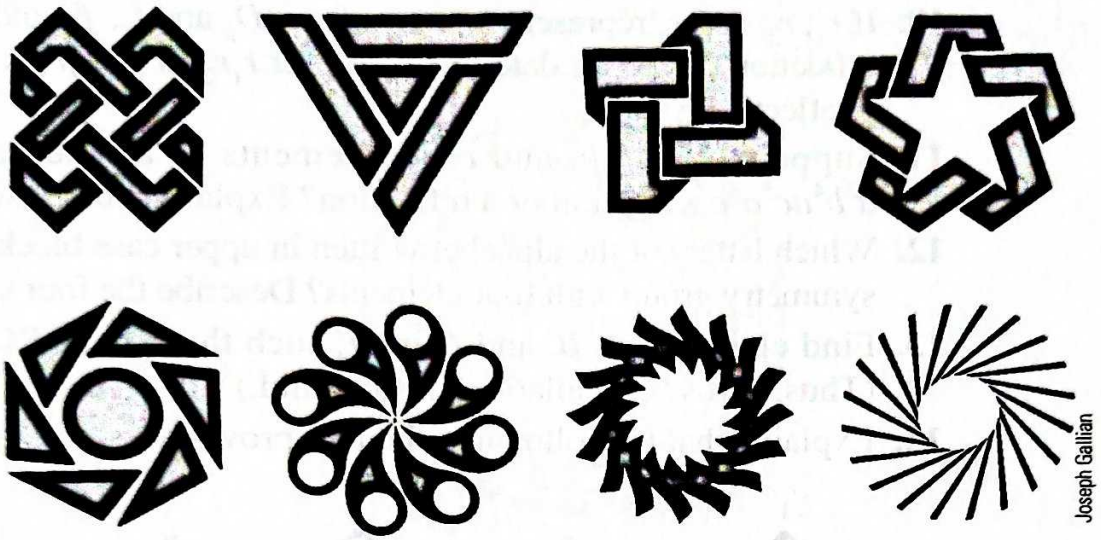


Figure 1.5 Logos with cyclic rotation symmetry groups.

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.

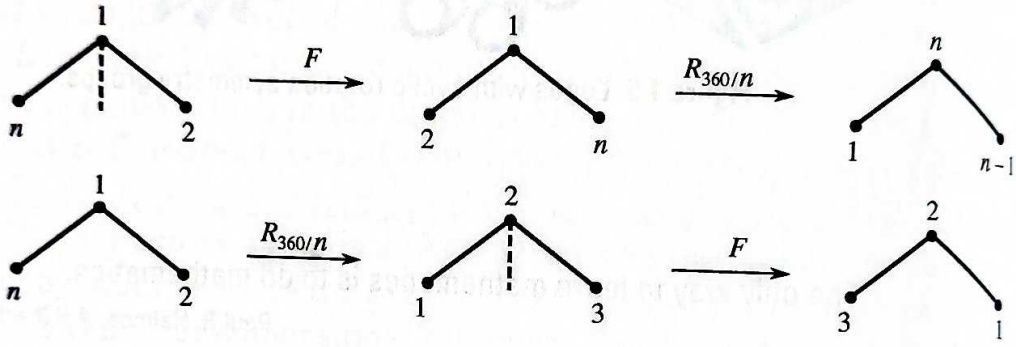
10. If r_1, r_2, and r_3 represent rotations from D_n and f_1, f_2, and f_3 represent reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

11. Suppose that a, b, and c are elements of a dihedral group. Is $a^2b^4ac^5a^3c$ a rotation or a reflection? Explain your reasoning.

12. Which letters of the alphabet written in upper case block style have a symmetry group with four elements? Describe the four symmetries.

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

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



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

16. 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.

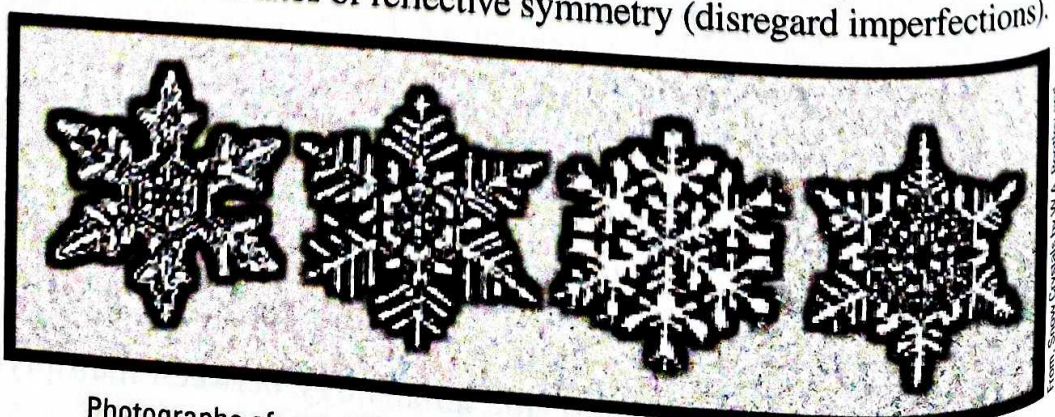
17. Describe the symmetries of a noncircular ellipse. Do the same for a hyperbola.

