Notations

(The number after the item indicates the page where the notation is defined.)

SET THEORY

$\cap_{i \in I} S_i$	intersection of sets S_i, $i \in I$
$\cup_{i \in I} S_i$	union of sets S_i, $i \in I$
$[a]$	$\{x \in S \mid x \sim a\}$, equivalence class of S containing a, 18
$\lvert s \rvert$	number of elements in the set of S

SPECIAL SETS

Z	integers, additive groups of integers, ring of integers
Q	rational numbers, field of rational numbers
Q^+	multiplicative group of positive rational numbers
F^*	set of nonzero elements of F
$\mathbf{R}$	real numbers, field of real numbers
$\mathbf{R}^+$	multiplicative group of positive real numbers
$\mathbf{C}$	complex numbers

FUNCTIONS AND ARITHMETIC

f^{-1}	inverse of the function f
$t \mid s$	t divides s, 3
$t \nmid s$	t does not divide s, 3
$\gcd(a, b)$	greatest common divisor of the integers a and b, 4
$\operatorname{lcm}(a, b)$	least common multiple of the integers a and b, 6
$\lvert a + b \rvert$	$\sqrt{a^2 + b^2}$, 13
$\phi(a)$	image of a under ϕ, 20
$\phi: A \to B$	mapping of A to B, 20
gf, $\alpha\beta$	composite function, 21

ALGEBRAIC SYSTEMS

D_4	group of symmetries of a square, dihedral group of order 8, 33
D_n	dihedral group of order $2n$, 34
e	identity element, 43
Z_n	group $\{0, 1, \ldots, n-1\}$ under addition modulo n, 44
$\det A$	the determinant of A, 45
$U(n)$	group of units modulo n (that is, the set of integers less than n and relatively prime to n under multiplication modulo n), 46
$\mathbf{R}^n$	$\{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbf{R}\}$, 47
$SL(2, F)$	group of 2×2 matrices over F with determinant 1, 48
$GL(2, F)$	2×2 matrices of nonzero determinants with coefficients from the field F (the general linear group), 48
g^{-1}	multiplicative inverse of g, 51
$-g$	additive inverse of g, 52
$\lvert G \rvert$	order of the group G, 60
$\lvert g \rvert$	order of the element g, 60
$H \leq G$	subgroup inclusion, 61
$H < G$	subgroup $H \neq G$, 61
$\langle a \rangle$	$\{a^n \mid n \in Z\}$, cyclic group generated by a, 65
$Z(G)$	$\{a \in G \mid ax = xa$ for all x in $G\}$, the center of G, 66

