

A BOOK OF ABSTRACT ALGEBRA

Second Edition

Charles C. Pinter
Professor of Mathematics
Bucknell University

Dover Publications, Inc., Mineola, New York

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

Bibliographical Note

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

Library of Congress Cataloging-in-Publication Data

Pinter, Charles C, 1932–

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

p. cm.

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

Includes bibliographical references and index.

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

ISBN-10: 0-486-47417-8

1. Algebra, Abstract. I. Title.

QA162.P56 2010

512'.02—dc22

2009026228

Manufactured in the United States by Courier Corporation
47417803

www.doverpublications.com

Preface

Chapter 1 Why Abstract Algebra?

History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.

Chapter 2 Operations

Operations on a Set. Properties of Operations.

Chapter 3 The Definition of Groups

Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables.

Theory of Coding: Maximum-Likelihood Decoding.

Chapter 4 Elementary Properties of Groups

Uniqueness of Identity and Inverses. Properties of Inverses.

Direct Product of Groups.

Chapter 5 Subgroups

Definition of Subgroup. Generators and Defining Relations.

Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.

Chapter 6 Functions

Injective, Surjective, Bijective Function. Composite and Inverse of Functions.

Finite-State Machines. Automata and Their Semigroups.

Chapter 7 Groups of Permutations

Symmetric Groups. Dihedral Groups.

An Application of Groups to Anthropology.

Chapter 8 Permutations of a Finite Set

Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.

Chapter 9 Isomorphism

The Concept of Isomorphism in Mathematics. Isomorphic and Nonisomorphic Groups. Cayley's Theorem.

Chapter 10 Order of Group Elements

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

Chapter 11 Cyclic Groups

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

Chapter 12 Partitions and Equivalence Relations

Chapter 13 Counting Cosets

Lagrange's Theorem and Elementary Consequences.

Survey of Groups of Order ≤ 10 .

Number of Conjugate Elements. Group Acting on a Set.

Chapter 14 Homomorphisms

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

Inner Direct Products. Conjugate Subgroups.

Chapter 15 Quotient Groups

Quotient Group Construction. Examples and Applications.

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

Chapter 16 The Fundamental Homomorphism Theorem

Fundamental Homomorphism Theorem and Some Consequences.

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

Chapter 17 Rings: Definitions and Elementary Properties

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

Chapter 18 Ideals and Homomorphisms

Chapter 19 Quotient Rings

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

Chapter 20 Integral Domains

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

Chapter 21 The Integers

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

Chapter 22 Factoring into Primes

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

Chapter 23 Elements of Number Theory (Optional)

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

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

Chapter 24 Rings of Polynomials

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

Polynomials in Several Variables. Fields of Polynomial Quotients.

Chapter 25 Factoring Polynomials

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

Euclidean Algorithm.

Chapter 26 Substitution in Polynomials

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

Chapter 27 Extensions of Fields

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

Chapter 28 Vector Spaces

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

Chapter 29 Degrees of Field Extensions

Simple and Iterated Extensions. Degree of an Iterated Extension.

Fields of Algebraic Elements. Algebraic Numbers. Algebraic Closure.

Chapter 30 Ruler and Compass

Constructible Points and Numbers. Impossible Constructions.

Constructible Angles and Polygons.

Chapter 31 Galois Theory: Preamble

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

Roots of Unity. Separable Polynomials. Normal Extensions.

Chapter 32 Galois Theory: The Heart of the Matter

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

Computing Galois Groups.

Chapter 33 Solving Equations by Radicals

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

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

* Italic headings indicate topics discussed in the exercise sections.

HOMOMORPHISMS

We have seen that if two groups are isomorphic, this means there is a one-to-one correspondence between them which transforms one of the groups into the other. Now if G and H are any groups, it may happen that there is a function which transforms G into H , although this function is *not* a one-to-one correspondence. For example, $\mathbb{Z}_6$ is transformed into $\mathbb{Z}_3$ by

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

as we may verify by comparing their tables:

+	0	1	2	3	4	5		+	0	1	2	0	1	2
0	0	1	2	3	4	5		0	0	1	2	0	1	2
1	1	2	3	4	5	0		1	1	2	0	1	2	0
2	2	3	4	5	0	1		2	2	0	1	2	0	1
3	3	4	5	0	1	2		0	0	1	2	0	1	2
4	4	5	0	1	2	3		1	1	2	0	1	2	0
5	5	0	1	2	3	4		2	2	0	1	2	0	1

Replace
 x by $f(x)$
→

Eliminate duplicate
information
→
(For example, $2 + 2 = 1$
appears four separate
times in table above.)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

If G and H are any groups, and there is a function f which transforms G into H , we say that if is a *homomorphic image* of G . The function f is called a *homomorphism* from G to f . This notion of homomorphism is one of the skeleton keys of algebra, and this chapter is devoted to explaining it and

defining it precisely.

First, let us examine carefully what we mean by saying that “ f transforms G into H .” To begin with, f must be a function from G onto H ; but that is not all, because f must also transform the table of G into the table of H . To accomplish this, f must have the following property: for any two elements a and b in G ,

$$\text{if } f(a) = a' \quad \text{and} \quad f(b) = b', \quad \text{then} \quad f(ab) = a' b' \quad (1)$$

Graphically,

$$\begin{array}{lcl} \text{if} & a & \xrightarrow{f} a' \\ \text{and} & b & \xrightarrow{f} b' \\ \text{then} & ab & \xrightarrow{f} a' b' \end{array}$$

Condition (1) may be written more succinctly as follows:

$$f(ab) = f(a)f(b) \quad (2)$$

Thus,

Definition if G and H are groups, a **homomorphism** from G to H is a function $f: G \rightarrow H$ such that for any two elements a and b in G ,

$$f(ab) = f(a)f(b)$$

If there exists a homomorphism from G **onto** H , we say that H is a **homomorphic image** of G .

Groups have a very important and privileged relationship with their homomorphic images, as the next few examples will show.

Let P denote the group consisting of two elements, e and o , with the table

+	e	o
e	e	o
o	o	e

We call this group the *parity group* of even and odd numbers. We should think of e as “even” and o as “odd,” and the table as describing the rule for adding even and odd numbers. For example, even + odd = odd, odd + odd = even, and so on.

The function $f: \mathbf{Z} \rightarrow P$ which carries every even integer to e and every odd integer to o is clearly a homomorphism from $\mathbf{Z}$ to P . This is easy to check because there are only four different cases: for arbitrary integers r and s , r and s are either both even, both odd, or mixed. For example, if r and s are both odd, their sum is even, so $f(r) = o$, $f(s) = o$, and $f(r + s) = e$. Since $e = o + o$,

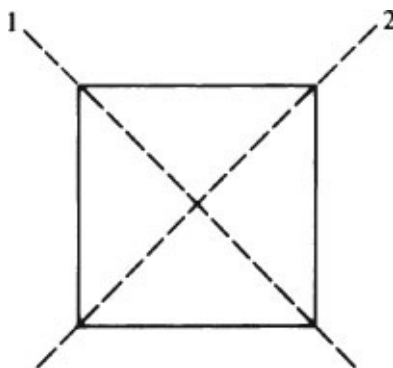
$$f(r + s) = f(r) + f(s)$$

This equation holds analogously in the remaining three cases; hence f is a homomorphism. (Note that the symbol $+$ is used on both sides of the above equation because the operation, in $\mathbf{Z}$ as well as in P , is denoted by $+$.)

It follows that P is a homomorphic image of $\mathbf{z}$!

Now, what do P and $\mathbf{z}$ have in common? P is a much smaller group than $\mathbf{z}$, therefore it is not surprising that very few properties of the integers are to be found in P . Nevertheless, *one* aspect of the structure of $\mathbf{z}$ is retained absolutely intact in P , namely, the structure of the odd and even numbers. (The fact of being odd or even is called the *parity* of integers.) In other words, *as we pass from $\mathbf{z}$ to P* we deliberately lose every aspect of the integers except their parity ; their parity alone (with its arithmetic) is retained, and faithfully preserved.

Another example will make this point clearer. Remember that D_4 is the group of the symmetries of the square. Now, every symmetry of the



square either interchanges the two diagonals here labeled 1 and 2, or leaves them as they were. In other words, every symmetry of the square brings about one of the permutations

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

of the diagonals.

For each $R_i \in D_4$, let $f(R_i)$ be the permutation of the diagonals produced by R_i . Then f is clearly a homomorphism from D_4 onto S_2 . Indeed, it is clear on geometrical grounds that when we perform the motion R_i followed by the motion R_j on the square, we are, at the same time, carrying out the motions $f(R_i)$ followed by $f(R_j)$ on the diagonals. Thus,

$$f(R_j \circ R_i) = f(R_j) \circ f(R_i)$$

It follows that S_2 is a homomorphic image of D_4 . Now S_2 is a smaller group than D_4 , and therefore very few of the features of D_4 are to be found in S_2 . Nevertheless, *one* aspect of the structure of D_4 is retained absolutely intact in S_2 , namely, the diagonal motions. Thus, as we pass from D_4 to S_2 , we deliberately lose every aspect of plane motions except the motions of the diagonals; these alone are retained and faithfully preserved.

A final example may be of some help; it relates to the group $\mathbb{B}^n$ described in [Chapter 3, Exercise E](#). Here, briefly, is the context in which this group arises: The most basic way of transmitting information is to code it into strings of Os and Is, such as 0010111, 1010011, etc. Such strings are called *binary words*, and the number of Os and Is in any binary word is called its *length*. The symbol $\mathbb{B}^n$ designates the group consisting of all binary words of length n , with an operation of addition described in [Chapter 3, Exercise E](#).

