.3 and Propositions 7.3.4 and 7.3.5 establish some of the basic notation and results. Let G be a group acting on the set S. For each element $x \in S$, the set $Gx = \{ax \mid a \in G\}$ is called the *orbit* of x under G, and the set $G_x = \{a \in G \mid ax = x\}$ is called the *stabilizer* of x in G. The orbits of the various elements of S form a partition of S. The stabilizer is a subgroup, and there is a one-to-one correspondence between the elements of the orbit Gx of x under the action of G and the left cosets of the stabilizer G_x of x in G. If G is finite, this means that the number of elements in an orbit Gx is equal to the index $[G : G_x]$ of the stabilizer.

The conjugacy class equation has a direct analog for group actions. First we need to define the set $S^G = \{x \in S \mid ax = x \text{ for all } a \in G\}$ which is called the *subset of S fixed by G*.

Theorem 7.3.6 (Generalized Class Equation) Let G be a finite group acting on the finite set S. Then

$$|S| = |S^G| + \textstyle\sum_\Gamma [G : G_x] \; ,$$

where Γ is a set of representatives of the orbits Gx for which $|Gx| > 1$.

Lemma 7.3.7 gives an interesting result when G is a p-group acting on a finite set S. In this case, $|S^G| \equiv |S| \pmod p$. With a clever choice of the group and the set, this simple result can be used to give another proof of Cauchy's theorem. (Check out the proof of Theorem 7.3.8.) Finally, we have a result that is very useful in showing that a group G is not a simple group. (This proposition is not given in the text.)

Proposition Let G be a group of order n, and assume that G acts nontrivially on a set S with k elements. If n is not a divisor of $k!$, then G has a proper nontrivial normal subgroup.

Proof: The given action of G on S defines a homomorphism $\phi : G \to \mathrm{Sym}(S)$. Since the action is nontrivial, $\ker(\phi)$ is a proper normal subgroup of G. We cannot have $\ker(\phi) = \langle 1 \rangle$, because this would mean that G is isomorphic to a subgroup of $\mathrm{Sym}(S)$, and hence n would be a divisor of $|\mathrm{Sym}(S)| = k!$. $\square$

Here is one strategy to use in proving that a group G is not simple. If you can find a large enough subgroup H of G, let G act on the set of left cosets of H via $g \cdot aH = (ga)H$. If H has index $[G : H] = k$, and $|G|$ is not a divisor of $k!$, then G cannot be simple. On the other hand, if you can find a subgroup H with a small number of conjugate subgroups, then you can let G act on the set of conjugates of H by setting $g \cdot aHa^{-1} = (ga)H(ga)^{-1}$. If H has k conjugates, and $|G|$ is not a divisor of $k!$, then G cannot be simple. (Actually the second situation can be handled like the first, since the number of conjugates of H is the same as the index in G of the normalizer of H.)

REVIEW PROBLEMS: SECTION 7.3

15. Let G be a group which has a subgroup of index 6. Prove that G has a normal subgroup whose index is a divisor of 720.

16. Let G act on the subgroup H by conjugation, let S be the set of all conjugates of H, and let $\phi : G \to \mathrm{Sym}(S)$ be the corresponding homomorphism. Show that $\ker(\phi)$ is the intersection of the normalizers $N(aHa^{-1})$ of all conjugates of H.

17. Let $F = \mathbf{Z}_3$, $G = \mathrm{GL}_2(F)$, and $S = F^2$. Find the generalized class equation (see Theorem 7.3.6) for the standard action of G on S.

18. Let $F = \mathbf{Z}_3$, $G = \mathrm{GL}_2(F)$, and let N be the center of G. Prove that $G/N \cong S_4$ by defining an action of G on the four one-dimensional subspaces of F^2.

7.4 The Sylow theorems

Summary: Our goal is to give a partial converse to Lagrange's theorem.

Lagrange's theorem states that if G is a group of order n, then the order of any subgroup of G is a divisor of n. The converse of Lagrange's theorem is not true, as shown by the alternating group A_4, which has order 12, but has no subgroup of order 6. The Sylow theorems give the best attempt at a converse, showing that if p^α is a prime power that divides $|G|$, then G has a subgroup of order p^α. The proofs in the text use group actions (they are simpler than the original proofs). Before studying the proofs, make sure you are comfortable with group actions. Otherwise the machinery may confuse you rather than enlighten you.

Let G be a finite group, and let p be a prime number. A subgroup P of G is called a *Sylow p-subgroup* of G if $|P| = p^\alpha$ for some integer $\alpha \geq 1$ such that p^α is a divisor of $|G|$ but $p^{\alpha+1}$ is not. The statements of the second and third Sylow theorems use this definition, and their proofs require Lemma 7.4.3, which states that if $|G| = mp^\alpha$, where $\alpha \geq 1$ and $p \not| \, m$, and P is a normal Sylow p-subgroup, then P contains every p-subgroup of G.

Theorems 7.4.1, 7.4.4 (The Sylow Theorems) Let G be a finite group, and let p be a prime number.

(a) If p is a prime such that p^α is a divisor of $|G|$ for some $\alpha \geq 0$, then G contains a subgroup of order p^α.

(b) All Sylow p-subgroups of G are conjugate, and any p-subgroup of G is contained in a Sylow p-subgroup.

(c) Let $n = mp^\alpha$, with $\gcd(m, p) = 1$, and let k be the number of Sylow p-subgroups of G. Then $k \equiv 1 \pmod{p}$ and k is a divisor of m.

Outline of the proof: Let P be a Sylow p-subgroup of G with $|P| = p^\alpha$, let S be the set of all conjugates of P, and let P act on S by conjugation. First show that the only member of S left fixed by the action of P is P itself, so $|S^P| = 1$, and therefore $|S| \equiv 1 \pmod{p}$.

Next let Q be any maximal p-subgroup, and now let Q act on S by conjugation. Then $|S^Q| \equiv 1 \pmod{p}$, so some conjugate K of P must be left fixed by Q, and it can be shown that $Q \subseteq K$, and therefore $Q = K$. This implies not only that all Sylow p-subgroups are conjugate, but that any maximal p-subgroup is a Sylow p-subgroup. Now S is the set of all Sylow p-subgroups of G, so $k \equiv 1 \pmod{p}$. Finally, $k = [G : N(P)]$, so $k|m$ since $[G : N(P)] \mid [G : P]$. □

In the review problems the notation $n_p(G)$ will be used to denote the number of Sylow p-subgroups of the finite group G.

REVIEW PROBLEMS: SECTION 7.4

15. By direct computation, find the number of Sylow 3-subgroups and the number of Sylow 5-subgroups of the symmetric group S_5. Check that your calculations are consistent with the Sylow theorems.

16. How many elements of order 7 are there in a simple group of order 168?

17. Let G be a group of order 340. Prove that G has a normal cyclic subgroup of order 85 and an abelian subgroup of order 4.

18. Show that any group of order 100 has a normal subgroup of order 25.

19. Show that there is no simple group of order 200.

20. Show that a group of order 108 has a normal subgroup of order 9 or 27.

21. Let p be a prime number. Find all Sylow p-subgroups of the symmetric group S_p.

22. Let G be the group of matrices $\left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \right\}$ such that $x \in \mathbf{Z}_7$ and $a \in \mathbf{Z}_7^\times$.

    (a) Find $n_7(G)$, and find a Sylow 7-subgroup of G.

    (b) Find $n_3(G)$, and find a Sylow 3-subgroup of G.

23. Prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G.

24. Prove that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

7.5 Finite abelian groups

Summary: The goal of this section is to prove that any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.

Any finite abelian group is a direct product of cyclic groups. To obtain some uniqueness for this decomposition, we can either split the group up as far as possible, into cyclic groups of prime power order, or we can combine some factors so that the cyclic groups go from largest to smallest, and the order of each factor is a divisor of the previous one.

In splitting a finite abelian group up into cyclic groups of prime power order, the first step is to split it into its Sylow subgroups. This decomposition is unique, because each Sylow p-subgroup consists precisely of the elements whose order is a power of p.

In studying abelian groups it is quite common to use additive notation rather than multiplicative notation. In this context, if $(G, +)$ is an abelian group with subgroups H_1, …, H_n, and each element $g \in G$ can be written uniquely in the form $g = h_1 + \ldots + h_n$, with $h_i \in H_i$, we say that G is the *direct sum* of the subgroups H_1, …, H_n, and write $G = H_1 \oplus \cdots \oplus H_n$. With this terminology, Theorem 7.5.3 states that any finite abelian group is the direct sum of its Sylow p-subgroups.

Lemma 7.5.5 is important in understanding the general decomposition. Its proof is rather technical, so if you need to learn it, go back to the text. The statement is the following. Let G be a finite abelian p-group. If $\langle a \rangle$ is a maximal cyclic subgroup of G, then there exists a subgroup H with $G \cong \langle a \rangle \oplus H$.

We finally come to the fundamental theorem of finite abelian groups.

Theorem 7.5.6 Any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. Any two such decompositions have the same number of factors of each order.

Proposition 7.5.7 gives a different way to write the decomposition. If G is a finite abelian group, then G is isomorphic to a direct product of cyclic groups

$$\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$$

such that $n_i \mid n_{i-1}$ for $i = 2, 3, \ldots, k$. The proof of Proposition 7.5.7 is best understood by looking at an example. Suppose that $|G| = 3456 = 2^7 3^3$. Also suppose that we have enough additional information to write G in the following form.

$$G = \mathbf{Z}_8 \times \mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_9 \times \mathbf{Z}_3$$

As long as two subscripts are relatively prime, we can recombine them. Taking the largest pairs first, we can rewrite G in the following form.

$$G \cong (\mathbf{Z}_8 \times \mathbf{Z}_9) \times (\mathbf{Z}_4 \times \mathbf{Z}_3) \times \mathbf{Z}_4 \cong \mathbf{Z}_{72} \times \mathbf{Z}_{12} \times \mathbf{Z}_4$$

The factors are still cyclic, and now each subscript is a divisor of the previous one.

REVIEW PROBLEMS: SECTION 7.5

13. Find all abelian groups of order 108 (up to isomorphism).

14. Let G and H be finite abelian groups, and assume that $G \times G$ is isomorphic to $H \times H$. Prove that G is isomorphic to H.

15. Let G be an abelian group which has 8 elements of order 3, 18 elements of order 9, and no other elements besides the identity. Find (with proof) the decomposition of G as a direct product of cyclic groups.

16. Let G be a finite abelian group with $|G| = 216$. If $|6G| = 6$, determine G up to isomorphism.
17. Apply both structure theorems to give the two decompositions of the abelian group $\mathbf{Z}_{216}^{\times}$.
18. Let G and H be finite abelian groups, and assume that they have the following property. For each positive integer m, G and H have the same number of elements of order m. Prove that G and H are isomorphic.

7.6 Solvable groups

Summary: This section introduces the concept of a composition series for a finite group. The terms in the composition series are simple groups, and the list of composition factors is completely determined by G. A group is solvable iff the composition factors are abelian.

A polynomial equation is solvable by radicals iff its Galois group is solvable (see Section 8.4). This provided the original motivation for studying the class of solvable groups.

In Definition 7.6.9, a chain of subgroups $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n$ such that
(i) N_i is a normal subgroup in N_{i-1} for $i = 1, 2, \ldots, n$,
(ii) N_{i-1}/N_i is simple for $i = 1, 2, \ldots, n$, and
(iii) $N_n = \langle 1 \rangle$
is called a *composition series* for G. The factor groups N_{i-1}/N_i are called the *composition factors* determined by the series, and n is called the *length* of the series.

For this idea of a composition series to be useful, there needs to be some uniqueness to the composition factors. The composition series itself does not determine the group–you also need to know how to put the factors together. For example, the same composition factors occur in S_3 and $\mathbf{Z}_6$, as shown by these composition series.

$$\mathbf{Z}_6 \supset 2\mathbf{Z}_6 \supset \{0\} \qquad S_3 \supset A_3 \supset \langle 1 \rangle$$

The composition factors are $\mathbf{Z}_2$ and $\mathbf{Z}_3$ in each case.

Theorem 7.6.10 (Jordan–Hölder) Any two composition series for a finite group have the same length. Furthermore, there is a one-to-one correspondence between composition factors of the two composition series under which corresponding composition factors are isomorphic.

In Definition 7.6.1, the group G is said to be *solvable* if there exists a finite chain of subgroups $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n$ such that
(i) N_i is a normal subgroup in N_{i-1} for $i = 1, 2, \ldots, n$,
(ii) N_{i-1}/N_i is abelian for $i = 1, 2, \ldots, n$, and
(iii) $N_n = \langle 1 \rangle$.
By Proposition 7.6.2, a finite group is solvable iff it has a composition series in which each composition factor is abelian. Theorem 7.6.3 produces a large class of examples: any finite p-group is solvable (p is prime).

An element g of the group G is called a *commutator* if $g = aba^{-1}b^{-1}$ for elements $a, b \in G$. The smallest subgroup that contains all commutators of G is called the *commutator subgroup* or *derived subgroup* of G, and is denoted by G'. Proposition 7.6.5 shows that G' is normal in G, and that G/G' is abelian. Furthermore, G' is the smallest normal subgroup for which the factor group is abelian. The higher derived subgroups $G^{(k)}$ are defined inductively, and give another way to characterize solvable groups.

Theorem 7.6.7 states that a group G is solvable iff $G^{(n)} = \langle 1 \rangle$ for some positive integer n. As a corollary of the theorem, it is possible to show that if G is solvable, then so is any subgroup or homomorphic image of G. Furthermore, if N is a normal subgroup of G such that both N and G/N are solvable, then G is solvable.

REVIEW PROBLEMS: SECTION 7.6

11. Let p be a prime and let G be a nonabelian group of order p^3. Show that the center $Z(G)$ of G is equal to the commutator subgroup G' of G.

12. Prove that the dihedral group D_n is solvable for all n.

13. Prove that any group of order 588 is solvable, given that any group of order 12 is solvable.

14. Let G be a group of order $780 = 2^2 \cdot 3 \cdot 5 \cdot 13$. Assume that G is not solvable. What are the composition factors of G? (Assume that the only nonabelian simple group of order ≤ 60 is the alternating group A_5.)

7.7 Simple groups

Summary: This section deals with two classes of groups: the alternating groups A_n, and the projective special linear groups $\mathrm{PSL}_2(F)$, which provide examples of simple groups. These can be used to classify all simple groups of order ≤ 200.

Theorem 7.7.2 The symmetric group S_n is not solvable for $n \geq 5$.

Theorem 7.7.4 The alternating group A_n is simple if $n \geq 5$.

Let F be a field. The set of all $n \times n$ matrices with entries in F and determinant 1 is called the *special linear group* over F, and is denoted by $SL_n(F)$. For any field F, the center of $SL_n(F)$ is the set of nonzero scalar matrices with determinant 1. The group $SL_n(F)$ modulo its center is called the *projective special linear group* and is denoted by $PSL_n(F)$.

Theorem 7.7.9 If F is a finite field with $|F| > 3$, then the projective special linear group $PSL_2(F)$ is simple.

It may be useful to review some of the tools you can use to show that a finite group G is *not* simple.

(1) It may be possible to use the Sylow theorems to show that some Sylow p-subgroup of G is normal. Recall that if $|G| = p^k m$, where $p \not| m$, then the number of Sylow p-subgroups is congruent to 1 modulo p and is a divisor of m. This approach works in Problem 15 below.

(2) If you can define a nontrivial homomorphism $\phi : G \to G'$ such that $|G|$ is not a divisor of $|G'|$, then ϕ cannot be one-to-one, and so $\ker(\phi)$ is a proper nontrivial subgroup of G, which shows that G is not simple. One way to do this is to define a group action of G on a set S, and then use the corresponding homomorphism from G into $\mathrm{Sym}(S)$. This approach depends on finding an action on a set S with n elements, for which $|G|$ is not a divisor of $n!$. (See the proposition in Section 7.2.)