$C(a)$	$\{g \in G \mid ga = ag\}$, the centralizer of a in G, 68
$\langle S \rangle$	subgroup generated by the set S, 71
$C(H)$	$\{x \in G \mid xh = hx \text{ for all } h \in H\}$, the centralizer of H, 72
$\phi(n)$	Euler phi function of n, 84
$N(H)$	$\{x \in G \mid xHx^{-1} = H\} = \{x \in G \mid Hx = xH\}$, the normalizer of H in G, 95
$\mathrm{cl}(a)$	conjugacy class of a, 95
G^n	$\{g^n \mid g \in G\}$, 96
S_n	group of one-to-one functions from $\{1, 2, \ldots, n\}$ to itself, 101
A_n	alternating group of degree n, 110
$G \approx \overline{G}$	G and $\overline{G}$ are isomorphic, 128
ϕ_a	mapping given by $\phi_a(x) = axa^{-1}$ for all x, 135
$\mathrm{Aut}(G)$	group of automorphisms of the group G, 136
$\mathrm{Inn}(G)$	group of inner automorphisms of G, 136
aH	$\{ah \mid h \in H\}$, 144
aHa^{-1}	$\{aha^{-1} \mid h \in H\}$, 144
$\lvert G:H \rvert$	the index of H in G, 148
HK	$\{hk \mid h \in H, k \in K\}$, 150
$\mathrm{stab}_G(i)$	$\{\phi \in G \mid \phi(i) = i\}$, the stabilizer of i under the permutation group G, 151
$\mathrm{orb}_G(i)$	$\{\phi(i) \mid \phi \in G\}$, the orbit of i under the permutation group G, 151
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$	external direct product of groups $G_1, G_2, \ldots, G_n$, 162
$U_k(n)$	$\{x \in U(n) \mid x \bmod k = 1\}$, 166
G'	commutator subgroup, 181
$H \lhd G$	H is a normal subgroup of G, 185
G/H	factor group, 187
$H \times K$	internal direct product of H and K, 196
$H_1 \times H_2 \times \cdots \times H_n$	internal direct product of $H_1, \ldots, H_n$, 197
$\mathrm{Ker}\ \phi$	kernel of the homomorphism ϕ, 208
$\phi^{-1}(g')$	inverse image of g' under ϕ, 210
$\phi^{-1}(\overline{K})$	inverse image of $\overline{K}$ under ϕ, 211
$Z[x]$	ring of polynomials with integer coefficients, 246
$M_2(Z)$	ring of all 2×2 matrices with integer entries, 246
$R_1 \oplus R_2 \oplus \cdots \oplus R_n$	direct sum of rings, 247
nZ	ring of multiples of n, 249
$Z[i]$	ring of Gaussian integers, 249
$U(R)$	group of units of the ring R, 251
$\mathrm{char}\ R$	characteristic of R, 258
$\langle a \rangle$	principal ideal generated by a, 268
$\langle a_1, a_2, \ldots, a_n \rangle$	ideal generated by $a_1, a_2, \ldots, a_n$, 268
R/A	factor ring, 268
$A + B$	sum of ideals A and B, 275
AB	product of ideals A and B, 275
$\mathrm{Ann}(A)$	annihilator of A, 277
$N(A)$	nil radical of A, 277
$F(x)$	field of quotients of $F[x]$, 291
$R[x]$	ring of polynomials over R, 298

$\deg f(x)$	degree of the polynomial, 300
$\Phi_p(x)$	pth cyclotomic polynomial, 316
$M_2(Q)$	ring of 2×2 matrices over Q, 352
$\langle v_1, v_2, \ldots, v_n \rangle$	subspace spanned by $v_1, v_2, \ldots, v_n$, 353
$F(a_1, a_2, \ldots, a_n)$	extension of F by $a_1, a_2, \ldots, a_n$, 363
$f'(x)$	the derivative of $f(x)$, 368
$[E:F]$	degree of E over F, 378
$\mathrm{GF}(p^n)$	Galois field of order p^n, 389
$\mathrm{GF}(p^n)^*$	nonzero elements of $\mathrm{GF}(p^n)$, 390
$\mathrm{cl}(a)$	$\{xax^{-1} \mid x \in G\}$, the conjugacy class of a, 409
$\Pr(G)$	probability that two elements from G commute, 411
n_p	the number of Sylow p-subgroups of a group, 416
$W(S)$	set of all words from S, 446
$\langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t \rangle$	group with generators $a_1, a_2, \ldots, a_n$ and relations $w_1 = w_2 = \cdots = w_t$, 449
Q_4	quarternions, 453
Q_6	dicyclic group of order 12, 453
D_∞	infinite dihedral group, 454
$\mathrm{fix}(\phi)$	$\{i \in S \mid \phi(i) = i\}$, elements fixed by ϕ, 497
$\mathrm{Cay}(S:G)$	Cayley digraph of the group G with generating set S, 506
$k * (a, b, \ldots, c)$	concatenation of k copies of $(a, b, \ldots, c)$, 514
(n, k)	linear code, k-dimensional subspace of F^n, 531
F^n	$F \oplus F \oplus \cdots \oplus F$, direct product of n copies of the field F, 531
$d(u, v)$	Hamming distance between vectors u and v, 532
$\mathrm{wt}(u)$	the number of nonzero components of the vector u (the Hamming weight of u), 532
$\mathrm{Gal}(E/F)$	the automorphism group of E fixing F, 554
E_H	fixed field of H, 554
$\Phi_n(x)$	nth cyclotomic polynomial, 571
$C^\perp$	dual code of a code C, 582

It is useful to note that if α is one-to-one and onto, the function α^{-1} described in part 4 of Theorem 0.8 has the property that if $\alpha(s) = t$, then $\alpha^{-1}(t) = s$. That is, the image of t under α^{-1} is the unique element s that maps to t under α. In effect, α^{-1} "undoes" what α does.

