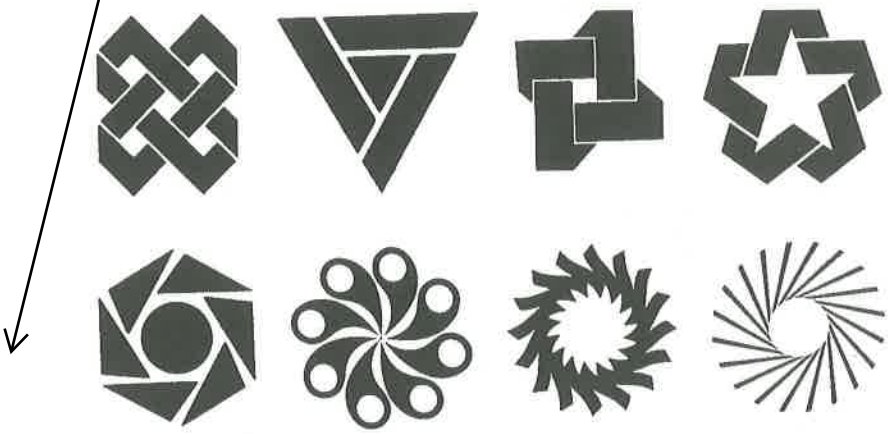


Figure 1.5 Logos with cyclic rotation symmetry groups.

Exercises

The only way to learn mathematics is to do mathematics.

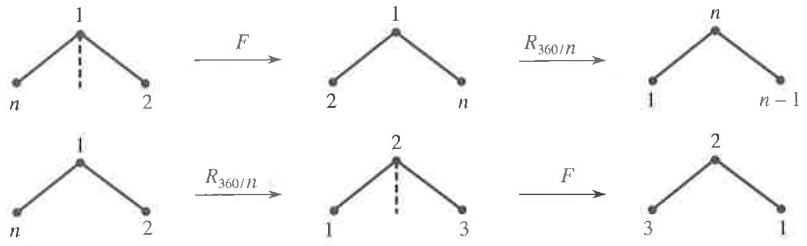
PAUL R. HALMOS, *A Hilbert Space Problem Book*

1. With pictures and words, describe each symmetry in D_3 (the set of symmetries of an equilateral triangle).
2. Write out a complete Cayley table for D_3. Is D_3 Abelian?
3. In D_4, find all elements X such that
   a. $X^3 = V$;
   b. $X^3 = R_{90}$;
   c. $X^3 = R_0$;
   d. $X^2 = R_0$;
   e. $X^2 = H$.
4. Describe in pictures or words the elements of D_5 (symmetries of a regular pentagon).
5. For $n \geq 3$, describe the elements of D_n. (*Hint:* You will need to consider two cases—n even and n odd.) How many elements does D_n have?
6. In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.
7. In D_n, explain geometrically why a rotation followed by a rotation must be a rotation.
8. In D_n, explain geometrically why a rotation and a reflection taken together in either order must be a reflection.
9. Associate the number 1 with a rotation and the number -1 with a reflection. Describe an analogy between multiplying these two numbers and multiplying elements of D_n.

10. If r_1, r_2, and r_3 represent rotations from D_n and f_1, f_2, and f_3 represent reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

11. Find elements A, B, and C in D_4 such that $AB = BC$ but $A \neq C$. (Thus, "cross cancellation" is not valid.)

12. Explain what the following diagram proves about the group D_n.



13. Describe the symmetries of a nonsquare rectangle. Construct the corresponding Cayley table.

14. Describe the symmetries of a parallelogram that is neither a rectangle nor a rhombus. Describe the symmetries of a rhombus that is not a rectangle.

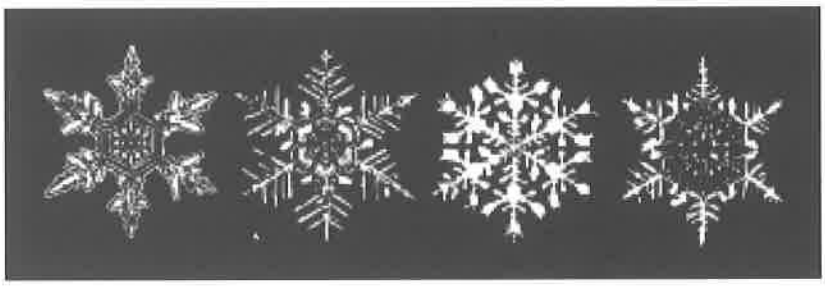
15. Describe the symmetries of a noncircular ellipse. Do the same for a hyperbola.

16. Consider an infinitely long strip of equally spaced H's:

$$\cdots \text{H H H H} \cdots$$

Describe the symmetries of this strip. Is the group of symmetries of the strip Abelian?

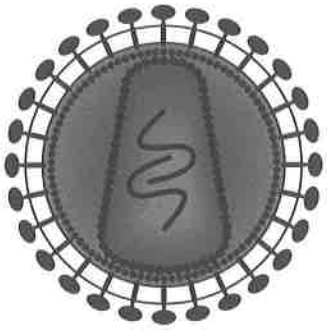
17. For each of the snowflakes in the figure, find the symmetry group and locate the axes of reflective symmetry (disregard imperfections).



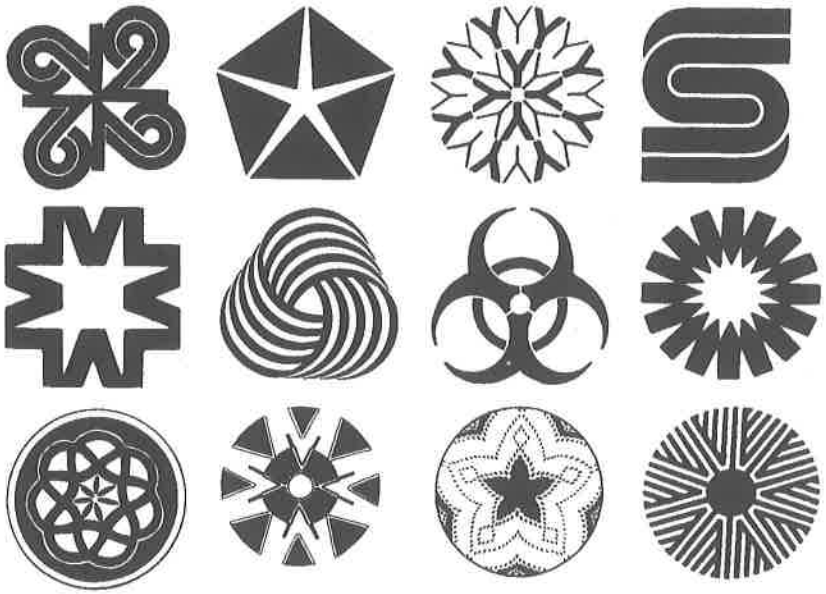
Snow Crystals, by W. A. Bentley & W. J. Humphreys © Dover Publications

Photographs of snowflakes from the Bentley and Humphreys atlas.

18. Determine the symmetry group of the outer shell of the cross section of the human immunodeficiency virus (HIV) shown below.



19. Does a fan blade have a cyclic symmetry group or a dihedral symmetry group?
20. Bottle caps that are pried off typically have 22 ridges around the rim. Find the symmetry group of such a cap.
21. What group theoretic property do uppercase letters F, G, J, L, P, Q, R have that is not shared by the remaining uppercase letters in the alphabet?
22. What symmetry property does the word "zoonosis" have when written in uppercase letters? (It means a disease of humans acquired from animals.)
23. What symmetry property do the words "mow," "sis," and "swims" have when written in uppercase letters?
24. For each design below, determine the symmetry group (ignore imperfections).



Chapter 2 Exercises

Exercises

"For example" is not proof.

JEWISH PROVERB

1. Which of the following binary operations are closed?
   a. subtraction of positive integers
   b. division of nonzero integers
   c. function composition of polynomials with real coefficients
   d. multiplication of 2×2 matrices with integer entries
2. Which of the following binary operations are associative?
   a. multiplication mod n
   b. division of nonzero rationals
   c. function composition of polynomials with real coefficients
   d. multiplication of 2×2 matrices with integer entries
3. Which of the following binary operations are commutative?
   a. substraction of integers
   b. division of nonzero real numbers
   c. function composition of polynomials with real coefficients
   d. multiplication of 2×2 matrices with real entries
4. Which of the following sets are closed under the given operation?
   a. $\{0, 4, 8, 12\}$ addition mod 16
   b. $\{0, 4, 8, 12\}$ addition mod 15
   c. $\{1, 4, 7, 13\}$ multiplication mod 15
   d. $\{1, 4, 5, 7\}$ multiplication mod 9
5. In each case, find the inverse of the element under the given operation.
   a. 13 in Z_{20}
   b. 13 in $U(14)$
   c. $n-1$ in $U(n)$ $(n > 2)$
   d. $3-2i$ in $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication
6. In each case, perform the indicated operation.
   a. In $\mathbf{C}^*$, $(7 + 5i)(-3 + 2i)$
   b. In $GL(2, Z_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$
   c. In $GL(2, \mathrm{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$
   d. In $GL(2, Z_{13})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

7. Give two reasons why the set of odd integers under addition is not a group.
8. Referring to Example 13, verify the assertion that subtraction is not associative.
9. Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.
10. Show that the group $GL(2, \mathbf{R})$ of Example 9 is non-Abelian by exhibiting a pair of matrices A and B in $GL(2, \mathbf{R})$ such that $AB \neq BA$.
11. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, Z_{11})$.
12. Give an example of group elements a and b with the property that $a^{-1}ba \neq b$.
13. Translate each of the following multiplicative expressions into its additive counterpart. Assume that the operation is commutative.
    a. a^2b^3
    b. $a^{-2}(b^{-1}c)^2$
    c. $(ab^2)^{-3}c^2 = e$
14. For group elements a, b, and c, express $(ab)^3$ and $(ab^{-2}\, c)^{-2}$ without parentheses.
15. Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Show that $G = H$ as sets.
16. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?
17. (From the GRE Practice Exam)* Let p and q be distinct primes. Suppose that H is a proper subset of the integers that is a group under addition that contains exactly three elements of the set $\{p, p + q, pq, p^q, q^p\}$. Determine which of the following are the three elements in H.
    a. pq, p^q, q^p
    b. $p + q, pq, p^q$
    c. $p, p + q, pq$
    d. p, p^q, q^p
    e. p, pq, p^q
18. List the members of $H = \{x^2 \mid x \in D_4\}$ and $K = \{x \in D_4 \mid x^2 = e\}$.
19. Prove that the set of all 2×2 matrices with entries from $\mathbf{R}$ and determinant $+1$ is a group under matrix multiplication.
20. For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.
21. An abstract algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead,

*GRE materials selected from the GRE Practice Exam, Question 9 by Educational Testing Service. Reprinted by permission of Educational Testing Service, the copyright owner.

one of the nine integers was inadvertently left out, so that the list appeared as 1, 9, 16, 22, 53, 74, 79, 81. Which integer was left out? (This really happened!)

22. Let G be a group with the property that for any x, y, z in the group, $xy = zx$ implies $y = z$. Prove that G is Abelian. ("Left-right cancellation" implies commutativity.)

23. (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

24. (Socks–Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. What would be an appropriate name for the group property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

25. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

26. Prove that in a group, $(a^{-1})^{-1} = a$ for all a.

27. For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

28. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?

29. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12.

30. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

31. Prove that every group table is a *Latin square*[†]; that is, each element of the group appears exactly once in each row and each column.

32. Construct a Cayley table for $U(12)$.

33. Suppose the table below is a group table. Fill in the blank entries.

	e	*a*	*b*	*c*	*d*
e	*e*	—	—	—	—
a	—	*b*	—	—	*e*
b	—	*c*	*d*	*e*	—
c	—	*d*	—	*a*	*b*
d	—	—	—	—	—

[†]Latin squares are useful in designing statistical experiments. There is also a close connection between Latin squares and finite geometries.

34. Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.
35. Let a, b, and c be elements of a group. Solve the equation $axb = c$ for x. Solve $a^{-1}xa = c$ for x.
36. Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.
37. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.
38. Give an example of a group with elements a, b, c, d, and x such that $axb = cxd$ but $ab \neq cd$. (Hence "middle cancellation" is not valid in groups.)
39. Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian. ("Middle cancellation" implies commutativity.)
40. Find an element X in D_4 such that $R_{90}VXH = D'$.
41. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n. Prove that $F_1F_2 \neq R_0$.
42. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.
43. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $R^kFR^k = F$.
44. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $FR^kF = R^{-k}$. Why does this imply that D_n is non-Abelian?
45. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.
    a. In D_4, $FR^{-2}FR^5$
    b. In D_5, $R^{-3}FR^4FR^{-2}$
    c. In D_6, $FR^5FR^{-2}F$
46. Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.
47. Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian. (This exercise is referred to in Chapter 26.)
48. Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group. (Multiplication is defined by

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + a' & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{bmatrix}.$$

This group, sometimes called the *Heisenberg group* after the Nobel Prize–winning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of quantum physics.)

49. Prove the assertion made in Example 20 that the set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime.

50. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 5. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

51. List the six elements of $GL(2, Z_2)$. Show that this group is non-Abelian by finding two elements that do not commute. (This exercise is referred to in Chapter 7.)

52. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with Example 10.)

53. Suppose that in the definition of a group G, the condition that there exists an element e with the property $ae = ea = a$ for all a in G is replaced by $ae = a$ for all a in G. Show that $ea = a$ for all a in G. (Thus, a one-sided identity is a two-sided identity.)

54. Suppose that in the definition of a group G, the condition that for each element a in G there exists an element b in G with the property $ab = ba = e$ is replaced by the condition $ab = e$. Show that $ba = e$. (Thus, a one-sided inverse is a two-sided inverse.)

Computer Exercises

Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Chapter 3 exercises

Although an element from a non-Abelian group does not necessarily commute with every element of the group, there are always some elements with which it will commute. For example, every element a commutes with all powers of a. This observation prompts the next definition and theorem.

Definition Centralizer of a in G

Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

EXAMPLE 15 In D_4, we have the following centralizers:

$$\begin{aligned} C(R_0) &= D_4 = C(R_{180}), \\ C(R_{90}) &= \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}), \\ C(H) &= \{R_0, H, R_{180}, V\} = C(V), \\ C(D) &= \{R_0, D, R_{180}, D'\} = C(D'). \end{aligned}$$

Notice that each of the centralizers in Example 15 is actually a subgroup of D_4. The next theorem shows that this was not a coincidence.

Theorem 3.6 $C(a)$ Is a Subgroup

For each a in a group G, the centralizer of a is a subgroup of G.

PROOF A proof similar to that of Theorem 3.5 is left to the reader to supply (Exercise 41).

Notice that for every element a of a group G, $Z(G) \subseteq C(a)$. Also, observe that G is Abelian if and only if $C(a) = G$ for all a in G.

Exercises

The purpose of proof is to understand, not to verify.

ARNOLD ROSS

1. For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

$$Z_{12}, \quad U(10), \quad U(12), \quad U(20), \quad D_4$$

2. Let Q be the group of rational numbers under addition and let Q^* be the group of nonzero rational numbers under multiplication. In Q, list the elements in $\langle \frac{1}{2} \rangle$. In Q^*, list the elements in $\langle \frac{1}{2} \rangle$.
3. Let Q and Q^* be as in Exercise 2. Find the order of each element in Q and in Q^*.
4. Prove that in any group, an element and its inverse have the same order.
5. Without actually computing the orders, explain why the two elements in each of the following pairs of elements from Z_{30} must have the same order: $\{2, 28\}$, $\{8, 22\}$. Do the same for the following pairs of elements from $U(15)$: $\{2, 8\}$, $\{7, 13\}$.
6. In the group Z_{12}, find $|a|$, $|b|$, and $|a + b|$ for each case.
   a. $a = 6, b = 2$
   b. $a = 3, b = 8$
   c. $a = 5, b = 4$
   Do you see any relationship between $|a|$, $|b|$, and $|a + b|$?
7. If a, b, and c are group elements and $|a| = 6$, $|b| = 7$, express $(a^4c^{-2}b^4)^{-1}$ without using negative exponents.
8. What can you say about a subgroup of D_3 that contains R_{240} and a reflection F? What can you say about a subgroup of D_3 that contains two reflections?
9. What can you say about a subgroup of D_4 that contains R_{270} and a reflection? What can you say about a subgroup of D_4 that contains H and D? What can you say about a subgroup of D_4 that contains H and V?
10. How many subgroups of order 4 does D_4 have?
11. Determine all elements of finite order in R^*, the group of nonzero real numbers under multiplication.
12. If a and b are group elements and $ab \neq ba$, prove that $aba \neq e$.
13. Suppose that H is a nonempty subset of a group G that is closed under the group operation and has the property that if a is not in H then a^{-1} is not in H. Is H a subgroup?
14. Let G be the group of polynomials under addition with coefficients from Z_{10}. Find the orders of $f(x) = 7x^2 + 5x + 4$, $g(x) = 4x^2 + 8x + 6$, and $f(x) + g(x) = x^2 + 3x$. If $h(x) = a_nx^n + a_n{-}1x^{n-1} + \cdots + a_0$ belongs to G, determine $|h(x)|$ given that $\gcd(a_1, a_2, \ldots, a_n) = 1$; $\gcd(a_1, a_2, \ldots, a_n) = 2$; $\gcd(a_1, a_2, \ldots, a_n) = 5$; and $\gcd(a_1, a_2, \ldots, a_n) = 10$.
15. If a is an element of a group G and $|a| = 7$, show that a is the cube of some element of G.