To use this method, you need to find an action of G on a comparatively small set. One way to define a group action is to let G act by conjugation on the set of conjugates of a particular Sylow p-subgroup. The number of conjugates of a Sylow p-subgroup H is equal to the index of the normalizer $N(H)$ in G, so if you prefer, you can let G act by multiplication on the left cosets of $N(H)$. In either case you need a Sylow p-subgroup with a number of conjugates that is small compared to $|G|$. This approach works in Problem 18 below.

(3) In some cases you can count the number of elements in the various Sylow p-subgroups and show that for at least one of the primes factors of $|G|$ there can be only 1 Sylow p-subgroup. The solution to Problem 19 below combines this approach with the previous one.

You must be very careful in counting the elements that belong to a Sylow p-subgroup and its conjugates. If $|G|$ has m subgroups of order p, then these subgroups can only intersect in the identity element, so you can count $m \cdot (p-1)$ elements. But if G has Sylow p-subgroups of order p^2, for example, these may have nontrivial intersection.

For example, the dihedral group D_6 has 3 Sylow 2-subgroups (each of order 4). Using our standard notation, these are $\{1, a^3, b, a^3b\}$, $\{1, a^3, ab, a^4b\}$, and $\{1, a^3, a^2b, a^5b\}$. The intersection of these Sylow 2-subgroups is the center $\{1, a^3\}$, and so having 3 Sylow 2-subgroups of order 4 only accounts for a total of 7 elements. Note that the Sylow 3-subgroup is $\{1, a^2, a^4\}$, and the elements a and a^5, which have order 6, do not belong to any Sylow subgroup.

As a further example, we can now show that the smallest nonabelian simple group has order 60. The special cases of Burnside's theorem given in Exercise 7.6.7 of the text take care of all cases except $24 = 2^3 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$, $36 = 2^2 \cdot 3^2$, $40 = 2^4 \cdot 5$, $42 = 2 \cdot 3 \cdot 7$, $48 = 2^4 \cdot 3$, and $56 = 2^3 \cdot 7$. The cases 30, 36, 48, and 56 are covered by Example 7.4.2, and Exercises 7.4.13, 7.4.12, and 7.4.10 in the text, respectively. If $|G| = 24$, then $n_2(G)$ is 1 or 3, and if 3 we get an embedding into S_3, a contradiction. If $|G| = 40$, then $n_5(G) = 1$. If $|G| = 42$, the Sylow 7-subgroup must be normal.

Exercise 7.7.1 in the text shows that there are no simple groups of order $2m$, where m is odd. Problem 16 below shows that if G is a simple group that contains a subgroup of index n, where $n > 2$, then G can be embedded in the alternating group A_n. These results, together with the techniques mentioned above, can be used to show that a simple group of order < 200 can only have one of these possible orders: 60, 120, 144, 168, or 180. We know that there are simple groups of order 60 and 168. The arguments needed to eliminate 120, 144, and 180 are somewhat more complicated, but aren't really beyond the level of the text. If you want to tackle some more challenging problems, try these last three cases.

REVIEW PROBLEMS: SECTION 7.7

1. Let G be a group of order $2m$, where m is odd. Show that G is not simple.

15. Prove that there are no simple groups of order 200.

16. Sharpen Exercise 7.7.3 (b) of the text by showing that if G is a simple group that contains a subgroup of index n, where $n > 2$, then G can be embedded in the alternating group A_n.

17. Prove that if G contains a nontrivial subgroup of index 3, then G is not simple.

18. Prove that there are no simple groups of order 96.

19. Prove that there are no simple groups of order 132.

20. Prove that there are no simple groups of order 160.

21. Prove that there are no simple groups of order 280.

22. Prove that there are no simple groups of order 1452.

Chapter 8

GALOIS THEORY

The theory of solvability of polynomial equations developed by Galois began with the attempt to find formulas for the solutions of polynomial equations of degree five. After the discovery of the fundamental theorem of algebra, the question of proving the existence of solutions changed to determining the form of the solutions. The question was whether or not the solutions could be expressed in a reasonable way by extracting square roots, cube roots, etc., of combinations of the coefficients of the polynomial. Galois saw that this involved a comparison of two fields, by determining how the field generated by the coefficients sits inside the larger field generated by the solutions of the equation.

8.0 Splitting fields

Summary: The first step in finding the Galois group of an polynomial over a field is to find the smallest extension of the field that contains all of the roots of the polynomial.

Beginning with a field K, and a polynomial $f(x) \in K$, we need to construct the smallest possible extension field F of K that contains all of the roots of $f(x)$. This will be called a *splitting field* for $f(x)$ over K. The word "the" is justified by proving that any two splitting fields are isomorphic. The first step in this section is to review a number of definitions and results from Chapter 6.

Let F be an extension field of K and let $u \in F$. If there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(u) = 0$, then u is said to be *algebraic* over K. If not, then u is said to be *transcendental* over K.

Proposition 6.1.2 If F is an extension field of K, and $u \in F$ is algebraic over K, then there exists a unique monic irreducible polynomial $p(x) \in K[x]$ such that $p(u) = 0$. It is the monic polynomial of minimal degree that has u as a root, and if $f(x)$ is any polynomial in $K[x]$ with $f(u) = 0$, then $p(x) \mid f(x)$.

Alternate proof: The proof in the text uses some elementary ring theory. I've decided to include a proof that depends only on basic facts about polynomials.

Assume that $u \in F$ is algebraic over K, and let I be the set of all polynomials $f(x) \in K[x]$ such that $f(u) = 0$. The division algorithm for polynomials can be used to show that if $p(x)$ is a nonzero monic polynomial in I of minimal degree, then $p(x)$ is a generator for I, and thus $p(x) \mid f(x)$ whenever $f(u) = 0$.

Furthermore, $p(x)$ must be an irreducible polynomial, since if $p(x) = g(x)h(x)$ for $g(x), h(x) \in K[x]$, then $g(u)h(u) = p(u) = 0$, and so either $g(u) = 0$ or $h(u) = 0$ since F is a field. From the choice of $p(x)$ as a polynomial of minimal degree that has u as a root, we see that either $g(x)$ or $h(x)$ has the same degree as $p(x)$, and so $p(x)$ must be irreducible. □

In the above proof, the monic polynomial $p(x)$ of minimal degree in $K[x]$ such that $p(u) = 0$ is called the *minimal polynomial* of u over K, and its degree is called the *degree* of u over K.

Let F be an extension field of K, and let $u_1, u_2, \ldots, u_n \in F$. The smallest subfield of F that contains K and $u_1, u_2, \ldots, u_n$ will be denoted by $K(u_1, u_2, \ldots, u_n)$. It is called the *extension field of K generated by* $u_1, u_2, \ldots, u_n$. If $F = K(u)$ for a single element $u \in F$, then F is said to be a *simple extension of* K.

Let F be an extension field of K, and let $u \in F$. Since $K(u)$ is a field, it must contain all elements of the form

$$\frac{a_0 + a_1 u + a_2 u^2 + \ldots + a_m u^m}{b_0 + b_1 u + b_2 u^2 + \ldots + b_n u^n} ,$$

where $a_i, b_j \in K$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. In fact, this set describes $K(u)$, and if u is transcendental over K, this description cannot be simplified. On the other hand, if u is algebraic over K, then the denominator in the above expression is unnecessary, and the degree of the numerator can be assumed to be less than the degree of the minimal polynomial of u over K.

If F is an extension field of K, then the multiplication of F defines a scalar multiplication, considering the elements of K as scalars and the elements of F as vectors. This gives F the structure of a vector space over K, and allows us to make use of the concept of the dimension of a vector space. The next result describes the structure of the extension field obtained by adjoining an algebraic element.

Proposition 6.1.5 Let F be an extension field of K and let $u \in F$ be an element algebraic over K.

(a) $K(u) \cong K[x]/\langle p(x)\rangle$, where $p(x)$ is the minimal polynomial of u over K.

(b) If the minimal polynomial of u over K has degree n, then $K(u)$ is an n-dimensional vector space over K.

Alternate proof: The standard proof uses the ring homomorphism $\theta : K[x] \to F$ defined by evaluation at u. Then the image of θ is $K(u)$, and the kernel is the ideal of $K[x]$ generated by the minimal polynomial $p(x)$ of u over K. Since $p(x)$ is irreducible, $\ker(\theta)$ is a prime ideal, and so $K[x]/\ker(\theta)$ is a field because every nonzero prime ideal of a principal ideal domain is maximal. Thus $K(u)$ is a field since $K(u) \cong K[x]/\ker(\theta)$.

The usual proof involves some ring theory, but the actual ideas of the proof are much simpler. To give an elementary proof, define $\phi : K[x]/\langle p(x)\rangle \to K(u)$ by $\phi([f(x)]) = f(u)$, for all congruence classes $[f(x)]$ of polynomials (modulo $p(x)$). This mapping makes sense because $K(u)$ contains u, together with all of the elements of K, and so it must contain any expression of the form $a_0 + a_1 u + \ldots + a_m u^m$, where $a_i \in K$, for each subscript i. The function ϕ is well-defined, since it is also independent of the choice of a representative of $[f(x)]$. In fact, if $g(x) \in K[x]$ and $f(x)$ is equivalent to $g(x)$, then $f(x) - g(x) = q(x)p(x)$ for some $q(x) \in K[x]$, and so $f(u) - g(u) = q(u)p(u) = 0$, showing that $\phi([f(x)]) = \phi([g(x)])$.

Since the function ϕ simply substitutes u into the polynomial $f(x)$, and it is not difficult to show that it preserves addition and multiplication. It follows from the definition of $p(x)$ that ϕ is one-to-one. Suppose that $f(x)$ represents a nonzero congruence class in $K[x]/\langle p(x)\rangle$. Then $p(x) \not| f(x)$, and so $f(x)$ is relatively prime to $p(x)$ since it is irreducible. Therefore there exist polynomials $a(x)$ and $b(x)$ in $K[x]$ such that $a(x)f(x) + b(x)p(x) = 1$. It follows that $[a(x)][f(x)] = [1]$ for the corresponding equivalence classes, and this shows that $K[x]/\langle p(x)\rangle$ is a field. Thus the image E of ϕ in F must be subfield of F. On the one hand, E contains u and K, and on the other hand, we have already shown that E must contain any expression of the form $a_0 + a_1 u + \ldots + a_m u^m$, where $a_i \in K$. It follows that $E = K(u)$, and we have the desired isomorphism.

(b) It follows from the description of $K(u)$ in part (a) that if $p(x)$ has degree n, then the set $B = \{1, u, u^2, \ldots, u^{n-1}\}$ is a basis for $K(u)$ over K. □

Let F be an extension field of K. The dimension of F as a vector space over K is called the *degree* of F over K, denoted by $[F : K]$. If the dimension of F over K is finite, then F is said to be a *finite* extension of K. Let F be an extension field of K and let $u \in F$. The following conditions are equivalent: (1) u is algebraic over K; (2) $K(u)$ is a finite extension of K; (3) u belongs to a finite extension of K.

Never underestimate the power of counting: the next result is crucial. If we have a tower of extensions $K \subseteq E \subseteq F$, where E is finite over K and F is finite over E, then F is finite over K, and $[F : K] = [F : E][E : K]$. This has a useful corollary, which states that the degree of any element of F is a divisor of $[F : K]$.

Let K be a field and let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial in $K[x]$ of degree $n > 0$. An extension field F of K is called a *splitting field for $f(x)$ over K* if there exist elements $r_1, r_2, \ldots, r_n \in F$ such that

(i) $f(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n)$ and

(ii) $F = K(r_1, r_2, \ldots, r_n)$.

In this situation we usually say that $f(x)$ *splits* over the field F. The elements $r_1, r_2, \ldots, r_n$ are roots of $f(x)$, and so F is obtained by adjoining to K a complete set of roots of $f(x)$. An induction argument (on the degree of $f(x)$) can be given to show that splitting fields always exist. Theorem 6.4.2 states that if $f(x) \in K[x]$ is a polynomial of degree $n > 0$, then there exists a splitting field F for $f(x)$ over K, with $[F : K] \leq n!$.

The uniqueness of splitting fields follows from two lemmas. Let $\phi : K \to L$ be an isomorphism of fields. Let F be an extension field of K such that $F = K(u)$ for an algebraic element $u \in F$. Let $p(x)$ be the minimal polynomial of u over K. If v is any root of the image $q(x)$ of $p(x)$ under ϕ, and $E = L(v)$, then there is a unique way to extend ϕ to an isomorphism $\theta : F \to E$ such that $\theta(u) = v$ and $\theta(a) = \phi(a)$ for all $a \in K$. The required isomorphism $\theta : K(u) \to L(v)$ must have the form

$$\theta(a_0 + a_1u + \ldots + a_{n-1}u^{n-1}) = \phi(a_0) + \phi(a_1)v + \ldots + \phi(a_{n-1})v^{n-1} .$$

The second lemma is stated as follows. Let F be a splitting field for the polynomial $f(x) \in K[x]$. If $\phi : K \to L$ is a field isomorphism that maps $f(x)$ to $g(x) \in L[x]$ and E is a splitting field for $g(x)$ over L, then there exists an isomorphism $\theta : F \to E$ such that $\theta(a) = \phi(a)$ for all $a \in K$. The proof uses induction on the degree of $f(x)$, together with the previous lemma.

Theorem 6.4.5 states that the splitting field over the field K of a polynomial $f(x) \in K[x]$ is unique up to isomorphism. Among other things, this result has important consequences for finite fields.

REVIEW PROBLEMS: SECTION 8.0

1. Find the splitting field over $\mathbf{Q}$ for the polynomial $x^4 + 4$.

2. Let p be a prime number. Find the splitting fields for $x^p - 1$ over $\mathbf{Q}$ and over $\mathbf{R}$.

3. Find the splitting field for $x^3 + x + 1$ over $\mathbf{Z}_2$.

4. Find the degree of the splitting field over $\mathbf{Z}_2$ for the polynomial $(x^3 + x + 1)(x^2 + x + 1)$.

5. Let F be an extension field of K. Show that the set of all elements of F that are algebraic over K is a subfield of F.

6. Let F be a field generated over the field K by u and v of relatively prime degrees m and n, respectively, over K. Prove that $[F : K] = mn$.

7. Let $F \supseteq E \supseteq K$ be extension fields. Show that if F is algebraic over E and E is algebraic over K, then F is algebraic over K.

8. Let $F \supset K$ be an extension field, with $u \in F$. Show that if $[K(u) : K]$ is an odd number, then $K(u^2) = K(u)$.

9. Find the degree $[F : \mathbf{Q}]$, where F is the splitting field of the polynomial $x^3 - 11$ over the field $\mathbf{Q}$ of rational numbers.

10. Determine the splitting field over $\mathbf{Q}$ for $x^4 + 2$.

11. Determine the splitting field over $\mathbf{Q}$ for $x^4 + x^2 + 1$.

12. Factor $x^6 - 1$ over $\mathbf{Z}_7$; factor $x^5 - 1$ over $\mathbf{Z}_{11}$.

8.1 Galois groups

Summary: This section gives the definition of the Galois group and some results that follow immediately from the definition. We can give the full story for Galois groups of finite fields.

We use the notation $\mathrm{Aut}(F)$ for the group of all automorphisms of F, that is, all one-to-one functions from F onto F that preserve addition and multiplication. The smallest subfield containing the identity element 1 is called the *prime subfield* of F. If F has characteristic zero, then its prime subfield is isomorphic to $\mathbf{Q}$, and if F has characteristic p, for some prime number p, then its prime subfield is isomorphic to $\mathbf{Z}_p$. In either case, for any automorphism ϕ of F we must have $\phi(x) = x$ for all elements in the prime subfield of F.

To study solvability by radicals of a polynomial equation $f(x) = 0$, we let K be the field generated by the coefficients of $f(x)$, and let F be a splitting field for $f(x)$ over K. Galois considered permutations of the roots that leave the coefficient field fixed. The modern approach is to consider the automorphisms determined by these permutations. The first result is that if F is an extension field of K, then the set of all automorphisms $\phi : F \to F$ such that $\phi(a) = a$ for all $a \in K$ is a group under composition of functions. This justifies the following definitions.