Consider the function $f: \mathbb{B}^7 \rightarrow \mathbb{B}^5$ which consists of *dropping the last two digits* of every seven-digit

word. This kind of function arises in many practical situations: for example, it frequently happens that the first five digits of a word carry the message while the last two digits are an error check. Thus, f separates the message from the error check.

It is easy to verify that f is a homomorphism; hence $\mathbb{B}^5$ is a homomorphic image of $\mathbb{B}^7$. As we pass from $\mathbb{B}^7$ to $\mathbb{B}^5$, the message component of words in $\mathbb{B}^7$ is exactly preserved while the error check is deliberately lost.

These examples illustrate the basic idea inherent in the concept of a homomorphic image. The cases which arise in practice are not always so clear-cut as these, but the underlying idea is still the same: In a homomorphic image of G , some aspect of G is isolated and faithfully preserved while all else is deliberately lost.

The next theorem presents two elementary properties of homomorphisms.

Theorem 1 *Let G and H be groups, and $f: G \rightarrow H$ a homomorphism. Then*

- (i) $f(e) = e$, and
- (ii) $f(a^{-1}) = [f(a)]^{-1}$ for every element $a \in G$.

In the equation $f(e) = e$, the letter e on the left refers to the neutral element in G , whereas the letter e on the right refers to the neutral element in H .

To prove (i), we note that in any group,

$$\text{if } yy = y \quad \text{then} \quad y = e$$

(Use the cancellation law on the equation $yy = ye$.) Now, $f(e)f(e) = f(ee) = f(e)$; hence $f(e) = e$.

To prove (ii), note that $f(a)f(a^{-1}) = f(aa^{-1}) = f(e)$. But $f(e) = e$, so $f(a)f(a^{-1}) = e$. It follows by [Theorem 2](#) of [Chapter 4](#) that $f(a^{-1})$ is the inverse of $f(a)$, that is, $f(a^{-1}) = [f(a)]^{-1}$.

Before going on with our study of homomorphisms, we must be introduced to an important new concept. If a is an element of a group G , a *conjugate* of a is any element of the form xax^{-1} , where $x \in G$. For example, the conjugates of a in S_3 are

$$\beta \circ a \circ \beta^{-1} = \gamma$$

$$\gamma \circ a \circ \gamma^{-1} = \kappa$$

$$\delta \circ a \circ \delta^{-1} = \kappa$$

$$\kappa \circ a \circ \kappa^{-1} = \gamma$$

as well as a itself, which may be written in two ways, as $\varepsilon \circ a \circ \varepsilon^{-1}$ or as $a \circ a \circ a^{-1}$. If H is any subset of a group G , we say that H is *closed with respect to conjugates* if every conjugate of every element of H is in H . Finally,

Definition *Let H be a subgroup of a group G . H is called a **normal** subgroup of G if it is closed with respect to conjugates, that is, if*

$$\text{for any } a \in H \quad \text{and} \quad x \in G \quad xax^{-1} \in H$$

(Note that according to this definition, a normal subgroup of G is any nonempty subset of G which is closed with respect to products, with respect to inverses, and with respect to conjugates.)

We now return to our discussion of homomorphisms.

Definition Let $f: G \rightarrow H$ be a homomorphism. The **kernel** of f is the set K of all the elements of G which are carried by f onto the neutral element of H . That is,

$$K = \{x \in G: f(x) = e\}$$

Theorem 2 Let $f: G \rightarrow H$ be a homomorphism.

- (i) The kernel of f is a normal subgroup of G , and
- (ii) The range of f is a subgroup of H .

PROOF: Let K denote the kernel of f . If $a, b \in K$, this means that $f(a) = e$ and $f(b) = e$. Thus, $f(ab) = f(a)f(b) = ee = e$; hence $ab \in K$.

If $a \in K$, then $f(a) = e$. Thus, $f(a^{-1}) = [f(a)]^{-1} = e^{-1} = e$, so $a^{-1} \in K$.

Finally, if $a \in K$ and $x \in G$, then $f(xax^{-1}) = f(x)f(a)f(x^{-1}) = f(x)f(a)[f(x)]^{-1} = e$, which shows that $xax^{-1} \in K$. Thus, K is a normal subgroup of G .

Now we must prove part (ii). If $f(a)$ and $f(b)$ are in the range of f , then their product $f(a)f(b) = f(ab)$ is also in the range of f .

If $f(a)$ is in the range of f , its inverse is $[f(a)]^{-1} = f(a^{-1})$, which is also in the range of f . Thus, the range of f is a subgroup of H . ■

If f is a homomorphism, we represent the kernel of f and the range of f with the symbols

$$\ker(f) \quad \text{and} \quad \text{ran}(f)$$

EXERCISES

A. Examples of Homomorphisms of Finite Groups

1 Consider the function $f: \mathbf{z}_8 \rightarrow \mathbf{z}_4$ given by

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{pmatrix}$$

Verify that f is a homomorphism, find its kernel K , and list the cosets of K . [REMARK: To verify that f is a homomorphism, you must show that $f(a + b) = f(a) + f(b)$ for all choices of a and b in $\mathbf{z}_8$; there are 64 choices. This may be accomplished by checking that f transforms the table of $\mathbf{z}_8$ to the table of $\mathbf{z}_4$, as on page 136.]

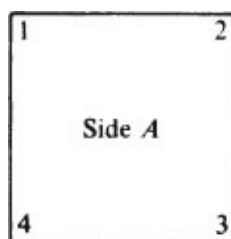
2 Consider the function $f: S_3 \rightarrow \mathbf{z}_2$ given by

$$f = \begin{pmatrix} \varepsilon & \alpha & \beta & \gamma & \delta & \kappa \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Verify that f is a homomorphism, find its kernel K , and list the cosets of K .

3 Find a homomorphism $f: \mathbf{z}_{15} \rightarrow \mathbf{z}_5$, and indicate its kernel. (Do not actually verify that f is a homomorphism.)

4 Imagine a square as a piece of paper lying on a table. The side facing you is side

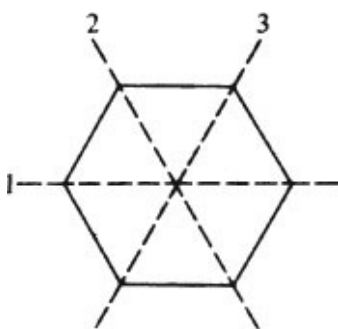


A. The side hidden from view is side B . Every motion of the square either interchanges the two sides (that is, side B becomes visible and side A hidden) or leaves the sides as they were. In other words, every motion R_i of the square brings about one of the permutations

$$\varepsilon = \begin{pmatrix} A & B \\ A & B \end{pmatrix} \quad \text{or} \quad \alpha = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

of the sides; call it $g(R_i)$. Verify that $g: D_4 \rightarrow S_2$ is a homomorphism, and give its kernel.

5 Every motion of the regular hexagon brings about a permutation of its diagonals, labeled 1, 2, and 3. For each $R_i \in D_6$, let $f(R_i)$ be the permutation of



the diagonals produced by R_i . Argue informally (appealing to geometric intuition) to explain why $f: D_6 \rightarrow S_3$ is a homomorphism. Then complete the following:

$$f\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon \quad f\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = \delta \quad \dots$$

(That is, find the value of f on all 12 elements of D_6 .)

6 Let $B \subset A$. Let $h: P_A \rightarrow P_B$ be defined by $h(C) = C \cap B$. For $A = \{1, 2, 3\}$ and $B = \{1, 2\}$, complete the following:

$$h = \begin{pmatrix} \emptyset & \{1\} & \{2\} & \{3\} & \{1, 2\} & \{1, 3\} & \{2, 3\} & A \end{pmatrix}$$

For any A and $B \subset A$, show that h is a homomorphism.

B. Examples of Homomorphisms of Infinite Groups

Prove that each of the following is a homomorphism, and describe its kernel.

1 The function $\phi: \mathcal{F}(\mathbb{R}) \rightarrow \mathbb{R}$ given by $\phi(f) = f(0)$.

2 The function $\phi: \mathcal{D}(\mathbb{R}) \rightarrow \mathcal{F}(\mathbb{R})$ given by $\phi(f) = f'$. $\mathcal{D}(\mathbb{R})$ is the group of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$; f' is the derivative of f .

3 The function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x, y) = x + y$.

4 The function $f: \mathbb{R}^* \rightarrow \mathbb{R}^{\text{pos}}$ defined by $f(x) = |x|$.

5 The function $f: \mathbb{C}^* \rightarrow \mathbb{R}^{\text{pos}}$ defined by $f(a + bi) = \sqrt{a^2 + b^2}$.

6 Let G be the multiplicative group of all 2×2 matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

satisfying $ad - bc \neq 0$. Let $f: G \rightarrow \mathbb{R}^*$ be given by $f(A) = \text{determinant of } A = ad - bc$.

C. Elementary Properties of Homomorphisms

Let G, H , and K be groups. Prove the following:

1 If $f: G \rightarrow G$ and $g: H \rightarrow K$ are homomorphisms, then their composite $g \circ f: G \rightarrow K$ is a homomorphism.

2 If $f: G \rightarrow H$ is a homomorphism with kernel K , then f is injective iff $K = \{e\}$.

3 If $f: G \rightarrow H$ is a homomorphism and J is any subgroup of G , then $f(J) = \{f(x) : x \in J\}$ is a subgroup of H .