16. Suppose that H is a nonempty subset of a group G with the property that if a and b belong to H then $a^{-1}b^{-1}$ belongs to H. Prove or disprove that this is enough to guarantee that H is a subgroup of G.
17. Prove that if an Abelian group has more than three elements of order 2, then it has at least 7 elements of order 2. Find an example that shows this is not true for non-Abelian groups.
18. Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.
19. If a is a group element and a has infinite order, prove that $a^m \neq a^n$ when $m \neq n$.
20. Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?
21. Show that if a is an element of a group G, then $|a| \leq |G|$.
22. Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. [Hence, $U(14)$ is cyclic.] Is $U(14) = \langle 11 \rangle$?
23. Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]
24. Suppose n is an even positive integer and H is a subgroup of Z_n. Prove that either every member of H is even or exactly half of the members of H are even.
25. Prove that for every subgroup of D_n, either every member of the subgroup is a rotation or exactly half of the members are rotations.
26. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.
27. For every even integer n, show that D_n has a subgroup of order 4.
28. Suppose that H is a proper subgroup of Z under addition and H contains 18, 30, and 40. Determine H.
29. Suppose that H is a proper subgroup of Z under addition and that H contains 12, 30, and 54. What are the possibilities for H?
30. Prove that the dihedral group of order 6 does not have a subgroup of order 4.
31. For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$. [For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.] List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$. Prove that $U_k(n)$ is a subgroup of $U(n)$. Let $H = \{x \in U(10) \mid x \bmod 3 = 1\}$. Is H a subgroup of $U(10)$? (This exercise is referred to in Chapter 8.)
32. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

33. Let G be a group. Show that $Z(G) = \cap_{a \in G} C(a)$. [This means the intersection of *all* subgroups of the form $C(a)$.]

34. Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

35. For any group element a and any integer k, show that $C(a) \subseteq C(a^k)$. Use this fact to complete the following statement: "In a group, if x commutes with a, then . . . ." Is the converse true?

36. Complete the partial Cayley group table given below.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

37. Suppose G is the group defined by the following Cayley table.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

a. Find the centralizer of each member of G.

b. Find $Z(G)$.

c. Find the order of each element of G. How are these orders arithmetically related to the order of the group?

38. If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

39. Let S be a subset of a group and let H be the intersection of all subgroups of G that contain S.

a. Prove that $\langle S \rangle = H$.

b. If S is nonempty, prove that $\langle S \rangle = \{s_1^{n_1} s_2^{n_2} \ldots s_m^{n_m} \mid m \geq 1, s_i \in S, n_i \in Z\}$. (The s_i terms need not be distinct.)

40. In the group Z, find

a. $\langle 8, 14\rangle$;

b. $\langle 8, 13\rangle$;

c. $\langle 6, 15\rangle$;

d. $\langle m, n\rangle$;

e. $\langle 12, 18, 45\rangle$.

In each part, find an integer k such that the subgroup is $\langle k\rangle$.

41. Prove Theorem 3.6.

42. If H is a subgroup of G, then by the *centralizer* $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

43. Must the centralizer of an element of a group be Abelian?

44. Must the center of a group be Abelian?

45. Let G be an Abelian group with identity e and let n be some fixed integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G. Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G. (This exercise is referred to in Chapter 11.)

46. Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

47. Let G be the set of all polynomials with coefficients from the set $\{0, 1, 2, 3\}$. We can make G a group under addition by adding the polynomials in the usual way, except that we use modulo 4 to combine the coefficients. With this group operation, determine the orders of the elements of G. Determine a necessary and sufficient condition for an element of G to have order 2.

48. In each case, find elements a and b from a group such that $|a| = |b| = 2$.

a. $|ab| = 3$ **b.** $|ab| = 4$ **c.** $|ab| = 5$

Can you see any relationship among $|a|$, $|b|$, and $|ab|$?

49. Suppose a group contains elements a and b such that $|a| = 4$, $|b| = 2$, and $a^3b = ba$. Find $|ab|$.

50. Suppose a and b are group elements such that $|a| = 2$, $b \neq e$, and $aba = b^2$. Determine $|b|$.

51. Let a be a group element of order n, and suppose that d is a positive divisor of n. Prove that $|a^d| = n/d$.

52. Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbf{R})$. Find |A|, |B|, and |AB|. Does your answer surprise you?

53. Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2, \mathbf{R})$. What is the order of A? If we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of $SL(2, Z_p)$ (p is a prime), what is the order of A?

54. For any positive integer n and any angle θ, show that in the group $SL(2, \mathbf{R})$,

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}.$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos \sqrt{2}^\circ & -\sin \sqrt{2}^\circ \\ \sin \sqrt{2}^\circ & \cos \sqrt{2}^\circ \end{bmatrix}.$$

(Geometrically, $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ represents a rotation of the plane θ degrees.)

55. Let G be the symmetry group of a circle. Show that G has elements of every finite order as well as elements of infinite order.

56. Let x belong to a group and $|x| = 6$. Find $|x^2|$, $|x^3|$, $|x^4|$, and $|x^5|$. Let y belong to a group and $|y| = 9$. Find $|y^i|$ for $i = 2, 3, \ldots, 8$. Do these examples suggest any relationship between the order of the power of an element and the order of the element?

57. D_4 has seven cyclic subgroups. List them.

58. $U(15)$ has six cyclic subgroups. List them.

59. Prove that a group of even order must have an element of order 2.

60. Suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

61. Let H be a subgroup of a finite group G. Suppose that g belongs to G and n is the smallest positive integer such that $g^n \in H$. Prove that n divides $|g|$.

62. Compute the orders of the following groups.

a. $U(3)$, $U(4)$, $U(12)$

b. $U(5)$, $U(7)$, $U(35)$

c. $U(4)$, $U(5)$, $U(20)$

d. $U(3)$, $U(5)$, $U(15)$

On the basis of your answers, make a conjecture about the relationship among $|U(r)|$, $|U(s)|$, and $|U(rs)|$.

63. Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication and let $H = \{x \in \mathbf{R}^* \mid x^2 \text{ is rational}\}$. Prove that H is a subgroup of $\mathbf{R}^*$. Can the exponent 2 be replaced by any positive integer and still have H be a subgroup?

64. Compute $|U(4)|$, $|U(10)|$, and $|U(40)|$. Do these groups provide a counterexample to your answer to Exercise 62? If so, revise your conjecture.

65. Find a cyclic subgroup of order 4 in $U(40)$.

66. Find a noncyclic subgroup of order 4 in $U(40)$.

67. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in Z \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid a+b+c+d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

68. Let $H = \{A \in GL(2, \mathbf{R}) \mid \det A \text{ is an integer power of } 2\}$. Show that H is a subgroup of $GL(2, \mathbf{R})$.

69. Let H be a subgroup of $\mathbf{R}$ under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $\mathbf{R}^*$ under multiplication.

70. Let G be a group of functions from $\mathbf{R}$ to $\mathbf{R}^*$, where the operation of G is multiplication of functions. Let $H = \{f \in G \mid f(2) = 1\}$. Prove that H is a subgroup of G. Can 2 be replaced by any real number?

71. Let $G = GL(2, \mathbf{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a \text{ and } b \text{ are nonzero integers} \right\}$ under the operation of matrix multiplication. Prove or disprove that H is a subgroup of $GL(2, \mathbf{R})$.

72. Let $H = \{a + bi \mid a, b \in \mathbf{R}, ab \geq 0\}$. Prove or disprove that H is a subgroup of $\mathbf{C}$ under addition.

73. Let $H = \{a + bi \mid a, b \in \mathbf{R}, a^2 + b^2 = 1\}$. Prove or disprove that H is a subgroup of $\mathbf{C}^*$ under multiplication. Describe the elements of H geometrically.

74. Let G be a finite Abelian group and let a and b belong to G. Prove that the set $\langle a, b \rangle = \{a^i b^j \mid i, j \in \mathrm{Z}\}$ is a subgroup of G. What can you say about $|\langle a, b \rangle|$ in terms of $|a|$ and $|b|$?

75. Let H be a subgroup of a group G. Prove that the set $HZ(G) = \{hz \mid h \in H, z \in Z(G)\}$ is a subgroup of G. This exercise is referred to in this chapter.

76. Let G be a group and H a subgroup. For any element g of G, define $gH = \{gh \mid h \in H\}$. If G is Abelian and g has order 2, show that the set $K = H \cup gH$ is a subgroup of G. Is your proof valid if we drop the assumption that G is Abelian and let $K = Z(G) \cup gZ(G)$?

77. Let a belong to a group and $|a| = m$. If n is relatively prime to m, show that a can be written as the nth power of some element in the group.

78. Let F be a reflection in the dihedral group D_n and R a rotation in D_n. Determine $C(F)$ when n is odd. Determine $C(F)$ when n is even. Determine $C(R)$.

79. Let $G = GL(2, \mathbf{R})$.

a. Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

b. Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

c. Find $Z(G)$.

80. Let G be a finite group with more than one element. Show that G has an element of prime order.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Readings

Ruth Berger, "Hidden Group Structure," *Mathematics Magazine* 78 (2005): 45–48.

In this note, the author investigates groups obtained from $U(n)$ by multiplying each element by some k in $U(n)$. Such groups have identities that are not obvious.

J. Gallian and M. Reid, "Abelian Forcing Sets," *American Mathematical Monthly* 100 (1993): 580–582.

A set S is called *Abelian forcing* if the only groups that satisfy $(ab)^n = a^n b^n$ for all a and b in the group and all n in S are the Abelian ones. This paper characterizes the Abelian forcing sets. It can be downloaded at **http://www.d.umn.edu/~jgallian/forcing.pdf**

Gina Kolata, "Perfect Shuffles and Their Relation to Math," *Science* 216 (1982): 505–506.

This is a delightful nontechnical article that discusses how group theory and computers were used to solve a difficult problem about shuffling a deck of cards. Serious work on the problem was begun by an undergraduate student as part of a programming course.

groups of a group can be
. This is a diagram that in-
nects a subgroup H at one
sequence of line segments
Although there are many
ns between the subgroups
present the diagram in an
Z_{30} is shown in Figure 4.2.
d $\langle 5\rangle$, but $\langle 6\rangle$ is not a sub-

e of Z_{30}.

reciated by comparing the
bgroups of Z_{30} with that of
nese groups have relatively

n portion of Theorem 4.3
he order of a subgroup di-
o see, however, that a finite
rresponding to each divisor
, there may be none at all,
ny. Indeed, D_4, the dihedral
2 and three of order 4.
cyclic groups is appropri-
ery narrow class of finite
play the role of building
the same way that primes
that chemical elements are
nds.

Chapter 4 exercises

Exercises

It is not unreasonable to use the hypothesis.

ARNOLD ROSS

1. Find all generators of Z_6, Z_8, and Z_{20}.
2. Suppose that $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ are cyclic groups of orders 6, 8, and 20, respectively. Find all generators of $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$.
3. List the elements of the subgroups $\langle 20\rangle$ and $\langle 10\rangle$ in Z_{30}. Let a be a group element of order 30. List the elements of the subgroups $\langle a^{20}\rangle$ and $\langle a^{10}\rangle$.
4. List the elements of the subgroups $\langle 3\rangle$ and $\langle 15\rangle$ in Z_{18}. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3\rangle$ and $\langle a^{15}\rangle$.
5. List the elements of the subgroups $\langle 3\rangle$ and $\langle 7\rangle$ in $U(20)$.
6. What do Exercises 3, 4, and 5 have in common? Try to make a generalization that includes these three cases.
7. Find an example of a noncyclic group, all of whose proper subgroups are cyclic.
8. Let a be an element of a group and let $|a| = 15$. Compute the orders of the following elements of G.
   a. a^3, a^6, a^9, a^{12}
   b. a^5, a^{10}
   c. a^2, a^4, a^8, a^{14}
9. How many subgroups does Z_{20} have? List a generator for each of these subgroups. Suppose that $G = \langle a\rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of these subgroups.
10. In Z_{24}, list all generators for the subgroup of order 8. Let $G = \langle a\rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.
11. Let G be a group and let $a \in G$. Prove that $\langle a^{-1}\rangle = \langle a\rangle$.
12. In Z, find all generators of the subgroup $\langle 3\rangle$. If a has infinite order, find all generators of the subgroup $\langle a^3\rangle$.
13. In Z_{24}, find a generator for $\langle 21\rangle \cap \langle 10\rangle$. Suppose that $|a| = 24$. Find a generator for $\langle a^{21}\rangle \cap \langle a^{10}\rangle$. In general, what is a generator for the subgroup $\langle a^m\rangle \cap \langle a^n\rangle$?
14. Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is a prime?

15. Let G be an Abelian group and let $H = \{g \in G \mid |g| \text{ divides } 12\}$. Prove that H is a subgroup of G. Is there anything special about 12 here? Would your proof be valid if 12 were replaced by some other positive integer? State the general result.

16. Find a collection of distinct subgroups $\langle a_1\rangle, \langle a_2\rangle, \ldots, \langle a_n\rangle$ of Z_{240} with the property that $\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle$ with n as large as possible.

17. Complete the following statement: $|a| = |a^2|$ if and only if $|a| \ldots$.

18. If a cyclic group has an element of infinite order, how many elements of finite order does it have?

19. List the cyclic subgroups of $U(30)$.

20. Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation $x^{35} = e$. Prove that G is cyclic. Does your argument work if 35 is replaced with 33?

21. Let G be a group and let a be an element of G.

a. If $a^{12} = e$, what can we say about the order of a?

b. If $a^m = e$, what can we say about the order of a?

c. Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a\rangle = G$.

22. Prove that a group of order 3 must be cyclic.

23. Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? Why? Describe all the subgroups of Z. Let a be a group element with infinite order. Describe all subgroups of $\langle a\rangle$.

24. For any element a in any group G, prove that $\langle a\rangle$ is a subgroup of $C(a)$ (the centralizer of a).

25. If d is a positive integer, $d \neq 2$, and d divides n, show that the number of elements of order d in D_n is $\phi(d)$. How many elements of order 2 does D_n have?

26. Find all generators of Z. Let a be a group element that has infinite order. Find all generators of $\langle a\rangle$.

27. Prove that C^*, the group of nonzero complex numbers under multiplication, has a cyclic subgroup of order n for every positive integer n.

28. Let a be a group element that has infinite order. Prove that $\langle a^i\rangle = \langle a^j\rangle$ if and only if $i = \pm j$.

29. List all the elements of order 8 in $Z_{8000000}$. How do you know your list is complete? Let a be a group element such that $|a| = 8000000$. List all elements of order 8 in $\langle a\rangle$. How do you know your list is complete?

30. Suppose a and b belong to a group, a has odd order, and $aba^{-1} = b^{-1}$. Show that $b^2 = e$.

31. Let G be a finite group. Show that there exists a fixed positive integer n such that $a^n = e$ for all a in G. (Note that n is independent of a.)
32. Determine the subgroup lattice for Z_{12}.
33. Determine the subgroup lattice for Z_{p^2q}, where p and q are distinct primes.
34. Determine the subgroup lattice for Z_8.
35. Determine the subgroup lattice for Z_{p^n}, where p is a prime and n is some positive integer.
36. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.
37. Show that the group of positive rational numbers under multiplication is not cyclic.
38. Consider the set $\{4, 8, 12, 16\}$. Show that this set is a group under multiplication modulo 20 by constructing its Cayley table. What is the identity element? Is the group cyclic? If so, find all of its generators.
39. Give an example of a group that has exactly 6 subgroups (including the trivial subgroup and the group itself). Generalize to exactly n subgroups for any positive integer n.
40. Let m and n be elements of the group Z. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.
41. Suppose that a and b are group elements that commute and have orders m and n. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.
42. Suppose that a and b belong to a group G, a and b commute, and $|a|$ and $|b|$ are finite. What are the possibilities for $|ab|$?
43. Suppose that a and b belong to a group G, a and b commute, and $|a|$ and $|b|$ are finite. Prove that G has an element of order $\text{lcm}(|a|, |b|)$.
44. Let F and F' be distinct reflections in D_{21}. What are the possibilities for $|FF'|$?
45. Suppose that H is a subgroup of a group G and $|H| = 10$. If a belongs to G and a^6 belongs to H, what are the possibilities for $|a|$?
46. Which of the following numbers could be the exact number of elements of order 21 in a group: 21600, 21602, 21604?
47. If G is an infinite group, what can you say about the number of elements of order 8 in the group? Generalize.
48. Suppose that K is a proper subgroup of D_{35} and K contains at least two reflections. What are the possible orders of K? Explain your reasoning.

49. For each positive integer n, prove that $\boldsymbol{C}^*$, the group of nonzero complex numbers under multiplication, has exactly $\phi(n)$ elements of order n.

50. Prove or disprove that $H = \{n \in Z \mid n \text{ is divisible by both 8 and 10}\}$ is a subgroup of Z.

51. Suppose that G is a finite group with the property that every nonidentity element has prime order (for example, D_3 and D_5). If $Z(G)$ is not trivial, prove that every nonidentity element of G has the same order.

52. Prove that an infinite group must have an infinite number of subgroups.

53. Let p be a prime. If a group has more than $p - 1$ elements of order p, why can't the group be cyclic?

54. Suppose that G is a cyclic group and that 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If a is one element of order 8, list the other elements of order 8.

55. List all the elements of Z_{40} that have order 10. Let $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.

56. Reformulate the corollary of Theorem 4.4 to include the case when the group has infinite order.

57. Determine the orders of the elements of D_{33} and how many there are of each.

58. If G is a cyclic group and 15 divides the order of G, determine the number of solutions in G of the equation $x^{15} = e$. If 20 divides the order of G, determine the number of solutions of $x^{20} = e$. Generalize.