Definition 8.1.2 Let F be an extension field of K. The set

$$\{\theta \in \mathrm{Aut}(F) \mid \theta(a) = a \text{ for all } a \in K\}$$

is called the *Galois group* of F over K, denoted by $\mathrm{Gal}(F/K)$.

Definition 8.1.3 Let K be a field, let $f(x) \in K[x]$, and let F be a splitting field for $f(x)$ over K. Then $\mathrm{Gal}(F/K)$ is called the *Galois group of* $f(x)$ *over* K, or the *Galois group of the equation* $f(x) = 0$ *over* K.

Proposition 8.1.4 states that if F is an extension field of K, and $f(x) \in K[x]$, then any element of $\mathrm{Gal}(F/K)$ defines a permutation of the roots of $f(x)$ that lie in F. The next theorem is extremely important.

Theorem 8.1.6 Let K be a field, let $f(x) \in K[x]$ have positive degree, and let F be a splitting field for $f(x)$ over K. If no irreducible factor of $f(x)$ has repeated roots, then $|\mathrm{Gal}(F/K)| = [F : K]$.

This result can be used to compute the Galois group of any finite extension of any finite field, but first we need to review the structure of finite fields. If F is a finite field of characteristic p, then it is a vector space over its prime subfield $\mathbf{Z}_p$, and so it has p^n elements, where $[F : \mathbf{Z}_p] = n$. The structure of F is determined by the following theorem.

Theorem 6.5.2 If F is a finite field with p^n elements, then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F.

The description of the splitting field of $x^{p^n} - x$ over $\mathbf{Z}_p$ shows that for each prime p and each positive integer n, there exists a field with p^n elements. The uniqueness of splitting fields shows that two finite fields are isomorphic iff they have the same number of elements. The field with p^n elements is called the *Galois field of order* p^n, denoted by $GF(p^n)$. Every finite field is a simple extension of its prime subfield, since the multiplicative group of nonzero elements is cyclic, and this implies that for each positive integer n there exists an irreducible polynomial of degree n in $\mathbf{Z}_p[x]$.

If F is a field of characteristic p, and $n \in \mathbf{Z}^+$, then $\{a \in F \mid a^{p^n} = a\}$ is a subfield of F, and this observation actually produces all subfields. In fact, Proposition 6.5.5 has the following statement: Let F be a field with p^n elements. Each subfield of F has p^m elements for some divisor m of n. Conversely, for each positive divisor m of n there exists a unique subfield of F with p^m elements.

If F is a field of characteristic p, consider the function $\phi : F \to F$ defined by $\phi(x) = x^p$. Since F has characteristic p, we have $\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$, because in the binomial expansion of $(a + b)^p$ each coefficient except those of a^p and b^p is zero. (The coefficient $(p!)/(k!(p - k)!)$ contains p in the numerator but not the denominator since p is prime, and so it must be equal to zero in a field of characteristic p.) It is clear that ϕ preserves products, and so ϕ is a ring homomorphism. Furthermore, since it is not the zero mapping, it must be one-to-one. If F is finite, then ϕ must also be onto, and so in this case ϕ is called the *Frobenius automorphism* of F.

Note that $\phi^n(x) = x^{p^n}$. (Inductively, $\phi^n(x) = (\phi^{n-1}(x))^p = (x^{p^{n-1}})^p = x^{p^n}$.) Using an appropriate power of the Frobenius automorphism, we can prove that the Galois group of any finite field must be cyclic.

Theorem 8.1.8 Let K be a finite field and let F be an extension of K with $[F : K] = m$. Then $\mathrm{Gal}(F/K)$ is a cyclic group of order m.

Outline of the proof: We start with the observation that F has p^n elements, for some positive integer n. Then K has p^r elements, for $r = n/m$, and F is the splitting field of $x^{p^n} - x$ over its prime subfield, and hence over K. Since $f(x)$ has no repeated roots, we may apply Theorem 8.1.6 to conclude that $|\,\mathrm{Gal}(F/K)| = m$. Now define $\theta : F \to F$ to be the rth power of the Frobenius automorphism. That is, define $\theta(x) = x^{p^r}$. To compute the order of θ in $\mathrm{Gal}(F/K)$, first note that θ^m is the identity since $\theta^m(x) = x^{p^{rm}} = x^{p^n} = x$ for all $x \in F$. But θ cannot have lower degree, since this would give a polynomial with too many roots. It follows that θ is a generator for $\mathrm{Gal}(F/K)$.

REVIEW PROBLEMS: SECTION 8.1

7. Determine the group of all automorphisms of a field with 4 elements.

8. Let F be the splitting field in $\mathbf{C}$ of $x^4 + 1$.

   (a) Show that $[F : \mathbf{Q}] = 4$.

   (b) Find automorphisms of F that have fixed fields $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, and $\mathbf{Q}(\sqrt{2}i)$, respectively.

9. Find the Galois group over $\mathbf{Q}$ of the polynomial $x^4 + 4$.

10. Find the Galois groups of $x^3 - 2$ over the fields $\mathbf{Z}_5$ and $\mathbf{Z}_{11}$.

11. Find the Galois group of $x^4 - 1$ over the field $\mathbf{Z}_7$.

12. Find the Galois group of $x^3 - 2$ over the field $\mathbf{Z}_7$.

8.2 Repeated roots

Summary: In computing the Galois group of a polynomial, it is important to know whether or not it has repeated roots. A field F is called perfect if no irreducible polynomial over F has repeated roots. This section includes the results that any field of characteristic zero is perfect, and that any finite field is perfect.

In the previous section, we showed that the order of the Galois group of a polynomial with no repeated roots is equal to the degree of its splitting field over the base field. The first thing in this section is to develop methods to determine whether or not a polynomial has repeated roots.

Let $f(x)$ be a polynomial in $K[x]$, and let F be a splitting field for $f(x)$ over K. If $f(x)$ has the factorization $f(x) = (x - r_1)^{m_1} \cdots (x - r_t)^{m_t}$ over F, then we say that the root r_i has *multiplicity* m_i. If $m_i = 1$, then r_i is called a *simple* root.

Let $f(x) \in K[x]$, with $f(x) = \sum_{k=0}^{t} a_k x^k$. The *formal derivative* $f'(x)$ of $f(x)$ is defined by the formula $f'(x) = \sum_{k=0}^{t} k a_k x^{k-1}$, where ka_k denotes the sum of a_k added to itself k times. It is not difficult to show from this definition that the standard differentiation formulas hold. Proposition 8.2.3 shows that the polynomial $f(x) \in K[x]$ has no multiple roots iff it is relatively prime to its formal derivative $f'(x)$. Proposition 8.2.4 shows that $f(x)$ has no multiple roots unless $\mathrm{char}(K) = p \neq 0$ and $f(x)$ has the form $f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_n x^{np}$.

A polynomial $f(x)$ over the field K is called *separable* if its irreducible factors have only simple roots. An algebraic extension field F of K is called *separable over* K if the minimal polynomial of each element of F is separable. The field F is called *perfect* if every polynomial over F is separable.

Theorem 8.2.6 states that any field of characteristic zero is perfect, and a field of characteristic $p > 0$ is perfect if and only if each of its elements has a pth root in the field. It follows immediately from the theorem that any finite field is perfect (just look at the Frobenius automorphism).

To give an example of a field that is *not* perfect, let p be a prime number, and let $K = \mathbf{Z}_p$. Then in the field $K(x)$ of rational functions over K, the element x has no pth root (see Exercise 8.2.8 in the text). Therefore this rational function field is not perfect.

The extension field F of K is called a simple extension if there exists an element $u \in F$ such that $F = K(u)$. In this case, u is called a *primitive* element. Note that if F is a finite field, then Theorem 6.5.10 shows that the multiplicative group $F^\times$ is cyclic. If the generator of this group is a, then it is easy to see that $F = K(a)$ for any subfield K. Theorem 8.2.8 shows that any finite separable extension is a simple extension.

REVIEW PROBLEMS: SECTION 8.2

8. Let $f(x) \in \mathbf{Q}[x]$ be irreducible over $\mathbf{Q}$, and let F be the splitting field for $f(x)$ over $\mathbf{Q}$. If $[F : \mathbf{Q}]$ is odd, prove that all of the roots of $f(x)$ are real.

9. Find an element α with $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha)$.

10. Find the Galois group of $x^6 - 1$ over $\mathbf{Z}_7$.

8.3 The fundamental theorem

Summary: In this section we study the connection between subgroups of $\mathrm{Gal}(F/K)$ *and fields between* K *and* F. *This is a critical step in proving that a polynomial is solvable by radicals if and only if its Galois group is solvable.*

Let F be a field, and let G be a subgroup of $\mathrm{Aut}(F)$. Then

$$\{a \in F \mid \theta(a) = a \text{ for all } \theta \in G\}$$

is called the *G-fixed subfield* of F, or the *G-invariant subfield* of F, and is denoted by F^G. (Proposition 8.3.1 shows that F^G is actually a subfield of F.) If F is the splitting field over K of a separable polynomial and $G = \mathrm{Gal}(F/K)$, then Proposition 8.3.3 shows that $F^G = K$. Artin's lemma (Lemma 8.3.4) provides the first really significant result of the section. It states that if G is a finite group of automorphisms of the field F, and $K = F^G$, then $[F : K] \leq |G|$.

Let F be an algebraic extension of the field K. Then F is said to be a *normal* extension of K if every irreducible polynomial in $K[x]$ that contains a root in F is a product of linear factors in $F[x]$. With this definition, the following theorem and its corollary can be proved from previous results. Some authors say that F is a *Galois extension* of K if the equivalent conditions of Theorem 8.2.6 are satisfied.

Theorem 8.3.6 The following are equivalent for an extension field F of K:

(1) F is the splitting field over K of a separable polynomial;

(2) $K = F^G$ for some finite group G of automorphisms of F;

(3) F is a finite, normal, separable extension of K.

As a corollary, we obtain the fact that if F is an extension field of K such that $K = F^G$ for some finite group G of automorphisms of F, then $G = \mathrm{Gal}(F/K)$.

The next theorem is the centerpiece of Galois theory. In the context of the fundamental theorem, we say that two intermediate subfields E_1 and E_2 are *conjugate* if there exists $\phi \in \mathrm{Gal}(F/K)$ such that $\phi(E_1) = E_2$. Proposition 8.3.9 states that if F is the splitting field of a separable polynomial over K, and $K \subseteq E \subseteq F$, with $H = \mathrm{Gal}(F/E)$, then $\mathrm{Gal}(F/\phi(E)) = \phi H \phi^{-1}$, for any $\phi \in \mathrm{Gal}(F/K)$.

Theorem 8.3.8. (The fundamental theorem of Galois theory) Let F be the splitting field of a separable polynomial over the field K, and let $G = \mathrm{Gal}(F/K)$.

(a) There is a one-to-one order-reversing correspondence between subgroups of G and subfields of F that contain K:

(i) The subfield F^H corresponds to the subgroup H, and $H = \mathrm{Gal}(F/F^H)$.

(ii) If $K \subseteq E \subseteq F$, then the corresponding subgroup is $\mathrm{Gal}(F/E)$, and $E = F^{\mathrm{Gal}(F/E)}$.

(b) $[F : F^H] = |H|$ and $[F^H : K] = [G : H]$, for any subgroup H of G.

(c) Under the above correspondence, the subgroup H is normal iff F^H is a normal extension of K. In this case, $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(F/K) \,/\, \mathrm{Gal}(F/E)$.

For example, suppose that F is a finite field of characteristic p, and has p^m elements. Then $[F : \mathrm{GF}(p)] = m$, and so $G = \mathrm{Gal}(F/\mathrm{GF}(p))$ is a cyclic group of degree m by Corollary 8.1.7. Since G is cyclic, the subgroups of G are in one-to-one correspondence with the positive divisors of m. Proposition 6.5.5 shows that the subfields of F are also in one-to-one correspondence with the positive divisors of m. Remember that the smaller the subfield, the more automorphisms will leave it invariant. By the Fundamental Theorem of Galois Theory, a subfield E with $[E : \mathrm{GF}(p)] = k$ corresponds to the cyclic subgroup with *index* k, not to the cyclic subgroup of *order* k.

REVIEW PROBLEMS: SECTION 8.3

6. Prove that if F is a field and $K = F^G$ for a finite group G of automorphisms of F, then there are only finitely many subfields between F and K.

7. Let F be the splitting field over K of a separable polynomial. Prove that if $\mathrm{Gal}(F/K)$ is cyclic, then for each divisor d of $[F : K]$ there is exactly one field E with $K \subseteq E \subseteq F$ and $[E : K] = d$.

8. Let F be a finite, normal extension of $\mathbf{Q}$ for which $|\operatorname{Gal}(F/\mathbf{Q})| = 8$ and each element of $\operatorname{Gal}(F/\mathbf{Q})$ has order 2. Find the number of subfields of F that have degree 4 over $\mathbf{Q}$.

9. Let F be a finite, normal, separable extension of the field K. Suppose that the Galois group $\operatorname{Gal}(F/K)$ is isomorphic to D_7. Find the number of distinct subfields between F and K. How many of these are normal extensions of K?

10. Show that $F = \mathbf{Q}(i, \sqrt{2})$ is normal over $\mathbf{Q}$; find its Galois group over $\mathbf{Q}$, and find all intermediate fields between $\mathbf{Q}$ and F.

11. Let $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$. Find $[F : \mathbf{Q}]$ and prove that F is not normal over $\mathbf{Q}$.

12. Find the order of the Galois group of $x^5 - 2$ over $\mathbf{Q}$.

8.4 Solvability by radicals

Summary: We must first determine the structure of the Galois group of a polynomial of the form $x^n - a$. Then we will make use of the fundamental theorem of Galois theory to see what happens when we successively adjoin roots of such polynomials.

An extension field F of K is called a *radical extension* of K if there exist elements $u_1, u_2, \ldots, u_m$ in F such that (i) $F = K(u_1, u_2, \ldots, u_m)$, and (ii) $u_1^{n_1} \in K$ and $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$ for $i = 2, \ldots, m$ and $n_1, n_2, \ldots, n_m \in \mathbf{Z}$. For $f(x) \in K[x]$, the polynomial equation $f(x) = 0$ is said to be *solvable by radicals* if there exists a radical extension F of K that contains all roots of $f(x)$.

Proposition 8.4.2 gives the first major result. If F is the splitting field of $x^n - 1$ over a field K of characteristic zero, then $\operatorname{Gal}(F/K)$ is an abelian group.

The roots of the polynomial $x^n - 1$ are called the nth *roots of unity.* Any generator of the group of all nth roots of unity is called a *primitive* nth root of unity. At this point we look ahead to one of the results from Section 8.5.

The complex roots of the polynomial $x^n - 1$ are the nth roots of unity. If we let α be the complex number $\alpha = \cos\theta + i\sin\theta$, where $\theta = 2\pi/n$, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are each roots of $x^n - 1$, and since they are distinct they must constitute the set of all nth roots of unity. Thus we have

$$x^n - 1 = \prod_{k=0}^{n-1}(x - \alpha^k)\ .$$

The set of nth roots of unity is a cyclic subgroup of $\mathbf{C}^\times$ of order n. Thus there are $\varphi(n)$ primitive nth roots of unity, the generators of the group. If $d|n$, then any element of order d generates a subgroup of order d, which has $\varphi(d)$ generators. Thus there are precisely $\varphi(d)$ complex numbers of order d, all living in the group of nth roots of unity.

If p is prime, then every nontrivial pth root of unity is primitive, and is a root of the irreducible polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$, which is a factor of $x^p - 1$. The situation is more complicated when n is not prime. The n*th cyclotomic polynomial.*

$$\Phi_n(x) = \prod_{(k,n)=1,\, 1 \le k < n}(x - \alpha^k)$$

where n is a positive integer, and $\alpha = \cos\theta + i\sin\theta$, with $\theta = 2\pi/n$. (See Definition 8.5.1.)