■ **EXAMPLE 21** Let **Z** denote the set of integers, **R** the set of real numbers, and **N** the set of nonnegative integers. The following table illustrates the properties of one-to-one and onto.

Domain	Range	Rule	One-to-One	Onto
Z	**Z**	$x \to x^3$	Yes	No
R	**R**	$x \to x^3$	Yes	Yes
Z	**N**	$x \to \lvert x \rvert$	No	Yes
Z	**Z**	$x \to x^2$	No	No

To verify that $x \to x^3$ is one-to-one in the first two cases, notice that if $x^3 = y^3$, we may take the cube roots of both sides of the equation to obtain $x = y$. Clearly, the mapping from **Z** to **Z** given by $x \to x^3$ is not onto, since 2 is the cube of no integer. However, $x \to x^3$ defines an onto function from **R** to **R**, since every real number is the cube of its cube root (that is, $\sqrt[3]{b} \to b$). The remaining verifications are left to the reader. ■

Exercises

I was interviewed in the Israeli Radio for five minutes and I said that more than 2000 years ago, Euclid proved that there are infinitely many primes. Immediately the host interrupted me and asked: "Are there still infinitely many primes?"

NOGA ALON

1. For $n = 5$, 8, 12, 20, and 25, find all positive integers less than n and relatively prime to n.
2. Determine $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ and $\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$.
3. Determine 51 mod 13, 342 mod 85, 62 mod 15, 10 mod 15, $(82 \cdot 73) \bmod 7$, $(51 + 68) \bmod 7$, $(35 \cdot 24) \bmod 11$, and $(47 + 68) \bmod 11$.
4. Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.
5. Show that if a and b are positive integers, then $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.
6. Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

7. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.
8. Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.
9. Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$. (This exercise is referred to in Chapters 6, 8, 10, and 15.)
10. Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.
11. Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \bmod n = 1$ has a solution if and only if $d = 1$. (This exercise is referred to in Chapter 2.)
12. Show that $5n + 3$ and $7n + 4$ are relatively prime for all n.
13. Suppose that m and n are relatively prime and r is any integer. Show that there are integers x and y such that $mx + ny = r$.
14. Let p, q, and r be primes other than 3. Show that 3 divides $p^2 + q^2 + r^2$.
15. Prove that every prime greater than 3 can be written in the form $6n + 1$ or $6n + 5$.
16. Determine $7^{1000} \bmod 6$ and $6^{1001} \bmod 7$.
17. Let a, b, s, and t be integers. If $a \bmod st = b \bmod st$, show that $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$. What condition on s and t is needed to make the converse true? (This exercise is referred to in Chapter 8.)
18. Determine $8^{402} \bmod 5$.
19. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. (This exercise is referred to in Chapter 8.)
20. Let $p_1, p_2, \ldots, p_n$ be primes. Show that $p_1 p_2 \cdots p_n + 1$ is divisible by none of these primes.
21. Prove that there are infinitely many primes. (*Hint:* Use Exercise 20.)
22. Express $(-7 - 3i)^{-1}$ in standard form.
23. Express $\dfrac{-5 + 2i}{4 - 5i}$ in standard form.
24. Express $(\cos 360^\circ + i \sin 360^\circ)^{1/8}$ in standard form without trig expressions. (Note that $\cos 360^\circ + i \sin 360^\circ = 1$.)
25. Prove that for any positive integer n, $(\cos \theta + i \sin \theta)^{1/n} = \cos \dfrac{\theta}{n} + i \sin \dfrac{\theta}{n}$.
26. For every positive integer n, prove that $1 + 2 + \cdots + n = n(n + 1)/2$.

27. For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

28. Prove that $2^n 3^{2n} - 1$ is always divisible by 17.

29. Prove that there is some positive integer n such that $n, n + 1, n + 2, \ldots, n + 200$ are all composite.

30. (Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \cdots a_n$, prove that p divides a_i for some i.