59. If G is an Abelian group and contains cyclic subgroups of orders 4 and 5, what other sizes of cyclic subgroups must G contain? Generalize.

60. If G is an Abelian group and contains cyclic subgroups of orders 4 and 6, what other sizes of cyclic subgroups must G contain? Generalize.

61. Prove that no group can have exactly two elements of order 2.

62. Given the fact that $U(49)$ is cyclic and has 42 elements, deduce the number of generators that $U(49)$ has without actually finding any of the generators.

63. Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

64. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

65. Let a and b belong to a group. If $|a| = 24$ and $|b| = 10$, what are the possibilities for $|\langle a\rangle \cap \langle b\rangle|$?

66. Prove that $U(2^n)$ $(n \geq 3)$ is not cyclic.

67. Suppose that G is a group of order 16 and that, by direct computation, you know that G has at least nine elements x such that $x^8 = e$. Can you conclude that G is not cyclic? What if G has at least five elements x such that $x^4 = e$? Generalize.

68. Prove that Z_n has an even number of generators if $n > 2$. What does this tell you about $\phi(n)$?

69. If $|a^5| = 12$, what are the possibilities for $|a|$? If $|a^4| = 12$, what are the possibilities for $|a|$?

70. Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r\rangle \subseteq \langle x^s\rangle$.

71. Suppose a is a group element such that $|a^{28}| = 10$ and $|a^{22}| = 20$. Determine $|a|$.

72. Let a be a group element such that $|a| = 48$. For each part, find a divisor k of 48 such that

a. $\langle a^{21}\rangle = \langle a^k\rangle$;

b. $\langle a^{14}\rangle = \langle a^k\rangle$;

c. $\langle a^{18}\rangle = \langle a^k\rangle$.

73. Let p be a prime. Show that in a cyclic group of order $p^n - 1$, every element is a pth power (that is, every element can be written in the form a^p for some a).

74. Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \,\middle|\, n \in Z \right\}$ is a cyclic subgroup of $GL(2, \mathbf{R})$.

75. Let a and b belong to a group. If $|a| = 12$, $|b| = 22$, and $\langle a\rangle \cap \langle b\rangle \neq \{e\}$, prove that $a^6 = b^{11}$.

76. (2008 GRE Practice Exam) If x is an element of a cyclic group of order 15 and exactly two of x^3, x^5, and x^9 are equal, determine $|x^{13}|$.

77. Determine the number of cyclic subgroups of order 4 in D_n.

78. If n is odd, prove that D_n has no subgroup of order 4.

79. If $n \geq 4$ and is even, show that D_n has exactly $n/2$ noncyclic subgroups of order 4.

80. If $n \geq 4$ and n is divisible by 2 but not by 4, prove that D_n has exactly $n/2$ subgroups of order 4.

81. How many subgroups of order n does D_n have?

82. Let G be the set of all polynomials of the form $ax^2 + bx + c$ with coefficients from the set $\{0, 1, 2\}$. We can make G a group under addition by adding the polynomials in the usual way, except that we use modulo 3 to combine the coefficients. With this operation, prove that G is a group of order 27 that is not cyclic.

83. Let a and b belong to some group. Suppose that $|a| = m$, $|b| = n$, and m and n are relatively prime. If $a^k = b^k$ for some integer k, prove that mn divides k.

84. For every integer n greater than 2, prove that the group $U(n^2 - 1)$ is not cyclic.

85. Prove that for any prime p and positive integer n, $\phi(p^n) = p^n - p^{n-1}$.

86. Give an example of an infinite group that has exactly two elements of order 4.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Reading

Deborah L. Massari, "The Probability of Generating a Cyclic Group," *Pi Mu Epsilon Journal* 7 (1979): 3–6.

In this easy-to-read paper, it is shown that the probability of a randomly chosen element from a cyclic group being a generator of the group depends only on the set of prime divisors of the order of the group, and not on the order itself. This article, written by an undergraduate student, received first prize in a Pi Mu Epsilon paper contest.

Supplementary Exercises for Chapters 1–4

If you really want something in this life, you have to work for it. Now quiet, they're about to announce the lottery numbers!

HOMER SIMPSON

True/false questions for Chapters 1–4 are available on the Web at:

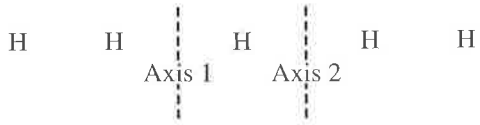
http://www.d.umn.edu/~jgallian/TF

1. Let G be a group and let H be a subgroup of G. For any fixed x in G, define $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Prove the following.
   a. xHx^{-1} is a subgroup of G.
   b. If H is cyclic, then xHx^{-1} is cyclic.
   c. If H is Abelian, then xHx^{-1} is Abelian.
   The group xHx^{-1} is called a *conjugate* of H. (Note that conjugation preserves structure.)
2. Let G be a group and let H be a subgroup of G. Define $N(H) = \{x \in G \mid xHx^{-1} = H\}$. Prove that $N(H)$ (called the *normalizer* of H) is a subgroup of G.†
3. Let G be a group. For each $a \in G$, define $\text{cl}(a) = \{xax^{-1} \mid x \in G\}$. Prove that these subsets of G partition G. [$\text{cl}(a)$ is called the *conjugacy class* of a.]
4. The group defined by the following table is called the *group of quaternions*. Use the table to determine each of the following.
   a. The center
   b. $\text{cl}(a)$
   c. $\text{cl}(b)$
   d. All cyclic subgroups

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

†This very important subgroup was first used by L. Sylow in 1872 to prove the existence of certain kinds of subgroups in a group. His work is discussed in Chapter 24.

5. (Conjugation preserves order.) Prove that, in any group, $|xax^{-1}| = |a|$. (This exercise is referred to in Chapter 24.)
6. Prove that, in any group, $|ab| = |ba|$.
7. If a and b are group elements, prove that $|ab| = |a^{-1}b^{-1}|$.
8. Prove that a group of order 4 cannot have a subgroup of order 3.
9. If a, b, and c are elements of a group, give an example to show that it need not be the case that $|abc| = |cba|$.
10. Let a and b belong to a group G. Prove that there is an element x in G such that $xax = b$ if and only if $ab = c^2$ for some element c in G.
11. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.
12. Let G be the plane symmetry group of the infinite strip of equally spaced H's shown below.

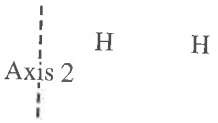


Let x be the reflection about Axis 1 and let y be the reflection about Axis 2. Calculate $|x|$, $|y|$, and $|xy|$. Must the product of elements of finite order have finite order? (This exercise is referred to in Chapter 27.)

13. What are the orders of the elements of D_{15}? How many elements have each of these orders?
14. Prove that a group of order 4 is Abelian.
15. Prove that a group of order 5 must be cyclic.
16. Prove that an Abelian group of order 6 must be cyclic.
17. Let G be an Abelian group and let n be a fixed positive integer. Let $G^n = \{g^n \mid g \in G\}$. Prove that G^n is a subgroup of G. Give an example showing that G^n need not be a subgroup of G when G is non-Abelian. (This exercise is referred to in Chapter 11.)
18. Let $G = \{a + b\sqrt{2}\}$, where a and b are rational numbers not both 0. Prove that G is a group under ordinary multiplication.
19. (1969 Putnam Competition) Prove that no group is the union of two proper subgroups. Does the statement remain true if "two" is replaced by "three"?
20. Prove that the subset of elements of finite order in an Abelian group forms a subgroup. (This subgroup is called the *torsion subgroup*.) Is the same thing true for non-Abelian groups?
21. Let p be a prime and let G be an Abelian group. Show that the set of all elements whose orders are powers of p is a subgroup of G.

Prove that, in any group, $|xax^{-1}| =$
in Chapter 24.)
$= |ba|$.
prove that $|ab| = |a^{-1}b^{-1}|$.
nnot have a subgroup of order 3.
roup, give an example to show that
$| = |cba|$.
. Prove that there is an element x in
if $ab = c^2$ for some element c in G.
nt of order 2 in a group, then a lies

oup of the infinite strip of equally



1 and let y be the reflection about
$y|$. Must the product of elements
? (This exercise is referred to in

ents of D_{15}? How many elements

belian.
t be cyclic.
der 6 must be cyclic.
n be a fixed positive integer. Let
is a subgroup of G. Give an ex-
be a subgroup of G when G is
erred to in Chapter 11.)
b are rational numbers not both
dinary multiplication.
e that no group is the union of
atement remain true if "two" is

s of finite order in an Abelian
group is called the *torsion sub-*
on-Abelian groups?
belian group. Show that the set
wers of p is a subgroup of G.

22. Suppose that a and b are group elements. If $|b| = 2$ and $bab = a^4$, determine the possibilities for $|a|$.

23. Suppose that a finite group is generated by two elements a and b (that is, every element of the group can be expressed as some product of a's and b's). Given that $a^3 = b^2 = e$ and $ba^2 = ab$, construct the Cayley table for the group. We have already seen an example of a group that satisfies these conditions. Name it.

24. If a is an element from a group and $|a| = n$, prove that $C(a) = C(a^k)$ when k is relatively prime to n.

25. Let x and y belong to a group G. If $xy \in Z(G)$, prove that $xy = yx$.

26. Suppose that H and K are nontrivial subgroups of Q under addition. Show that $H \cap K$ is a nontrivial subgroup of Q. Is this true if Q is replaced by $\mathbf{R}$?

27. Let H be a subgroup of G and let g be an element of G. Prove that $N(gHg^{-1}) = gN(H)g^{-1}$. See Exercise 2 for the notation.

28. Let H be a subgroup of a group G and let $|g| = n$. If g^m belongs to H, and m and n are relatively prime, prove that g belongs to H.

29. Find a group that contains elements a and b such that $|a| = 2$, $|b| = 11$, and $|ab| = 2$.

30. Suppose that G is a group with exactly eight elements of order 10. How many cyclic subgroups of order 10 does G have?

31. (1989 Putnam Competition) Let S be a nonempty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a^n \mid n = 1, 2, 3, \ldots\}$ is finite. Must S be a group?

32. Let $H_1, H_2, H_3, \ldots$ be a sequence of subgroups of a group with the property that $H_1 \subseteq H_2 \subseteq H_3 \ldots$. Prove that the union of the sequence is a subgroup.

33. Let n be an integer greater than 1. Find a noncyclic subgroup of $U(4n)$ of order 4 that contains the element $2n - 1$.

34. Let G be an Abelian group and $H = \{x \in G \mid x^n = e$ for some odd integer n (n may vary with x)$\}$. Prove that H is a subgroup of G. Is H a subgroup if "odd" is replaced by "even"?

35. Let $H = \{A \in GL(2, \mathbf{R}) \mid \det A$ is rational$\}$. Prove or disprove that H is a subgroup of $GL(2, \mathbf{R})$. What if "rational" is replaced by "an integer"?

36. Suppose that G is a group that has exactly one nontrivial proper subgroup. Prove that G is cyclic and $|G| = p^2$, where p is prime.

37. Suppose that G is a group and G has exactly two nontrivial proper subgroups. Prove that G is cyclic and $|G| = pq$, where p and q are distinct primes, or that G is cyclic and $|G| = p^3$, where p is prime.

38. If $|a^2| = |b^2|$, prove or disprove that $|a| = |b|$.

39. (1995 Putnam Competition) Let S be a set of real numbers that is closed under multiplication. Let T and U be disjoint subsets of S whose union is S. Given that the product of any three (not necessarily distinct) elements of T is in T and that the product of any three elements of U is in U, show that at least one of the two subsets T and U is closed under multiplication.

40. If p is an odd prime, prove that there is no group that has exactly p elements of order p.

41. Give an example of a group G with infinitely many distinct subgroups $H_1, H_2, H_3, \ldots$ such that $H_1 \subset H_2 \subset H_3 \ldots$.

42. Suppose a and b are group elements and $b \neq e$. If $a^{-1}ba = b^2$ and $|a| = 3$, find $|b|$. What is $|b|$, if $|a| = 5$? What can you say about $|b|$ in the case where $|a| = k$?

43. Let a and b belong to a group G. Show that there is an element g in G such that $g^{-1}abg = ba$.

44. Suppose G is a group and $x^3y^3 = y^3x^3$ for every x and y in G. Let $H = \{x \in G \mid |x| \text{ is relatively prime to } 3\}$. Prove that elements of H commute with each other and that H is a subgroup of G. Is your argument valid if 3 is replaced by an arbitrary positive integer n? Explain why or why not.

45. Let G be a finite group and let S be a subset of G that contains more than half of the elements of G. Show that every element of G can be expressed in the form s_1s_2 where s_1 and s_2 belong to S.

46. Let G be a group and let f be a function from G to some set. Show that $H = \{g \in G \mid f(xg) = f(x) \text{ for all } x \in G\}$ is a subgroup of G. In the case that G is the group of real numbers under addition and $f(x) = \sin x$, describe H.

47. Let G be a cyclic group of order n and let H be the subgroup of order d. Show that $H = \{x \in G \mid |x| \text{ divides } d\}$.

48. Let a be an element of maximum order from a finite Abelian group G. Prove that for any element b in G, $|b|$ divides $|a|$. Show by example that this need not be true for finite non-Abelian groups.

49. Define an operation $*$ on the set of integers by $a * b = a + b - 1$. Show that the set of integers under this operation is a cyclic group.

50. Let n be an integer greater than 1. Find a noncyclic subgroup of $U(4n)$ of order 4 that contains the element $2n - 1$.

Chapter 5 exercises

Exercises

When you feel how depressingly
slowly you climb,
it's well to remember that
Things Take Time.

PIET HEIN, "T. T. T.," *Grooks (1966)*†*

1. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$

Compute each of the following.

a. α^{-1}

b. $\beta\alpha$

c. $\alpha\beta$

2. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \text{and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

Write α, β, and $\alpha\beta$ as

a. products of disjoint cycles;

b. products of 2-cycles.

3. Write each of the following permutations as a product of disjoint cycles.

a. (1235)(413)

b. (13256)(23)(46512)

c. (12)(13)(23)(142)

4. Find the order of each of the following permutations.

a. (14)

b. (147)

c. (14762)

d. $(a_1a_2 \cdots a_k)$

5. What is the order of each of the following permutations?

a. (124)(357)

b. (124)(3567)

c. (124)(35)

d. (124)(357869)

e. (1235)(24567)

f. (345)(245)

---

†Hein is a Danish engineer and poet and is the inventor of the game *Hex*.

PIET HEIN, "T. T. T.," *Grooks (1966)*†*

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

tions as a product of disjoint

g permutations.

wing permutations?

ntor of the game *Hex*.

) Piet Hein Grooks. Reprinted with delfart, Denmark.

6. What is the order of each of the following permutations?
   a. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$
   b. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$
7. What is the order of the product of a pair of disjoint cycles of lengths 4 and 6?
8. Show that A_8 contains an element of order 15.
9. What are the possible orders for the elements of S_6 and A_6? What about A_7? (This exercise is referred to in Chapter 25.)
10. What is the maximum order of any element in A_{10}?
11. Determine whether the following permutations are even or odd.
    a. (135)
    b. (1356)
    c. (13567)
    d. (12)(134)(152)
    e. (1243)(3521)
12. Show that a function from a finite set S to itself is one-to-one if and only if it is onto. Is this true when S is infinite? (This exercise is referred to in Chapter 6.)
13. Suppose that α is a mapping from a set S to itself and $\alpha(\alpha(x)) = x$ for all x in S. Prove that α is one-to-one and onto.
14. Find eight elements in S_6 that commute with (12)(34)(56). Do they form a subgroup of S_6?
15. Let n be a positive integer. If n is odd, is an n-cycle an odd or an even permutation? If n is even, is an n-cycle an odd or an even permutation?
16. If α is even, prove that α^{-1} is even. If α is odd, prove that α^{-1} is odd.
17. Prove Theorem 5.6.
18. In S_n, let α be an r-cycle, β an s-cycle, and γ a t-cycle. Complete the following statements: $\alpha\beta$ is even if and only if $r + s$ is . . . ; $\alpha\beta\gamma$ is even if and only if $r + s + t$ is . . . .
19. Let α and β belong to S_n. Prove that $\alpha\beta$ is even if and only if α and β are both even or both odd.
20. Associate an even permutation with the number $+1$ and an odd permutation with the number -1. Draw an analogy between the result of multiplying two permutations and the result of multiplying their corresponding numbers $+1$ or -1.

21. Let σ be the permutation of the letters A through Z that takes each letter to the one directly below it in the display following. Write σ in cycle form.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
H D B G J E C M I L O N P F K R U S A W Q T V Z X Y

22. If α and β are distinct 2-cycles, what are the possibilities for $|\alpha\beta|$?

23. Show that if H is a subgroup of S_n, then either every member of H is an even permutation or exactly half of the members are even. (This exercise is referred to in Chapter 25.)

24. Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n.

25. Give two reasons why the set of odd permutations in S_n is not a subgroup.

26. Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

27. Use Table 5.1 to compute the following.
a. The centralizer of $\alpha_3 = (13)(24)$
b. The centralizer of $\alpha_{12} = (124)$

28. How many elements of order 5 are in S_7?

29. How many elements of order 4 does S_6 have? How many elements of order 2 does S_6 have?

30. Prove that (1234) is not the product of 3-cycles.

31. Let $\beta \in S_7$ and suppose $\beta^4 = (2143567)$. Find β. What are the possibilities for β if $\beta \in S_9$?

32. Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.