The following conditions hold for $\Phi_n(x)$: (a) $\deg(\Phi_n(x)) = \varphi(n)$; (b) $x^n - 1 = \prod_{d|n}\Phi_d(x)$; (c) $\Phi_n(x)$ is monic, with integer coefficients; and (d) $\Phi_n(x)$ is irreducible over $\mathbf{Q}$. (See Proposition 8.5.2 and Theorem 8.5.3.) Condition (b) shows how to compute $\Phi_n(x)$ inductively.

The Galois group of the nth cyclotomic polynomial is computed in Theorem 8.5.4. This theorem states that for every positive integer n, the Galois group of the nth cyclotomic polynomial $\Phi_n(x)$ over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}_n^\times$. Theorem 8.4.3 shows more generally that if K is a field of characteristic zero that contains all nth roots of unity, $a \in K$, and F is the splitting field of $x^n - a$ over K, then $\text{Gal}(F/K)$ is a cyclic group whose order is a divisor of n.

We have finally reached our goal, stated in the following two theorems.

Theorem 8.4.6. Let $f(x)$ be a polynomial over a field K of characteristic zero. The equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f(x)$ over K is solvable.

Theorem 8.4.8. There exists a polynomial of degree 5 with rational coefficients that is not solvable by radicals.

Theorem 7.7.2 shows that S_n is not solvable for $n \geq 5$, and so to give an example of a polynomial equation of degree n that is not solvable by radicals, we only need to find a polynomial of degree n whose Galois group over $\mathbf{Q}$ is S_n. As a special case of a more general construction, it can be shown that $f(x) = (x^2+2)(x+2)(x)(x-2) - 2 = x^5 - 2x^3 - 8x - 2$ has Galois group S_5 because it has precisely three real roots. This requires the following group theoretic lemma: Any subgroup of S_5 that contains both a transposition and a cycle of length 5 must be equal to S_5 itself.

REVIEW PROBLEMS: SECTION 8.4

7. Let $f(x)$ be irreducible over $\mathbf{Q}$, and let F be its splitting field over $\mathbf{Q}$. Show that if $\text{Gal}(F/\mathbf{Q})$ is abelian, then $F = \mathbf{Q}(u)$ for all roots u of $f(x)$.

8. Find the Galois group of $x^9 - 1$ over $\mathbf{Q}$.

9. Show that $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbf{Q}$, and use it to find the Galois group of $x^{10} - 1$ over $\mathbf{Q}$.

10. Show that $p(x) = x^5 - 4x + 2$ is irreducible over $\mathbf{Q}$, and find the number of real roots. Find the Galois group of $p(x)$ over $\mathbf{Q}$, and explain why the group is not solvable.

Chapter 7

Group Theory Solutions

SOLUTIONS: §7.0 Examples

1. Prove that if G is a group of order n, and F is any field, then $\mathrm{GL}_n(F)$ contains a subgroup isomorphic to G.

   Solution: Given a permutation $\sigma \in S_n$, we can consider σ to be a permutation of the standard basis for the n-dimensional vector space F^n. As such, it determines a matrix, which can also be described by letting σ permute the columns of the identity matrix. In short, the set of "permutation" matrices in $\mathrm{GL}_n(F)$ is a subgroup isomorphic to S_n. Cayley's theorem shows that G is isomorphic to a subgroup of S_n, and therefore G is isomorphic to a subgroup of $\mathrm{GL}_n(F)$.

2. What is the largest order of an element in $\mathbf{Z}_{200}^\times$?

   Solution: Recall that $\mathbf{Z}_n^\times$ is the multiplicative group of elements relatively prime to n, and its order is given by the Euler φ-function. Since $\mathbf{Z}_{200} \cong \mathbf{Z}_4 \times \mathbf{Z}_{25}$, we have $\mathbf{Z}_{200}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_{25}^\times$, and $\mathbf{Z}_4^\times \cong \mathbf{Z}_2$.

   Since $|\mathbf{Z}_{25}^\times| = 5^2 - 5 = 20$, by the fundamental structure theorem for finite abelian groups (Theorem 7.5.6) we either have $\mathbf{Z}_{200}^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$ or $\mathbf{Z}_{200}^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5$. In the first case, the largest possible order is 20, and in the second case it is 10. In either case, the answer depends on the largest order of an element in $\mathbf{Z}_{25}^\times$. The first guess might be to check the order of the element 2. We have $2^5 = 32 \equiv 7$, so $2^{10} \equiv 49 \equiv -1 \pmod{25}$, and thus 2 has order 20.

   Alternate solution: A proof can also be given using Corollary 7.5.13, which states that $\mathbf{Z}_n^\times$ is cyclic if n is a power of an odd prime. Thus $\mathbf{Z}_{200}^\times \cong \mathbf{Z}_4^\times \times \mathbf{Z}_{25}^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_{20}$.

3. Let G be a finite group, and suppose that for any two subgroups H and K either $H \subseteq K$ or $K \subseteq H$. Prove that G is cyclic of prime power order.

   Solution: Since G is finite, it has an element of maximal order, say a. Then $\langle a \rangle$ cannot be properly contained in any other cyclic subgroup, so it follows that $\langle b \rangle \subseteq \langle a \rangle$ for every $b \in G$, and thus every element of G is a power of a. This shows that G is cyclic, say $G = \langle a \rangle$. Now suppose that $|G|$ has two distinct prime divisors p and q. Then there will be corresponding subgroups of G of order p and q, and neither can be contained in the other, contradicting the hypothesis.

4. Let $G = S_4$ and $N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Prove that N is normal, and that $G/N \cong S_3$.

   Solution: The set $\{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ forms a conjugacy class of S_4, which shows that N is normal. The subgroup H of S_4 generated by $(1,2,3)$ and $(1,2)$ is isomorphic to S_3, and does not contain any elements of H. The inclusion $\iota : H \to G$ followed by the projection $\pi : G \to G/N$ has trivial kernel since $H \cap N = \langle 1 \rangle$. Thus $|\pi\iota(H)| = 6$, so we must have $\pi\iota(H) = G/N$, and thus $G/N \cong H \cong S_3$.

5. Problem 4 can be used to construct a composition series $S_4 \supset N_1 \supset N_2 \supset N_3 \supset \langle 1 \rangle$ in which $N_1 = A_4$ and $N_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Show that there is no composition series in which $N_2 \cong \mathbf{Z}_4$.

   Solution: Any subgroup H of S_4 that is isomorphic to $\mathbf{Z}_4$ must be generated by a 4-cycle (a, b, c, d). By Exercise 2.3.13 (b) there exists $\sigma \in S_4$ with $\sigma(1, 2, 3, 4)\sigma^{-1} = (a, b, c, d)$. That is, there exists an inner automorphism of S_4 that maps $(1, 2, 3, 4)$ to (a, b, c, d). Since any isomorphism will map one composition series to another, this shows that to answer the question it suffices to show that the second term in the composition series cannot be $\langle (1, 2, 3, 4) \rangle$.

   Suppose that we have a composition series $S_4 \supset K_1 \supset K_2 \supset K_3 \supset \langle 1 \rangle$ in which $K_2 = \langle (1, 2, 3, 4) \rangle$. Then K_2 is a normal subgroup of K_1, so this means we should compute the normalizer $N(K_2)$. We know that K_2 is normal in the subgroup D generated by $(1, 2, 3, 4)$ and $(2, 4)$, since $D \cong D_4$ (see Table 3.6.1). We could also show that K_2 is a normal subgroup of D by observing that fact K_2 has index 2 in D.

   Now $K_2 \subset D \subseteq N(K_2) \subseteq S_4$, and since D has index 3 in S_4, it follows that either $D = N(K_2)$ or $N(K_2) = S_4$. Because $(1, 2)(1, 2, 3, 4)(1, 2) = (1, 3, 4, 2) \notin K_2$, it follows that K_2 is not a normal subgroup of S_4, and so $D = N(K_2)$. This forces $K_1 = D$ in our supposed composition series, which is impossible since D is not a normal subgroup of S_4. (In the above calculation, $(1, 2)(1, 2, 3, 4)(1, 2) = (1, 3, 4, 2) \notin D$.)

6. Find the center of the alternating group A_n.

   Solution: In the case $n = 3$, we have $Z(A_3) = A_3$ since A_3 is abelian. If $n \geq 4$, then $Z(A_n) = \{(1)\}$. One way to see this is to use conjugacy classes, since showing that the center is trivial is equivalent to showing that the identity is the only element whose conjugacy class consists of exactly one element. The comments in this section of the review material show that a conjugacy class of A_n is either a conjugacy class of S_n or half of a conjugacy class of S_n. Since a conjugacy class of S_n consists of all permutations with a given cycle structure, if $n \geq 4$ every conjugacy class contains more than 2 elements (except for the conjugacy class of the identity).

   Alternate proof: We can also use the deeper theorem that if $n \geq 5$, then A_n is simple and nonabelian. Since the center is always a normal subgroup, this forces the center to be trivial for $n \geq 5$. That still leaves the case $n = 4$. A direct computation shows that (a, b, c) does not commute with (a, b, d) or $(a, b)(c, d)$. Since every nontrivial element of A_4 has one of these two forms, this implies that the center of A_4 is trivial.

7. In a group G, any element of the form $xyx^{-1}y^{-1}$, with $x, y \in G$, is called a *commutator* of G.

   (a) Find all commutators in the dihedral group D_n. Using the standard description of D_n via generators and relations, consider the cases $x = a^i$ or $x = a^i b$ and $y = a^j$ or $y = a^j b$.

   Solution: Case 1: If $x = a^i$ and $y = a^j$, the commutator is trivial.

   Case 2: If $x = a^i$ and $y = a^j b$, then $xyx^{-1}y^{-1} = a^i a^j b a^{-i} a^j b = a^i a^j a^i b a^j b = a^i a^j a^i a^{-j} b^2 = a^{2i}$, and thus each even power of a is a commutator.

   Case 3: If $x = a^j b$ and $y = a^i$, we get the inverse of the element in Case 2.

   Case 4: If $x = a^i b$ and $y = a^j b$, then $xyx^{-1}y^{-1} = a^i b a^j b a^i b a^j b$, and so we get $xyx^{-1}y^{-1} = a^i a^{-j} b^2 a^i a^{-j} b^2 = a^{2(i-j)}$, and again we get even powers of a.

   If n is odd, then the commutators form the subgroup $\langle a \rangle$. If n is even, then the commutators form the subgroup $\langle a^2 \rangle$.

(b) Show that the commutators of D_n form a normal subgroup N of D_n, and that D_n/N is abelian.

Solution: If $x = a^{2i}$, then conjugation by $y = a^j b$ yields $yxy^{-1} = a^j ba^{2i} a^j b = a^j a^{-2i} b^2 a^{-j} = a^{-2i} = x^{-1}$, which is again in the subgroup. It follows that the commutators form a normal subgroup. The corresponding factor group has order 2 or 4, so it must be abelian.

8. Prove that $\mathrm{SL}_2(\mathbf{Z}_2) \cong S_3$.

   Solution: Every invertible matrix over $\mathbf{Z}_2$ has determinant 1, so $\mathrm{SL}_2(\mathbf{Z}_2)$ coincides with $\mathrm{GL}_2(\mathbf{Z}_2)$. Example 3.4.5 shows that $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$.

   The problem can also be solved by quoting the result that any nonabelian group of order 6 is isomorphic to S_3.

9. Find $|\,\mathrm{PSL}_3(\mathbf{Z}_2)|$ and $|\,\mathrm{PSL}_3(\mathbf{Z}_3)|$.

   Solution: The number of linearly independent vectors in $\mathbf{Z}_2^3$ is $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 7 \cdot 6 \cdot 4 = 2^3 \cdot 3 \cdot 7 = 168$. The corresponding matrices over $\mathbf{Z}_2$ all have determinant 1, and the identity matrix is the only scalar matrix. Thus $|\,\mathrm{PSL}_3(\mathbf{Z}_2)| = 168$.

   Similarly, we have $|\,\mathrm{GL}_3(\mathbf{Z}_3)| = (3^3-1)(3^3-3)(3^3-3^2)$. Half of these matrices have determinant 1 and half have determinant -1. Finally, the center of $\mathrm{SL}_3(\mathbf{Z}_3)$ is trivial, since the only scalar matrix with determinant 1 is the identity matrix. Thus $|\,\mathrm{PSL}_3(\mathbf{Z}_3)| = \frac{1}{2}\cdot 26\cdot 24\cdot 18 = 2^4\cdot 3^3\cdot 13 = 5616$.

   Note: These are the orders of the nonabelian finite simple groups of order less than 10,000: 60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, 5616, 6048, 6072, 7800, 7920, 9828.

10. For a commutative ring R with identity, define $\mathrm{GL}_2(R)$ to be the set of invertible 2×2 matrices with entries in R. Prove that $\mathrm{GL}_2(R)$ is a group.

    Solution: The fact that R is a ring, with addition and multiplication, allows us to define matrix multiplication. The associative and distributive laws in R can be used to show that multiplication is associative (the question only asks for the 2×2 case). Since R has an identity, the identity matrix serves as the identity element. Finally, if $A \in \mathrm{GL}_2(R)$, then A^{-1} exists, and $A^{-1} \in \mathrm{GL}_2(R)$ since $(A^{-1})^{-1} = A$.

11. Let G be the subgroup of $\mathrm{GL}_2(\mathbf{Z}_4)$ defined by the set $\left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \right\}$ such that $b \in \mathbf{Z}_4$ and $m = \pm 1$. Show that G is isomorphic to a known group of order 8.

    Hint: The answer is either D_4 or the quaternion group (see Example 3.3.7).

    Solution: Let $a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Then it is easy to check that a has order 4 and b has order 2. Since $aba = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = b$, we have the identity $ba = a^{-1}b$. Finally, each element has the form $a^i b$, so the group is isomorphic to D_4.

12. Let G be the subgroup of $\mathrm{GL}_3(\mathbf{Z}_2)$ defined by the set $\left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$ such that $a, b, c \in \mathbf{Z}_2$. Show that G is isomorphic to a known group of order 8.

    Solution: A short computation shows the following.

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

As the following computation shows, we have an element of order 4 and an element of order 2 that satisfy the relations of D_4 (just as in the solution of the previous problem).

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

SOLUTIONS: §7.1 Isomorphism theorems

16. Let G_1 and G_2 be groups of order 24 and 30, respectively. Let G_3 be a nonabelian group that is a homomorphic image of both G_1 and G_2. Describe G_3, up to isomorphism.

    Solution: The order of G_3 must be a common divisor of 24 and 30, so it is a divisor of 6. Since any group of order less than 6 is abelian, G_3 must be isomorphic to the symmetric group S_3.

17. Prove that a finite group whose only automorphism is the identity map must have order at most two.

    Solution: All inner automorphisms are trivial, so G is abelian. Then $\alpha(x) = x^{-1}$ is an automorphism, so it is trivial, forcing $x = x^{-1}$ for all $x \in G$. If G is written additively, then G has a vector space structure over the field $\mathbf{Z}_2$. (Since every element of G has order 2, it works to define $0 \cdot x = 0$ and $1 \cdot x = x$, for all $x \in G$.) With this vector space structure, any group homomorphism is a linear transformation (and vice versa), so the automorphism group of G is a group of invertible matrices. Therefore $\text{Aut}(G)$ is nontrivial, unless G is zero or one-dimensional.

18. Let H be a nontrivial subgroup of S_n. Show that either $H \subseteq A_n$, or exactly half of the permutations in H are odd.

    Solution: Look at the composition of the inclusion from H to S_n followed by the projection of S_n onto S_n/A_n. Since S_n/A_n has only 2 elements, this composition either maps H to the identity, in which case $H \subseteq A_n$, or else it maps onto S_n/A_n, in which case the kernel $H \cap A_n$ has index 2 in H.

19. Let p be a prime number, and let A be a finite abelian group in which every element has order p. Show that $\text{Aut}(A)$ is isomorphic to a group of matrices over $\mathbf{Z}_p$.