4 If $f: G \rightarrow H$ is a homomorphism and J is any subgroup of H , then

$$f^{-1}(J) = \{x \in G : f(x) \in J\}$$

is a subgroup of G . Furthermore, $\ker f \subseteq f^{-1}(J)$.

5 If $f: G \rightarrow H$ is a homomorphism with kernel K , and J is a subgroup of G , let f_J designate the restriction of f to J . (In other words f_J is the same function as f , except that its domain is restricted to J .) Then $\ker f_J = J \cap K$.

6 For any group G , the function $f: G \rightarrow G$ defined by $f(x) = e$ is a homomorphism.

7 For any group G , $\{e\}$ and G are homomorphic images of G .

8 The function $f: G \rightarrow G$ defined by $f(x) = x^2$ is a homomorphism iff G is abelian.

9 The functions $f_1(x, y) = x$ and $f_2(x, y) = y$, from $G \times H$ to G and H , respectively, are homomorphisms.

D. Basic Properties of Normal Subgroups

In the following, let G denote an arbitrary group.

1 Find all the normal subgroups (a) of S_3 and (b) of D_4 .

Prove the following:

2 Every subgroup of an abelian group is normal.

3 The center of any group G is a normal subgroup of G .

4 Let H be a subgroup of G . H is normal iff it has the following property: For all a and b in G , $ab \in H$ iff $ba \in H$.

5 Let H be a subgroup of G . H is normal iff $aH = Ha$ for every $a \in G$.

6 Any intersection of normal subgroups of G is a normal subgroup of G .

E. Further Properties of Normal Subgroups

Let G denote a group, and H a subgroup of G . Prove the following:

- # **1** If H has index 2 in G , then H is normal. (HINT: Use [Exercise D5](#).)
- 2** Suppose an element $a \in G$ has order 2. Then $\langle a \rangle$ is a normal subgroup of G iff a is in the center of G .
- 3** If a is any element of G , $\langle a \rangle$ is a normal subgroup of G iff a has the following property: For any $x \in G$, there is a positive integer k such that $xa = a^kx$.
- 4** In a group G , a *commutator* is any product of the form $aba^{-1}b^{-1}$, where a and b are any elements of G . If a subgroup H of G contains *all* the commutators of G , then H is normal.
- 5** If H and K are subgroups of G , and K is normal, then HK is a subgroup of G . (HK denotes the set of all products hk as h ranges over H and k ranges over K .)
- # **6** Let S be the union of all the cosets Ha such that $Ha = aH$. Then S is a subgroup of G , and H is a normal subgroup of S .

F. Homomorphism and the Order of Elements

If $f: G \rightarrow H$ is a homomorphism, prove each of the following:

- 1** For each element $a \in G$, the order of $f(a)$ is a divisor of the order of a .
- 2** The order of any element $b \neq e$ in the range of f is a common divisor of $|G|$ and $|H|$. (Use part 1.)
- 3** If the range of f has n elements, then $x^n \in \ker f$ for every $x \in G$.
- 4** Let m be an integer such that m and $|H|$ are relatively prime. For any $x \in G$, if $x^m \in \ker f$, then $x \in \ker f$.
- 5** Let the range of f have m elements. If $a \in G$ has order n , where m and n are relatively prime, then a is in the kernel of f . (Use part 1.)
- 6** Let p be a prime. If $\text{ran } f$ has an element of order p , then G has an element of order p .

G. Properties Preserved under Homomorphism

A property of groups is said to be “preserved under homomorphism” if, whenever a group G has that property, every homomorphic image of G does also. In this exercise set, we will survey a few typical properties preserved under homomorphism. If $f: G \rightarrow H$ is a homomorphism of G *onto* H , prove each of the following:

- 1** If G is abelian, then H is abelian.
- 2** If G is cyclic, then H is cyclic.
- 3** If every element of G has finite order, then every element of H has finite order.
- 4** If every element of G is its own inverse, every element of H is its own inverse.
- 5** If every element of G has a square root, then every element of H has a square root.
- 6** If G is finitely generated, then H is finitely generated. (A group is said to be “finitely generated” if it is generated by finitely many of its elements.)

† H. Inner Direct Products

If G is any group, let H and K be normal subgroups of G such that $H \cap K = \{e\}$. Prove the following:

- 1** Let h_1 and h_2 be any two elements of H , and k_1 and k_2 any two elements of K .

$$h_1k_1 = h_2k_2 \quad \text{implies} \quad h_1 = h_2 \quad \text{and} \quad k_1 = k_2$$

(HINT: If $h_1k_1 = h_2k_2$, then $h_2^{-1}h_1 \in H \cap K$ and $k_2k_1^{-1} \in H \cap K$. Explain why.)

2 For any $h \in H$ and $k \in K$, $hk = kh$. (HINT: $hk = kh$ iff $hkh^{-1}k^{-1} = e$. Use the fact that H and K are normal.)

3 Now, make the additional assumption that $G = HK$ that is, every x in G can be written as $x = hk$ for some $h \in H$ and $k \in K$. Then the function $\phi(h,k) = hk$ is an isomorphism from $H \times K$ onto G .

We have thus proved the following: *If H and K are normal subgroups of G , such that $H \cap K = \{e\}$ and $G = HK$, then $G \cong H \times K$. G is sometimes called the inner direct product of H and K .*

† I. Conjugate Subgroups

Let H be a subgroup of G . For any $a \in G$, let $aHa^{-1} = \{axa^{-1} : x \in H\}$; aHa^{-1} is called a conjugate of H . Prove the following:

1 For each $a \in G$, aHa^{-1} is a subgroup of G .

2 For each $a \in G$, $H \cong aHa^{-1}$.

3 H is a normal subgroup of G iff $H = aHa^{-1}$ for every $a \in G$.

In the remaining exercises of this set, let G be a finite group. By the normalizer of H we mean the set $N(H) = \{a \in G : axa^{-1} \in H \text{ for every } x \in H\}$.

4 If $a \in N(H)$, then $aHa^{-1} = H$. (Remember that G is now a finite group.)

5 $N(H)$ is a subgroup of G .

6 $H \subseteq N(H)$. Furthermore, H is a normal subgroup of $N(H)$.

In parts 7–10, let $N = N(H)$.

7 For any $a, b \in G$, $aHa^{-1} = bHb^{-1}$ iff $b^{-1}a \in N(H)$.

8 There is a one-to-one correspondence between the set of conjugates of H and the set of cosets of N . (Thus, there are as many conjugates of H as cosets of N .)

9 H has exactly $(G : N)$ conjugates. In particular, the number of distinct conjugates of H is a divisor of $|G|$.

10 Let K be any subgroup of G , let $K^* = \{Na : a \in K\}$, and let

$$X_K = \{aHa^{-1} : a \in K\}$$

Argue as in part 8 to prove that X_K is in one-to-one correspondence with K^* . Conclude that the number of elements in X_K is a divisor of $|K|$.

QUOTIENT GROUPS

In [Chapter 14](#) we learned to recognize when a group H is a homomorphic image of a group G . Now we will make a great leap forward by learning a method for actually *constructing all the homomorphic images of any group*. This is a remarkable procedure, of great importance in algebra. In many cases this construction will allow us to deliberately select *which* properties of a group G we wish to preserve in a homomorphic image, and which other properties we wish to discard.

The most important instrument to be used in this construction is the notion of a normal subgroup. Remember that a *normal* subgroup of G is any subgroup of G which is closed with respect to conjugates. We begin by giving an elementary property of normal subgroups.

Theorem 1 *If H is a normal subgroup of G , then $aH = Ha$ for every $a \in G$.*

(In other words, there is no distinction between left and right cosets for a normal subgroup.)

PROOF: Indeed, if x is any element of aH , then $x = ah$ for some $h \in H$. But H is closed with respect to conjugates; hence $aha^{-1} \in H$. Thus, $x = ah = (aha^{-1})a$ is an element of Ha . This shows that every element of aH is in Ha ; analogously, every element of Ha is in aH . Thus, $aH = Ha$. ■

Let G be a group and let H be a subgroup of G . There is a way of combining cosets, called *coset multiplication*, which works as follows: *the coset of a , multiplied by the coset of b , is defined to be the coset of ab* . In symbols,

$$Ha \cdot Hb = H(ab)$$

This definition is deceptively simple, for it conceals a fundamental difficulty. Indeed, it is not at all clear that the product of two cosets Ha and Hb , multiplied together in this fashion, is *uniquely defined*. Remember that Ha may be the same coset as Hc (this happens iff c is in Ha), and, similarly, Hb may be the same coset as Hd . Therefore, the product $Ha \cdot Hb$ is the same as the product $He \cdot Hd$. Yet it may easily happen that $H(ab)$ is *not* the same coset as $H(cd)$. Graphically,

$$\begin{array}{ccc} Ha \cdot Hb = H(ab) \\ \parallel \quad \parallel \quad \nparallel \\ Hc \cdot Hd = H(cd) \end{array}$$

For example, if $G = S_3$ and $H = \{\varepsilon, \alpha\}$, then

$$H\beta = \{\beta, \gamma\} = H\gamma$$

$$H\delta = \{\delta, \kappa\} = H\kappa$$

and yet

$$H(\beta \circ \delta) = H\varepsilon \neq H\beta = H(\gamma \circ \kappa)$$

Thus, coset multiplication *does not work* as an operation on the cosets of $H = \{\varepsilon, \alpha\}$ in S_3 . The reason is that, although H is a subgroup of S_3 , H is *not a normal subgroup* of S_3 . If H were a normal subgroup, coset multiplication would work. The next theorem states exactly that!