33. Find three elements σ in S_9 with the property that $\sigma^3 = (157)(283)(469)$.

34. What cycle is $(a_1a_2 \cdots a_n)^{-1}$?

35. Let G be a group of permutations on a set X. Let $a \in X$ and define $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$. We call $\text{stab}(a)$ the *stabilizer of a in G* (since it consists of all members of G that leave a fixed). Prove that $\text{stab}(a)$ is a subgroup of G. (This subgroup was introduced by Galois in 1832.) This exercise is referred to in Chapter 7.

36. Let $\beta = (1,3,5,7,9,8,6)(2,4,10)$. What is the smallest positive integer n for which $\beta^n = \beta^{-5}$?

37. Let $\alpha = (1,3,5,7,9)(2,4,6)(8,10)$. If α^m is a 5-cycle, what can you say about m?

38. Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. How many elements are in H? Is your argument valid when S_5 is replaced by S_n for $n \geq 3$? How many elements are in H when S_5 is replaced by A_n for $n \geq 4$?

39. How many elements of order 5 are there in A_6?
40. In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.
41. Suppose that β is a 10-cycle. For which integers i between 2 and 10 is β^i also a 10-cycle?
42. In S_3, find elements α and β such that $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.
43. Find group elements α and β in S_5 such that $|\alpha| = 3$, $|\beta| = 3$, and $|\alpha\beta| = 5$.
44. Represent the symmetry group of an equilateral triangle as a group of permutations of its vertices (see Example 3).
45. Prove that S_n is non-Abelian for all $n \geq 3$.
46. Prove that A_n is non-Abelian for all $n \geq 4$.
47. For $n \geq 3$, let $H = \{\beta \in S_n \mid \beta(1) = 1 \text{ or } 2 \text{ and } \beta(2) = 1 \text{ or } 2\}$. Prove that H is a subgroup of S_n. Determine $|H|$.
48. Show that in S_7, the equation $x^2 = (1234)$ has no solutions but the equation $x^3 = (1234)$ has at least two.
49. If (ab) and (cd) are distinct 2-cycles in S_n, prove that (ab) and (cd) commute if and only if they are disjoint.
50. Let α be a 2-cycle and β be a t-cycle in S_n. Prove that $\alpha\beta\alpha$ is a t-cycle.
51. Use the previous exercise to prove that, if α and β belong to S_n and β is the product of k-cycles of lengths $n_1, n_2, \ldots, n_k$, then $\alpha\beta\alpha^{-1}$ is the product of k-cycles of lengths $n_1, n_2, \ldots n_k$.
52. Let α and β belong to S_n. Prove that $\beta\alpha\beta^{-1}$ and α are both even or both odd.
53. What is the smallest positive integer n such that S_n has an element of order greater than $2n$?
54. Let n be an even positive integer. Prove that A_n has an element of order greater than n if and only if $n \geq 8$.
55. Let n be an odd positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 13$.
56. Let n be an even positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 14$.
57. Viewing the members of D_4 as a group of permutations of a square labeled 1, 2, 3, 4 as described in Example 3, which geometric symmetries correspond to even permutations?
58. Viewing the members of D_5 as a group of permutations of a regular pentagon with consecutive vertices labeled 1, 2, 3, 4, 5, what geometric symmetry corresponds to the permutation (14253)? Which symmetry corresponds to the permutation (25)(34)?

59. Let n be an odd integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled $1, 2, \ldots, n$, explain why the rotation subgroup of D_n is a subgroup of A_n.

60. Let n be an integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled $1, 2, \ldots, n$, determine for which n all the permutations corresponding to reflections in D_n are even permutations. Hint: Consider the fours cases for n mod 4.

61. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2. (This exercise is referred to in Chapter 25.)

62. Find a cyclic subgroup of A_8 that has order 4.

63. Find a noncyclic subgroup of A_8 that has order 4.

64. Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?

65. Show that every element in A_n for $n \geq 3$ can be expressed as a 3-cycle or a product of 3-cycle.

66. Show that for $n \geq 3$, $Z(S_n) = \{\varepsilon\}$.

67. Verify the statement made in the discussion of the Verhoeff check digit scheme based on D_5 that $a * \sigma(b) \neq b * \sigma(a)$ for distinct a and b. Use this to prove that $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ for all i. Prove that this implies that all transposition errors involving adjacent digits are detected.

68. Use the Verhoeff check-digit scheme based on D_5 to append a check digit to 45723.

69. Prove that every element of S_n $(n > 1)$ can be written as a product of elements of the form $(1k)$.

70. (Indiana College Mathematics Competition) A card-shuffling machine always rearranges cards in the same way relative to the order in which they were given to it. All of the hearts arranged in order from ace to king were put into the machine, and then the shuffled cards were put into the machine again to be shuffled. If the cards emerged in the order 10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7, in what order were the cards after the first shuffle?

71. Show that a permutation with odd order must be an even permutation.

72. Let G be a group. Prove or disprove that $H = \{g^2 \mid g \in G\}$ is a subgroup of G. (Compare with Example 5 in Chapter 3.)

73. Let $H = \{\alpha^2 \mid \alpha \in S_4\}$ and $K = \{\alpha^2 \mid \alpha \in S_5\}$. Prove $H = A_4$ and $K = A_5$.

74. Let $H = \{\alpha^2 \mid \alpha \in S_6\}$. Prove $H \neq A_6$.

75. Determine integers n for which $H = \{\alpha \in A_n \mid \alpha^2 = \varepsilon\}$ is a subgroup of A_n.

76. Given that β and γ are in S_4 with $\beta\gamma = (1432)$, $\gamma\beta = (1243)$, and $\beta(1) = 4$, determine β and γ.

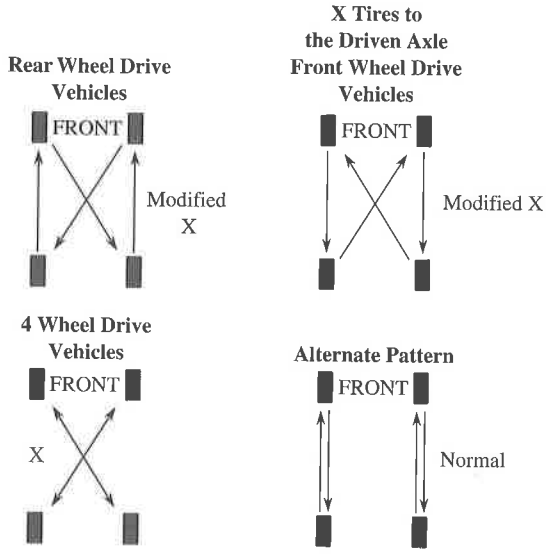
77. Why does the fact that the orders of the elements of A_4 are 1, 2, and 3 imply that $|Z(A_4)| = 1$?

78. Find five subgroups of S_5 of order 24.

79. Find six subgroups of order 60 in S_6.

80. For $n > 1$, let H be the set of all permutations in S_n that can be expressed as a product of a multiple of four transpositions. Show that $H = A_n$.

81. Shown below are four tire rotation patterns recommended by the Dunlop Tire Company. Explain how these patterns can be represented as permutations in S_4 and find the smallest subgroup of S_4 that contains these four patterns. Is the subgroup Abelian?



82. Label the four locations of tires on an automobile with the labels 1, 2, 3, and 4, clockwise. Let a represent the operation of switching the tires in positions 1 and 3 and switching the tires in positions 2 and 4. Let b represent the operation of rotating the tires in positions 2, 3, and 4 clockwise and leaving the tire in position 1 as is. Let G be the group of all possible combinations of a and b. How many elements are in G?

83. What would be wrong with using the 2-cycle notation (11) instead of the 1-cycle (1) to indicate that a cycle sends 1 to 1?

Chapter 6 exercises

PROOF As in Example 13, any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspondence from $\text{Aut}(Z_n)$ to $U(n)$ given by T: $\alpha \to \alpha(1)$. The fact that $\alpha(k) = k\alpha(1)$ (see Example 13) implies that T is a one-to-one mapping. For if α and β belong to $\text{Aut}(Z_n)$ and $\alpha(1) = \beta(1)$, then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$ for all k in Z_n, and therefore $\alpha = \beta$.

To prove that T is onto, let $r \in U(n)$ and consider the mapping α from Z_n to Z_n defined by $\alpha(s) = sr \pmod n$ for all s in Z_n. We leave it as an exercise to verify that α is an automorphism of Z_n (see Exercise 27). Then, since $T(\alpha) = \alpha(1) = r$, T is onto $U(n)$.

Finally, we establish the fact that T is operation-preserving. Let α, $\beta \in \text{Aut}(Z_n)$. We then have

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)})$$

$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)} = \alpha(1)\beta(1)$$

$$= T(\alpha)T(\beta).$$

This completes the proof. ∎

Exercises

Being a mathematician is a bit like being a manic depressive: you spend your life alternating between giddy elation and black despair.

STEVEN G. KRANTZ, *A Primer of Mathematical Writing*

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.
2. Find $\text{Aut}(Z)$.
3. Let $\mathbf{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbf{R}^+$.
4. Show that $U(8)$ is not isomorphic to $U(10)$.
5. Show that $U(8)$ is isomorphic to $U(12)$.
6. Prove that isomorphism is an equivalence relation. That is, for any groups G, H, and K, $G \approx G$, $G \approx H$ implies $H \approx G$, and $G \approx H$ and $H \approx K$ implies $G \approx K$.
7. Prove that S_4 is not isomorphic to D_{12}.
8. Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbf{R}^+$ under multiplication to $\mathbf{R}$ under addition.
9. In the notation of Theorem 6.1, prove that T_e is the identity and that $(T_g)^{-1} = T_{g^{-1}}$.

10. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.
11. If g and h are elements from a group, prove that $\phi_g \phi_h = \phi_{gh}$.
12. Find two groups G and H such that $G \not\approx H$, but $\text{Aut}(G) \approx \text{Aut}(H)$.
13. Prove the assertion in Example 12 that the inner automorphisms ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, and ϕ_D of D_4 are distinct.
14. Find $\text{Aut}(Z_6)$.
15. If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups.
16. If a group G is isomorphic to H, prove that $\text{Aut}(G)$ is isomorphic to $\text{Aut}(H)$.
17. Suppose ϕ belongs to $\text{Aut}(Z_n)$ and a is relatively prime to n. If $\phi(a) = b$, determine a formula for $\phi(x)$.
18. Let H be the subgroup of all rotations in D_n and let ϕ be an automorphism of D_n. Prove that $\phi(H) = H$. (In words, an automorphism of D_n carries rotations to rotations.)
19. Let $H = \{\beta \in S_5 \mid \beta(1) = 1\}$ and $K = \{\beta \in S_5 \mid \beta(2) = 2\}$. Prove that H is isomorphic to K. Is the same true if S_5 is replaced by S_n, where $n \geq 3$?
20. Show that Z has infinitely many subgroups isomorphic to Z.
21. Let n be an even integer greater than 2 and let ϕ be an automorphism of D_n. Determine $\phi(R_{180})$.
22. Let ϕ be an automorphism of a group G. Prove that $H = \{x \in G \mid \phi(x) = x\}$ is a subgroup of G.
23. Give an example of a cyclic group of smallest order that contains a subgroup isomorphic to Z_{12} and a subgroup isomorphic to Z_{20}. No need to prove anything, but explain your reasoning.
24. Suppose that $\phi: Z_{20} \to Z_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?
25. Identify a group G that has subgroups isomorphic to Z_n for all positive integers n.
26. Prove that the mapping from $U(16)$ to itself given by $x \to x^3$ is an automorphism. What about $x \to x^5$ and $x \to x^7$? Generalize.
27. Let $r \in U(n)$. Prove that the mapping $\alpha: Z_n \to Z_n$ defined by $\alpha(s) = sr \bmod n$ for all s in Z_n is an automorphism of Z_n. (This exercise is referred to in this chapter.)
28. The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in Z \right\}$ is isomorphic to what familiar group? What if Z is replaced by $\mathbf{R}$?

29. If ϕ and γ are isomorphisms from the cyclic group $\langle a \rangle$ to some group and $\phi(a) = \gamma(a)$, prove that $\phi = \gamma$.

30. Suppose that ϕ: $Z_{50} \to Z_{50}$ is an automorphism with $\phi(11) = 13$. Determine a formula for $\phi(x)$.

31. Prove property 1 of Theorem 6.3.

32. Prove property 4 of Theorem 6.3.

33. Referring to Theorem 6.1, prove that T_g is indeed a permutation on the set G.

34. Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

35. Show that the mapping $\phi(a + bi) = a - bi$ is an automorphism of the group of complex numbers under addition. Show that ϕ preserves complex multiplication as well—that is, $\phi(xy) = \phi(x)\phi(y)$ for all x and y in $\mathbf{C}$. (This exercise is referred to in Chapter 15.)

36. Let

$$G = \{a + b\sqrt{2} \mid a, b \text{ are rational}\}$$

and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \middle| \, a, b \text{ are rational} \right\}.$$

Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition? (G and H are examples of rings—a topic we will take up in Part 3.)

37. Prove that Z under addition is not isomorphic to Q under addition.

38. Prove that the quaternion group (see Exercise 4, Supplementary Exercises for Chapters 1–4) is not isomorphic to the dihedral group D_4.

39. Let $\mathbf{C}$ be the complex numbers and

$$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\}.$$

Prove that $\mathbf{C}$ and M are isomorphic under addition and that $\mathbf{C}^*$ and M^*, the nonzero elements of M, are isomorphic under multiplication.

40. Let $\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbf{R}\}$. Show that the mapping ϕ: $(a_1, a_2, \ldots, a_n) \to (-a_1, -a_2, \ldots, -a_n)$ is an automorphism of the group $\mathbf{R}^n$ under componentwise addition. This automorphism is called *inversion*. Describe the action of ϕ geometrically.

41. Consider the following statement: The order of a subgroup divides the order of the group. Suppose you could prove this for finite permutation groups. Would the statement then be true for all finite groups? Explain.

42. Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that there is an infinite Abelian group for which the mapping $g \to g^2$ is one-to-one and operation-preserving but not an automorphism.
43. Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, that the mappings ϕ_g and ϕ_{zg} are equal).
44. Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbf{R}^+$ under multiplication to $\mathbf{R}$ under addition.
45. Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.
46. Combine the results of Exercises 43 and 45 into a single "if and only if" theorem.
47. If x and y are elements in S_n ($n \geq 3$), prove that $\phi_x = \phi_y$ implies $x = y$. (Here, ϕ_x is the inner automorphism of S_n induced by x.)
48. Let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.
49. Suppose the ϕ and γ are isomorphisms of some group G to the same group. Prove that $H = \{g \in G \mid \phi(g) = \gamma(g)\}$ is a subgroup of G.
50. Suppose that β is an automorphism of a group G. Prove that $H = \{g \in G \mid \beta^2(g) = g\}$ is a subgroup of G. Generalize.
51. Suppose that G is an Abelian group and ϕ is an automorphism of G. Prove that $H = \{x \in G \mid \phi(x) = x^{-1}\}$ is a subgroup of G.
52. Given a group G, define a new group G^* that has the same elements as G with the operation $*$ defines by $a * b = ba$ for all a and b in G^*. Prove that the mapping from G to G^* defined by $\phi(x) = x^{-1}$ for all x in G is an isomorphism from G onto G^*.
53. Let a belong to a group G and let $|a|$ be finite. Let ϕ_a be the automorphism of G given by $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$. Exhibit an element a from a group for which $1 < |\phi_a| < |a|$.
54. Let $G = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Show that G and H are isomorphic groups under addition. Does your isomorphism preserve multiplication? Generalize to the case when $G = \langle m \rangle$ and $H = \langle n \rangle$, where m and n are integers.
55. Suppose that ϕ is an automorphism of D_4 such that $\phi(R_{90}) = R_{270}$ and $\phi(V) = V$. Determine $\phi(D)$ and $\phi(H)$.
56. In $\text{Aut}(Z_9)$, let α_i denote the automorphism that sends 1 to i where $\gcd(i, 9) = 1$. Write α_5 and α_8 as permutations of $\{0, 1, \ldots, 8\}$ in disjoint cycle form. [For example, $\alpha_2 = (0)(124875)(36)$.]

57. Write the permutation corresponding to R_{90} in the left regular representation of D_4 in cycle form.

58. Show that every automorphism ϕ of the rational numbers Q under addition to itself has the form $\phi(x) = x\phi(1)$.

59. Prove that Q^+, the group of positive rational numbers under multiplication, is isomorphic to a proper subgroup.

60. Prove that Q, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

61. Prove that every automorphism of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication, maps positive numbers to positive numbers and negative numbers to negative numbers.

62. Let G be a finite group. Show that in the disjoint cycle form of the right regular representation $T_g(x) = xg$ of G, each cycle has length $|g|$.

63. Give a group theoretic proof that Q under addition is not isomorphic to $\mathbf{R}^+$ under multiplication.

Reference

1. J. R. Clay, "The Punctured Plane Is Isomorphic to the Unit Circle," *Journal of Number Theory* 1 (1969): 500–501.

Computer Exercises

Software for the computer exercise in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Chapter 7 exercises

to about 56 million cosets for testing. Cosets played a role in this effort because Rokicki's program could handle the 19.5+ billion elements in the same coset in about 20 seconds.

Exercises

I don't know, Marge. Trying is the first step towards failure.