    Solution: The first step in seeing this is to recognize that if every element of A has order p, then the usual multiplication na, for integers $n \in \mathbf{Z}$, actually define a scalar multiplication on A, for scalars in $\mathbf{Z}_p$. Thus A is a vector space over $\mathbf{Z}_p$, and as such it has some dimension, say n. Note that scalar multiplication by an element of $\mathbf{Z}_p$ is really defined in terms of repeated addition. Therefore every automorphism of A is a linear transformation, so $\text{Aut}(A)$ is isomorphic to the general linear group $\text{GL}_n(\mathbf{Z}_p)$.

20. Let G be a group and let N be a normal subgroup of G of finite index. Suppose that H is a finite subgroup of G and that the order of H is relatively prime to the index of N in G. Prove that H is contained in N.

    Solution: Let $\pi : G \to G/N$ be the natural projection. Then $\pi(H)$ is a subgroup of G/N, so its order must be a divisor of $|G/N|$. On the other hand, $|\pi(H)|$ must be a divisor of $|H|$. Since $\gcd(|H|, [G : N]) = 1$, we must have $|\pi(H)| = 1$, which implies that $H \subseteq \ker(\pi) = N$.

21. Let G be a finite group and let K be a normal subgroup of G such that $\gcd(|K|, [G : K]) = 1$. Prove that K is a characteristic subgroup of G.

    Note: Recall the definition given in Exercise 7.6.8 of the text. The subgroup K is a *characteristic subgroup* of G if $\phi(K) \subseteq K$ for all $\phi \in \text{Aut}(G)$. In this case we say that K is *invariant* under all automorphisms of G.

Solution: Let ϕ be any automorphism of G. Then $\phi(K)$ is a subgroup of G, with $|K|$ elements. Since $\gcd(|K|, [G : K]) = 1$, we can apply the result in the previous problem, which implies that $\phi(K) \subseteq K$.

22. Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and $|G|$ is odd. Prove that N is contained in the center of G.

    Solution: Since $|N| = 5$, the subgroup N is cyclic, say $N = \langle a \rangle$. It suffices to show that $a \in Z(G)$, which is equivalent to showing that a has no conjugates other than itself. We first note that since N is normal in G, any conjugate of a must be in N. We next note that if x is conjugate to y, which we will write xSy, then $x^n \sim y^n$. Finally, we note that the number of conjugates of a must be a divisor of G.

    Case 1. If $a \sim a^2$, then $a^2 \sim a^4$, and $a^4 \sim a^8 = a^3$.

    Case 2. If $a \sim a^3$, then $a^3 \sim a^9 = a^4$, and $a^4 \sim a^{12} = a^2$.

    Case 3. If $a \sim a^4$, then $a^2 \sim a^8 = a^3$.

    In the first two cases a has 4 conjugates, which contradicts the assumption that G has odd order. In the last case, a has either 2 or 4 conjugates, which again leads to the same contradiction.

SOLUTIONS: §7.2 Conjugacy

19. Prove that if the center of the group G has index n, then every conjugacy class of G has at most n elements.

    Solution: The conjugacy class of $a \in G$ has $[G : C(a)]$ elements. Since the center $Z(G)$ is contained in $C(a)$, we have $[G : C(a)] \leq [G : Z(G)] = n$. (In fact, $[G : C(a)]$ must be a divisor of n.)

20. Let G be a group with center $Z(G)$. Prove that $G/Z(G)$ is abelian iff for each element $x \notin Z(G)$ the conjugacy class of x is contained in the coset $Z(G)x$.

    Solution: First suppose that $G/Z(G)$ is abelian and $x \in G$ but $x \notin Z(G)$. For any $a \in G$ we have $ax = zxa$ for some $z \in Z(G)$, since $Z(G)ax = Z(G)xa$ in the factor group $G/Z(G)$. Thus $axa^{-1} = zx$ for some $z \in Z(G)$, showing that the conjugate axa^{-1} belongs to the coset $Z(G)x$.

    Conversely, assume the given condition, and let $x, y \in G$. Then $yxy^{-1} \in Z(G)x$, so $yx \in Z(G)xy$, which shows that $Z(G)yx = Z(G)xy$, and thus $G/Z(G)$ is abelian.

21. Find all finite groups that have exactly two conjugacy classes.

    Solution: Suppose that $|G| = n$. The identity element forms one conjugacy class, so the second conjugacy class must have $n - 1$ elements. But the number of elements in any conjugacy class is a divisor of $|G|$, so the only way that $n - 1$ is a divisor of n is if $n = 2$.

22. Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. Let $H = \{1, a^3, b, a^3b\}$. Find the normalizer of H in G and find the subgroups of G that are conjugate to H.

    Solution: The normalizer of H is a subgroup containing H, so since H has index 3, either $N_G(H) = H$ or $N_G(H) = G$. Choose any element not in H to do the first conjugation.

    $$aHa^{-1} = \{1, a(a^3)a^5, aba^5, a(a^3b)a^5\} = \{1, a^3, a^2b, a^5b\}$$

    This computation shows that a is not in the normalizer, so $N_G(H) = H$. Conjugating by any element in the same left coset $aH = \{a, a^4, ab, a^4b\}$ will give the same subgroup. Therefore it makes sense to choose a^2 to do the next computation.

$a^2Ha^{-2} = \{1, a^3, a^2ba^4, a^2(a^3b)a^4\} = \{1, a^3, a^4b, ab\}$

It is interesting to note that we had shown earlier that b, a^2b, and a^4b form one conjugacy class, while ab, a^3b, and a^5b form a second conjugacy class. In the above computations, notice how the orbits of individual elements combine to give the orbit of a subgroup.

23. Write out the class equation for the dihedral group D_n. Note that you will need two cases: one when n is even, and one when n is odd.

Solution: From Exercise 7.2.13 in the text we have the following results. When n is odd the center is trivial and elements of the form a^ib are all conjugate. Elements of the form a^i are conjugate in pairs; $a^m \neq a^{-m}$ since $a^{2m} \neq 1$. We could write the class equation in the following form.

$$|G| = 1 + \underbrace{2 + \ldots + 2}_{(n-1)/2 \text{ times}} + n$$

When n is even, the center has two elements. (The element $a^{n/2}$ is conjugate to itself since $a^{n/2} = a^{-n/2}$, so $Z(G) = \{1, a^{n/2}\}$.) Therefore elements of the form a^ib split into two conjugacy classes. In this case the class equation has the following form.

$$|G| = 2 + \underbrace{2 + \ldots + 2}_{(n-2)/2 \text{ times}} + \frac{n}{2} + \frac{n}{2}$$

24. Show that for all $n \geq 4$, the centralizer of the element $(1,2)(3,4)$ in S_n has order $8 \cdot (n-4)!$. Determine the elements in $C_{S_n}((1,2)(3,4))$ explicitly.

Solution: The conjugates of $a = (1,2)(3,4)$ in S_n are the permutations of the form $(a,b)(c,d)$. The number of ways to construct such a permutation is

$$\frac{n(n-1)}{2} \cdot \frac{(n-2)(n-3)}{2} \cdot \frac{1}{2}\,,$$

and dividing this into $n!$ gives the order $8 \cdot (n-4)!$ of the centralizer.

We first compute the centralizer of a in S_4. The elements $(1,2)$ and $(3,4)$ clearly commute with $(1,2)(3,4)$. Note that a is the square of $b = (1,3,2,4)$; it follows that the centralizer contains $\langle b \rangle$, so $b^3 = (1,4,2,3)$ also belongs. Computing products of these elements shows that we must include $(1,3)(2,4)$ and $(1,4)(2,3)$, and this gives the required total of 8 elements.

To find the centralizer of a in S_n, any of the elements listed above can be multiplied by any permutation disjoint from $(1,2)(3,4)$. This produces the required total $|C(a)| = 8 \cdot (n-4)!$.

SOLUTIONS: §7.3 Group actions

15. Let G be a group which has a subgroup of index 6. Prove that G has a normal subgroup whose index is a divisor of 720.

Solution: Suppose that H is a subgroup with index 6. Letting G act by multiplication on the left cosets of H produces a homomorphism from G into S_6. The order of the image must be a divisor of $|S_6| = 720$, and so the index of the kernel is a divisor of 720.

16. Let G act on the subgroup H by conjugation, let S be the set of all conjugates of H, and let $\phi : G \to \text{Sym}(S)$ be the corresponding homomorphism. Show that $\ker(\phi)$ is the intersection of the normalizers $N(aHa^{-1})$ of all conjugates of H.

Solution: We have $x \in \ker(\phi)$ iff $x(aHa^{-1})x^{-1} = aHa^{-1}$ for all $a \in G$.

17. Let $F = \mathbf{Z}_3$, $G = \mathrm{GL}_2(F)$, and $S = F^2$. Find the generalized class equation (see Theorem 7.3.6) for the standard action of G on S.

Solution: There are only two orbits, since the zero vector is left fixed, and any nonzero vector can be mapped by G to any other nonzero vector. Thus $|S| = 9$, $|S^G| = 1$, and $[G : G_x] = 8$ for $x = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, so the generalized class equation is $9 = 1 + 8$.

To double check this, we can compute G_x. A direct computation shows that the elements of G_x must have the form $\begin{bmatrix} 1 & a \\ 1 & b \end{bmatrix}$, where $a \neq b$ since the matrix must have nonzero determinant. There are 6 matrices of this type, so $[G : G_x] = 8$ since $|G| = 48$, as noted in Section 7.0.

18. Let $F = \mathbf{Z}_3$, $G = \mathrm{GL}_2(F)$, and let N be the center of G. Prove that $G/N \cong S_4$ by defining an action of G on the four one-dimensional subspaces of F^2.

Solution: In the previous problem, F^2 contains 4 one-dimensional subspaces. (You can easily write out the list.) Each matrix in G represents an isomorphism of F^2, and so it simply permutes these one-dimensional subspaces. Thus we can let S be the set of one-dimensional subspaces, and let G act on them as described above. Multiplying by a scalar leaves each one-dimensional subspace fixed, and this is the only linear transformation to do so. Thus the action of G defines a homomorphism into S_4 whose kernel is the set of scalar matrices, which is precisely the center N. The group $G = \mathrm{GL}_2(\mathbf{Z}_3)$ has $(3^2 - 1)(3^3 - 3)$ elements (see Exercise 7.7.11). The center consists of two scalar matrices, so $|G/N| = 24$. It follows that the homomorphism must map G/N onto S_4, since $|S_4| = 4! = 24$.

SOLUTIONS: §7.4 The Sylow theorems

15. By direct computation, find the number of Sylow 3-subgroups and the number of Sylow 5-subgroups of the symmetric group S_5. Check that your calculations are consistent with the Sylow theorems.

Solution: In S_5 there are $(5 \cdot 4 \cdot 3)/3 = 20$ three cycles. These will split up into 10 subgroups of order 3. This number *is* congruent to 1 mod 3, and is a divisor of $5 \cdot 4 \cdot 2$.

There are $(5!)/5 = 24$ five cycles. These will split up into 6 subgroups of order 5. This number *is* congruent to 1 mod 5, and is a divisor of $4 \cdot 3 \cdot 2$.

16. How many elements of order 7 are there in a simple group of order 168?

Solution: First, $168 = 2^3 \cdot 3 \cdot 7$. The number of Sylow 7-subgroups must be congruent to 1 mod 7 and must be a divisor of 24. The only possibilities are 1 and 8. By assumption there is no proper normal subgroup, so the number must be 8. The subgroups all have the identity in common, leaving $8 \cdot 6 = 48$ elements of order 7.

17. Let G be a group of order 340. Prove that G has a normal cyclic subgroup of order 85 and an abelian subgroup of order 4.

Solution: First, $340 = 2^2 \cdot 5 \cdot 17$. There exists a Sylow 2-subgroup of order 4, and it must be abelian. No nontrivial divisor of $68 = 2^2 \cdot 17$ is congruent to 1 mod 5, so the Sylow 5-subgroup is normal. Similarly, the Sylow 17-subgroup is normal. These subgroups have trivial intersection, so their product is a direct product, and hence must be cyclic of order $85 = 5 \cdot 17$. The product of two normal subgroups is again normal, so this produces the required normal cyclic subgroup of order 85.

18. Show that any group of order 100 has a normal subgroup of order 25.

Solution: The number of Sylow 5-subgroups is congruent to 1 modulo 5 and a divisor of 4, so it must be 1.

19. Show that there is no simple group of order 200.

    Solution: Since $200 = 2^3 \cdot 5^2$, the number of Sylow 5-subgroups is congruent to 1 mod 5 and a divisor of 8. Thus there is only one Sylow 5-subgroup, and it is a proper nontrivial normal subgroup.

20. Show that a group of order 108 has a normal subgroup of order 9 or 27.

    Solution: Let S be a Sylow 3-subgroup of G. Then $[G : S] = 4$, since $|G| = 2^2 3^3$, so we can let G act by multiplication on the cosets of S. This defines a homomorphism $\phi : G \to S_4$, so it follows that $|\phi(G)|$ is a divisor of 12, since it must be a common divisor of 108 and 24. Thus $|\ker(\phi)| \geq 9$, and it follows from Exercise 7.3.2 (a) of the text that $\ker(\phi) \subseteq S$. Thus $|\ker(\phi)|$ must be a divisor of 27, and so either $|\ker(\phi)| = 9$ or $|\ker(\phi)| = 27$.

21. Let p be a prime number. Find all Sylow p-subgroups of the symmetric group S_p.

    Solution: Since $|S_p| = p!$, and p is a prime number, the highest power of p that divides $|S_p|$ is p. Therefore the Sylow p-subgroups are precisely the cyclic subgroups of order p, each generated by a p-cycle. There are $(p-1)! = p!/p$ ways to construct a p-cycle $(a_1, \ldots, a_p)$. The subgroup generated by a given p-cycle will contain the identity and the $p-1$ powers of the cycle. Two different such subgroups intersect in the identity, since they are of prime order, so the total number of subgroups of order p in S_p is $(p-2)! = (p-1)!/(p-1)$.

22. Let G be the group of matrices $\left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \right\}$ such that $x \in \mathbf{Z}_7$ and $a \in \mathbf{Z}_7^\times$.

    (a) Find $n_7(G)$, and find a Sylow 7-subgroup of G.

    Solution: The group has order $42 = 6 \cdot 7$, so $n_7(G) = 1$. A Sylow 7-subgroup must have 7 elements, and the set of matrices of the form $\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$ forms such a subgroup.

    (b) Find $n_3(G)$, and find a Sylow 3-subgroup of G.

    Solution: The number of Sylow 3-subgroups is $\equiv 1 \pmod 3$ and a divisor of 14, so it must be 1 or 7. The element $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ has order 3, so it generates a Sylow 3-subgroup H. Conjugating this element by $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ gives $\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$, so H is not normal, and therefore there must 7 Sylow 3-subgroups.

23. Prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G.

    Solution: Suppose that N contains the Sylow p-subgroup P. Then since N is normal it also contains all of the conjugates of P. But this means that N contains all of the Sylow p-subgroups of G, since they are all conjugate by Theorem 7.4.4 (a). We conclude that N and G have the same number of Sylow p-subgroups.

24. Prove that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

    Solution: Use the previous problem. Since $105 = 3 \cdot 5 \cdot 7$, we have $n_3 = 1$ or 7, $n_5 = 1$ or 21, and $n_7 = 1$ or 15 for the numbers of Sylow subgroups. Let P be a Sylow 5-subgroup and let Q be a Sylow 7-subgroup. At least one of these subgroups must be normal, since otherwise we would have $21 \cdot 4$ elements of order 5 and $15 \cdot 6$ elements of order 7. Therefore PQ is a subgroup, and it must be normal since its index is the smallest prime divisor of $|G|$. (See Exercise 7.3.12 in the text.) If follows that we can apply Problem 23. Since PQ is normal and contains a Sylow 5-subgroup, we can reduce to the number 35 when considering the number of Sylow 5-subgroups, and thus $n_5(G) = n_5(PQ) = 1$. Similarly, since PQ is normal and contains a Sylow 7-subgroup, we have $n_7(G) = n_7(PQ) = 1$.