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

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

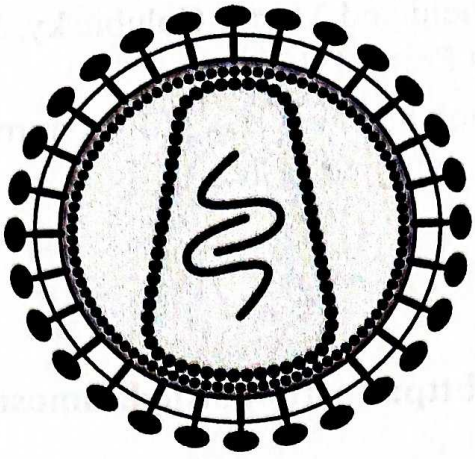
Describe the symmetries of this strip. Is the group of symmetries of the strip Abelian?

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



Photographs of snowflakes from the Bentley and Humphreys atlas.

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



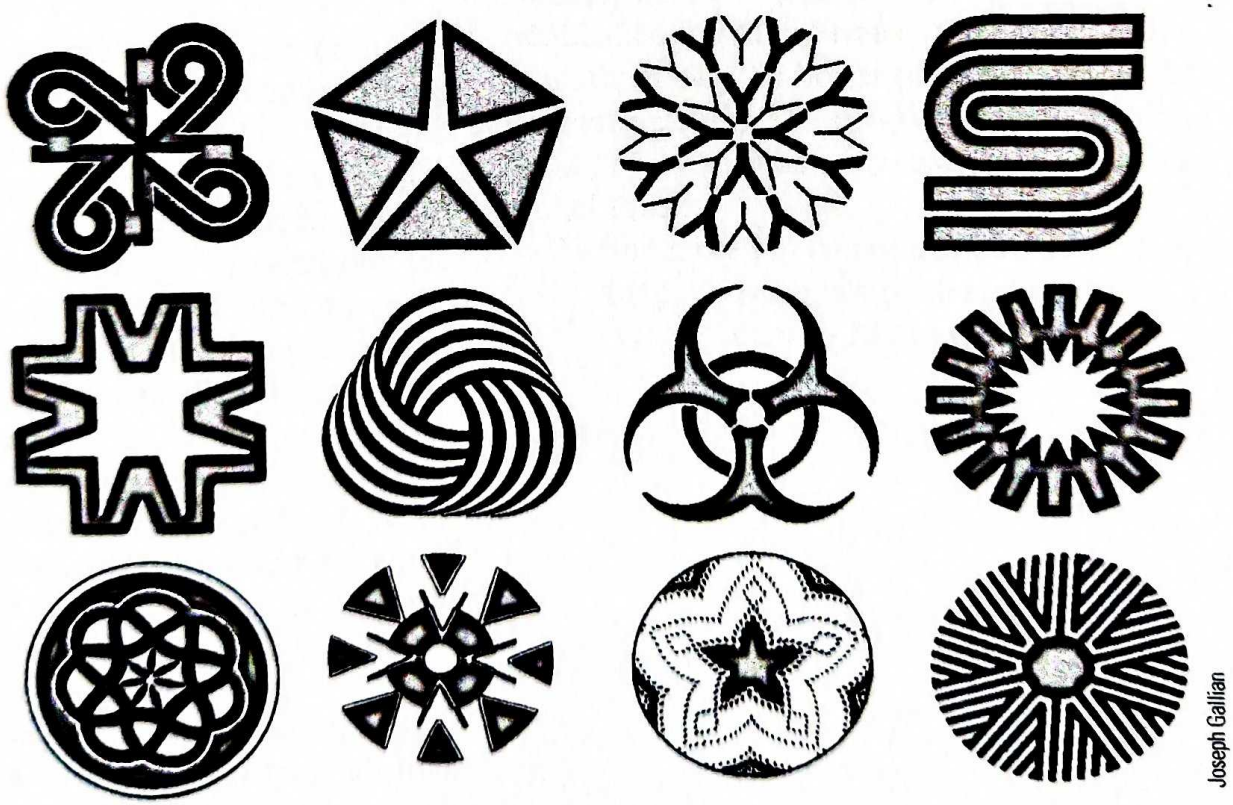
George V. Kelvin

21. Let X, Y, R_{90} be elements of D_4 with $Y \neq R_{90}$ and $X^2Y = R_{90}$. Determine Y. Show your reasoning.

22. If F is a reflection in the dihedral group D_n find all elements X in D_n such that $X^2 = F$ and all elements X in D_n such that $X^3 = F$.