Theorem 2 *Let H be a normal subgroup of G . If $Ha = He$ and $Hb = Hd$, then $H(ab) = H(cd)$.*

PROOF: If $Ha = Hc$, then $a \in Hc$; hence $a = h_1c$ for some $h_1 \in H$. If $Hb = Hd$, then $b \in Hd$; hence $b = h_2d$ from some $h_2 \in H$. Thus,

$$ab = h_1ch_2d = h_1(ch_2)d$$

But $ch_2 \in cH = Hc$ (the last equality is true by [Theorem 1](#)). Thus, $ch_2 = h_3c$ for some $h_3 \in H$. Returning to ab ,

$$ab = h_1(ch_2)d = h_1(h_3c)d = (h_1h_3)(cd)$$

and this last element is clearly in $H(cd)$.

We have shown that $ab \in H(cd)$. Thus, by Property (1) in [Chapter 13](#), $H(ab) = H(cd)$. ■

We are now ready to proceed with the construction promised at the beginning of the chapter. Let G be a group and let H be a normal subgroup of G . Think of the set which consists of *all the cosets of H* . This set is conventionally denoted by the symbol G/H . Thus, if $Ha, Hb, Hc, \dots$ are cosets of H , then

$$G/H = \{Ha, Hb, Hc, \dots\}$$

We have just seen that *coset multiplication* is a valid operation on this set. In fact,

Theorem 3 *G/H with coset multiplication is a group.*

PROOF: Coset multiplication is associative, because

$$\begin{aligned} Ha \cdot (Hb \cdot Hc) &= Ha \cdot H(bc) = Ha(bc) = H(ab)c \\ &= H(ab) \cdot Hc = (Ha \cdot Hb) \cdot Hc \end{aligned}$$

The identity element of G/H is $H = He$, for $Ha \cdot He = Ha$ and $He \cdot Ha = Ha$ for every coset Ha .

Finally, the inverse of any coset Ha is the coset Ha^{-1} , because $Ha \cdot Ha^{-1} = Haa^{-1} = He$ and $Ha^{-1} \cdot Ha = Ha^{-1}aHe$.

The group G/H is called the *factor group*, or *quotient group* of G by H .

And now, the pièce de résistance:

Theorem 4 G/H is a homomorphic image of G .

PROOF: The most obvious function from G to G/H is the function f which carries every element to its own coset, that is, the function given by

$$f(x) = Hx$$

This function is a homomorphism, because

$$f(xy) = Hxy = Hx \cdot Hy = f(x)f(y)$$

f is called the *natural homomorphism* from G onto G/H . Since there is a homomorphism from G onto G/H , G/H is a homomorphic image of G . ■

Thus, when we construct quotient groups of G , we are, in fact, constructing homomorphic images of G . The quotient group construction is useful because it is a way of actually manufacturing homomorphic images of any group G . In fact, as we will soon see, it is a way of manufacturing *all* the homomorphic images of G .

Our first example is intended to clarify the details of quotient group construction. Let $\mathbf{z}$ be the group of the integers, and let $\langle 6 \rangle$ be the cyclic subgroup of $\mathbf{z}$ which consists of all the multiples of 6. Since $\mathbf{z}$ is abelian, and every subgroup of an abelian group is normal, $\langle 6 \rangle$ is a normal subgroup of $\mathbf{z}$. Therefore, we may form the quotient group $\mathbf{z}/\langle 6 \rangle$. The elements of this quotient group are all the cosets of the subgroup $\langle 6 \rangle$, namely:

$$\langle 6 \rangle + 0 = \{ \dots, -18, -12, -6, 0, 6, 12, 18, \dots \}$$

$$\langle 6 \rangle + 1 = \{ \dots, -17, -11, -5, 1, 7, 13, 19, \dots \}$$

$$\langle 6 \rangle + 2 = \{ \dots, -16, -10, -4, 2, 8, 14, 20, \dots \}$$

$$\langle 6 \rangle + 3 = \{ \dots, -15, -9, -3, 3, 9, 15, 21, \dots \}$$

$$\langle 6 \rangle + 4 = \{ \dots, -14, -8, -2, 4, 10, 16, 22, \dots \}$$

$$\langle 6 \rangle + 5 = \{ \dots, -13, -7, -1, 5, 11, 17, 23, \dots \}$$

These are *all* the different cosets of $\langle 6 \rangle$, for it is easy to see that $\langle 6 \rangle + 6 = \langle 6 \rangle + 0$, $\langle 6 \rangle + 7 = \langle 6 \rangle + 1$, $\langle 6 \rangle + 8 = \langle 6 \rangle + 2$, and so on.

Now, the operation on $\mathbf{z}$ is denoted by $+$, and therefore we will call the operation on the cosets *coset addition* rather than coset multiplication. But nothing is changed except the name; for example, the coset $\langle 6 \rangle + 1$ added to the coset $\langle 6 \rangle + 2$ is the coset $\langle 6 \rangle + 3$. The coset $\langle 6 \rangle + 3$ added to the coset $\langle 6 \rangle + 4$ is the coset $\langle 6 \rangle + 7$, which is the same as $\langle 6 \rangle + 1$. To simplify our notation, let us agree to write the cosets in the following shorter form:

$$\bar{0} = \langle 6 \rangle + 0 \quad \bar{1} = \langle 6 \rangle + 1 \quad \bar{2} = \langle 6 \rangle + 2$$

$$\bar{3} = \langle 6 \rangle + 3 \quad \bar{4} = \langle 6 \rangle + 4 \quad \bar{5} = \langle 6 \rangle + 5$$

Then $\mathbf{z}/\langle 6 \rangle$ consists of the six elements $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$, and $\bar{5}$, and its operation is summarized in the following table:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

The reader will perceive immediately the similarity between this group and $\mathbf{Z}_6$. As a matter of fact, the quotient group construction of $\mathbf{Z}/\langle 6 \rangle$ is considered to be the rigorous way of constructing $\mathbf{Z}_6$. So from now on, we will consider $\mathbf{Z}_6$ to be the same as $\mathbf{Z}/\langle 6 \rangle$; and, in general, we will consider $\mathbf{Z}_n$ to be the same as $\mathbf{Z}/\langle n \rangle$. In particular, we can see that for any n , $\mathbf{Z}_n$ is a homomorphic image of $\mathbf{Z}$.

Let us repeat: The motive for the quotient group construction is that it gives us a way of actually *producing* all the homomorphic images of any group G . However, what is even more fascinating about the quotient group construction is that, in practical instances, we can often choose H so as to “factor out” unwanted properties of G , and preserve in G/H only “desirable” traits. (By “desirable” we mean desirable within the context of some specific application or use.) Let us look at a few examples.

First, we will need two simple properties of cosets, which are given in the next theorem.

Theorem 5 *Let G be a group and H a subgroup of G . Then*

- (i) $Ha = Hb$ iff $ab^{-1} \in H$ and
- (ii) $Ha = H$ iff $a \in H$

PROOF: If $Ha = Hb$, then $a \in Hb$, so $a = hb$ for some $h \in H$. Thus,

$$ab^{-1} = h \in H$$

If $ab^{-1} \in H$, then $ab^{-1} = h$ for $h \in H$, and therefore $a = hb \in Hb$. It follows by Property (1) of [Chapter 13](#) that $Ha = Hb$.

This proves (i). It follows that $Ha = He$ iff $ae^{-1} = a \in H$, which proves (ii). ■

For our first example, let G be an abelian group and let H consist of *all the elements of G which have finite order*. It is easy to show that H is a subgroup of G . (The details may be supplied by the reader.) Remember that in an abelian group every subgroup is normal; hence H is a normal subgroup of G , and therefore we may form the quotient group G/H . We will show next that in G/H , *no* element except the neutral element has finite order.

For suppose G/H has an element Hx of finite order. Since the neutral element of G/H is H , this means there is an integer $m \neq 0$ such that $(Hx)^m = H$, that is, $Hx^m = H$. Therefore, by [Theorem 5\(ii\)](#), $x^m \in H$, so x^m has finite order, say t :

$$(x^m)^t = x^{mt} = e$$

But then x has finite order, so $x \in H$. Thus, by [Theorem 5\(ii\)](#), $Hx = H$. This proves that in G/H , the only element Hx of finite order is the neutral element H .

Let us recapitulate: If H is the subgroup of G which consists of all the elements of G which have

finite order, then in G/H , *no* element (except the neutral element) has finite order. Thus, in a sense, we have “*factored out*” *all the elements of finite order (they are all in H) and produced a quotient group G/H whose elements all have infinite order* (except for the neutral element, which necessarily has order 1).

Our next example may bring out this idea even more clearly. Let G be an arbitrary group; by a *commutator* of G we mean any element of the form $aba^{-1}b^{-1}$ where a and b are in G . The reason such a product is called a commutator is that

$$aba^{-1}b^{-1} = e \quad \text{iff} \quad ab = ba$$

In other words, $aba^{-1}b^{-1}$ reduces to the neutral element whenever a and b commute—and *only* in that case! Thus, in an abelian group all the commutators are equal to e . In a group which is not abelian, the number of distinct commutators may be regarded as a measure of the extent to which G departs from being commutative. (The fewer the commutators, the closer the group is to being an abelian group.)

We will see in a moment that if H is a subgroup of G which *contains all the commutators of G* , then G/H is abelian! What this means, in a fairly accurate sense, is that *when we factor out the commutators of G we get a quotient group which has no commutators* (except, trivially, the neutral element) *and which is therefore abelian*.