SOLUTIONS: §7.5 Finite abelian groups

13. Find all abelian groups of order 108 (up to isomorphism).

    Solution: The prime factorization is $108 = 2^2 \cdot 3^3$. There are two possible groups of order 4: $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$. There are three possible groups of order 27: $\mathbf{Z}_{27}$, $\mathbf{Z}_9 \times \mathbf{Z}_3$, and $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$. This gives us the following possible groups:

$$\begin{array}{cc}
\mathbf{Z}_4 \times \mathbf{Z}_{27} & \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{27} \\
\mathbf{Z}_4 \times \mathbf{Z}_9 \times \mathbf{Z}_3 & \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_3 \\
\mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 & \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3\ .
\end{array}$$

14. Let G and H be finite abelian groups, and assume that $G \times G$ is isomorphic to $H \times H$. Prove that G is isomorphic to H.

    Solution: Let p be a prime divisor of $|G|$, and let $q = p^\alpha$ be the order of a cyclic component of G. If G has k such components, then $G \times G$ has $2k$ components of order q. An isomorphism between $G \times G$ and $H \times H$ must preserve these components, so it follows that H also has k cyclic components of order q. Since this is true for every such q, Theorem 7.5.6 gives identical decompositions for G and H. It follows that $G \cong H$.

15. Let G be an abelian group which has 8 elements of order 3, 18 elements of order 9, and no other elements besides the identity. Find (with proof) the decomposition of G as a direct product of cyclic groups.

    Solution: We have $|G| = 27$. First, G is not cyclic since there is no element of order 27. Since there are elements of order 9, G must have $\mathbf{Z}_9$ as a factor. To give a total of 27 elements, the only possibility is $G \cong \mathbf{Z}_9 \times \mathbf{Z}_3$.

    Check: The elements 3 and 6 have order 3 in $\mathbf{Z}_9$, while 1 and 2 have order 3 in $\mathbf{Z}_3$. Thus the following 8 elements have order 3 in the direct product: $(3,0)$, $(6,0)$, $(3,1)$, $(6,1)$, $(3,2)$, $(6,2)$, $(0,1)$, and $(0,2)$.

16. Let G be a finite abelian group with $|G| = 216$. If $|6G| = 6$, determine G up to isomorphism.

    Solution: Assume that G is written additively. Since $216 = 2^3 \cdot 3^3$, we have $G = H \oplus K$, where H is the Sylow 2-subgroup of G and K is the Sylow 3-subgroup K of G. Since H and K are invariant under any automorphism and $6G \cong \mathbf{Z}_2 \times \mathbf{Z}_3$, it follows that $6H \cong \mathbf{Z}_2$ and $6K \cong \mathbf{Z}_3$.

    Multiplication by 3 defines an automorphism of H, so we only need to consider $2H$. Thus $2H \cong \mathbf{Z}_2$, so we know that there are elements of order greater than 2, and that H is not cyclic, since $2\mathbf{Z}_8 \cong \mathbf{Z}_4$. We conclude that $H \cong \mathbf{Z}_4 \times \mathbf{Z}_2$. A similar argument shows that K must be isomorphic to $\mathbf{Z}_9 \times \mathbf{Z}_3$. Thus $G \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_3$, or $G \cong \mathbf{Z}_{36} \times \mathbf{Z}_6$.

17. Apply both structure theorems to give the two decompositions of the abelian group $\mathbf{Z}_{216}^\times$.

    Solution: $\mathbf{Z}_{216}^\times \cong \mathbf{Z}_8^\times \times \mathbf{Z}_{27}^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{27}^\times$

    Since 27 is a power of an odd prime, it follows from Corollary 7.5.13 that $\mathbf{Z}_{27}^\times$ is cyclic.

    This can also be shown directly by guessing that 2 is a generator. Since $\mathbf{Z}_{27}^\times$ has order $3^3 - 3^2 = 18$, an element can only have order 1, 2, 3, 6, 9 or 18. We have $2^2 = 4$, $2^3 = 8$, $2^6 \equiv 8^2 \equiv 10$, and $2^9 \equiv 2^3 \cdot 2^6 \equiv 8 \cdot 10 \equiv -1$, so it follows that 2 must be a generator.

    We conclude that $\mathbf{Z}_{216}^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \cong \mathbf{Z}_{18} \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

18. Let G and H be finite abelian groups, and assume that they have the following property. For each positive integer m, G and H have the same number of elements of order m. Prove that G and H are isomorphic.

Solution: We give a proof by induction on the order of $|G|$. The statement is clearly true for groups of order 2 and 3, so suppose that G and H are given, and the statement holds for all groups of lower order. Let p be a prime divisor of $|G|$, and let G_p and H_p be the Sylow p-subgroups of G and H, respectively. If we can show that $G_p \cong H_p$ for all p, then it will follow that $G \cong H$, since G and H are direct products of their Sylow subgroups.

Since the Sylow p-subgroups contain all elements of order a power of p, the induction hypothesis applies to G_p and H_p. Let x be an element of G_p with maximal order $q = p^\alpha$. Then $\langle x \rangle$ is a direct factor of G_p by Lemma 7.5.5, so there is a subgroup G' with $G_p = \langle x \rangle \times G_0$. By the same argument we can write $H_p = \langle y \rangle \times H_0$, where y has the same order as x. Thus $\langle x \rangle \cong \langle y \rangle$, and then $G_p \cong H_p$ if we can show that $G_0 \cong H_0$.

To show that $G_0 \cong H_0$, we need to verify that G_0 and H_0 satisfy the induction hypothesis. We certainly have $|G_0| = |H_0|$, but we must look at the number of elements of each order. Consider $G_1 = \langle x^p \rangle \times G_0$ and $H_1 = \langle y^p \rangle \times H_0$. To obtain G_1 as a subgroup of G_p we have removed elements of the form (x^k, g_0), where x^k has order q and g_0 is any element of G_0. Because x has maximal order in a p-group, in each case the order of g_0 is a divisor of q, and so (x^k, g_1) has order q since the order of an element in a direct product is the least common multiple of the orders of the components. Thus to construct G_1 we have removed $(p^\alpha - p^{\alpha-1}) \cdot |G_0|$ elements, each having order q. The same is true of H_1. It follows from the hypothesis that we are left with the same number of elements of each order, and so the induction hypothesis implies that $G_1 \cong H_1$. But then $G_0 \cong H_0$, and so $G_p \cong H_p$, completing the proof.

SOLUTIONS: §7.6 Solvable groups

11. Let p be a prime and let G be a nonabelian group of order p^3. Show that the center $Z(G)$ of G is equal to the commutator subgroup G' of G.

    Solution: Since G is nonabelian, by Exercise 7.2.17 of the text we have $|Z(G)| = p$. (The center is nontrivial by Theorem 7.2.8, and if $|Z(G)| = p^2$, then $G/Z(G)$ is cyclic, and Exercise 3.8.14 of the text implies that G is abelian.) On the other hand, any group of order p^2 is abelian by Corollary 7.2.9, so $G/Z(G)$ is abelian, which implies that $G' \subseteq Z(G)$. Since G is nonabelian, $G' \neq \langle 1 \rangle$, and therefore $G' = Z(G)$.

12. Prove that the dihedral group D_n is solvable for all n.

    Solution: By Problem 7.0.7, with the standard description of the dihedral group the commutator subgroup D_n' is either $\langle a \rangle$ or $\langle a^2 \rangle$. In either case, the commutator subgroup is abelian, so $D_n'' = \langle 1 \rangle$.

13. Prove that any group of order 588 is solvable, given that any group of order 12 is solvable.

    Solution: We have $588 = 2^2 \cdot 3 \cdot 7^2$. Let S be the Sylow 7-subgroup. It must be normal, since 1 is the only divisor of 12 that is $\equiv 1 \pmod 7$. By assumption, G/S is solvable since $|G/S| = 12$. Furthermore, S is solvable since it is a p-group. Since both S and G/S are solvable, it follows from Corollary 7.6.8 (b) that G is solvable.

14. Let G be a group of order $780 = 2^2 \cdot 3 \cdot 5 \cdot 13$. Assume that G is not solvable. What are the composition factors of G? (Assume that the only nonabelian simple group of order ≤ 60 is the alternating group A_5.)

    Solution: The Sylow 13-subgroup N is normal, since 1 is the only divisor of 60 that is $\equiv 1 \pmod{13}$. Using the fact that the smallest simple nonabelian group has order 60, we see that the factor G/N must be simple, since otherwise each composition factor would be abelian and G would be solvable. Thus the composition factors are $\mathbf{Z}_{13}$ and A_5.

SOLUTIONS: §7.7 Simple groups

1. Let G be a group of order $2m$, where m is odd. Show that G is not simple.

   Solution: Since this problem from the text is very useful, it seemed worthwhile to include a solution in the review material.

   Let $|G| = 2m$, where m is odd and $m > 1$, and assume that G is simple. Let $\phi : G \to \mathrm{Sym}(G)$ be defined for all $g \in G$ by $\phi(g) = \lambda_g$, where $\lambda_g : G \to G$ is given by $\lambda_g(x) = gx$ for all $x \in G$. Since G is simple, $\ker(\phi) = \langle 1 \rangle$, and so $G \subseteq \mathrm{Sym}(G) = S_{2m}$. Since $|G| = 2m$, it follows from Exercise 3.1.24 of the text that there exists $a \in G$ with $a^2 = 1$ but $a \neq 1$. For each $x \in G$ we have $\lambda_a(x) = ax$ and $\lambda_a(ax) = a^2x = x$, which implies that λ_a is a product of m transpositions (x, ax). Hence λ_a is an odd permutation since m is odd. Let $H = \{x \in G \mid \phi(x) = \lambda_x \text{ is even}\}$. Then H is a subgroup of G, and since $a \in G - H$, it is easy to check that $[G : H] = 2$, and so H is normal, contradicting the assumption that G is simple.

15. Prove that there are no simple groups of order 200.

    Solution: Suppose that $|G| = 200 = 2^3 \cdot 5^2$. The number of Sylow 5 subgroups must be a divisor of 8 and congruent to 1 modulo 5, so it can only be 1, and this gives us a proper nontrivial normal subgroup.

16. Sharpen Exercise 7.7.3 (b) of the text by showing that if G is a simple group that contains a subgroup of index n, where $n > 2$, then G can be embedded in the alternating group A_n.

    Solution: Assume that H is a subgroup with $[G : H] = n$, and let G act by multiplication on the left cosets of H. This action is nontrivial, so the corresponding homomorphism $\phi : G \to S_n$ is nontrivial. Therefore $\ker(\phi)$ is trivial, since G is simple. Thus G can be embedded in S_n. Then $A_n \cap \phi(G)$ is a normal subgroup of $\phi(G)$, so since G is simple, either $\phi(G) \subseteq A_n$, or $A_n \cap \phi(G) = \langle 1 \rangle$. The second case implies $|G| = 2$, since the square of any odd permutation is even, and this cannot happen since $n > 2$.

17. Prove that if G contains a nontrivial subgroup of index 3, then G is not simple.

    Solution: If G is simple and contains a subgroup of index 3, then G can be embedded in A_3 by Problem 16. If the subgroup of index 3 is nontrivial, then $|G| > 3 = |A_3|$, a contradiction.

18. Prove that there are no simple groups of order 96.

    Solution: Suppose that $|G| = 96 = 2^5 \cdot 3$. Then the Sylow 2-subgroup of G has index 3, and so Problem 17 shows that G cannot be simple.

    An alternate proof is to observe that $|G|$ is not a divisor of 3!.

19. Prove that there are no simple groups of order 132.

    Solution: Since $132 = 2^2 \cdot 3 \cdot 11$, for the number of Sylow subgroups we have $n_2 = 1$, 3, 11, or 33; $n_3 = 1$, 4, or 22; and $n_{11} = 1$ or 12. We will focus on n_3 and n_{11}. If $n_3 = 4$ we can let the group act on the Sylow 3-subgroups to produce a homomorphism into S_4. Because 132 is not a divisor of $24 = |S_4|$ this cannot be one-to-one and therefore has a nontrivial kernel. If $n_3 = 22$ and $n_{11} = 12$ we get too many elements: 44 of order 3 and 120 of order 11. Thus either $n_3 = 1$ or $n_{11} = 1$, and the group has a proper nontrivial normal subgroup.

20. Prove that there are no simple groups of order 160.

    Solution: Suppose that $|G| = 160 = 2^5 \cdot 5$. Then the Sylow 2-subgroup of G has index 5, and $2^5 \cdot 5$ is not a divisor of $5! = 120$, so G must have a proper nontrivial normal subgroup.

21. Prove that there are no simple groups of order 280.

    Solution: Since $280 = 2^3 \cdot 5 \cdot 7$, in this case for the number of Sylow subgroups we have $n_2 = 1$, 5, 7, or 35; $n_5 = 1$ or 56; and $n_7 = 1$ or 8. Suppose that $n_5 = 56$ *and* $n_7 = 8$, since otherwise either there is 1 Sylow 5-subgroup or 1 Sylow 7-subgroup, showing that the group is not simple. Since the corresponding Sylow subgroups are cyclic of prime order, their intersections are always trivial. Thus we have $8 \cdot 6$ elements of order 7 and $56 \cdot 4$ elements of order 5, leaving a total of 8 elements to construct all of the Sylow 2-subgroups. It follows that there can be only one Sylow 2-subgroup, so it is normal, and the group is not simple in this case.

22. Prove that there are no simple groups of order 1452.

    Solution: We have $1452 = 2^2 \cdot 3 \cdot 11^2$, so we must have $n_{11} = 1$ or 12. In the second case, we can let the group act by conjugation on the set of Sylow 11-subgroups, producing a nontrivial homomorphism from the group into S_{12}. But 1452 is not a divisor of $|S_{12}| = 12!$ since it has 11^2 as a factor, while 12! does not. Therefore the kernel of the homomorphism is a proper nontrivial normal subgroup, so the group cannot be simple.

Chapter 8

Galois Theory Solutions

SOLUTIONS: §8.0 Splitting fields

1. Find the splitting field over $\mathbf{Q}$ for the polynomial $x^4 + 4$.

   Solution: It is useful to first recall Eisenstein's irreducibility criterion. Let

   $$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

   be a polynomial with integer coefficients. If there exists a prime number p such that

   $$a_{n-1} \equiv a_{n-2} \equiv \ \ldots \ \equiv a_0 \equiv 0 \pmod{p}$$

   but $a_n \not\equiv 0 \pmod{p}$ and $a_0 \not\equiv 0 \pmod{p^2}$, then $f(x)$ is irreducible over the field of $\mathbf{Q}$ rational numbers.

   We have the factorization $x^4+4 = (x^2+2x+2)(x^2-2x+2)$, where the factors are irreducible by Eisenstein's criterion ($p = 2$). The roots are $\pm 1 \pm i$, so the splitting field is $\mathbf{Q}(i)$, which has degree 2 over $\mathbf{Q}$.

   An alternate solution is to solve $x^4 = -4$. To find one root, use DeMoivre's theorem to get $\sqrt[4]{-1} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i$, and then multiply by $\sqrt[4]{4} = \sqrt{2}$, to get $1 + i$. The other roots are found by multiplying by the powers of i, because it is a primitive 4th root of unity.

2. Let p be a prime number. Find the splitting fields for $x^p - 1$ over $\mathbf{Q}$ and over $\mathbf{R}$.

   Solution: We have $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, and the second factor is irreducible over $\mathbf{Q}$ by Corollary 4.4.7 (substitute $x + 1$ and then apply Eisenstein's criterion, using the prime p). Any root $\zeta \neq 1$ is a primitive pth root of unity, so $\mathbf{Q}(\zeta)$ contains the other pth roots of unity and therefore is a splitting field with $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p - 1$.

   If $p \neq 2$, then $x^p - 1$ has at least one root that is not a real number. Therefore the splitting field for $x^p - 1$ over $\mathbf{R}$ must be $\mathbf{C}$.