31. Use the Generalized Euclid's Lemma (see Exercise 30) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

32. What is the largest bet that cannot be made with chips worth \$7.00 and \$9.00? Verify that your answer is correct with both forms of induction.

33. Prove that the First Principle of Mathematical Induction is a consequence of the Well Ordering Principle.

34. The Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, 21, 34, ... In general, the Fibonacci numbers are defined by $f_1 = 1$, $f_2 = 1$, and for $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Prove that the nth Fibonacci number f_n satisfies $f_n < 2^n$.

35. Prove by induction on n that for all positive integers n, $n^3 + (n + 1)^3 + (n + 2)^3$ is a multiple of 9.

36. Suppose that there is a statement involving a positive integer parameter n and you have an argument that shows that whenever the statement is true for a particular n it is also true for $n + 2$. What remains to be done to prove the statement is true for every positive integer? Describe a situation in which this strategy would be applicable.

37. In the cut "As" from *Songs in the Key of Life*, Stevie Wonder mentions the equation $8 \times 8 \times 8 = 4$. Find all integers n for which this statement is true, modulo n.

38. Prove that for every integer n, $n^3 \bmod 6 = n \bmod 6$.

39. If it is 2:00 A.M. now, what time will it be 3736 hours from now?

40. Determine the check digit for a money order with identification number 7234541780.

41. Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9 or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.

42. Suppose that a money order identification number and check digit of 21720421168 is erroneously copied as 27750421168. Will the check digit detect the error?

43. A transposition error involving distinct adjacent digits is one of the form $\ldots ab \ldots \rightarrow \ldots ba \ldots$ with $a \neq b$. Prove that the money order check-digit scheme will not detect such errors unless the check digit itself is transposed.

44. Determine the check digit for the Avis rental car with identification number 540047. (See Example 5.)

45. Show that a substitution of a digit a_i' for the digit a_i $(a_i' \neq a_i)$ in a noncheck position of a UPS number is detected if and only if $|a_i - a_i'| \neq 7$.

46. Determine which transposition errors involving adjacent digits are detected by the UPS check digit.

47. Use the UPC scheme to determine the check digit for the number 07312400508.

48. Explain why the check digit for a money order for the number N is the repeated decimal digit in the real number $N \div 9$.

49. The 10-digit International Standard Book Number (ISBN-10) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ has the property $(a_1, a_2, \ldots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \bmod 11 = 0$. The digit a_{10} is the check digit. When a_{10} is required to be 10 to make the dot product 0, the character X is used as the check digit. Verify the check digit for the ISBN-10 assigned to this book.

50. Suppose that an ISBN-10 has a smudged entry where the question mark appears in the number 0-716?-2841-9. Determine the missing digit.

51. Suppose three consecutive digits *abc* of an ISBN-10 are scrambled as *bca*. Which such errors will go undetected?

52. The ISBN-10 0-669-03925-4 is the result of a transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN-10.

53. Suppose the weighting vector for ISBN-10s were changed to (1, 2, 3, 4, 5, 6, 7, 8, 9, 10). Explain how this would affect the check digit.

54. Use the two-check-digit error-correction method described in this chapter to append two check digits to the number 73445860.

55. Suppose that an eight-digit number has two check digits appended using the error-correction method described in this chapter and it is incorrectly transcribed as 4302511568. If exactly one digit is incorrect, determine the correct number.

56. The state of Utah appends a ninth digit a_9 to an eight-digit driver's license number $a_1a_2 \ldots a_8$ so that $(9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 + a_9) \bmod 10 = 0$. If you know that the license number 149105267 has exactly one digit incorrect, explain why the error cannot be in position 2, 4, 6, or 8.

57. Complete the proof of Theorem 0.8.

58. Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

59. Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

60. Let S be the set of integers. If $a, b \in S$, define aRb if $a + b$ is even. Prove that R is an equivalence relation and determine the equivalence classes of S.

61. Complete the proof of Theorem 0.7 by showing that $\sim$ is an equivalence relation on S.

62. Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.