To say that G/H is abelian is to say that for any two elements Hx and Hy in G/H , $HxHy = HyHx$; that is, $Hxy = Hyx$. But by [Theorem 5\(ii\)](#),

$$Hxy = Hyx \quad \text{iff} \quad xy(yx)^{-1} \in H$$

Now $xy(yx)^{-1}$ is the commutator $xyx^{-1}y^{-1}$; so if all commutators are in H , then G/H is abelian.

EXERCISES

A. Examples of Finite Quotient Groups

In each of the following, G is a group and H is a normal subgroup of G . List the elements of G/H and then write the table of G/H .

Example $G = \mathbf{Z}_6$ and $H = \{0, 3\}$

The elements of G/H are the three cosets $H = H + 0 = \{0, 3\}$, $H + 1 = \{1, 4\}$, and $H + 2 = \{2, 5\}$. (Note that $H + 3$ is the same as $H + 0$, $H + 4$ is the same as $H + 1$, and $H + 5$ is the same as $H + 2$.) The table of G/H is

+	H	$H + 1$	$H + 2$
H	H	$H + 1$	$H + 2$
$H + 1$	$H + 1$	$H + 2$	H
$H + 2$	$H + 2$	H	$H + 1$

1 $G = \mathbf{Z}_{10}$, $H = \{0, 5\}$. (Explain why $G/H \cong \mathbf{Z}_5$.)

2 $G = S_3$, $H = \{\varepsilon, \beta, \delta\}$.

- 3 $G = D_4$, $H = \{R_0, R_2\}$. (See page 73.)
- 4 $G = D_4$, $H = \{R_0, R_2, R_4, R_5\}$.
- 5 $G = \mathbf{z}_4 \times \mathbf{z}_2$, $H = \langle(0,1)\rangle =$ the subgroup of $\mathbf{z}_4 \times \mathbf{z}_2$ generated by $(0,1)$.
- 6 $G = P_3$, $H = \{\emptyset, \{1\}\}$. (P_3 is the group of subsets of $\{1, 2, 3\}$.)

B. Examples of Quotient Groups of $\mathbb{R} \times \mathbb{R}$

In each of the following, H is a subset of $\mathbb{R} \times \mathbb{R}$.

(a) Prove that H is a normal subgroup of $\mathbb{R} \times \mathbb{R}$. (Remember that every subgroup of an abelian group is normal.)

(b) In geometrical terms, describe the elements of the quotient group G/H .

(c) In geometrical terms or otherwise, describe the operation of G/H .

1 $H = \{(x,0):x \in \mathbb{R}\}$

2 $H = \{(x,y):y = -x\}$

3 $H = \{(x,y):y = 2x\}$

C. Relating Properties of H to Properties of G/H

In parts 1-5 below, G is a group and H is a normal subgroup of G . Prove the following (Theorem 5 will play a crucial role):

1 If $x^2 \in H$ for every $x \in G$, then every element of G/H is its own inverse. Conversely, if every element of G/H is its own inverse, then $x^2 \in H$ for all $x \in G$.

2 Let m be a fixed integer. If $x^m \in H$ for every $x \in G$, then the order of every element in G/H is a divisor of m . Conversely, if the order of every element in G/H is a divisor of m , then $x^m \in H$ for every $x \in G$.

3 Suppose that for every $x \in G$, there is an integer n such that $x^n \in H$; then every element of G/H has finite order. Conversely, if every element of G/H has finite order, then for every $x \in G$ there is an integer n such that $x^n \in H$.

4 Every element of G/H has a square root iff for every $x \in G$, there is some $y \in G$ such that $xy^2 \in H$.

5 G/H is cyclic iff there is an element $a \in G$ with the following property: for every $x \in G$, there is some integer n such that $xa^n \in H$.

6 If G is an abelian group, let H_p be the set of all $x \in H$ whose order is a power of p . Prove that H_p is a subgroup of G . Prove that G/H_p has no elements whose order is a nonzero power of p .

7 (a) If G/H is abelian, prove that H contains all the commutators of G .

(b) Let K be a normal subgroup of G , and H a normal subgroup of K . If G/H is abelian, prove that G/K and K/H are both abelian.

D. Properties of G Determined by Properties of G/H and H

There are some group properties which, if they are true in G/H and in H , must be true in G . Here is a sampling. Let G be a group, and H a normal subgroup of G . Prove the following:

1 If every element of G/H has finite order, and every element of H has finite order, then every element of G has finite order.

- 2** If every element of G/H has a square root, and every element of H has a square root, then every element of G has a square root. (Assume G is abelian.)
- 3** Let p be a prime number. If G/H and H are p -groups, then G is a p -group. A group G is called a p -group if the order of every element x in G is a power of p .
- # 4** If G/H and H are finitely generated, then G is finitely generated. (A group is said to be finitely generated if it is generated by a finite subset of its elements.)

E. Order of Elements in Quotient Groups

Let G be a group, and H a normal subgroup of G . Prove the following:

- 1** For each element $a \in G$, the order of the element Ha in G/H is a divisor of the order of a in G . (HINT: Use [Chapter 14, Exercise F1](#).)
- 2** If $(G:H) = m$, the order of every element of G/H is a divisor of m .
- 3** If $(G:H) = p$, where p is a prime, then the order of every element $a \notin H$ in G is a multiple of p . (Use part 1.)
- 4** If G has a normal subgroup of index p , where p is a prime, then G has at least one element of order p .
- 5** If $(G:H) = m$, then $a^m \in H$ for every $a \in G$.
- # 6** In $\mathbb{Q}/\mathbb{Z}$, every element has finite order.

† F. Quotient of a Group by Its Center

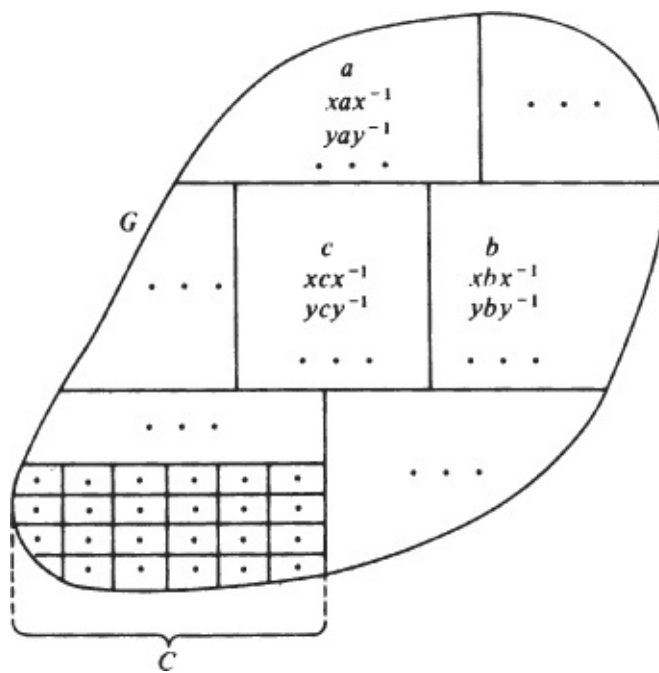
The *center* of a group G is the normal subgroup C of G consisting of all those elements of G which commute with every element of G . Suppose the quotient group G/C is a cyclic group; say it is generated by the element Ca of G/C . Prove parts 1-3:

- 1** For every $x \in G$, there is some integer m such that $Cx = Ca^m$.
- 2** For every $x \in G$, there is some integer m such that $x = ca^m$, where $c \in C$.
- 3** For any two elements x and y in G , $xy = yx$. (HINT: Use part 2 to write $x = ca^m$, $y = c'a^n$, and remember that $c, c' \in C$.)
- 4** Conclude that if G/C is cyclic, then G is abelian.

† G. Using the Class Equation to Determine the Size of the Center

{Prerequisite: [Chapter 13, Exercise I](#).)

Let G be a finite group. Elements a and b in G are called *conjugates* of one another (in symbols, $a \sim b$) iff $a = xbx^{-1}$ for some $x \in G$ (this is the same as $b = x^{-1}ax$). The relation $\sim$ is an equivalence relation in G ; the equivalence class of any element a is called its *conjugacy class*. Hence G is partitioned into conjugacy classes (as shown in the diagram); the size of each conjugacy class divides the order of G . (For these facts, see [Chapter 13, Exercise I](#).)



“Each element of the center C is alone in its conjugacy class.”

Let $S_1, S_2, \dots, S_t$ be the distinct conjugacy classes of G , and let $k_1, k_2, \dots, k_t$ be their sizes. Then $|G| = k_1 + k_2 + \dots + k_t$ (This is called the *class equation* of G .)

Let G be a group whose order is a power of a prime p , say $|G| = p^k$. Let C denote the center of G . Prove parts 1-3:

- 1 The conjugacy class of a contains a (and no other element) iff $a \in C$.
 - 2 Let c be the order of C . Then $|G| = c + k_s + k_{s+1} + \dots + k_t$, where $k_s, \dots, k_t$ are the sizes of all the distinct conjugacy classes of elements $x \notin C$.
 - 3 For each $i \in \{s, s+1, \dots, t\}$, k_i is equal to a power of p . (See [Chapter 13, Exercise I6](#).)
 - 4 Solving the equation $|G| = c + k_s + \dots + k_t$ for c , explain why c is a multiple of p .
- We may conclude from part 4 that C must contain more than just the one element e ; in fact, $|C|$ is a multiple of p .
- 5 Prove: If $|G| = p^2$, G must be abelian. (Use the preceding Exercise F.)
 - # 6 Prove: If $|G| = p^2$, then either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

† H. Induction on $|G|$: An Example

Many theorems of mathematics are of the form “ $P(n)$ is true for every positive integer n .” [Here, $P(n)$ is used as a symbol to denote some statement involving n .] Such theorems can be proved by induction as follows:

- (a) Show that $P(n)$ is true for $n = 1$.
- (b) For any fixed positive integer k , show that, if $P(n)$ is true for every $n < k$, then $P(n)$ must also be true for $n = k$.