HOMER SIMPSON

1. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (see Table 5.1 on page 111).
2. Let H be as in Exercise 1. How many left cosets of H in S_4 are there? (Determine this without listing them.)
3. Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in Z.
4. Rewrite the condition $a^{-1}b \in H$ given in property 5 of the lemma on page 145 in additive notation. Assume that the group is Abelian.
5. Let H be as in Exercise 3. Use Exercise 4 to decide whether or not the following cosets of H are the same.
   a. $11 + H$ and $17 + H$
   b. $-1 + H$ and $5 + H$
   c. $7 + H$ and $23 + H$
6. Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in Z. How many are there?
7. Find all of the left cosets of $\{1, 11\}$ in $U(30)$.
8. Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.
9. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.
10. Give an example of a group G and subgroups H and K such that $HK = \{h \in H, k \in K\}$ is not a subgroup of G.
11. If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.
12. Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.
13. Let H be a subgroup of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication. If $\mathbf{R}^+ \subseteq H \subseteq \mathbf{R}^*$, prove that $H = \mathbf{R}^+$ or $H = \mathbf{R}^*$.
14. Let $\mathbf{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbf{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.

15. Let G be a group of order 60. What are the possible orders for the subgroups of G?
16. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?
17. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.
18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \bmod n = 1$.
19. Compute $5^{15} \bmod 7$ and $7^{13} \bmod 11$.
20. Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.
21. Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.
22. Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.
23. Suppose that H is a subgroup of S_4 and that H contains (12) and (234). Prove that $H = S_4$.
24. Suppose that H and K are subgroups of G and there are elements a and b in G such that $aH \subseteq bK$. Prove that $H \subseteq K$.
25. Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.
26. Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)
27. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.
28. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?
29. Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.
30. Let $|G| = 8$. Show that G must have an element of order 2.
31. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.
32. Determine all finite subgroups of $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication.

33. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K|\,|K:H|$.

34. Suppose that a group contains elements of orders 1 through 10. What is the minimum possible order of the group?

35. Give an example of the dihedral group of smallest order that contains a subgroup isomorphic to Z_{12} and a subgroup isomorphic to Z_{20}. No need to prove anything, but explain your reasoning.

36. Show that in any group of order 100, either every element has order that is a power of a prime or there is an element of order 10.

37. Suppose that a finite Abelian group G has at least three elements of order 3. Prove that 9 divides $|G|$.

38. Prove that if G is a finite group, the index of $Z(G)$ cannot be prime.

39. Find an example of a subgroup H of a group G and elements a and b in G such that $aH \neq Hb$ and $aH \cap Hb \neq \phi$. (Compare with property 5 of cosets.)

40. Prove that a group of order 63 must have an element of order 3.

41. Let G be a group of order 100 that has a subgroup H of order 25. Prove that every element of G of order 5 is in H.

42. Let G be a group of order n and k be any integer relatively prime to n. Show that the mapping from G to G given by $g \to g^k$ is one-to-one. If G is also Abelian, show that the mapping given by $g \to g^k$ is an automorphism of G.

43. Let G be a group of permutations of a set S. Prove that the orbits of the members of S constitute a partition of S. (This exercise is referred to in this chapter and in Chapter 29.)

44. Prove that every subgroup of D_n of odd order is cyclic.

45. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.

- **a.** Find the stabilizer of 1 and the orbit of 1.
- **b.** Find the stabilizer of 3 and the orbit of 3.
- **c.** Find the stabilizer of 5 and the orbit of 5.

46. Prove that a group of order 12 must have an element of order 2.

47. Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all a in G.

48. Let G be a group of order pqr, where p, q, and r are distinct primes. If H and K are subgroups of G with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$.

49. Prove that a group that has more than one subgroup of order 5 must have order at least 25.

50. Prove that A_5 has a subgroup of order 12.

51. Prove that A_5 has no subgroup of order 30.

52. Prove that A_5 has no subgroup of order 15 to 20.

53. Suppose that α is an element from a permutation group G and one of its cycles in disjoint cycle form is $(a_1 a_2 \cdots a_k)$. Show that $\{a_1, a_2, \ldots, a_k\} \subseteq \text{orb}_G(a_i)$ for $1 = 1, 2, \ldots, k$.

54. Let G be a group and suppose that H is a subgroup of G with the property that for any a in G we have $aH = Ha$. (That is, every element of the form ah where h is some element of H can be written in the form $h_1 a$ for some $h_1 \in H$.) If a has order 2, prove that the set $K = H \cup aH$ is a subgroup of G. Generalize to the case that $|a| = k$.

55. Prove that A_5 is the only subgroup of S_5 of order 60.

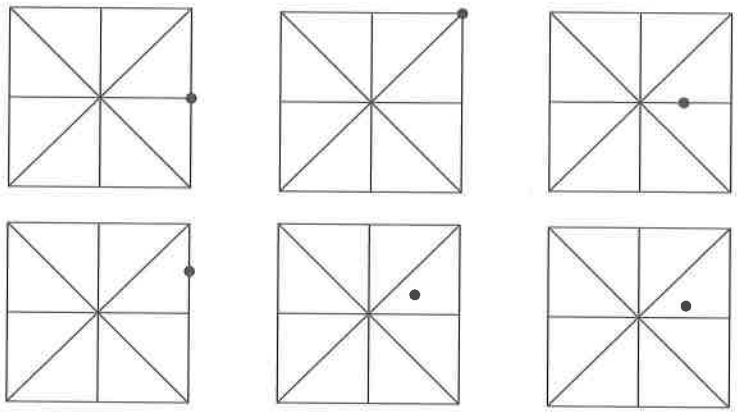
56. Why does the fact that A_4 has no subgroup of order 6 imply that $|Z(A_4)| = 1$?

57. Let $G = GL(2, \mathbf{R})$ and $H = SL(2, \mathbf{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2.

58. Let G be the group of rotations of a plane about a point P in the plane. Thinking of G as a group of permutations of the plane, describe the orbit of a point Q in the plane. (This is the motivation for the name "orbit.")

59. Let G be the rotation group of a cube. Label the faces of the cube 1 through 6, and let H be the subgroup of elements of G that carry face 1 to itself. If σ is a rotation that carries face 2 to face 1, give a physical description of the coset $H\sigma$.

60. The group D_4 acts as a group of permutations of the square regions shown below. (The axes of symmetry are drawn for reference purposes.) For each square region, locate the points in the orbit of the indicated point under D_4. In each case, determine the stabilizer of the indicated point.



61. Let $G = GL(2, \mathbf{R})$, the group of 2×2 matrices over $\mathbf{R}$ with nonzero determinant. Let H be the subgroup of matrices of determinant ± 1. If $a, b \in G$ and $aH = bH$, what can be said about det (a) and det (b)? Prove or disprove the converse. [Determinants have the property that det (xy) = det (x)det (y).]

62. Calculate the orders of the following (refer to Figure 27.5 for illustrations).

- **a.** The group of rotations of a regular tetrahedron (a solid with four congruent equilateral triangles as faces)
- **b.** The group of rotations of a regular octahedron (a solid with eight congruent equilateral triangles as faces)
- **c.** The group of rotations of a regular dodecahedron (a solid with 12 congruent regular pentagons as faces)
- **d.** The group of rotations of a regular icosahedron (a solid with 20 congruent equilateral triangles as faces)

63. Prove that the eight-element set in the proof of Theorem 7.5 is a group.

64. A soccer ball has 20 faces that are regular hexagons and 12 faces that are regular pentagons. Use Theorem 7.4 to explain why a soccer ball cannot have a 60° rotational symmetry about a line through the centers of two opposite hexagonal faces.

65. If G is a finite group with fewer than 100 elements and G has subgroups of orders 10 and 25, what is the order of G?

Computer Exercises

A computer exercise for this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Chapter 8 exercises

Exercises

What's the most difficult aspect of your life as a mathematician, Diane Maclagan, an assistant professor at Rutgers, was asked. "Trying to prove theorems," she said. And the most fun? "Trying to prove theorems."

1. Prove that the external direct product of any finite number of groups is a group. (This exercise is referred to in this chapter.)
2. Show that $Z_2 \oplus Z_2 \oplus Z_2$ has seven subgroups of order 2.
3. Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.
4. Show that $G \oplus H$ is Abelian if and only if G and H are Abelian. State the general case.
5. Prove or disprove that $Z \oplus Z$ is a cyclic group.
6. Prove, by comparing orders of elements, that $Z_8 \oplus Z_2$ is not isomorphic to $Z_4 \oplus Z_4$.
7. Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$. State the general case.
8. Is $Z_3 \oplus Z_9$ isomorphic to Z_{27}? Why?
9. Is $Z_3 \oplus Z_5$ isomorphic to Z_{15}? Why?
10. How many elements of order 9 does $Z_3 \oplus Z_9$ have? (Do not do this exercise by brute force.)
11. How many elements of order 4 does $Z_4 \oplus Z_4$ have? (Do not do this by examining each element.) Explain why $Z_4 \oplus Z_4$ has the same number of elements of order 4 as does $Z_{8000000} \oplus Z_{400000}$. Generalize to the case $Z_m \oplus Z_n$.
12. Give examples of four groups of order 12, no two of which are isomorphic. Give reasons why no two are isomorphic.
13. For each integer $n > 1$, give examples of two nonisomorphic groups of order n^2.
14. The dihedral group D_n of order $2n$ ($n \geq 3$) has a subgroup of n rotations and a subgroup of order 2. Explain why D_n cannot be isomorphic to the external direct product of two such groups.
15. Prove that the group of complex numbers under addition is isomorphic to $\mathbf{R} \oplus \mathbf{R}$.
16. Suppose that $G_1 \approx G_2$ and $H_1 \approx H_2$. Prove that $G_1 \oplus H_1 \approx G_2 \oplus H_2$. State the general case.
17. If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.
18. In $Z_{40} \oplus Z_{30}$, find two subgroups of order 12.

19. If r is a divisor of m and s is a divisor of n, find a subgroup of $Z_m \oplus Z_n$ that is isomorphic to $Z_r \oplus Z_s$.
20. Find a subgroup of $Z_{12} \oplus Z_{18}$ that is isomorphic to $Z_9 \oplus Z_4$.
21. Let G and H be finite groups and $(g, h) \in G \oplus H$. State a necessary and sufficient condition for $\langle (g, h) \rangle = \langle g \rangle \oplus \langle h \rangle$.
22. Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $Z_{30} \oplus Z_{20}$.
23. What is the order of any nonidentity element of $Z_3 \oplus Z_3 \oplus Z_3$? Generalize.
24. Let $m > 2$ be an even integer and let $n > 2$ be an odd integer. Find a formula for the number of elements of order 2 in $D_m \oplus D_n$.
25. Let M be the group of all real 2×2 matrices under addition. Let $N = \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R}$ under componentwise addition. Prove that M and N are isomorphic. What is the corresponding theorem for the group of $m \times n$ matrices under addition?
26. The group $S_3 \oplus Z_2$ is isomorphic to one of the following groups: Z_{12}, $Z_6 \oplus Z_2$, A_4, D_6. Determine which one by elimination.
27. Let G be a group, and let $H = \{(g, g) \mid g \in G\}$. Show that H is a subgroup of $G \oplus G$. (This subgroup is called the *diagonal* of $G \oplus G$.) When G is the set of real numbers under addition, describe $G \oplus G$ and H geometrically.
28. Find a subgroup of $Z_4 \oplus Z_2$ that is not of the form $H \oplus K$, where H is a subgroup of Z_4 and K is a subgroup of Z_2.
29. Find all subgroups of order 3 in $Z_9 \oplus Z_3$.
30. Find all subgroups of order 4 in $Z_4 \oplus Z_4$.
31. What is the largest order of any element in $Z_{30} \oplus Z_{20}$?
32. What is the order of the largest cyclic subgroup of $Z_6 \oplus Z_{10} \oplus Z_{15}$? What is the order of the largest cyclic subgroup of $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$?
33. Find three cyclic subgroups of maximum possible order in $Z_6 \oplus Z_{10} \oplus Z_{15}$ of the form $\langle a \rangle \oplus \langle b \rangle \oplus \langle c \rangle$, where $a \in Z_6$, $b \in Z_{10}$, and $c \in Z_{15}$.
34. How many elements of order 2 are in $Z_{2000000} \oplus Z_{4000000}$? Generalize.
35. Find a subgroup of $Z_{800} \oplus Z_{200}$ that is isomorphic to $Z_2 \oplus Z_4$.
36. Find a subgroup of $Z_{12} \oplus Z_4 \oplus Z_{15}$ that has order 9.
37. Prove that $\mathbf{R}^* \oplus \mathbf{R}^*$ is not isomorphic to $\mathbf{C}^*$. (Compare this with Exercise 15.)
38. Let

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b \in Z_3 \right\}.$$

(See Exercise 48 in Chapter 2 for the definition of multiplication.) Show that H is an Abelian group of order 9. Is H isomorphic to Z_9 or to $Z_3 \oplus Z_3$?

39. Let $G = \{3^m 6^n \mid m, n \in Z\}$ under multiplication. Prove that G is isomorphic to $Z \oplus Z$. Does your proof remain valid if $G = \{3^m 9^n \mid m, n \in Z\}$?

40. Let $(a_1, a_2, \ldots, a_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Give a necessary and sufficient condition for $|(a_1, a_2, \ldots, a_n)| = \infty$.

41. Prove that $D_3 \oplus D_4 \ncong D_{12} \oplus Z_2$.

42. Determine the number of cyclic subgroups of order 15 in $Z_{90} \oplus Z_{36}$. Provide a generator for each of the subgroups of order 15.

43. List the elements in the groups $U_5(35)$ and $U_7(35)$.

44. Prove or disprove that $U(40) \oplus Z_6$ is isomorphic to $U(72) \oplus Z_4$.

45. Prove or disprove that C^* has a subgroup isomorphic to $Z_2 \oplus Z_2$.

46. Let G be a group isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{nk}$. Let x be the product of all elements in G. Describe all possibilities for x.

47. If a group has exactly 24 elements of order 6, how many cyclic subgroups of order 6 does it have?

48. For any Abelian group G and any positive integer n, let $G^n = \{g^n \mid g \in G\}$ (see Exercise 17, Supplementary Exercises for Chapters 1–4). If H and K are Abelian, show that $(H \oplus K)^n = H^n \oplus K^n$.

49. Express $\mathrm{Aut}(U(25))$ in the form $Z_m \oplus Z_n$.

50. Determine $\mathrm{Aut}(Z_2 \oplus Z_2)$.

51. Suppose that $n_1, n_2, \ldots, n_k$ are positive even integers. How many elements of order 2 does $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ have ? How many are there if we drop the requirement that $n_1, n_2, \ldots, n_k$ must be even?

52. Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{60} \oplus Z_6 \oplus Z_2$?

53. Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{15} \oplus Z_4 \oplus Z_{12}$?

54. Find an isomorphism from Z_{12} to $Z_4 \oplus Z_3$.

55. How many isomorphisms are there from Z_{12} to $Z_4 \oplus Z_3$?

56. Suppose that ϕ is an isomorphism from $Z_3 \oplus Z_5$ to Z_{15} and $\phi(2, 3) = 2$. Find the element in $Z_3 \oplus Z_5$ that maps to 1.

57. If ϕ is an isomorphism from $Z_4 \oplus Z_3$ to Z_{12}, what is $\phi(2, 0)$? What are the possibilities for $\phi(1, 0)$? Give reasons for your answer.

58. Prove that $Z_5 \oplus Z_5$ has exactly six subgroups of order 5.

59. Let (a, b) belong to $Z_m \oplus Z_n$. Prove that $|(a, b)|$ divides $\mathrm{lcm}(m, n)$.

60. Let $G = \{ax^2 + bx + c \mid a, b, c \in Z_3\}$. Add elements of G as you would polynomials with integer coefficients, except use modulo 3 addition. Prove that G is isomorphic to $Z_3 \oplus Z_3 \oplus Z_3$. Generalize.

61. Determine all cyclic groups that have exactly two generators.
62. Explain a way that a string of length n of the four nitrogen bases A, T, G, and C could be modeled with the external direct product of n copies of $Z_2 \oplus Z_2$.
63. Let p be a prime. Prove that $Z_p \oplus Z_p$ has exactly $p + 1$ subgroups of order p.
64. Give an example of an infinite non-Abelian group that has exactly six elements of finite order.
65. Give an example to show that there exists a group with elements a and b such that $|a| = \infty$, $|b| = \infty$, and $|ab| = 2$.
66. Express $U(165)$ as an external direct product of cyclic groups of the form Z_n.
67. Express $U(165)$ as an external direct product of U-groups in four different ways.
68. Without doing any calculations in $\text{Aut}(Z_{20})$, determine how many elements of $\text{Aut}(Z_{20})$ have order 4. How many have order 2?
69. Without doing any calculations in $\text{Aut}(Z_{720})$, determine how many elements of $\text{Aut}(Z_{720})$ have order 6.
70. Without doing any calculations in $U(27)$, decide how many subgroups $U(27)$ has.
71. What is the largest order of any element in $U(900)$?
72. Let p and q be odd primes and let m and n be positive integers. Explain why $U(p^m) \oplus U(q^n)$ is not cyclic.
73. Use the results presented in this chapter to prove that $U(55)$ is isomorphic to $U(75)$.
74. Use the results presented in this chapter to prove that $U(144)$ is isomorphic to $U(140)$.
75. For every $n > 2$, prove that $U(n)^2 = \{x^2 \mid x \in U(n)\}$ is a proper subgroup of $U(n)$.
76. Show that $U(55)^3 = \{x^3 \mid x \in U(55)\}$ is $U(55)$.
77. Find an integer n such that $U(n)$ contains a subgroup isomorphic to $Z_5 \oplus Z_5$.
78. Find a subgroup of order 6 in $U(700)$.
79. Show that there is a U-group containing a subgroup isomorphic to $Z_3 \oplus Z_3$.
80. Find an integer n such that $U(n)$ is isomorphic to $Z_2 \oplus Z_4 \oplus Z_9$.
81. What is the smallest positive integer k such that $x^k = e$ for all x in $U(7 \cdot 17)$? Generalize to $U(pq)$ where p and q are distinct primes.
82. If k divides m and m divides n, how are $U_m(n)$ and $U_k(n)$ related?