3. Find the splitting field for $x^3 + x + 1$ over $\mathbf{Z}_2$.

   Solution: Adjoin a root α of the polynomial to obtain $F = \mathrm{GF}(2^3)$. We can realize F as the set $\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$, with $\alpha^3 = \alpha + 1$ and $\alpha^4 = \alpha^2 + \alpha$. Dividing $x^3 + x + 1$ by $x - \alpha$ produces the factorization $x^3 + x + 1 = (x - \alpha)(x^2 + \alpha x + (\alpha^2 + 1))$.

   To verify that F is indeed the splitting field for $x^3 + x + 1$, we need to know that $x^3 + x + 1$ factors into linear factors over F. This follows from Corollary 6.6.2, or from the following calculations, which show that α^2 and $\alpha^2 + \alpha$ are roots of the polynomial $x^2 + \alpha x + (\alpha^2 + 1)$.

   $(\alpha^2)^2 + \alpha(\alpha^2) + (\alpha^2 + 1) = (\alpha^2 + \alpha) + \alpha^3 + \alpha^2 + 1 = \alpha^3 + \alpha + 1 = 0$

   $(\alpha^2 + \alpha)^2 + \alpha(\alpha^2 + \alpha) + (\alpha^2 + 1) = (\alpha^2 + \alpha + \alpha^2) + \alpha^3 + \alpha^2 + \alpha^2 + 1 = \alpha^3 + \alpha + 1 = 0$

4. Find the degree of the splitting field over $\mathbf{Z}_2$ for the polynomial $(x^3+x+1)(x^2+x+1)$.

   Solution: The two polynomials are irreducible (you can check that they have no roots). Therefore the splitting field must have subfields of degree 3 and of degree 2, so the degree of the splitting field over $\mathbf{Z}_2$ must be 6.

5. Let F be an extension field of K. Show that the set of all elements of F that are algebraic over K is a subfield of F.

   Solution: The solution is actually given in Corollary 6.2.8, but it is worth repeating. Whatever you do, don't try to start with two elements and work with their respective minimal polynomials.

   If u, v are algebraic elements of F, then $K(u,v)$ is a finite extension of K. Since $u+v$, $u-v$, and uv all belong to the finite extension $K(u,v)$, these elements are algebraic. The same argument applies to u/v, if $v \neq 0$.

6. Let F be a field generated over the field K by u and v of relatively prime degrees m and n, respectively, over K. Prove that $[F:K]=mn$.

   Solution: Since $F=K(u,v) \supseteq K(u) \supseteq K$, where $[K(u):K]=m$ and $[K(u,v):K(u)] \leq n$, we have $[F:K] \leq mn$. But $[K(v):K]=n$ is a divisor of $[F:K]$, and since $\gcd(m,n)=1$, we must have $[F:K]=mn$.

7. Let $F \supseteq E \supseteq K$ be extension fields. Show that if F is algebraic over E and E is algebraic over K, then F is algebraic over K.

   Solution: Again, this is a result from Chapter 6 that is a good review problem.

   We need to show that each element $u \in F$ is algebraic over K. It is enough to show that u belongs to a finite extension of K. You need to resist your first reaction to work with $E(u)$, because although it is a finite extension of E, you cannot conclude that $E(u)$ is a finite extension of K, since E need not be a finite extension of K.

   Going back to the definition of an algebraic element, we can use the fact that u is a root of some nonzero polynomial $f(x)=a_0+a_1x+\ldots+a_nx^n$ over E. Instead of using all of E, let E' be the subfield $K(a_0,a_1,\ldots,a_n) \subseteq E$, which is a finite extension of K since each coefficient $a_i \in E$ is algebraic over K. Now u is actually algebraic over the smaller field E', so u lies in the finite extension $E'(u)$ of K. This proves that u is algebraic over K, and completes the proof that F is algebraic over K.

8. Let $F \supset K$ be an extension field, with $u \in F$. Show that if $[K(u):K]$ is an odd number, then $K(u^2)=K(u)$.

   Solution: Since $u^2 \in K(u)$, we have $K(u) \supseteq K(u^2) \supset K$. Suppose that $u \notin K(u^2)$. Then x^2-u^2 is irreducible over $K(u^2)$ since it has no roots in $K(u^2)$, so u is a root of the irreducible polynomial x^2-u^2 over $K(u^2)$. Thus $[K(u):K(u^2)]=2$, and therefore 2 is a factor of $[K(u):K]$. This contracts the assumption that $[K(u):K]$ is odd.

9. Find the degree $[F:\mathbf{Q}]$, where F is the splitting field of the polynomial x^3-11 over the field $\mathbf{Q}$ of rational numbers.

   Solution: The roots of the polynomial are $\sqrt[3]{11}$, $\omega\sqrt[3]{11}$, and $\omega^2\sqrt[3]{11}$, where ω is a primitive cube root of unity. Since ω is not real, it cannot belong to $\mathbf{Q}(\sqrt[3]{11})$. Since ω is a root of x^2+x+1 and $F=\mathbf{Q}(\sqrt[3]{11},\omega)$, we have $[F:\mathbf{Q}]=6$.

10. Determine the splitting field over $\mathbf{Q}$ for x^4+2.

    Solution: To get the splitting field F, we need to adjoin the 4th roots of -2, which have the form $\omega^i\sqrt[4]{2}$, where ω is a primitive 8th root of unity and $i=1,3,5,7$. To construct the roots we only need to adjoin $\sqrt[4]{2}$ and i.

To show this, using the polar form $\cos\theta + i\sin\theta$ of the complex numbers, we can see that $\omega = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $\omega^3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $\omega^5 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$, and $\omega^7 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$. Thus $\sqrt[4]{2}\sqrt{2} = \omega\sqrt[4]{2} + \omega^7\sqrt[4]{2}$ must belong to F, and then the cube of this element, which is $4\sqrt[4]{2}$, must also belong to F. Therefore $\sqrt[4]{2} \in F$ (which is somewhat surprising) and the square of this element is $\sqrt{2}$, so it follows that $\sqrt{2} \in F$, and therefore $i \in F$. The splitting field is thus $\mathbf{Q}(\sqrt[4]{2}, i)$, which has degree 8 over $\mathbf{Q}$.

Note: This is the same field as in Example 8.3.3 in the text, which computes the Galois group of $x^4 - 2$ over $\mathbf{Q}$.

11. Determine the splitting field over $\mathbf{Q}$ for $x^4 + x^2 + 1$.

Solution: Be careful here–this polynomial is not irreducible. In fact, $x^6 - 1$ factors in two ways, and provides an important clue. Note that $x^6 - 1 = (x^3)^2 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$ and $x^6 - 1 = (x^2)^3 - 1 = (x^2 - 1)(x^4 + x^2 + 1)$. Thus $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$, and the roots of the first factor are the primitive 3rd roots of unity, while the roots of the second factor are the primitive 6th roots of unity. Adjoining a root ω of $x^2 - x + 1$ gives all 4 roots, and so the splitting field $\mathbf{Q}(\omega)$ has degree 2 over $\mathbf{Q}$.

Comments Since $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a primitive 6th root of unity, the splitting field is contained in $\mathbf{Q}(\sqrt{3}, i)$, but not equal to it, since the latter field has degree 4 over $\mathbf{Q}$. However, the splitting field could be described as $\mathbf{Q}(\sqrt{3}i)$. It is interesting that you also obtain the splitting field by adjoining a primitive cube root of unity.

12. Factor $x^6 - 1$ over $\mathbf{Z}_7$; factor $x^5 - 1$ over $\mathbf{Z}_{11}$.

Solution: Since the multiplicative group $\mathbf{Z}_7^\times$ has order 6, each nonzero element of $\mathbf{Z}_7$ is a root of $x^6 - 1$. Thus $\mathbf{Z}_7$ itself is the splitting field of $x^6 - 1$. (Of course, this can also be proved directly from Theorem 6.5.2.) Therefore over $\mathbf{Z}_7$ we have the factorization

$$x^6 - 1 = x(x-1)(x+1)(x-2)(x+2)(x-3)(x+3) \; .$$

In solving the second half of the problem, looking for roots of $x^5 - 1$ in $\mathbf{Z}_{11}$ is the same as looking for elements of order 5 in the multiplicative group $\mathbf{Z}_{11}^\times$. Theorem 6.5.10 implies that the multiplicative group $F^\times$ is cyclic if F is a finite field, so $\mathbf{Z}_{11}^\times$ is cyclic of order 10. Thus it contains 4 elements of order 5, which means the $x^5 - 1$ must split over $\mathbf{Z}_{11}$. To look for a generator, we might as well start with 2, since it is the smallest element. The relevant powers of 2 are $2^2 = 4$ and $2^5 \equiv -1$, so 2 must be a generator since it has order 10. The even powers of 2 have order 5, and these are $2^2 = 4$, $2^4 \equiv 5$, $2^6 \equiv 9$, and $2^8 \equiv 3$. Therefore $x^5 - 1 = (x-1)(x-3)(x-4)(x-5)(x-9)$ over $\mathbf{Z}_5$.

Comment: The proof that the multiplicative group of a finite field is cyclic is an existence proof, rather than a constructive one. There is no known algorithm for finding a generator for the group.

SOLUTIONS: §8.1 Galois groups

7. Determine the group of all automorphisms of a field with 4 elements.

Solution: The automorphism group consists of two elements: the identity mapping and the Frobenius automorphism.

Read on only if you need more detail. By Corollary 6.5.3, up to isomorphism there is only one field with 4 elements, and it can be constructed as $F = \mathbf{Z}_2[x]/\left\langle x^2 + x + 1 \right\rangle$. Letting α be the coset of x, we have $F = \{0, 1, \alpha, 1+\alpha\}$. Any automorphism of F must leave 0 and 1 fixed, so the only possibility for an automorphism other than the identity is to interchange α and $1+\alpha$.

Is this an automorphism? Since $x^2 + x + 1 \equiv 0$, we have $x^2 \equiv -x - 1 \equiv x + 1$, so $\alpha^2 = 1 + \alpha$ and $(1 + \alpha)^2 = 1 + 2\alpha + \alpha^2 = \alpha$. Thus the function that fixes 0 and 1 while interchanging α and $1 + \alpha$ is in fact the Frobenius automorphism of F.

8. Let F be the splitting field in $\mathbf{C}$ of $x^4 + 1$.

   (a) Show that $[F : \mathbf{Q}] = 4$.

   Solution: We have $x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$, giving the factorization over $\mathbf{Q}$. The factor $x^4 + 1$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion. The roots of x^4+1 are thus the primitive 8th roots of unity, $\pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i$, and adjoining one of these roots also gives the others, together with i. Thus the splitting field is obtained in one step, by adjoining one root of $x^4 + 1$, so its degree over $\mathbf{Q}$ is 4.

   It is clear that the splitting field can also be obtained by adjoining first $\sqrt{2}$ and then i, so it can also be expressed as $\mathbf{Q}(\sqrt{2}, i)$.

   (b) Find automorphisms of F that have fixed fields $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, and $\mathbf{Q}(\sqrt{2}i)$, respectively.

   Solution: These subfields of $\mathbf{Q}(\sqrt{2}, i)$ are the splitting fields of $x^2 - 2$, $x^2 + 1$, and $x^2 + 2$, respectively. Any automorphism must take roots to roots, so if θ is an automorphism of $\mathbf{Q}(\sqrt{2}, i)$, we must have $\theta(\sqrt{2}) = \pm\sqrt{2}$, and $\theta(i) = \pm i$. These possibilities must in fact define 4 automorphisms of the splitting field.

   If we define $\theta_1(\sqrt{2}) = \sqrt{2}$ and $\theta_1(i) = -i$, then the subfield fixed by θ_1 is $\mathbf{Q}(\sqrt{2})$. If we define $\theta_2(\sqrt{2}) = -\sqrt{2}$ and $\theta_2(i) = i$, then the subfield fixed by θ_2 is $\mathbf{Q}(i)$. Finally, for $\theta_3 = \theta_2\theta_1$ we have $\theta_3(\sqrt{2}) = -\sqrt{2}$ and $\theta(i) = -i$, and thus $\theta_3(\sqrt{2}i) = \sqrt{2}i$, so θ_3 has $\mathbf{Q}(\sqrt{2}i)$ as its fixed subfield.

9. Find the Galois group over $\mathbf{Q}$ of the polynomial $x^4 + 4$.

   Solution: Problem 8.0.1 shows that the splitting field of the polynomial has degree 2 over $\mathbf{Q}$, and so the Galois group must be cyclic of order 2.

10. Find the Galois groups of $x^3 - 2$ over the fields $\mathbf{Z}_5$ and $\mathbf{Z}_{11}$.

    Solution: The polynomial is not irreducible over $\mathbf{Z}_5$, since $x^3 - 2 = (x + 2)(x^2 - 2x - 1)$. The quadratic factor will have a splitting field of degree 2 over $\mathbf{Z}_5$, so the Galois group of $x^3 - 2$ over $\mathbf{Z}_5$ is cyclic of order 2.

    A search in $\mathbf{Z}_{11}$ for roots of $x^3 - 2$ yields one and only one: $x = 7$. Then $x^3 - 2$ can be factored as $x^3 - 2 = (x - 7)(x^2 + 7x + 5)$, and the second factor must be irreducible. The splitting field has degree 2 over $\mathbf{Z}_{11}$, and can be described as $\mathbf{Z}_{11}[x]/\left\langle x^2 + 7x + 5\right\rangle$. Thus the Galois group of $x^3 - 2$ over $\mathbf{Z}_{11}$ is again cyclic of order 2.

11. Find the Galois group of $x^4 - 1$ over the field $\mathbf{Z}_7$.

    Solution: We first need to find the the splitting field of $x^4 - 1$ over $\mathbf{Z}_7$. We have $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$. A quick check of ± 2 and ± 3 shows that they are not roots of $x^2 + 1$ over $\mathbf{Z}_7$, so $x^2 + 1$ is irreducible over $\mathbf{Z}_7$. To obtain the splitting field we must adjoin a root of $x^2 + 1$, so we get a splitting field $\mathbf{Z}_7[x]/\left\langle x^2 + 1\right\rangle$ of degree 2 over $\mathbf{Z}_7$.

    It follows from Theorem 8.1.6 that the Galois group of $x^4 - 1$ over $\mathbf{Z}_7$ is cyclic of order 2.

12. Find the Galois group of $x^3 - 2$ over the field $\mathbf{Z}_7$.

    Solution: In this case, $x^3 - 2$ has no roots in $\mathbf{Z}_7$, so it is irreducible. We adjoin a root α of $x^3 - 2$ to $\mathbf{Z}_7$. The resulting extension $\mathbf{Z}_7(\alpha)$ has degree 3 over $\mathbf{Z}_7$, so it has $7^3 = 343$ elements, and each element is a root of the polynomial $x^{343} - x$. It follows from Corollary 6.6.2 that $\mathbf{Z}_7(\alpha)$ is the splitting field of $x^3 - 2$ over $\mathbf{Z}_7$. Since the splitting field has degree 3 over $\mathbf{Z}_7$, it follows from Theorem 8.1.6 that the Galois group of the polynomial is cyclic of order 3.

To show directly that we have found the correct splitting field, let β be a generator of the multiplicative group of the extension. Then $(\beta^{114})^3 = \beta^{342} = 1$, showing that $\mathbf{Z}_7(\alpha)$ contains a nontrivial cube root of 1. It follows that x^3-2 has three distinct roots in $\mathbf{Z}_7(\alpha)$: α, $\alpha\beta^{114}$, and $\alpha\beta^{228}$, so therefore $\mathbf{Z}_7(\alpha)$ is indeed a splitting field for x^3-2 over $\mathbf{Z}_7$.

SOLUTIONS: §8.2 Repeated roots

8. Let $f(x) \in \mathbf{Q}[x]$ be irreducible over $\mathbf{Q}$, and let F be the splitting field for $f(x)$ over $\mathbf{Q}$. If $[F : \mathbf{Q}]$ is odd, prove that all of the roots of $f(x)$ are real.