If we can show (a) and (b), we may safely conclude that $P(n)$ is true for all positive integers n .

Some theorems of algebra can be proved by induction on the order n of a group. Here is a classical example: Let G be a finite abelian group. We will show that G must contain at least one element of

order p , for every prime factor p of $|G|$. If $|G| = 1$, this is true by default, since no prime p can be a factor of 1. Next, let $|G| = k$, and suppose our claim is true for every abelian group whose order is less than k . Let p be a prime factor of k .

Take any element $a \neq e$ in G . If $\text{ord}(a) = p$ or a multiple of p , we are done!

- 1 If $\text{ord}(a) = tp$ (for some positive integer t), what element of G has order p ?
- 2 Suppose $\text{ord}(a)$ is *not equal to a multiple of p* . Then $G/\langle a \rangle$ is a group having fewer than k elements. (Explain why.) The order of $G/\langle a \rangle$ is a multiple of p . (Explain why.)
- 3 Why must $G/\langle a \rangle$ have an element of order p ?
- 4 Conclude that G has an element of order p . (HINT: Use Exercise E1.)

THE FUNDAMENTAL HOMOMORPHISM THEOREM

Let G be any group. In [Chapter 15](#) we saw that every quotient group of G is a homomorphic image of G . Now we will see that, conversely, every homomorphic image of G is a quotient group of G . More exactly, *every homomorphic image of G is isomorphic to a quotient group of G .*

It will follow that, for any groups G and H , H is a homomorphic image of G iff H is (or is isomorphic to) a quotient group of G . Therefore, the notions of *homomorphic image* and of *quotient group* are interchangeable.

The thread of our reasoning begins with a simple theorem.

Theorem 1 *Let $f: G \rightarrow H$ be a homomorphism with kernel K . Then*

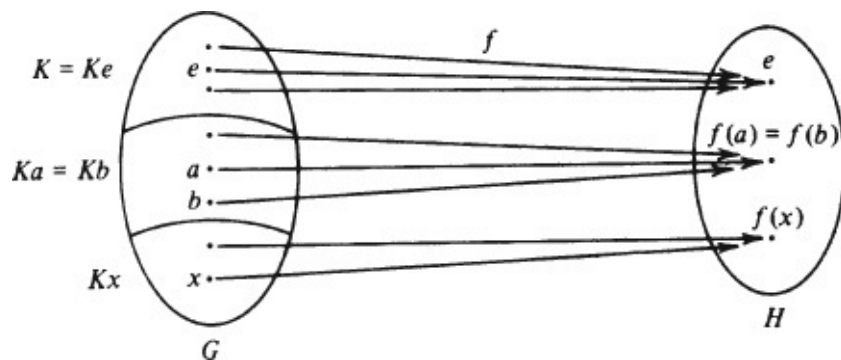
$$f(a) = f(b) \quad \text{iff} \quad Ka = Kb$$

(In other words, any two elements a and b in G have the *same image* under f iff they are in the same coset of K .)

Indeed,

$$\begin{aligned} f(a) = f(b) & \quad \text{iff} \quad f(a)[f(b)]^{-1} = e \\ & \quad \text{iff} \quad f(ab^{-1}) = e \\ & \quad \text{iff} \quad ab^{-1} \in K \\ & \quad \text{iff} \quad Ka = Kb \quad (\text{by Chapter 15, theorem 5i}) \end{aligned}$$

What does this theorem really tell us? It says that if f is a homomorphism from G to H with kernel K , then all the elements in any fixed coset of K have the same image, and, conversely, elements which have the same image are in the same coset of K .



It is therefore clear already that there is a one-to-one correspondence matching cosets of K with elements in H . It remains only to show that this correspondence is an isomorphism. But first, how exactly does this correspondence match up specific cosets of K with specific elements of H ? Clearly, for each x , the coset Kx is matched with the element $f(x)$. Once this is understood, the next theorem is easy.

Theorem 2 Let $f: G \rightarrow H$ be a homomorphism of G onto H . If K is the kernel of f , then

$$H \cong G/K$$

PROOF: To show that G/K is isomorphic to H , we must look for an isomorphism from G/K to H . We have just seen that there is a function from G/K to H which matches each coset Kx with the element $f(x)$; call this function ϕ . Thus, ϕ is defined by the identity

$$\phi(Kx) = f(x)$$

This definition does not make it obvious that $\phi(Kx)$ is *uniquely defined*. (If it is not, then we cannot properly call ϕ a function.) We must make sure that if Ka is the same coset as Kb , then $\phi(Ka)$ is the same as $\phi(Kb)$: that is,

$$\text{if } Ka = Kb \text{ then } f(a) = f(b)$$

As a matter of fact, this is true by [Theorem 1](#).

Now, let us show that ϕ is an isomorphism:

ϕ is *injective*: If $\phi(Ka) = \phi(Kb)$ then $f(a) = f(b)$; so by [Theorem 1](#), $Ka = Kb$.

ϕ is *surjective*, because every element of H is of the form $f(x) = \phi(Kx)$. Finally, $\phi(Ka \cdot Kb) = \phi(Kab) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$.

Thus, ϕ is an isomorphism from G/K onto H . ■

[Theorem 2](#) is often called the *fundamental homomorphism theorem*. It asserts that every homomorphic image of G is isomorphic to a quotient group of G . Which specific quotient group of G ? Well, if f is a homomorphism from G onto H , then H is isomorphic to the quotient group of G by the kernel of f .

The fact that f is a homomorphism from G onto H may be symbolized by writing

$$f: G \longrightarrow H$$

Furthermore, the fact that K is the kernel of this homomorphism may be indicated by writing

$$f: G \xrightarrow{K} H$$

Thus, in capsule form, the fundamental homomorphism theorem says that

$$\text{If } f : G \xrightarrow{K} H \text{ then } H \cong G/K$$

Let us see a few examples:

We saw in the opening paragraph of [Chapter 14](#) that

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

is a homomorphism from $\mathbf{z}_6$ onto $\mathbf{z}_3$. Visibly, the kernel of f is $\{0, 3\}$, which is the subgroup of $\mathbf{z}_6$ generated by $\langle 3 \rangle$, that is, the subgroup (3) . This situation may be symbolized by writing

$$f : \mathbb{Z}_6 \xrightarrow{\langle 3 \rangle} \mathbb{Z}_3$$

We conclude by [Theorem 2](#) that

$$\mathbf{z}_3 \cong \mathbf{z}_6 / \langle 3 \rangle$$

For another kind of example, let G and H be any groups and consider their direct product $G \times H$. Remember that $G \times H$ consists of all the ordered pairs (x, y) as x ranges over G and y ranges over H . You multiply ordered pairs by multiplying corresponding components; that is, the operation on $G \times H$ is given by

$$(a, b) \cdot (c, d) = (ac, bd)$$

Now, let f be the function from $G \times H$ onto H given by

$$f(x, y) = y$$

It is easy to check that f is a homomorphism. Furthermore, (x, y) is in the kernel of f iff $f(x, y) = y = e$. This means that the kernel of f consists of all the ordered pairs whose second component is e . Call this kernel G^* ; then

$$G^* = \{(x, e) : x \in G\}$$

We symbolize all this by writing

$$f : G \times H \xrightarrow{G^*} H$$

By the fundamental homomorphism theorem, we deduce that $H \cong (G \times H)/G^*$. [It is easy to see that G^* is an isomorphic copy of G ; thus, identifying G^* with G , we have shown that, roughly speaking, $(G \times H)/G \cong H$.]

Other uses of the fundamental homomorphism theorem are given in the exercises.

EXERCISES

In the exercises which follow, FHT will be used as an abbreviation for fundamental homomorphism

theorem.

A. Examples of the FHT Applied to Finite Groups

In each of the following, use the fundamental homomorphism theorem to prove that the two given groups are isomorphic. Then display their tables.

Example $\mathbf{z}_2$ and $\mathbf{z}_6/\langle 2 \rangle$.

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

is a homomorphism from $\mathbf{z}_6$ onto $\mathbf{z}_2$. (Do not prove that f is a homomorphism.) The kernel of f is $\{0, 2, 4\} = \langle 2 \rangle$. Thus,

$$f: \mathbb{Z}_6 \xrightarrow{\langle 2 \rangle} \mathbb{Z}_2$$

It follows by the FHT that $\mathbf{z}_2 \cong \mathbf{z}_6/\langle 2 \rangle$.

1 $\mathbf{z}_5$ and $\mathbf{z}_{20}/\langle 5 \rangle$.

2 $\mathbf{z}_3$ and $\mathbf{z}_6/\langle 3 \rangle$.

3 $\mathbf{z}_2$ and $S_3/\{\varepsilon, \beta, \delta\}$.

4 P_2 and P_3/K , where $K = \{0, \{c\}\}$. [HINT: Consider the function $f(C) = C \cap \{a, b\}$. P_3 is the group of subsets of $\{a, b, c\}$, and P_2 of $\{a, b\}$.]

5 $\mathbf{z}_3$ and $(\mathbf{z}_3 \times \mathbf{z}_3)/K$, where $K = \{(0, 0), (1, 1), (2, 2)\}$. [HINT: Consider the function $f(a, b) = a - b$ from $\mathbf{z}_3 \times \mathbf{z}_3$ to $\mathbf{z}_3$.]