83. Let $p_1, p_2, \ldots, p_k$ be distinct odd primes and $n_1, n_2, \ldots, n_k$ be positive integers. Determine the number of elements of order 2 in $U(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$. How many are there in $U(2^n p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$ where n is at least 3?

84. Show that no U-group has order 14.

85. Show that there is a U-group containing a subgroup isomorphic to Z_{14}.

86. Show that no U-group is isomorphic to $Z_4 \oplus Z_4$.

87. Show that there is a U-group containing a subgroup isomorphic to $Z_4 \oplus Z_4$.

88. Using the RSA scheme with $p = 37$, $q = 73$, and $e = 5$, what number would be sent for the message "RM"?

89. Assuming that a message has been sent via the RSA scheme with $p = 37$, $q = 73$, and $e = 5$, decode the received message "34."

Computer Exercises

Computer exercises in this chapter are available at the website:

http://www.d.umn.edu/~jgallian

References

1. J. A. Gallian and D. Rusin, "Factoring Groups of Integers Modulo n," *Mathematics Magazine* 53 (1980): 33–36.
2. D. Shanks, *Solved and Unsolved Problems in Number Theory,* 2nd ed., New York: Chelsea, 1978.
3. S. Washburn, T. Marlowe, and C. Ryan, *Discrete Mathematics,* Reading, MA: Addison-Wesley, 1999.

Suggested Readings

Y. Cheng, "Decompositions of U-Groups," *Mathematics Magazine* 62 (1989): 271–273.

This article explores the decomposition of $U(st)$, where s and t are relatively prime, in greater detail than we have provided.

David J. Devries, "The Group of Units in Z_m," *Mathematics Magazine* 62 (1989): 340–342.

This article provides a simple proof that $U(n)$ is not cyclic when n is not of the form 1, 2, 4, p^k, or $2p^k$, where p is an odd prime.

Leonard Aldeman

honors are: the
uting Machinery
Kanallakis Award
nd election to the
Engineering, the
rts and Sciences,
of Sciences.
ition is the Henry
hair in Computer
Computer Science
t the University of
ere he has been

n Adleman, visit:

kipedia.com

s.com/1994/12/13/
t-work-leonard-
ne-high-spots-of-
eory.html?
all&src=pm

Supplementary Exercises for Chapters 5–8

My mind rebels at stagnation. Give me problems, give me work, give me the most obstruse cryptogram, or the most intricate analysis, and I am in my own proper atmosphere.

SHERLOCK HOLMES, *The Sign of Four*

True/false questions for Chapters 5–8 are available on the Web at:

www.d.umn.edu/~jgallian/TF

1. A subgroup N of a group G is called a *characteristic subgroup* if $\phi(N) = N$ for all automorphisms ϕ of G. (The term *characteristic* was first applied by G. Frobenius in 1895.) Prove that every subgroup of a cyclic group is characteristic.
2. Prove that the center of a group is characteristic.
3. The *commutator subgroup* G' of a group G is the subgroup generated by the set $\{x^{-1}y^{-1}xy \mid x, y \in G\}$. (That is, every element of G' has the form $a_1^{i_1}a_2^{i_2} \cdots a_k^{i_k}$, where each a_j has the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$, and k is any positive integer.) Prove that G' is a characteristic subgroup of G. (This subgroup was first introduced by G. A. Miller in 1898.)
4. Prove that the property of being a characteristic subgroup is transitive. That is, if N is a characteristic subgroup of K and K is a characteristic subgroup of G, then N is a characteristic subgroup of G.
5. Let $G = Z_3 \oplus Z_3 \oplus Z_3$ and let H be the subgroup of $SL(3, Z_3)$ consisting of

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c \in Z_3 \right\}.$$

   (See Exercise 48 in Chapter 2 for the definition of multiplication.) Determine the number of elements of each order in G and H. Are G and H isomorphic? (This exercise shows that two groups with the same number of elements of each order need not be isomorphic.)
6. Let H and K be subgroups of a group G and let $HK = \{hk \mid h \in H, k \in K\}$ and $KH = \{kh \mid k \in K, h \in H\}$. Prove that HK is a group if and only if $HK = KH$.
7. Let G be a finite Abelian group in which every nonidentity element has order 2. If $|G| > 2$, prove that the product of all the elements in G is the identity.

8. Prove that S_4 is not isomorphic to $D_4 \oplus Z_3$.
9. Let G be a group. For any element g of G, define $gZ(G) = \{gh \mid h \in Z(G)\}$. If a is an element of G of order 4, prove that $H = Z(G) \cup aZ(G) \cup a^2Z(G) \cup a^3Z(G)$ is a subgroup of G. Generalize to the case that $|a| = k$.
10. The *exponent* of a group is the smallest positive integer n such that $x^n = e$ for all x in the group. Prove that every finite group has an exponent that divides the order of the group.
11. Determine all U-groups of exponent 2.
12. Suppose that H and K are subgroups of a group and that $|H|$ and $|K|$ are relatively prime. Show that $H \cap K = \{e\}$.
13. Let $\mathbf{R}^+$ denote the multiplicative group of positive real numbers and let $T = \{a + bi \in \mathbf{C}^* \mid a^2 + b^2 = 1\}$ be the multiplicative group of complex numbers on the unit circle. Show that every element of $\mathbf{C}^*$ can be uniquely expressed in the form rz, where $r \in \mathbf{R}^+$ and $z \in T$.
14. Prove that Q^* under multiplication is not isomorphic to $\mathbf{R}^*$ under multiplication.
15. Prove that Q under addition is not isomorphic to $\mathbf{R}$ under addition.
16. Prove that $\mathbf{R}$ under addition is not isomorphic to $\mathbf{R}^*$ under multiplication.
17. Show that Q^+ (the set of positive rational numbers) under multiplication is not isomorphic to Q under addition.
18. Suppose that $G = \{e, x, x^2, y, yx, yx^2\}$ is a non-Abelian group with $|x| = 3$ and $|y| = 2$. Show that $xy = yx^2$.
19. Let p be an odd prime. Show that 1 is the only solution of $x^{p-2} = 1$ in $U(p)$.
20. Let G be an Abelian group under addition. Let n be a fixed positive integer and let $H = \{(g, ng) \mid g \in G\}$. Show that H is a subgroup of $G \oplus G$. When G is the set of real numbers under addition, describe H geometrically.
21. Find a subgroup of $Z_{12} \oplus Z_{20}$ that is isomorphic to $Z_4 \oplus Z_5$.
22. Suppose that $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Prove that $Z(G) = Z(G_1) \oplus Z(G_2) \oplus \cdots \oplus Z(G_n)$.
23. Exhibit four nonisomorphic groups of order 18.
24. What is the order of the largest cyclic subgroup in $\mathrm{Aut}(Z_{720})$? (*Hint:* It is not necessary to consider automorphisms of Z_{720}.)
25. Let G be the group of all permutations of the positive integers. Let H be the subset of elements of G that can be expressed as a product of a finite number of cycles. Prove that H is a subgroup of G.

26. Let G be a group and let $g \in G$. Show that $Z(G)\langle g\rangle$ is a subgroup of G.

27. Show that $D_{11} \oplus Z_3 \ncong D_3 \oplus Z_{11}$. (This exercise is referred to in Chapter 24.)

28. Show that $D_{33} \ncong D_{11} \oplus Z_3$. (This exercise is referred to in Chapter 24.)

29. Show that $D_{33} \ncong D_3 \oplus Z_{11}$. (This exercise is referred to in Chapter 24.)

30. Exhibit four nonisomorphic groups of order 66. (This exercise is referred to in Chapter 24.)

31. Prove that $|\text{Inn}(G)| = 1$ if and only if G is Abelian.

32. Prove that $x^{100} = 1$ for all x in $U(1000)$.

33. Find a subgroup of order 6 in $U(450)$.

34. List four elements of $Z_{20} \oplus Z_5 \oplus Z_{60}$ that form a noncyclic subgroup.

35. In S_{10}, let $\beta = (13)(17)(265)(289)$. Find an element in S_{10} that commutes with β but is not a power of β.

36. Prove or disprove that $Z_4 \oplus Z_{15} \approx Z_6 \oplus Z_{10}$.

37. Prove or disprove that $D_{12} \approx Z_3 \oplus D_4$.

38. Describe a three-dimensional solid whose symmetry group is isomorphic to D_5.

39. Let $G = U(15) \oplus Z_{10} \oplus S_5$. Find the order of $(2, 3, (123)(15))$. Find the inverse of $(2, 3, (123)(15))$.

40. Let $G = Z \oplus Z_{10}$ and let $H = \{g \in G \mid |g| = \infty \text{ or } |g| = 1\}$. Prove or disprove that H is a subgroup of G.

41. Find a subgroup H of $Z_{p^2} \oplus Z_{p^2}$ such that $(Z_{p^2} \oplus Z_{p^2})/H$ is isomorphic to $Z_p \oplus Z_p$.

42. Find three subgroups H_1, H_2, and H_3 of $Z_{p^2} \oplus Z_{p^2}$ such that $(Z_{p^2} \oplus Z_{p^2})/H_i$ is isomorphic to Z_{p^2} for $i = 1, 2, 3$.

43. Find an element of order 10 in A_9.

44. In the left regular representation for D_4, write $T_{R_{90}}$ and T_H in matrix form and in cycle form.

45. How many elements of order 6 are in S_7?

46. Prove that $S_3 \oplus S_4$ is not isomorphic to a subgroup of S_6.

47. Find a permutation β such that $\beta^2 = (13579)(268)$.

48. In $\mathbf{R} \oplus \mathbf{R}$ under componentwise addition, let $H = \{(x, 3x) \mid x \in \mathbf{R}\}$. (Note that H is the subgroup of all points on the line $y = 3x$.) Show that $(2, 5) + H$ is a straight line passing through the point $(2, 5)$ and parallel to the line $y = 3x$.

49. In $\mathbf{R} \oplus \mathbf{R}$, suppose that H is the subgroup of all points lying on a line through the origin. Show that any left coset of H is a line parallel to H.

50. Let G be a group of permutations on the set $\{1, 2, \ldots, n\}$. Recall that $\text{stab}_G(1) = \{\alpha \in G \mid \alpha(1) = 1\}$. If γ sends 1 to k, prove that $\gamma\,\text{stab}_G(1) = \{\beta \in G \mid \beta(1) = k\}$.

51. Let H be a subgroup of G and let $a, b \in G$. Show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

52. Suppose that G is a finite Abelian group that does not contain a subgroup isomorphic to $Z_p \oplus Z_p$ for any prime p. Prove that G is cyclic.

53. Let p be a prime. Determine the number of elements of order p in $Z_{p^2} \oplus Z_{p^2}$.

54. Show that $Z_{p^2} \oplus Z_{p^2}$ has exactly one subgroup isomorphic to $Z_p \oplus Z_p$.

55. Let p be a prime. Determine the number of subgroups of $Z_{p^2} \oplus Z_{p^2}$ that are isomorphic to Z_{p^2}.

56. Find a group of order $3^2 \cdot 5^2 \cdot 7^2 \cdot 2^8$ that contains a subgroup isomorphic to A_8.

57. Let p and q be distinct odd primes. Let $n = \text{lcm}(p - 1, q - 1)$. Prove that $x^n = 1$ for all $x \in U(pq)$.

58. Give a simple characterization of all positive integers n for which $Z_n \approx H \oplus Z_n/H$ for every subgroup H of Z_n.

59. Prove that the permutations (12) and (123 . . . n) generate S_n. (That is, every member of S_n can be expressed as some combination of these elements.)

60. Suppose that n is even and σ is an $(n - 1)$-cycle in S_n. Show that σ does not commute with any element of order 2.

61. Suppose that n is odd and σ is an n-cycle in S_n. Prove that σ does not commute with any element of order 2.

62. Let $H = \{\alpha \in S_n \mid \alpha$ maps the set $\{1, 2\}$ to itself$\}$. Prove that $C((12)) = H$.

63. Let m be a positive integer. For any n-cycle σ, show that σ^m is the product of $\gcd(m, n)$ disjoint cycles, each of length $n/\gcd(m, n)$.

Chapter 9 exercises

The U-groups provide a convenient way to illustrate the preceding ideas and to clarify the distinction between internal and external direct products. It follows directly from Theorem 8.3, its corollary, and Theorem 9.6 that if $m = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$, then

$$\begin{aligned} U(m) &= U_{m/n_1}(m) \times U_{m/n_2}(m) \times \cdots \times U_{m/n_k}(m) \\ &\approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k). \end{aligned}$$

Let us return to the examples given following Theorem 8.3.

$$\begin{aligned} U(105) &= U(15 \cdot 7) = U_{15}(105) \times U_7(105) \\ &= \{1, 16, 31, 46, 61, 76\} \times \{1, 8, 22, 29, 43, 64, 71, 92\} \\ &\approx U(7) \oplus U(15), \\ U(105) &= U(5 \cdot 21) = U_5(105) \times U_{21}(105) \\ &= \{1, 11, 16, 26, 31, 41, 46, 61, 71, 76, 86, 101\} \\ &\quad \times \{1, 22, 43, 64\} \approx U(21) \oplus U(5), \\ U(105) &= U(3 \cdot 5 \cdot 7) = U_{35}(105) \times U_{21}(105) \times U_{15}(105) \\ &= \{1, 71\} \times \{1, 22, 43, 64\} \times \{1, 16, 31, 46, 61, 76\} \\ &\approx U(3) \oplus U(5) \oplus U(7). \end{aligned}$$

Exercises

The heart of mathematics is its problems.

Paul Halmos

1. Let $H = \{(1), (12)\}$. Is H normal in S_3?
2. Prove that A_n is normal in S_n.
3. In D_4, let $K = \{R_0, R_{90}, R_{180}, R_{270}\}$. Write HR_{90} in the form xH, where $x \in K$. Write DR_{270} in the form xD, where $x \in K$. Write $R_{90}V$ in the form Vx, where $x \in K$.
4. Write $(12)(13)(14)$ in the form $\alpha(12)$, where $\alpha \in A_4$. Write $(1234)(12)(23)$, in the form $\alpha(1234)$, where $\alpha \in A_4$.
5. Show that if G is the internal direct product of $H_1, H_2, \ldots, H_n$ and $i \neq j$ with $1 \leq i \leq n$, $1 \leq j \leq n$, then $H_i \cap H_j = \{e\}$. (This exercise is referred to in this chapter.)
6. Let $H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle| a, b, d \in \mathbf{R}, ad \neq 0 \right\}$. Is H a normal subgroup of $GL(2, \mathbf{R})$?
7. Let $G = GL(2, \mathbf{R})$ and let K be a subgroup of $\mathbf{R}^*$. Prove that $H = \{A \in G \mid \det A \in K\}$ is a normal subgroup of G.
8. Viewing $\langle 3 \rangle$ and $\langle 12 \rangle$ as subgroups of Z, prove that $\langle 3 \rangle / \langle 12 \rangle$ is isomorphic to Z_4. Similarly, prove that $\langle 8 \rangle / \langle 48 \rangle$ is isomorphic to Z_6. Generalize to arbitrary integers k and n.

9. Prove that if H has index 2 in G, then H is normal in G. (This exercise is referred to in Chapters 24 and 25 and this chapter.)
10. Let $H = \{(1), (12)(34)\}$ in A_4.
    a. Show that H is not normal in A_4.
    b. Referring to the multiplication table for A_4 in Table 5.1 on page 111, show that, although $\alpha_6 H = \alpha_7 H$ and $\alpha_9 H = \alpha_{11} H$, it is not true that $\alpha_6\alpha_9 H = \alpha_7\alpha_{11} H$. Explain why this proves that the left cosets of H do not form a group under coset multiplication.
11. Let $G = Z_4 \oplus U(4)$, $H = \langle(2, 3)\rangle$, and $K = \langle(2, 1)\rangle$. Show that G/H is not isomorphic to G/K. (This shows that $H \approx K$ does not imply that $G/H \approx G/K$.)
12. Prove that a factor group of a cyclic group is cyclic.
13. Prove that a factor group of an Abelian group is Abelian.
14. What is the order of the element $14 + \langle 8\rangle$ in the factor group $Z_{24}/\langle 8\rangle$?
15. What is the order of the element $4U_5(105)$ in the factor group $U(105)/U_5(105)$?
16. Recall that $Z(D_6) = \{R_0, R_{180}\}$. What is the order of the element $R_{60}Z(D_6)$ in the factor group $D_6/Z(D_6)$?
17. Let $G = Z/\langle 20\rangle$ and $H = \langle 4\rangle/\langle 20\rangle$. List the elements of H and G/H.
18. What is the order of the factor group $Z_{60}/\langle 15\rangle$?
19. What is the order of the factor group $(Z_{10} \oplus U(10))/\langle(2, 9)\rangle$?
20. Construct the Cayley table for $U(20)/U_5(20)$.
21. Prove that an Abelian group of order 33 is cyclic.
22. Determine the order of $(Z \oplus Z)/\langle(2, 2)\rangle$. Is the group cyclic?
23. Determine the order of $(Z \oplus Z)/\langle(4, 2)\rangle$. Is the group cyclic?
24. The group $(Z_4 \oplus Z_{12})/\langle(2, 2)\rangle$ is isomorphic to one of Z_8, $Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$. Determine which one by elimination.
25. Let $G = U(32)$ and $H = \{1, 31\}$. The group G/H is isomorphic to one of Z_8, $Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$. Determine which one by elimination.
26. Let G be the group of quaternions given by the table in Exercise 4 of the Supplementary Exercises for Chapters 1–4, and let H be the subgroup $\{e, a^2\}$. Is G/H isomorphic to Z_4 or $Z_2 \oplus Z_2$?
27. Let $G = U(16)$, $H = \{1, 15\}$, and $K = \{1, 9\}$. Are H and K isomorphic? Are G/H and G/K isomorphic?
28. Let $G = Z_4 \oplus Z_4$, $H = \{(0, 0), (2, 0), (0, 2), (2, 2)\}$, and $K = \langle(1, 2)\rangle$. Is G/H isomorphic to Z_4 or $Z_2 \oplus Z_2$? Is G/K isomorphic to Z_4 or $Z_2 \oplus Z_2$?
29. Prove that $A_4 \oplus Z_3$ has no subgroup of order 18.