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).



Joseph Gallian

25. 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?

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
   e. exponentiation of integers
2. Which of the following binary operations are associative?
   a. subtraction of integers
   b. division of nonzero rationals
   c. function composition of polynomials with real coefficients
   d. multiplication of 2×2 matrices with integer entries
   e. exponentiation of integers
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
   e. exponentiation of integers
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 $GL(2, \mathbf{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

d. In $GL(2, Z_7)$, $\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{-1}$

7. Give two reasons why the set of odd integers under addition is not a group.

8. List the elements of $U(20)$.

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. Let a belong to a group and $a^{12} = e$. Express the inverse of each of the elements a, a^6, a^8, and a^{11} in the form a^k for some positive integer k.

12. In $U(9)$ find the inverse of 2, 7, and 8.

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. Suppose that a and b belong to a group and $a^5 = e$ and $b^7 = e$. Write $a^{-2}b^{-4}$ and $(a^2b^4)^{-2}$ without using negative exponents.

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. Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Show that $G = H$ as sets.

18. List the members of $K = \{x^2 \mid x \in D_4\}$ and $L = \{x \in D_4 \mid x^2 = e\}$.

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, 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 $a_1a_2 \cdots a_n$?

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 $ab = ba$.
Prove that in a group, $(ab)^{-2} = b^{-2}a^{-2}$ 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 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.)

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. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

49. 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.)

50. Prove the assertion made in Example 19 that the set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime.

51. 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.)

52. 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.)

omputer Exercises

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

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

ferences

1. Max Born, *My Life: Recollections of a Nobel Laureate*, New York: Charles Scribner's Sons, 1978.

2. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, Vol. 3, New York: Springer-Verlag, 1982.

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 43).

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. Complete the statement "A group element x is its own inverse if and only if $|x| =$ _____."
13. For any group elements a and x, prove that $|xax^{-1}| = |a|$. This exercise is referred to in Chapter 24.
14. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.
15. (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"?
16. Let G be the group of symmetries of a circle and R be a rotation of the circle of $\sqrt{2}$ degrees. What is $|R|$?

17. For each proper divisor $k > 1$ of a positive integer 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.)

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. For any group elements a and b, prove that $|ab| = |ba|$.

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. Let n be a positive even integer and let H be a subgroup of Z_n of odd order. Prove that every member of H is an even integer.

26. 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.

27. Let H be a subgroup of D_n of odd order. Prove that every member of H is a rotation.

28. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

29. For every even integer n, show that D_n has a subgroup of order 4.

30. Suppose that H is a proper subgroup of Z under addition and H contains 18, 30, and 40. Determine H.

31. 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?

32. Suppose that H is a subgroup of Z under addition and that H contains 2^{50} and 3^{50}. What are the possibilities for H?

33. Prove that the dihedral group of order 6 does not have a subgroup of order 4.

34. 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?)

35. 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 $C(a)$.]

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

37. 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?

38. 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.

39. Let G be an Abelian group and $H = \{x \in G \mid |x|$ is 1 or even$\}$. Give an example to show that H need not be a subgroup of G.

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

41. 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 $\langle S \rangle = \{s_1^{n_1} s_2^{n_2} \cdots s_m^{n_m} \mid m \geq 1, s_i \in S, n_i \in Z\}$. (The s_i terms need not be distinct.)

42. 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 $\langle k \rangle$.

43. Prove Theorem 3.6.

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

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

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 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.)

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. Prove that a group of even order must have an odd number of elements of order 2.

50. 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?

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. Give an example of elements a and b from a group such that a has finite order, b has infinite order and ab has finite order.

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. In the group $\mathbf{R}^*$ find elements a and b such that $|a| = \infty$, $|b| = \infty$ and $|ab| = 2$.

57. Let G be the symmetry group of a circle. Explain why G contains D_n for all n.

58. 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?

59. 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 $|g|$.

60. 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 $|U(rs)|$.

61. 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?

62. Compute $|U(4)|$, $|U(10)|$, and $|U(40)|$. Do these groups provide a counterexample to your answer to Exercise 60? If so, revise your conjecture.

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

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

65. 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?

66. 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 $GL(2, \mathbf{R})$.

67. 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.

68. 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?

69. 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 $GL(2, \mathbf{R})$.

70. 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.

71. 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.

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

73. 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.

74. If H and K are nontrivial subgroups of the rational numbers under addition, prove that $H \cap K$ is nontrivial.

75. Let H be a nontrival subgroup of the group of rational numbers under addition. Prove that H has a nontrivial proper subgroup.