B. Example of the FHT Applied to $\mathcal{F}(\mathbb{R})$

Let $\alpha: \mathcal{F}(\mathbb{R}) \rightarrow \mathbb{R}$ be defined by $\alpha(f) = f(1)$ and let $\beta: \mathcal{F}(\mathbb{R}) \rightarrow \mathbb{R}$ be defined by $\beta(f) = f(2)$.

1 Prove that α and β are homomorphisms from $\mathcal{F}(\mathbb{R})$ onto $\mathbb{R}$.

2 Let J be the set of all the functions from $\mathbb{R}$ to $\mathbb{R}$ whose graph passes through the point $(1, 0)$ and let K be the set of all the functions whose graph passes through $(2, 0)$. Use the FHT to prove that $\mathbb{R} \cong \mathcal{F}(\mathbb{R})/J$ and $\mathbb{R} \cong \mathcal{F}(\mathbb{R})/K$

3 Conclude that $\mathcal{F}(\mathbb{R})/J \cong \mathcal{F}(\mathbb{R})/K$

C. Example of the FHT Applied to Abelian Groups

Let G be an abelian group. Let $H = \{x^2: x \in G\}$ and $K = \{x \in G: x^2 = e\}$.

1 Prove that $f(x) = x^2$ is a homomorphism of G onto H .

2 Find the kernel of f .

3 Use the FHT to conclude that $H \cong G/K$

† D. Group of Inner Automorphisms of a Group G

Let G be a group. By an *automorphism* of G we mean an isomorphism $f: G \rightarrow G$.

1 The symbol $\text{Aut}(G)$ is used to designate the set of all the automorphisms of G . Prove that the set $\text{Aut}(G)$, with the operation $\circ$ of composition, is a group *by proving that $\text{Aut}(G)$ is a subgroup of S_G* .

2 By an *inner automorphism* of G we mean any function ϕ_a of the following form:

$$\text{for every } x \in G \quad \phi_a(x) = axa^{-1}$$

Prove that every inner automorphism of G is an automorphism of G .

3 Prove that, for arbitrary $a, b \in G$.

$$\phi_a \circ \phi_b = \phi_{ab} \quad \text{and} \quad (\phi_a)^{-1} = \phi_{a^{-1}}$$

4 Let $I(G)$ designate the set of all the inner automorphisms of G . That is, $I(G) = \{\phi_a: a \in G\}$. Use part 3 to prove that $I(G)$ is a subgroup of $\text{Aut}(G)$. Explain why $I(G)$ is a group.

5 By the *center* of G we mean the set of all those elements of G which commute with every element of G , that is, the set C defined by

$$C = \{a \in G: ax = xa \text{ for every } x \in G\}$$

Prove that $a \in C$ if and only if $axa^{-1} = x$ for every $x \in G$.

6 Let $h: G \rightarrow I(G)$ be the function defined by $h(a) = \phi_a$. Prove that h is a homomorphism from G onto $I(G)$ and that C is its kernel.

7 Use the FHT to conclude that $I(G)$ is isomorphic with G/C .

† E. The FHT Applied to Direct Products of Groups

Let G and H be groups. Suppose J is a normal subgroup of G and K is a normal subgroup of H .

1 Show that the function $f(x, y) = (Jx, Ky)$ is a homomorphism from $G \times H$ onto $(G/J) \times (H/K)$.

2 Find the kernel of f .

3 Use the FHT to conclude that $(G \times H)/(J \times K) \cong (G/J) \times (H/K)$.

† F. First Isomorphism Theorem

Let G be a group; let H and K be subgroups of G , with H a normal subgroup of G . Prove the following:

1 $H \cap K$ is a normal subgroup of K

2 If $HK = \{xy: x \in H \text{ and } y \in K\}$, then HK is a subgroup of G .

3 H is a normal subgroup of HK .

4 Every member of the quotient group HK/H may be written in the form Hk for some $k \in K$.

5 The function $f(k) = Hk$ is a homomorphism from K onto HK/H , and its kernel is $H \cap K$.

6 By the FHT, $K/(H \cap K) \cong HK/H$. (This is referred to as the *first isomorphism theorem*.)

† G. A Sharper Cayley Theorem

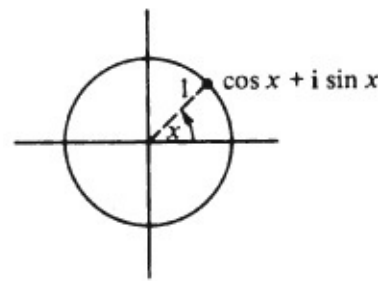
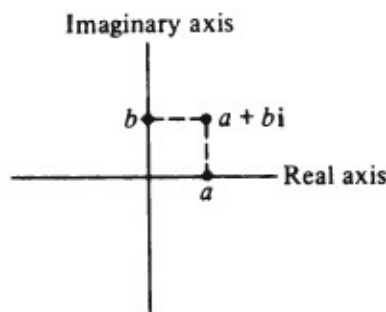
If H is a subgroup of a group G , let X designate the set of all the left cosets of H in G . For each element $a \in G$, define $p_a: X \rightarrow X$ as follows:

$$p_a(xH) = (ax)H$$

- 1 Prove that each p_a is a permutation of X .
- 2 Prove that $h: G \rightarrow S_X$ defined by $h(a) = p_a$ is a homomorphism.
- # 3 Prove that the set $\{a \in H: xax^{-1} \in H \text{ for every } x \in G\}$, that is, the set of all the elements of H whose conjugates are all in H , is the kernel of h .
- 4 Prove that if H contains no normal subgroup of G except $\{e\}$, then G is isomorphic to a subgroup of S_X .

† H. Quotient Groups Isomorphic to the Circle Group

Every complex number $a + bi$ may be represented as a point in the complex plane.



The *unit circle* in the complex plane consists of all the complex numbers whose distance from the origin is 1; thus, clearly, the unit circle consists of all the complex numbers which can be written in the form

$$\cos x + i \sin x$$

for some real number x .

- # 1 For each $x \in \mathbb{R}$, it is conventional to write $\text{cis } x = \cos x + i \sin x$. Prove that $\text{cis } (x + y) = (\text{cis } x)(\text{cis } y)$.
- 2 Let T designate the set $\{\text{cis } x: x \in \mathbb{R}\}$, that is, the set of all the complex numbers lying on the unit circle, with the operation of multiplication. Use part 1 to prove that T is a group. (T is called the *circle group*.)
- 3 Prove that $f(x) = \text{cis } x$ is a homomorphism from $\mathbb{R}$ onto T .
- 4 Prove that $\ker f = \{2n\pi: n \in \mathbb{Z}\} = \langle 2\pi \rangle$.
- 5 Use the FHT to conclude that $T \cong \mathbb{R}/\langle 2\pi \rangle$.
- 6 Prove that $g(x) = \text{cis } 2\pi x$ is a homomorphism from $\mathbb{R}$ onto T , with kernel $\mathbb{Z}$.
- 7 Conclude that $T \cong \mathbb{R}/\mathbb{Z}$.

† I. The Second Isomorphism Theorem

Let H and K be normal subgroups of a group G , with $H \subseteq K$. Define $\phi: G/H \rightarrow G/K$ by $\phi(Ha) = Ka$. Prove parts 1–4:

- 1 ϕ is a well-defined function. [That is, if $Ha = Hb$, then $\phi(Ha) = \phi(Hb)$.]

2 ϕ is a homomorphism.

3 ϕ is surjective.

4 $\ker \phi \subseteq K/H$

5 Conclude (using the FHT) that $(G/H)K/H \cong G/K$.

† J. The Correspondence Theorem

Let f be a homomorphism from G onto H with kernel K :

$$f : G \xrightarrow{K} H$$

If S is any subgroup of H , let $S^* = \{x \in G : f(x) \in S\}$. Prove:

1 S^* is a subgroup of G .

2 $K \subseteq S^*$.

3 Let g be the restriction of f to S^* . [That is, $g(x) = f(x)$ for every $x \in S^*$, and S^* is the domain of g .] Then g is a homomorphism from S^* onto S , and $K = \ker g$.

4 $S \cong S^*/K$.

† K. Cauchy's Theorem

Prerequisites: [Chapter 13, Exercise I](#), and [Chapter 15, Exercises G and H](#).

If G is a group and p is any prime divisor of $|G|$, it will be shown here that G has at least one element of order p . This has already been shown for abelian groups in [Chapter 15, Exercise H4](#). Thus, assume here that G is not abelian. The argument will proceed by induction; thus, let $|G| = k$, and assume our claim is true for any group of order less than k . Let C be the center of G , let C_a be the centralizer of a for each $a \in G$, and let $k = c + k_s + \dots + k_t$ be the class equation of G , as in [Chapter 15, Exercise G2](#).

1 Prove: If p is a factor of $|C_a|$ for any $a \in G$, where $a \notin C$, we are done. (Explain why.)

2 Prove that for any $a \notin C$ in G , if p is not a factor of $|C_a|$, then p is a factor of $(G : C_a)$.

3 Solving the equation $k = c + k_s + \dots + k_t$ for c , explain why p is a factor of c . We are now done. (Explain why.)

† L. Subgroups of p -Groups (Prelude to Sylow)

Prerequisites: [Exercise J](#); [Chapter 15, Exercises G and H](#).