30. Express $U(165)$ as an internal direct product of proper subgroups in four different ways.

31. Let $\mathbf{R}^*$ denote the group of all nonzero real numbers under multiplication. Let $\mathbf{R}^+$ denote the group of positive real numbers under multiplication. Prove that $\mathbf{R}^*$ is the internal direct product of $\mathbf{R}^+$ and the subgroup $\{1, -1\}$.

32. Prove that D_4 cannot be expressed as an internal direct product of two proper subgroups.

33. Let H and K be subgroups of a group G. If $G = HK$ and $g = hk$, where $h \in H$ and $k \in K$, is there any relationship among $|g|$, $|h|$, and $|k|$? What if $G = H \times K$?

34. In Z, let $H = \langle 5 \rangle$ and $K = \langle 7 \rangle$. Prove that $Z = HK$. Does $Z = H \times K$?

35. Let $G = \{3^a 6^b 10^c \mid a, b, c \in Z\}$ under multiplication and $H = \{3^a 6^b 12^c \mid a, b, c \in Z\}$ under multiplication. Prove that $G = \langle 3 \rangle \times \langle 6 \rangle \times \langle 10 \rangle$, whereas $H \neq \langle 3 \rangle \times \langle 6 \rangle \times \langle 12 \rangle$.

36. Determine all subgroups of $\mathbf{R}^*$ (nonzero reals under multiplication) of index 2.

37. Let G be a finite group and let H be a normal subgroup of G. Prove that the order of the element gH in G/H must divide the order of g in G.

38. Let H be a normal subgroup of G and let a belong to G. If the element aH has order 3 in the group G/H and $|H| = 10$, what are the possibilities for the order of a?

39. If H is a normal subgroup of a group G, prove that $C(H)$, the centralizer of H in G, is a normal subgroup of G.

40. Let ϕ be an isomorphism from a group G onto a group $\overline{G}$. Prove that if H is a normal subgroup of G, then $\phi(H)$ is a normal subgroup of $\overline{G}$.

41. Show that Q, the group of rational numbers under addition, has no proper subgroup of finite index.

42. An element is called a *square* if it can be expressed in the form b^2 for some b. Suppose that G is an Abelian group and H is a subgroup of G. If every element of H is a square and every element of G/H is a square, prove that every element of G is a square. Does your proof remain valid when "square" is replaced by "nth power," where n is any integer?

43. Show, by example, that in a factor group G/H it can happen that $aH = bH$ but $|a| \neq |b|$.

44. Observe from the table for A_4 given in Table 5.1 on page 111 that the subgroup given in Example 9 of this chapter is the only subgroup of A_4 of order 4. Why does this imply that this subgroup must be normal in A_4? Generalize this to arbitrary finite groups.

45. Let p be a prime. Show that if H is a subgroup of a group of order $2p$ that is not normal, then H has order 2.

46. Show that D_{13} is isomorphic to $\mathrm{Inn}(D_{13})$.

47. Suppose that N is a normal subgroup of a finite group G and H is a subgroup of G. If $|G/N|$ is prime, prove that H is contained in N or that $NH = G$.

48. If G is a group and $|G: Z(G)| = 4$, prove that $G/Z(G) \approx Z_2 \oplus Z_2$.

49. Suppose that G is a non-Abelian group of order p^3, where p is a prime, and $Z(G) \neq \{e\}$. Prove that $|Z(G)| = p$.

50. If $|G| = pq$, where p and q are primes that are not necessarily distinct, prove that $|Z(G)| = 1$ or pq.

51. Let N be a normal subgroup of G and let H be a subgroup of G. If N is a subgroup of H, prove that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G.

52. Let G be an Abelian group and let H be the subgroup consisting of all elements of G that have finite order. (See Exercise 20 in the Supplementary Exercises for Chapters 1–4.) Prove that every nonidentity element in G/H has infinite order.

53. Determine all subgroups of $\mathbf{R}^*$ that have finite index.

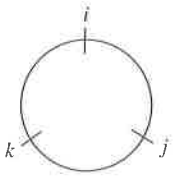
54. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1$, $-i = (-1)i$, $1^2 = (-1)^2 = 1$, $ij = -ji = k, jk = -kj = i$, and $ki = -ik = j$.

a. Construct the Cayley table for G.

b. Show that $H = \{1, -1\} \lhd G$.

c. Construct the Cayley table for G/H. Is G/H isomorphic to Z_4 or $Z_2 \oplus Z_2$?

(The rules involving i, j, and k can be remembered by using the circle below.



Going clockwise, the product of two consecutive elements is the third one. The same is true for going counterclockwise, except that we obtain the negative of the third element.) This is the group of quaternions that was given in another form in Exercise 4 in the Supplementary Exercises for Chapters 1–4. It was invented by William Hamilton in 1843. The quaternions are used to describe rotations in three-dimensional space, and they are used in physics. The quaternions can be used to extend the complex numbers in a natural way.

55. In D_4, let $K = \{R_0, D\}$ and let $L = \{R_0, D, D', R_{180}\}$. Show that $K \lhd L \lhd D_4$, but that K is not normal in D_4. (Normality is not transitive. Compare Exercise 4, Supplementary Exercises for Chapters 5–8.)

56. Show that the intersection of two normal subgroups of G is a normal subgroup of G. Generalize.

57. Give an example of subgroups H and K of a group G such that HK is not a subgroup of G.

58. If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.

59. Let N be a normal subgroup of a group G. If N is cyclic, prove that every subgroup of N is also normal in G. (This exercise is referred to in Chapter 24.)

60. Without looking at inner automorphisms of D_n, determine the number of such automorphisms.

61. Let H be a normal subgroup of a finite group G and let $x \in G$. If $\gcd(|x|, |G/H|) = 1$, show that $x \in H$. (This exercise is referred to in Chapter 25.)

62. Let G be a group and let G' be the subgroup of G generated by the set $S = \{x^{-1}y^{-1}xy \mid x, y \in G\}$. (See Exercise 3, Supplementary Exercises for Chapters 5–8, for a more complete description of G'.)

a. Prove that G' is normal in G.

b. Prove that G/G' is Abelian.

c. If G/N is Abelian, prove that $G' \leq N$.

d. Prove that if H is a subgroup of G and $G' \leq H$, then H is normal in G.

63. If N is a normal subgroup of G and $|G/N| = m$, show that $x^m \in N$ for all x in G.

64. Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a normal subgroup of G.

65. If G is non-Abelian, show that $\mathrm{Aut}(G)$ is not cyclic.

66. Let $|G| = p^n m$, where p is prime and $\gcd(p, m) = 1$. Suppose that H is a normal subgroup of G of order p^n. If K is a subgroup of G of order p^k, show that $K \subseteq H$.

67. Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n. Show, by example, that the assumption that G is finite is necessary.

68. Recall that a subgroup N of a group G is called characteristic if $\phi(N) = N$ for all automorphisms ϕ of G. If N is a characteristic subgroup of G, show that N is a normal subgroup of G.

69. In D_4, let $\mathcal{H} = \{R_0, H\}$. Form an operation table for the cosets $\mathcal{H}$, $D\mathcal{H}$, $V\mathcal{H}$, and $D'\mathcal{H}$. Is the result a group table? Does your answer contradict Theorem 9.2?

70. Prove that A_4 is the only subgroup of S_4 of order 12.

71. If $|G| = 30$ and $|Z(G)| = 5$, what is the structure of $G/Z(G)$?

72. If H is a normal subgroup of G and $|H| = 2$, prove that H is contained in the center of G.

73. Prove that A_5 cannot have a normal subgroup of order 2.

74. Let G be a finite group and let H be an odd-order subgroup of G of index 2. Show that the product of all the elements of G (taken in any order) cannot belong to H.

75. Let G be a group and p a prime. Suppose that $H = \{g^p \mid g \in G\}$ is a subgroup of G. Show that H is normal and that every nonidentity element of G/H has order p.

76. Suppose that H is a normal subgroup of G. If $|H| = 4$ and gH has order 3 in G/H, find a subgroup of order 12 in G.

77. Let G be a group and H an odd-order subgroup of G of index 2. Show that H contains every element of G of odd order.

78. A proper subgroup H of a group G is called *maximal* if there is no subgroup K such that $H \subset K \subset G$ (that is, there is no subgroup K properly contained between H and G). Show that $Z(G)$ is never a maximal subgroup of a group G.

79. Let G be a group of order 100 that has exactly one subgroup of order 5. Prove that it has a subgroup of order 10.

Suggested Readings

Michael Brennan and Des MacHale, "Variations on a Theme: A_4 Definitely Has No Subgroup of Order Six!," *Mathematics Magazine* 73 (2000): 36–40.

The authors offer 11 proofs that A_4 has no subgroup of order 6. These proofs provide a review of many of the ideas covered thus far in this text.

J. A. Gallian, R. S. Johnson, and S. Peng, "On Quotient Structures of Z^n," *Pi Mu Epsilon Journal* 9 (1993): 524–526.

The authors determine the structure of the group $(Z \oplus Z)/\langle(a, b)\rangle$ and related groups.

Although an isomorphism is a special case of a homomorphism, the two concepts have entirely different roles. Whereas isomorphisms allow us to look at a group in an alternative way, homomorphisms act as investigative tools. The following analogy between homomorphisms and photography may be instructive.† A photograph of a person cannot tell us the person's exact height, weight, or age. Nevertheless, we *may* be able to decide from a photograph whether the person is tall or short, heavy or thin, old or young, male or female. In the same way, a homomorphic image of a group gives us *some* information about the group.

In certain branches of group theory, and especially in physics and chemistry, one often wants to know all homomorphic images of a group that are matrix groups over the complex numbers (these are called *group representations*). Here, we may carry our analogy with photography one step further by saying that this is like wanting photographs of a person from many different angles (front view, profile, head-to-toe view, close-up, etc.), as well as x-rays! Just as this composite information from the photographs reveals much about the person, several homomorphic images of a group reveal much about the group.

Exercises

The greater the difficulty, the more glory in surmounting it. Skillful pilots gain their reputation from storms and tempests.

EPICURUS

1. Prove that the mapping given in Example 2 is a homomorphism.
2. Prove that the mapping given in Example 3 is a homomorphism.
3. Prove that the mapping given in Example 4 is a homomorphism.
4. Prove that the mapping given in Example 11 is a homomorphism.
5. Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication, and let r be a positive integer. Show that the mapping that takes x to x^r is a homomorphism from $\mathbf{R}^*$ to $\mathbf{R}^*$ and determine the kernel. Which values of r yield an isomorphism?
6. Let G be the group of all polynomials with real coefficients under addition. For each f in G, let $\int f$ denote the antiderivative of f that passes through the point $(0, 0)$. Show that the mapping $f \to \int f$ from G to G is a homomorphism. What is the kernel of this mapping? Is this mapping a homomorphism if $\int f$ denotes the antiderivative of f that passes through $(0, 1)$?

†"All perception of truth is the detection of an analogy." Henry David Thoreau, *Journal.*

7. If ϕ is a homomorphism from G to H and σ is a homomorphism from H to K, show that $\sigma\phi$ is a homomorphism from G to K. How are Ker ϕ and Ker $\sigma\phi$ related? If ϕ and σ are onto and G is finite, describe [Ker $\sigma\phi$:Ker ϕ] in terms of $|H|$ and $|K|$.

8. Let G be a group of permutations. For each σ in G, define

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Prove that sgn is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this homomorphism allow you to conclude that A_n is a normal subgroup of S_n of index 2? Why does this prove Exercise 23 of Chapter 5?

9. Prove that the mapping from $G \oplus H$ to G given by $(g, h) \to g$ is a homomorphism. What is the kernel? This mapping is called the *projection* of $G \oplus H$ onto G.

10. Let G be a subgroup of some dihedral group. For each x in G, define

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation,} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

Prove that ϕ is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this prove Exercise 25 of Chapter 3?

11. Prove that $(Z \oplus Z)/(\langle(a, 0)\rangle \times \langle(0, b)\rangle)$ is isomorphic to $Z_a \oplus Z_b$.

12. Suppose that k is a divisor of n. Prove that $Z_n/\langle k\rangle \approx Z_k$.

13. Prove that $(A \oplus B)/(A \oplus \{e\}) \approx B$.

14. Explain why the correspondence $x \to 3x$ from Z_{12} to Z_{10} is not a homomorphism.

15. Suppose that ϕ is a homomorphism from Z_{30} to Z_{30} and Ker $\phi = \{0, 10, 20\}$. If $\phi(23) = 9$, determine all elements that map to 9.

16. Prove that there is no homomorphism from $Z_8 \oplus Z_2$ onto $Z_4 \oplus Z_4$.

17. Prove that there is no homomorphism from $Z_{16} \oplus Z_2$ onto $Z_4 \oplus Z_4$.

18. Can there be a homomorphism from $Z_4 \oplus Z_4$ onto Z_8? Can there be a homomorphism from Z_{16} onto $Z_2 \oplus Z_2$? Explain your answers.

19. Suppose that there is a homomorphism ϕ from Z_{17} to some group and that ϕ is not one-to-one. Determine ϕ.

20. How many homomorphisms are there from Z_{20} onto Z_8? How many are there to Z_8?

21. If ϕ is a homomorphism from Z_{30} onto a group of order 5, determine the kernel of ϕ.

22. Suppose that ϕ is a homomorphism from a finite group G onto $\overline{G}$ and that $\overline{G}$ has an element of order 8. Prove that G has an element of order 8. Generalize.
23. Suppose that ϕ is a homomorphism from Z_{36} to a group of order 24.
    a. Determine the possible homomorphic images.
    b. For each image in part a, determine the corresponding kernel of ϕ.
24. Suppose that ϕ: $Z_{50} \to Z_{15}$ is a group homomorphism with $\phi(7) = 6$.
    a. Determine $\phi(x)$.
    b. Determine the image of ϕ.
    c. Determine the kernel of ϕ.
    d. Determine $\phi^{-1}(3)$. That is, determine the set of all elements that map to 3.
25. How many homomorphisms are there from Z_{20} onto Z_{10}? How many are there to Z_{10}?
26. Determine all homomorphisms from Z_4 to $Z_2 \oplus Z_2$.
27. Determine all homomorphisms from Z_n to itself.
28. Suppose that ϕ is a homomorphism from S_4 onto Z_2. Determine Ker ϕ. Determine all homomorphisms from S_4 to Z_2.
29. Suppose that there is a homomorphism from a finite group G onto Z_{10}. Prove that G has normal subgroups of indexes 2 and 5.
30. Suppose that ϕ is a homomorphism from a group G onto $Z_6 \oplus Z_2$ and that the kernel of ϕ has order 5. Explain why G must have normal subgroups of orders 5, 10, 15, 20, 30, and 60.
31. Suppose that ϕ is a homomorphism from $U(30)$ to $U(30)$ and that Ker $\phi = \{1, 11\}$. If $\phi(7) = 7$, find all elements of $U(30)$ that map to 7.
32. Find a homomorphism ϕ from $U(30)$ to $U(30)$ with kernel $\{1, 11\}$ and $\phi(7) = 7$.
33. Suppose that ϕ is a homomorphism from $U(40)$ to $U(40)$ and that Ker $\phi = \{1, 9, 17, 33\}$. If $\phi(11) = 11$, find all elements of $U(40)$ that map to 11.
34. Find a homomorphism ϕ from $U(40)$ to $U(40)$ with kernel $\{1, 9, 17, 33\}$ and $\phi(11) = 11$.
35. Prove that the mapping ϕ: $Z \oplus Z \to Z$ given by $(a, b) \to a - b$ is a homomorphism. What is the kernel of ϕ? Describe the set $\phi^{-1}(3)$ (that is, all elements that map to 3).
36. Suppose that there is a homomorphism ϕ from $Z \oplus Z$ to a group G such that $\phi((3, 2)) = a$ and $\phi((2, 1)) = b$. Determine $\phi((4, 4))$ in terms of a and b. Assume that the operation of G is addition.

37. Let $H = \{z \in C^* \mid |z| = 1\}$. Prove that C^*/H is isomorphic to $\mathbf{R}^+$, the group of positive real numbers under multiplication.

38. Let α be a homomorphism from G_1 to H_1 and β be a homomorphism from G_2 to H_2. Determine the kernel of the homomorphism γ from $G_1 \oplus G_2$ to $H_1 \oplus H_2$ defined by $\gamma(g_1, g_2) = (\alpha(g_1), \beta(g_2))$.