76. Prove that a group of order n greater than 2 cannot have a subgroup of order $n - 1$.

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 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.

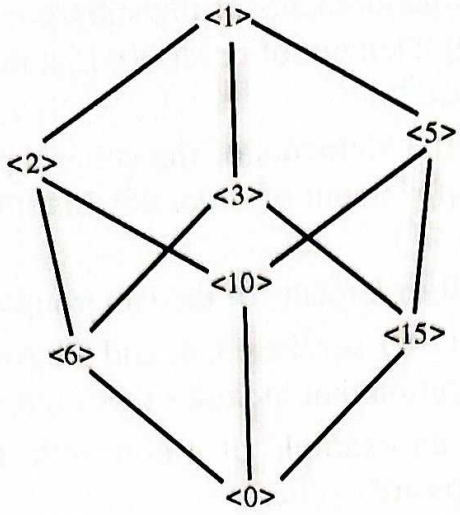


Figure 4.2 Subgroup lattice of Z_{30}.

The precision of Theorem 4.3 can be appreciated by comparing the ease with which we are able to identify the subgroups of Z_{30} with that of doing the same for, say, $U(30)$ or D_{30}. And these groups have relatively simple structures among noncyclic groups.

We will prove in Chapter 7 that a certain portion of Theorem 4.3 extends to arbitrary finite groups; namely, the order of a subgroup divides the order of the group itself. We will also see, however, that a finite group need not have exactly one subgroup corresponding to each divisor of the order of the group. For some divisors, there may be none at all, whereas for other divisors, there may be many. Indeed, D_4, the dihedral group of order 8, has five subgroups of order 2 and three of order 4.

One final remark about the importance of cyclic groups is appropriate. Although cyclic groups constitute a very narrow class of finite groups, we will see in Chapter 11 that they play the role of building blocks for all finite Abelian groups in much the same way that primes are the building blocks for the integers and that chemical elements are the building blocks for the chemical compounds.

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. Complete the statement: $|a| = |a^2|$ if and only if $|a|$ . . . .
17. Complete the statement: $|a^2| = |a^{12}|$ if and only if . . . .
18. Let a be a group element and $|a| = \infty$. Complete the following statement: $|a^i| = |a^j|$ if and only if . . . .

19. If a cyclic group has an element of infinite order, how many elements of finite order does it have?
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 that G is a group with more than one element. If the only subgroups of G are $\{e\}$ and G, prove that G is cyclic and has prime order.
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}. Generalize to Z_{p^2q}, where p and q are distinct primes.
33. Determine the subgroup lattice for Z_8. Generalize to Z_{p^n}, where p is a prime and n is some positive integer.
34. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

35. Show that the group of positive rational numbers under multiplication is not cyclic. Why does this prove that the group of nonzero rationals under multiplication is not cyclic?

36. 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.

37. 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.

38. Let m and n be elements of the group Z. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

39. Suppose that a and b are group elements that commute. If $|a|$ is finite and $|b|$ infinite, prove that $|ab|$ has infinite order.

40. 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 $|ab|$?

41. Let a belong to a group and $|a| = 100$. Find $|a^{98}|$ and $|a^{70}|$.

42. Let F and F' be distinct reflections in D_{21}. What are the possibilities for $|FF'|$?

43. 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 $|a|$?

44. Which of the following numbers could be the exact number of elements of order 21 in a group: 21600, 21602, 21604?

45. If G is an infinite group, what can you say about the number of elements of order 8 in the group? Generalize.

46. If G is a cyclic group of order n, prove that for every element a in G, $a^n = e$.

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

48. Prove or disprove that $H = \{n \in Z \mid n \text{ is divisible by both 8 and 10}\}$ is a subgroup of Z. What happens if "divisible by both 8 and 10" is changed to "divisible by 8 or 10?"

49. 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.

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

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

52. 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.

53. 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.

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

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

56. When checking to see if $\langle 2 \rangle = U(25)$ explain why it is sufficient to check that $2^{10} \neq 1$ and $2^4 \neq 1$.

57. 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.

58. 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.

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

60. 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.

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

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

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

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

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

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

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

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

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

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

71. Suppose that $|a|$ and $|b|$ are elements of a group and a and b commute. If $|a| = 5$ and $|b| = 16$, prove that $|ab| = 80$.

72. 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 $a^6 = b^{11}$.

73. Determine $\phi(81)$, $\phi(60)$ and $\phi(105)$ where ϕ is the Euler phi function.

74. If n is an even integer prove that $\phi(2n) = 2\phi(n)$.

75. 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. Give an example to show that the condition that m and n are relatively prime is necessary.

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

77. (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 $|x^{13}|$.

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.