Let p be a prime number. A p -group is any group whose order is a power of p . It will be shown here that if $|G| = p^k$ then G has a normal subgroup of order p^m for every m between 1 and k . The proof is by induction on $|G|$; we therefore assume our result is true for all p -groups smaller than G . Prove parts 1 and 2:

1 There is an element a in the center of G such that $\text{ord}(a) = p$. (See [Chapter 15, Exercises G and H](#).)

2 $\langle a \rangle$ is a normal subgroup of G .

3 Explain why it may be assumed that $G/\langle a \rangle$ has a normal subgroup of order p^{m-1} .

4 Use [Exercise J4](#) to prove that G has a normal subgroup of order p^m .

Exercise sets M through Q are included as a challenge for the ambitious reader. Two important results of group theory are proved in these exercises: one is called Sylow's theorem, the other is called the basis theorem of finite abelian groups.

† M. p -Sylow Subgroups

Prerequisites: [Exercises J and K](#) of this Chapter, [Exercise I1](#) of [Chapter 14](#), and [Exercise D3](#) of [Chapter 15](#).

Let p be a prime number. A finite group G is called a p -group if the order of every element x in G is a power of p . (The orders of different elements may be different powers of p .) If H is a subgroup of any finite group G , and H is a p -group, we call H a p -subgroup of G . Finally, if K is a p -subgroup of G , and K is maximal (in the sense that K is not contained in any larger p -subgroup of G), then K is called a p -Sylow subgroup of G .

- 1 Prove that the order of any p -group is a power of p . (HINT: Use [Exercise K](#).)
- 2 Prove that every conjugate of a p -Sylow subgroup of G is a p -Sylow subgroup of G .

Let K be a p -Sylow subgroup of G , and $N = N(K)$ the normalizer of K .

- 3 Let $a \in N$, and suppose the order of Ka in N/K is a power of p . Let $S = \langle Ka \rangle$ be the cyclic subgroup of N/K generated by Ka . Prove that N has a subgroup S^* such that S^*/K is a p -group. (HINT: See [Exercise J4](#).)

- 4 Prove that S^* is a p -subgroup of G (use [Exercise D3](#), [Chapter 15](#)). Then explain why $S^* = K$, and why it follows that $Ka = K$.

- 5 Use parts 3 and 4 to prove: no element of N/K has order a power of p (except, trivially, the identity element).

- 6 If $a \in N$ and the order of p is a power of p , then the order of Ka (in N/K) is also a power of p . (Why?) Thus, $Ka = K$. (Why?)

- 7 Use part 6 to prove: if $aKa^{-1} = K$ and the order of a is a power of p , then $a \in K$.

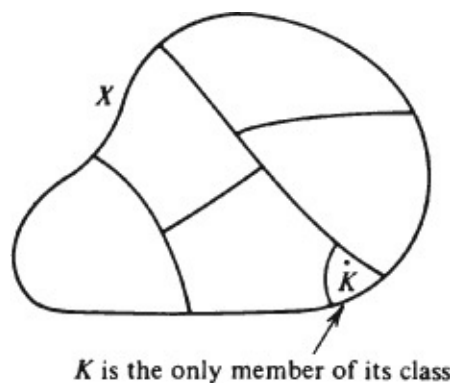
† N. Sylow's Theorem

Prerequisites: [Exercises K](#) and [M](#) of this Chapter and [Exercise I](#) of [Chapter 14](#).

Let G be a finite group, and K a p -Sylow subgroup of G . Let X be the set of all the conjugates of K . See [Exercise M2](#). If $C_1, C_2 \in X$, let $C_1 \sim C_2$ iff $C_1 = aC_2a^{-1}$ for some $a \in K$.

- 1 Prove that $\sim$ is an equivalence relation on X .

Thus, $\sim$ partitions X into equivalence classes. If $C \in X$ let the equivalence class of C be denoted by $[C]$.



- 2 For each $C \in X$, prove that the number of elements in $[C]$ is a divisor of $|K|$. (HINT: Use [Exercise I10](#) of [Chapter 14](#).) Conclude that for each $C \in X$, the number of elements in $[C]$ is either 1 or a power of p .
- 3 Use [Exercise M7](#) to prove that the only class with a single element is $[K]$,
- 4 Use parts 2 and 3 to prove that the number of elements in X is $kp + 1$, for some integer k .
- 5 Use part 4 to prove that $(G:N)$ is *not* a multiple of p .
- 6 Prove that $(N:K)$ is *not* a multiple of p . (Use [Exercises K](#) and [M5](#).)
- 7 Use parts 5 and 6 to prove that $(G:K)$ is *not* a multiple of p .
- 8 Conclude: Let G be a finite group of order $p^k m$, where p is not a factor of m . Every p -Sylow subgroup K of G has order p^k .

Combining part 8 with [Exercise L](#) gives

Let G be a finite group and let p be a prime number. For each n such that p^n divides $|G|$, G has a subgroup of order p^n .

This is known as Sylow's theorem.

† O. Lifting Elements from Cosets

The purpose of this exercise is to prove a property of cosets which is needed in [Exercise Q](#). Let G be a finite abelian group, and let a be an element of G such that $\text{ord}(a)$ is a multiple of $\text{ord}(x)$ for every $x \in G$. Let $H = \langle a \rangle$. We will prove:

For every $x \in G$, there is some $y \in G$ such that $Hx = Hy$ and $\text{ord}(y) = \text{ord}(Hy)$.

This means that every coset of H contains an element y whose order is the same as the coset's order.

Let x be any element in G , and let $\text{ord}(a) = t$, $\text{ord}(x) = s$, and $\text{ord}(Hx) = r$.

- 1 Explain why r is the least positive integer such that x^r equals some power of a , say $x^r = a^m$.
- 2 Deduce from our hypotheses that r divides s , and s divides t .

Thus, we may write $s = ru$ and $t = sv$, so in particular, $t = ruv$.

- 3 Explain why $a^{mu} = e$, and why it follows that $mu = tz$ for some integer z . Then explain why $m = rvz$.
- 4 Setting $y = xa^{-vz}$, prove that $Hx = Hy$ and $\text{ord}(y) = r$, as required.

† P. Decomposition of a Finite Abelian Group into p -Groups

Let G be an abelian group of order $p^k m$, where p^k and m are relatively prime (that is, p^k and m have no common factors except ± 1). (REMARK: If two integers j and k are relatively prime, then there are integers s and t such that $sj + tk = 1$. This is proved on page 220.)

Let G_{p^k} be the subgroup of G consisting of all elements whose order divides p^k . Let G_m be the subgroup of G consisting of all elements whose order divides m . Prove:

- 1 For any $x \in G$ and integers s and t , $x^{sp^k} \in G_m$ and $x^{tm} \in G_{p^k}$.
- 2 For every $x \in G$, there are $y \in G_{p^k}$ and $z \in G_m$ such that $x = yz$.
- 3 $G_{p^k} \cap G_m = \{e\}$.
- 4 $G \cong G_{p^k} \times G_m$. (See [Exercise H](#), [Chapter 14](#).)
- 5 Suppose $|G|$ has the following factorization into primes: $|G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$. Then $G \cong G_1 \times G_2 \times \cdots \times G_n$ where for each $i = 1, \dots, n$, G_i is a p_i -group.

Q. Basis Theorem for Finite Abelian Groups

Prerequisite: [Exercise P](#).

As a provisional definition, let us call a finite abelian group “decomposable” if there are elements $a_1, \dots, a_n \in G$ such that:

(D1) For every $x \in G$, there are integers $k_1, \dots, k_n$ such that $x = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$. (D2) If there are integers $l_1, \dots, l_n$ such that $a_1^{l_1} a_2^{l_2} \dots a_n^{l_n} = e$ then $a_1^{l_1} = a_2^{l_2} = \dots = a_n^{l_n} = e$.

If (D1) and (D2) hold, we will write $G = [a_1, a_2, \dots, a_n]$. Assume this in parts 1 and 2.

1 Let G' be the set of all products $a_2^{l_2} \dots a_n^{l_n}$, as $l_2, \dots, l_n$ range over $\mathbb{Z}$. Prove that G' is a subgroup of G , and $G' = [a_2, \dots, a_n]$.

2 Prove: $G \cong \langle a_1 \rangle \times G'$. Conclude that $G \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_n \rangle$.

In the remaining exercises of this set, let p be a prime number, and assume G is a finite abelian group such that the order of every element in G is some power of p . Let $a \in G$ be an element whose order is the highest possible in G . We will argue by induction to prove that G is “decomposable.” Let $H = \langle a \rangle$.

3 Explain why we may assume that $G/H = [Hb_1, \dots, Hb_n]$ for some $b_1, \dots, b_n \in G$.

By [Exercise O](#), we may assume that for each $i = 1, \dots, n$, $\text{ord}(b_i) = (Hb_i)$. We will show that $G = [a, b_1, \dots, b_n]$.

4 Prove that for every $x \in G$, there are integers $k_0, k_1, \dots, k_n$ such that

$$x = a^{k_0} b_1^{k_1} \dots b_n^{k_n}$$

5 Prove that if $a^{l_0} b_1^{l_1} \dots b_n^{l_n} = e$, then $a^{l_0} = b_1^{l_1} = \dots = b_n^{l_n} = e$. Conclude that $G = [a, b_1, \dots, b_n]$.

6 Use [Exercise P5](#), together with parts 2 and 5 above, to prove: Every finite abelian group G is a direct product of cyclic groups of prime power order. (This is called the basis theorem of finite abelian groups.)

It can be proved that the above decomposition of a finite abelian group into cyclic p -groups is unique, except for the order of the factors. We leave it to the ambitious reader to supply the proof of uniqueness.