63. What is the last digit of 3^{100}? What is the last digit of 2^{100}?

64. Prove that none of the integers 11, 111, 1111, 11111, . . . is a square of an integer.

65. (Cancellation Property) Suppose α, β, and γ are functions. If $\alpha\gamma = \beta\gamma$ and γ is one-to-one and onto, prove that $\alpha = \beta$.

Computer Exercises

Computer exercises for this chapter are available at the website:

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

Suggested Readings

Linda Deneen, "Secret Encryption with Public Keys," *The UMAP Journal* 8 (1987): 9–29.

This well-written article describes several ways in which modular arithmetic can be used to code secret messages. They range from a simple scheme used by Julius Caesar to a highly sophisticated scheme invented in 1978 and based on modular n arithmetic, where n has more than 200 digits.

J. A. Gallian, "Assigning Driver's License Numbers," *Mathematics Magazine* 64 (1991): 13–22.

This article describes various methods used by the states to assign driver's license numbers. Several include check digits for error detection. This article can be downloaded at **http://www.d.umn.edu/~jgallian/license.pdf**

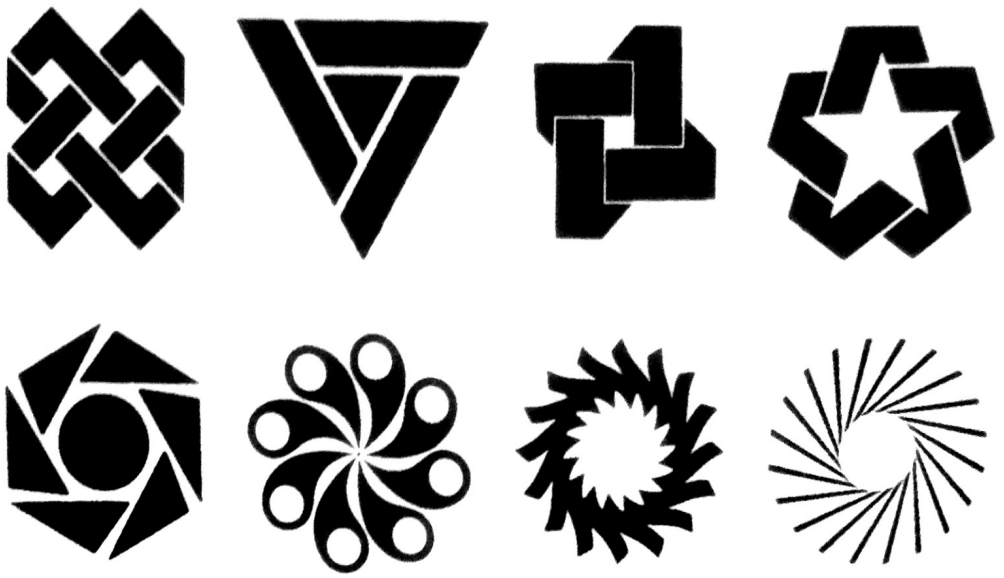


Figure 1.5 Logos with cyclic rotation symmetry groups.

Exercises

The only way to learn mathematics is to do mathematics.

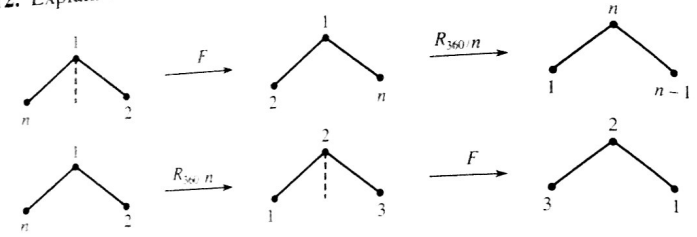
PAUL R. HALMOS, *A Hilbert Space Problem Book*

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 $A \neq C$.

12. Explain what the following diagram proves about the group D_n. (Thus, "cross cancellation" is not valid.)



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.