39. Prove that the mapping $x \to x^6$ from $\mathbf{C}^*$ to $\mathbf{C}^*$ is a homomorphism. What is the kernel?

40. For each pair of positive integers m and n, we can define a homomorphism from Z to $Z_m \oplus Z_n$ by $x \to (x \bmod m, x \bmod n)$. What is the kernel when $(m, n) = (3, 4)$? What is the kernel when $(m, n) = (6, 4)$? Generalize.

41. (Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

42. (Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.

43. Let $\phi(d)$ denote the Euler phi function of d (see page 85). Show that the number of homomorphisms from Z_n to Z_k is $\Sigma\phi(d)$, where the sum runs over all common divisors d of n and k. [It follows from number theory that this sum is actually $\gcd(n, k)$.]

44. Let k be a divisor of n. Consider the homomorphism from $U(n)$ to $U(k)$ given by $x \to x \bmod k$. What is the relationship between this homomorphism and the subgroup $U_k(n)$ of $U(n)$?

45. Determine all homomorphic images of D_4 (up to isomorphism).

46. Let N be a normal subgroup of a finite group G. Use the theorems of this chapter to prove that the order of the group element gN in G/N divides the order of g.

47. Suppose that G is a finite group and that Z_{10} is a homomorphic image of G. What can we say about $|G|$? Generalize.

48. Suppose that Z_{10} and Z_{15} are both homomorphic images of a finite group G. What can be said about $|G|$? Generalize.

49. Suppose that for each prime p, Z_p is the homomorphic image of a group G. What can we say about $|G|$? Give an example of such a group.

50. (For students who have had linear algebra.) Suppose that x is a particular solution to a system of linear equations and that S is the entire solution set of the corresponding homogeneous system of linear equations. Explain why property 6 of Theorem 10.1 guarantees that $x + S$ is the entire solution set of the nonhomogeneous system. In particular, describe the relevant groups and the homomorphism between them.

51. Let N be a normal subgroup of a group G. Use property 7 of Theorem 10.2 to prove that every subgroup of G/N has the form H/N, where H is a subgroup of G. (This exercise is referred to in Chapter 24.)
52. Show that a homomorphism defined on a cyclic group is completely determined by its action on a generator of the group.
53. Use the First Isomorphism Theorem to prove Theorem 9.4.
54. Let α and β be group homomorphisms from G to $\overline{G}$ and let $H = \{g \in G \mid \alpha(g) = \beta(g)\}$. Prove or disprove that H is a subgroup of G.
55. Let $Z[x]$ be the group of polynomials in x with integer coefficients under addition. Prove that the mapping from $Z[x]$ into Z given by $f(x) \to f(3)$ is a homomorphism. Give a geometric description of the kernel of this homomorphism. Generalize.
56. Prove that the mapping from $\mathbf{R}$ under addition to $GL(2, \mathbf{R})$ that takes x to

$$\begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}$$

is a group homomorphism. What is the kernel of the homomorphism?
57. Suppose there is a homomorphism ϕ from G onto $Z_2 \oplus Z_2$. Prove that G is the union of three proper normal subgroups.
58. If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \oplus G/K$.
59. Suppose that H and K are distinct subgroups of G of index 2. Prove that $H \cap K$ is a normal subgroup of G of index 4 and that $G/(H \cap K)$ is not cyclic.
60. Suppose that the number of homomorphisms from G to H is n. How many homomorphisms are there from G to $H \oplus H \oplus \cdots \oplus H$ (s terms)? When H is Abelian, how many homomorphisms are there from $G \oplus G \oplus \cdots \oplus G$ (s terms) to H?
61. Prove that every group of order 77 is cyclic.
62. Determine all homomorphisms from Z onto S_3. Determine all homomorphisms from Z to S_3.
63. Let G be an Abelian group. Determine all homomorphisms from S_3 to G.
64. If ϕ is an isomorphism from a group G under addition to a group $\overline{G}$ under addition, prove that for any integer n, the mapping from G to $\overline{G}$ defined by $\gamma(x) = n\phi(x)$ is a homomorphism from G to $\overline{G}$.
65. Prove that the mapping from $\mathbf{C}^*$ to $\mathbf{C}^*$ given by $\phi(z) = z^2$ is a homomorphism and that $\mathbf{C}^*/\{1, -1\}$ is isomorphic to $\mathbf{C}^*$.

66. Let p be a prime. Determine the number of homomorphisms from $Z_p \oplus Z_p$ into Z_p.

67. Suppose G is an Abelian group under addition with the property that for every positive integer n, the set $nG = \{ng \mid g \in G\} = G$. Show that every proper subgroup of G is properly contained in a proper subgroup of G. Name two familiar groups that satisfy the hypothesis.

Computer Exercise

A computer exercise for this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Chapter 11 exercises

Exercises

You know it ain't easy, you know how hard it can be.

JOHN LENNON AND PAUL McCARTNEY,
"The Ballad of John and Yoko"*

1. What is the smallest positive integer n such that there are two nonisomorphic groups of order n? Name the two groups.
2. What is the smallest positive integer n such that there are three nonisomorphic Abelian groups of order n? Name the three groups.
3. What is the smallest positive integer n such that there are exactly four nonisomorphic Abelian groups of order n? Name the four groups.
4. Calculate the number of elements of order 2 in each of Z_{16}, $Z_8 \oplus Z_2$, $Z_4 \oplus Z_4$, and $Z_4 \oplus Z_2 \oplus Z_2$. Do the same for the elements of order 4.
5. Prove that any Abelian group of order 45 has an element of order 15. Does every Abelian group of order 45 have an element of order 9?
6. Show that there are two Abelian groups of order 108 that have exactly one subgroup of order 3.
7. Show that there are two Abelian groups of order 108 that have exactly four subgroups of order 3.
8. Show that there are two Abelian groups of order 108 that have exactly 13 subgroups of order 3.
9. Suppose that G is an Abelian group of order 120 and that G has exactly three elements of order 2. Determine the isomorphism class of G.
10. Find all Abelian groups (up to isomorphism) of order 360.
11. Prove that every finite Abelian group can be expressed as the (external) direct product of cyclic groups of orders $n_1, n_2, \ldots, n_t$, where n_{i+1} divides n_i for $i = 1, 2, \ldots, t - 1$. (This exercise is referred to in this chapter.)
12. Suppose that the order of some finite Abelian group is divisible by 10. Prove that the group has a cyclic subgroup of order 10.
13. Show, by example, that if the order of a finite Abelian group is divisible by 4, the group need not have a cyclic subgroup of order 4.
14. On the basis of Exercises 12 and 13, draw a general conclusion about the existence of cyclic subgroups of a finite Abelian group.

15. How many Abelian groups (up to isomorphism) are there
    a. of order 6?
    b. of order 15?
    c. of order 42?
    d. of order pq, where p and q are distinct primes?
    e. of order pqr, where p, q, and r are distinct primes?
    f. Generalize parts d and e.
16. How does the number (up to isomorphism) of Abelian groups of order n compare with the number (up to isomorphism) of Abelian groups of order m where
    a. $n = 3^2$ and $m = 5^2$?
    b. $n = 2^4$ and $m = 5^4$?
    c. $n = p^r$ and $m = q^r$, where p and q are prime?
    d. $n = p^r$ and $m = p^r q$, where p and q are distinct primes?
    e. $n = p^r$ and $m = p^r q^2$, where p and q are distinct primes?
17. Up to isomorphism, how many additive Abelian groups of order 16 have the property that $x + x + x + x = 0$ for all x in the group?
18. Let $p_1, p_2, \cdots, p_n$ be distinct primes. Up to isomorphism, how many Abelian groups are there of order $p_1^4 p_2^4 \cdots p_n^4$?
19. The symmetry group of a nonsquare rectangle is an Abelian group of order 4. Is it isomorphic to Z_4 or $Z_2 \oplus Z_2$?
20. Verify the corollary to the Fundamental Theorem of Finite Abelian Groups in the case that the group has order 1080 and the divisor is 180.
21. The set $\{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ is a group under multiplication modulo 91. Determine the isomorphism class of this group.
22. Suppose that G is a finite Abelian group that has exactly one subgroup for each divisor of $|G|$. Show that G is cyclic.
23. Characterize those integers n such that the only Abelian groups of order n are cyclic.
24. Characterize those integers n such that any Abelian group of order n belongs to one of exactly four isomorphism classes.
25. Refer to Example 1 in this chapter and explain why it is unnecessary to compute the orders of the last five elements listed to determine the isomorphism class of G.
26. Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ under multiplication modulo 96. Express G as an external and an internal direct product of cyclic groups.

27. Let $G = \{1, 7, 43, 49, 51, 57, 93, 99, 101, 107, 143, 149, 151, 157, 193, 199\}$ under multiplication modulo 200. Express G as an external and an internal direct product of cyclic groups.

28. The set $G = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ is a group under multiplication modulo 45. Write G as an external and an internal direct product of cyclic groups of prime-power order.

29. Suppose that G is an Abelian group of order 9. What is the maximum number of elements (excluding the identity) of which one needs to compute the order to determine the isomorphism class of G? What if G has order 18? What about 16?

30. Suppose that G is an Abelian group of order 16, and in computing the orders of its elements, you come across an element of order 8 and two elements of order 2. Explain why no further computations are needed to determine the isomorphism class of G.

31. Let G be an Abelian group of order 16. Suppose that there are elements a and b in G such that $|a| = |b| = 4$ and $a^2 \neq b^2$. Determine the isomorphism class of G.

32. Prove that an Abelian group of order 2^n $(n \geq 1)$ must have an odd number of elements of order 2.

33. Without using Lagrange's Theorem, show that an Abelian group of odd order cannot have an element of even order.

34. Let G be the group of all $n \times n$ diagonal matrices with ± 1 diagonal entries. What is the isomorphism class of G?

35. Prove the assertion made in the proof of Lemma 2 that $G = \langle a \rangle K$.

36. Suppose that G is a finite Abelian group. Prove that G has order p^n, where p is prime, if and only if the order of every element of G is a power of p.

37. Dirichlet's Theorem says that, for every pair of relatively prime integers a and b, there are infinitely many primes of the form $at + b$. Use Dirichlet's Theorem to prove that every finite Abelian group is isomorphic to a subgroup of a U-group.

38. Determine the isomorphism class of $\text{Aut}(Z_2 \oplus Z_3 \oplus Z_5)$.

39. Give an example to show that Lemma 2 is false if G is non-Abelian.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Supplementary Exercises for Chapters 9–11

Every prospector drills many a dry hole, pulls out his rig, and moves on.

JOHN L. HESS

True/false questions for Chapters 9–11 are available on the Web at:

http://www.d.umn.edu/~jgallian/TF

1. Suppose that H is a subgroup of G and that each left coset of H in G is some right coset of H in G. Prove that H is normal in G.
2. Use a factor group-induction argument to prove that a finite Abelian group of order n has a subgroup of order m for every positive divisor m of n.
3. Let $\text{diag}(G) = \{(g, g) \mid g \in G\}$. Prove that $\text{diag}(G) \lhd G \oplus G$ if and only if G is Abelian. When G is finite, what is the index of $\text{diag}(G)$ in $G \oplus G$?
4. Let H be any group of rotations in D_n. Prove that H is normal in D_n.
5. Prove that $\text{Inn}(G) \lhd \text{Aut}(G)$.
6. Let H be a subgroup of G. Prove that H is a normal subgroup if and only if, for all a and b in G, $ab \in H$ implies $ba \in H$.
7. The factor group $GL(2, \mathbf{R})/SL(2, \mathbf{R})$ is isomorphic to some very familiar group. What is the group?
8. Let k be a divisor of n. The factor group $(Z/\langle n\rangle)/(\langle k\rangle/\langle n\rangle)$ is isomorphic to some very familiar group. What is the group?
9. Let

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c \in Q \right\}$$

under matrix multiplication.

   a. Find $Z(H)$.
   b. Prove that $Z(H)$ is isomorphic to Q under addition.
   c. Prove that $H/Z(H)$ is isomorphic to $Q \oplus Q$.
   d. Are your proofs for parts a and b valid when Q is replaced by $\mathbf{R}$? Are they valid when Q is replaced by Z_p, where p is prime?
10. Prove that $D_4/Z(D_4)$ is isomorphic to $Z_2 \oplus Z_2$.
11. Prove that Q/Z under addition is an infinite group in which every element has finite order.
12. Show that the intersection of any collection of normal subgroups of a group is a normal subgroup.

13. Let $n > 1$ be a fixed integer and let G be a group. If the set $H = \{x \in G \mid |x| = n\}$ together with the identity forms a subgroup of G, prove that it is a normal subgroup of G. In the case where such a subgroup exists, what can be said about n? Give an example of a non-Abelian group that has such a subgroup. Give an example of a group G and a prime n for which the set H together with the identity is not a subgroup.
14. Show that Q/Z has a unique subgroup of order n for each positive integer n.
15. If H and K are normal Abelian subgroups of a group and $H \cap K = \{e\}$, prove that HK is Abelian.
16. Let G be a group of odd order. Prove that the mapping $x \to x^2$ from G to itself is one-to-one.
17. Suppose that G is a group of permutations on some set. If $|G| = 60$ and $\text{orb}_G(5) = \{1, 5\}$, prove that $\text{stab}_G(5)$ is normal in G.
18. Suppose that $G = H \times K$ and that N is a normal subgroup of H. Prove that N is normal in G.
19. Show that there is no homomorphism from $Z_8 \oplus Z_2 \oplus Z_2$ onto $Z_4 \oplus Z_4$.
20. Show that there is no homomorphism from A_4 onto a group of order 2, 4, or 6, but that there is a homomorphism from A_4 onto a group of order 3.
21. Let H be a normal subgroup of S_4 of order 4. Prove that S_4/H is isomorphic to S_3.
22. Suppose that ϕ is a homomorphism of $U(36)$, $\text{Ker}\ \phi = \{1, 13, 25\}$, and $\phi(5) = 17$. Determine all elements that map to 17.
23. Let $n = 2m$, where m is odd. How many elements of order 2 does $D_n/Z(D_n)$ have? How many elements are in the subgroup $\langle R_{360/n}\rangle/Z(D_n)$? How do these numbers compare with the number of elements of order 2 in D_m?
24. Suppose that H is a normal subgroup of a group G of odd order and that $|H| = 5$. Show that $H \subseteq Z(G)$.
25. Let G be an Abelian group and let n be a positive integer. Let $G_n = \{g \mid g^n = e\}$ and $G^n = \{g^n \mid g \in G\}$. Prove that G/G_n is isomorphic to G^n.
26. Let $\mathbf{R}^+$ denote the multiplicative group of positive reals and let $T = \{a + bi \in \mathbf{C} \mid a^2 + b^2 = 1\}$ be the multiplicative group of complex numbers of norm 1. Show that $\mathbf{C}^*$ is the internal direct product of $\mathbf{R}^+$ and T.

27. Let G be a finite group and let p be a prime. If $p^2 > |G|$, show that any subgroup of order p is normal in G.

28. Let $G = Z \oplus Z$ and $H = \{(x, y) \mid x \text{ and } y \text{ are even integers}\}$. Show that H is a subgroup of G. Determine the order of G/H. To which familiar group is G/H isomorphic?

29. Let n be a positive integer. Prove that every element of order n in Q/Z is contained in $\langle 1/n + Z \rangle$.

30. (1997 Putnam Competition) Let G be a group and let $\phi: G \to G$ be a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1g_2g_3 = e = h_1h_2h_3$. Prove that there exists an element a in G such that $\psi(x) = a\phi(x)$ is a homomorphism.

31. Prove that every homomorphism from $Z \oplus Z$ into Z has the form $(x, y) \to ax + by$, where a and b are integers.

32. Prove that every homomorphism from $Z \oplus Z$ into $Z \oplus Z$ has the form $(x, y) \to (ax + by, cx + dy)$, where a, b, c, and d are integers.

33. Prove that Q/Z is not isomorphic to a proper subgroup of itself.

34. Prove that for each positive integer n, the group Q/Z has exactly $\phi(n)$ elements of order n (ϕ is the Euler phi function).

35. Show that any group with more than two elements has an automorphism other than the identity mapping.

36. A proper subgroup H of a group G is called *maximal* if there is no subgroup K such that $H \subset K \subset G$. Prove that Q under addition has no maximal subgroups.

37. Let G be the group of quaternions as given in Exercise 4 of the Supplementary Exercises for Chapters 1–4 and let $H = \langle a^2 \rangle$. Determine whether G/H is isomorphic to Z_4 or $Z_2 \oplus Z_2$. Is G/H isomorphic to a subgroup of G?

38. Write the dihedral group D_8 as $\{R_0, R_{45}, R_{90}, R_{135}, R_{180}, R_{225}, R_{270}, R_{315}, F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8\}$ and let $N = \{R_0, R_{90}, R_{180}, R_{270}\}$. Prove that N is normal in D_8. Given that $F_1N = \{F_1, F_4, F_3, F_2\}$, determine whether D_8/N is cyclic.

39. Let G be the group $\left\{ \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} \middle| \text{ where } a, b \in \mathbf{R}, b \neq 0 \right\}$ and $H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \middle| \text{ where } x \in \mathbf{R} \right\}$. Show that H is a subgroup of G. Is H a normal subgroup of G? Justify your answer.

40. Find a subgroup H of $Z_{p^2} \oplus Z_{p^2}$ such that $(Z_{p^2} \oplus Z_{p^2})/H$ is isomorphic to $Z_p \oplus Z_p$.

41. Recall that H is a characteristic subgroup of K if $\phi(H) = H$ for every automorphism ϕ of K. Prove that if H is a characteristic subgroup of K, and K is a normal subgroup of G, then H is a normal subgroup of G.