   Solution: Theorem 8.2.6 implies that $f(x)$ has no repeated roots, so $\mathrm{Gal}(F/\mathbf{Q})$ has odd order. If u is a nonreal root of $f(x)$, then since $f(x)$ has rational coefficients, its conjugate $\overline{u}$ must also be a root of $f(x)$. It follows that F is closed under taking complex conjugates. Since complex conjugation defines an automorphism of the complex numbers, it follows that restricting the automorphism to F defines a homomorphism from F into F. Because F has finite degree over $\mathbf{Q}$, the homomorphism must be onto as well as one-to-one. Thus complex conjugation defines an element of the Galois group of order 2, and this contradicts the fact that the Galois group has odd order. We conclude that every root of $f(x)$ must be real.

9. Find an element α with $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha)$.

   Solution: It follows from the solution of Problem 8.1.8 that we could take $\alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$.

   To give another solution, if we follow the proof of Theorem 8.2.8, we have $u = u_1 = \sqrt{2}$, $u_2 = -\sqrt{2}$, $v = v_1 = i$, and $v_2 = -i$. The proof shows the existence of an element a with $u + av \neq u_i + av_j$ for all i and all $j \neq 1$. To find such an element we need $\sqrt{2} + ai \neq \sqrt{2} + a(-i)$ and $\sqrt{2} + ai \neq -\sqrt{2} + a(-i)$. The easiest solution is to take $a = 1$, and so we consider the element $\alpha = \sqrt{2} + i$. We have $\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\sqrt{2}, i)$, and since $\alpha^{-1} \in \mathbf{Q}(\alpha)$, we must have $(\sqrt{2}+i)^{-1} = (\sqrt{2}-i)/3 \in \mathbf{Q}(\alpha)$. But then $\sqrt{2} - i$ belongs, and it follows immediately that $\sqrt{2}$ and i both belong to $\mathbf{Q}(\alpha)$, which gives us the desired equality $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, i)$.

10. Find the Galois group of $x^6 - 1$ over $\mathbf{Z}_7$.

    Solution: The Galois group is trivial because $x^6 - 1$ already splits over $\mathbf{Z}_7$.

    Comment: Recall that $\mathbf{Z}_7$ is the splitting field of $x^7 - x = x(x^6 - 1)$.

SOLUTIONS: §8.3 The fundamental theorem

6. Prove that if F is a field and $K = F^G$ for a finite group G of automorphisms of F, then there are only finitely many subfields between F and K.

   Solution: By Theorem 8.3.6 the given condition is equivalent to the condition that F is the splitting field over K of a separable polynomial. Since we must have $G = \mathrm{Gal}(F/K)$, the fundamental theorem of Galois theory implies that the subfields between F and K are in one-to-one correspondence with the subgroups of F. Because G is a finite group, it has only finitely many subgroups.

7. Let F be the splitting field over K of a separable polynomial. Prove that if $\mathrm{Gal}(F/K)$ is cyclic, then for each divisor d of $[F : K]$ there is exactly one field E with $K \subseteq E \subseteq F$ and $[E : K] = d$.

   Solution: By assumption we are in the situation of the fundamental theorem of Galois theory, so that there is a one-to-one order-reversing correspondence between subfields of F that contain K and subgroups of $G = \mathrm{Gal}(F/K)$. Because G is cyclic of order $[F : K]$, there is a one-to-one correspondence between subgroups of G and divisors of $[F : K]$. Thus for each divisor d of

$[F : K]$ there is a unique subgroup H of *index* d. By the fundamental theorem, $[F^H : K] = [G : H]$, and so $E = F^H$ is the unique subfield with $[E : K] = d$.

Comment: Pay careful attention to the fact that the correspondence between subfields and subgroups reverses the order.

8. Let F be a finite, normal extension of $\mathbf{Q}$ for which $|\operatorname{Gal}(F/\mathbf{Q})| = 8$ and each element of $\operatorname{Gal}(F/\mathbf{Q})$ has order 2. Find the number of subfields of F that have degree 4 over $\mathbf{Q}$.

   Solution: Since F has characteristic zero, the extension is automatically separable, and so the fundamental theorem of Galois theory can be applied. Any subfield E of F must contain $\mathbf{Q}$, its prime subfield, and then $[E : \mathbf{Q}] = 4$ iff $[F : E] = 2$, since $[F : \mathbf{Q}] = 8$. Thus the subfields of F that have degree 4 over $\mathbf{Q}$ correspond to the subgroups of $\operatorname{Gal}(F/\mathbf{Q})$ that have order 2. Because each nontrivial element has order 2 there are precisely 7 such subgroups.

9. Let F be a finite, normal, separable extension of the field K. Suppose that the Galois group $\operatorname{Gal}(F/K)$ is isomorphic to D_7. Find the number of distinct subfields between F and K. How many of these are normal extensions of K?

   Solution: The fundamental theorem of Galois theory converts this question into the question of enumerating the subgroups of D_7, and determining which are normal. If we use the usual description of D_7 via generators a of order 7 and b of order 2, with $ba = a^{-1}b$, then a generates a subgroup of order 7, while each element of the form a^ib generates a subgroup of order 2, for $0 \le i < 7$. Thus there are 8 proper nontrivial subgroups of D_7, and the only one that is normal is $\langle a \rangle$, since it has $|D_7|/2$ elements. As you should recall from the description of the conjugacy classes of D_7 (see Problem 7.2.23), conjugating one of the 2-element subgroups by a produces a different subgroup, showing that none of them are normal.

10. Show that $F = \mathbf{Q}(i, \sqrt{2})$ is normal over $\mathbf{Q}$; find its Galois group over $\mathbf{Q}$, and find all intermediate fields between $\mathbf{Q}$ and F.

    Solution: It is clear that F is the splitting field over $\mathbf{Q}$ of the polynomial $(x^2+1)(x^2-2)$, and this polynomial is certainly separable. Thus F is a normal extension of $\mathbf{Q}$.

    The work necessary to compute the Galois group over $\mathbf{Q}$ has already been done in the solution to Problem 8.1.8, which shows the existence of 3 nontrivial elements of the Galois group, each of order 2. It follows that the Galois group is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$. Since the Galois group has 3 proper nontrivial subgroups, there will be 3 intermediate subfields E with $\mathbf{Q} \subset E \subset F$. These have been found in Problem 8.1.8, and are $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, and $\mathbf{Q}(\sqrt{2}i)$.

    Note: Problem 8.1.8 begins with the splitting field of $x^4 + 1$ over $\mathbf{Q}$.

11. Let $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$. Find $[F : \mathbf{Q}]$ and prove that F is not normal over $\mathbf{Q}$.

    Solution: The element $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbf{Q}$. Since $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbf{Q}$, we see that $\mathbf{Q}(\sqrt{2})$ cannot be contained in $\mathbf{Q}(\sqrt[3]{2})$ since the first extension has degree 2 over $\mathbf{Q}$ while the second has degree 3 over $\mathbf{Q}$. It follows that $[F : \mathbf{Q}] = 6$.

    If F were a normal extension of $\mathbf{Q}$, then since it contains one root $\sqrt[3]{2}$ of the irreducible polynomial $x^3 - 2$ it would have to contain all of the roots. But $F \subseteq \mathbf{R}$, while the other two roots of $x^3 - 2$ are non-real, so F cannot be a normal extension of $\mathbf{Q}$.

12. Find the order of the Galois group of $x^5 - 2$ over $\mathbf{Q}$.

    Solution: Let G be the Galois group in question, and let ζ be a primitive 5th root of unity. Then the roots of $x^5 - 2$ are $\alpha = \sqrt[5]{2}$ and $\alpha\zeta^j$, for $1 \le j \le 4$. The splitting field over $\mathbf{Q}$ is $F = \mathbf{Q}(\sqrt[5]{2}, \zeta)$. Since $p(x) = x^5 - 2$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion, it is the minimal polynomial of $\sqrt[5]{2}$. The element ζ is a root of $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$, so its minimal polynomial is $q(x) = x^4 + x^3 + x^2 + x + 1$. Thus $[F : \mathbf{Q}] \le 20$, but since the degree must be divisible by 5 and 4, it follows that $[F : \mathbf{Q}] = 20$, and therefore $|G| = 20$.

Note: With a good deal of additional work, G can be shown to be isomorphic to the group F_{20} studied in Exercises 7.1.12, 7.1.13, and 7.2.14 of the text. Any automorphism of F must map roots to roots, for both $p(x)$ and $q(x)$. Define the automorphisms σ_{ij}, for $0 \le i \le 5$ and $0 \le j \le 4$, by setting $\sigma_{ij}(\alpha) = \alpha\zeta^i$ and $\sigma_{ij}(\zeta) = \zeta^j$. It can be shown that $\sigma_{kl}\sigma_{ij} = \sigma_{(k+il),(jl)}$. If F_{20} is given by generators a of order 5 and b of order 4, with the relation $ba = a^2 b$, define $\Phi : G \to F_{20}$ by $\Phi(\sigma_{ij}) = a^i b^j$.

SOLUTIONS: §8.4 Solvability

7. Let $f(x)$ be irreducible over $\mathbf{Q}$, and let F be its splitting field over $\mathbf{Q}$. Show that if $\text{Gal}(F/\mathbf{Q})$ is abelian, then $F = \mathbf{Q}(u)$ for all roots u of $f(x)$.

   Solution: Since F has characteristic zero, we are in the situation of the fundamental theorem of Galois theory. Because $\text{Gal}(F/\mathbf{Q})$ is abelian, every intermediate extension between $\mathbf{Q}$ and F must be normal. Therefore if we adjoin any root u of $f(x)$, the extension $\mathbf{Q}(u)$ must contain all other roots of $f(x)$, since it is irreducible over $\mathbf{Q}$. Thus $\mathbf{Q}(u)$ is a splitting field for $f(x)$, so $\mathbf{Q}(u) = F$.

8. Find the Galois group of $x^9 - 1$ over $\mathbf{Q}$.

   Solution: We can construct the splitting field F of $x^9 - 1$ over $\mathbf{Q}$ by adjoining a primitive 9th root of unity to $\mathbf{Q}$. Since $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$, and the roots of $x^2 + x + 1$ are the primitive cube roots of unity, we need to check that the last factor is irreducible. Substituting $x + 1$ in this factor yields $(x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. This polynomial satisfies Eisenstein's criterion for the prime 3, which implies that the factor $x^6 + x^3 + 1$ is irreducible over $\mathbf{Q}$. The roots of this factor are the primitive 9th roots of unity, so it follows that $[F : \mathbf{Q}] = 6$. The proof of Theorem 8.4.2 (which is worth remembering) shows that $\text{Gal}(F/\mathbf{Q})$ is isomorphic to a subgroup of $\mathbf{Z}_9^\times$. Since $\mathbf{Z}_9^\times$ is abelian of order 6, it is isomorphic to $\mathbf{Z}_6$. It follows that $\text{Gal}(F/\mathbf{Q}) \cong \mathbf{Z}_6$.

   Comment: Section 8.5 of the text contains the full story. Theorem 8.5.4 shows that the Galois group of $x^n - 1$ over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}_n^\times$, and so the Galois group is cyclic of order $\varphi(n)$ iff $n = 2$, 4, p^k, or $2p^k$, for an odd prime p.

9. Show that $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbf{Q}$, and use it to find the Galois group of $x^{10} - 1$ over $\mathbf{Q}$.

   Solution: We can construct the splitting field F of $x^{10} - 1$ over $\mathbf{Q}$ by adjoining a primitive 10th root of unity to $\mathbf{Q}$. We have the factorization

   $$x^{10} - 1 = (x^5 - 1)(x^5 + 1) = (x-1)(x^4 + x^3 + x^2 + x + 1)(x+1)(x^4 - x^3 + x^2 - x + 1).$$

   Substituting $x - 1$ in the last factor yields

   $$\begin{aligned} &(x-1)^4 - (x-1)^3 + (x-1)^2 - (x-1) + 1 \\ &\quad = (x^4 - 4x^3 + 6x^2 - 4x + 1) - (x^3 - 3x^2 + 3x - 1) + (x^2 - 2x + 1) - (x-1) + 1 \\ &\quad = x^4 - 5x^3 + 10x^2 - 10x + 5. \end{aligned}$$

   This polynomial satisfies Eisenstein's criterion for the prime 5, which implies that the factor $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbf{Q}$.

   The roots of this factor are the primitive 10th roots of unity, so it follows that $[F : \mathbf{Q}] = \varphi(10) = 4$. The proof of Theorem 8.4.2 shows that $\text{Gal}(F/\mathbf{Q}) \cong \mathbf{Z}_{10}^\times$, and so the Galois group is cyclic of order 4.

10. Show that $p(x) = x^5 - 4x + 2$ is irreducible over $\mathbf{Q}$, and find the number of real roots. Find the Galois group of $p(x)$ over $\mathbf{Q}$, and explain why the group is not solvable.

    Solution: The polynomial $p(x)$ is irreducible over $\mathbf{Q}$ since it satisfies Eisenstein's criterion for $p = 2$. Since $p(-2) = -22$, $p(-1) = 5$, $p(0) = 2$, $p(1) = -1$, and $p(2) = 26$, we see that $p(x)$ has a real root between -2 and -1, another between 0 and 1, and a third between 1 and 2. The derivative $p'(x) = 5x^4 - 4$ has two real roots, so $p(x)$ has one relative maximum and one relative minimum, and thus it must have exactly three real roots. It follows as in the proof of Theorem 8.4.8 that the Galois group of $p(x)$ over $\mathbf{Q}$ is S_5, and so it is not solvable.

Final comments

In Sections 8.5 and 8.6, the text provides some additional information about actually calculating Galois groups. In particular, the last section outlines some of the results that are necessary in using a computer algebra program to compute Galois groups (over $\mathbf{Q}$) of polynomials of low degree.

You can find additional information in Sections 14.6 and 14.8 of the text by Dummit and Foote. To calculate the Galois group of a polynomial in more difficult situations, you need to learn about the discriminant of a polynomial, reduction modulo a prime, and about transitive subgroups of the symmetric group.

BIBLIOGRAPHY

Abstract Algebra (undergraduate)

Allenby, R. B. J. T., *Rings, Fields and Groups: An Introduction to Abstract Algebra* (4^{th} ed.). Elsevier, 1991.
Artin, M., *Algebra*, Prentice-Hall, 1991
Birkhoff, G., and S. Mac Lane, *A Survey of Modern Algebra* (5^{th} ed.). A.K. Peters, 1997.
Fraleigh, J., *A First Course in Abstract Algebra* (7^{th} ed.). Addison-Wesley, 2003.
Gallian, J., *Contemporary Abstract Algebra* (5^{th} ed.). Houghton Mifflin, 2002.
Herstein, I. N., *Abstract Algebra.* (3^{rd} ed.). John Wiley & Sons, 1996.
———, *Topics in Algebra* (2^{nd} ed.). John Wiley & Sons, 1975.
McCoy, N., and G. Janusz, *Introduction to Modern Algebra*, (5^{th} ed.). W. C. Brown, 1992.

Abstract Algebra (graduate)

Clark, A., *Elements of Abstract Algebra.* Dover Publications, 1984.
Dummit, D., and R. Foote, *Abstract Algebra* (3^{rd} ed.). John Wiley & Sons, 2003.
Hungerford, T., *Algebra.* Springer-Verlag New York, 1980.
Jacobson, N. *Basic Algebra I* (2^{nd} ed.). W. H. Freeman, 1985.
Rotman, J. J., *Advanced Algebra.* (2^{nd} ed.). Springer-Verlag New York, 2002.
Van der Waerden, B. L., *Algebra*, vol. 1. Springer-Verlag New York, 2003.

Linear Algebra

Hoffman, K. and Kunze, R., *Linear Algebra* (2^{nd} ed.). Prentice-Hall, 1971.

Group Theory

Rotman, J. J., *An Introduction to the Theory of Groups.* (4^{th} ed.). Springer-Verlag New York, 1995.

Field Theory

Artin, E., *Galois theory* (2^{nd} ed.). Dover Publications, 1998.
Garling, D.H.J., *A Course in Galois Theory*, Cambridge Univ. Press, 1986
Stewart, I., *Galois Theory*, (3^{rd} ed.). Chapman and Hall, 2003.

Index