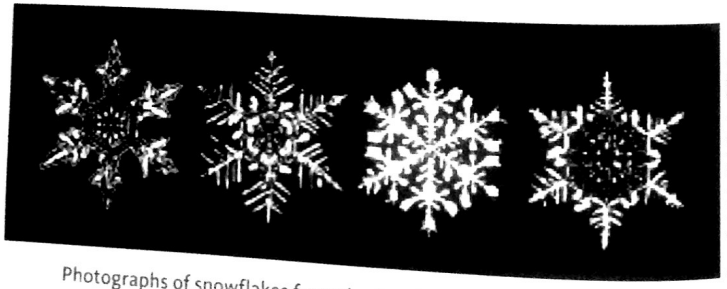
15. Describe the symmetries of a noncircular ellipse. Do the same for a hyperbola.

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).



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?

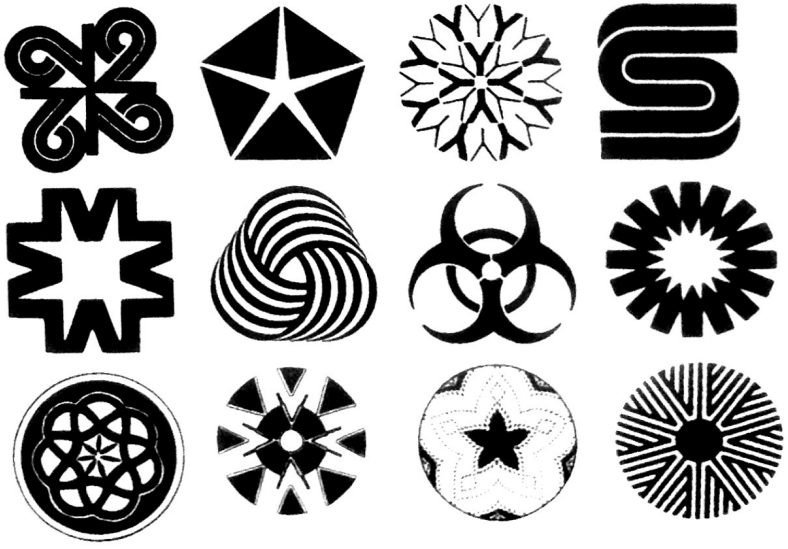
20. Bottle caps that are pried off typically have 22 ridges around the rim. Find the symmetry group of such a cap.

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).



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 $GL(2, \mathbf{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$
   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

References

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.

Suggested Readings

Marcia Ascher, *Ethnomathematics*, Pacific Grove, CA: Brooks/Cole, 1991.

Chapter 3 of this book describes how the dihedral group of order 8 can be used to encode the social structure of the kin system of family relationships among a tribe of native people of Australia.

Arie Bialostocki, "An Application of Elementary Group Theory to Central Solitaire," *The College Mathematics Journal*, May 1998: 208–212.

The author uses properties of groups to analyze the peg board game central solitaire (which also goes by the name peg solitaire).

J. E. White, "Introduction to Group Theory for Chemists," *Journal of Chemical Education* 44 (1967): 128–135.

Students interested in the physical sciences may find this article worthwhile. It begins with easy examples of groups and builds up to applications of group theory concepts and terminology to chemistry.

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:

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

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 $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 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 $Z(G) = \bigcap_{a \in G} C(a)$. [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 $\langle S \rangle = \{s_1^{n_1} s_2^{n_2} \cdots s_m^{n_m} \mid m \geq 1, s_i \in S, n_i \in Z\}$. (The s_i terms need not be distinct.)

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 $\langle a, b \rangle = \{a^i b^j \mid i, j \in \mathbf{Z}\}$ 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.

The relationships among the various subgroups of a group can be illustrated with a *subgroup lattice* of the group. This is a diagram that includes all the subgroups of the group and connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if H is a proper subgroup of K. Although there are many ways to draw such a diagram, the connections between the subgroups must be the same. Typically, one attempts to present the diagram in an eye-pleasing fashion. The lattice diagram for Z_{30} is shown in Figure 4.2. Notice that $\langle 10\rangle$ is a subgroup of both $\langle 2\rangle$ and $\langle 5\rangle$, but $\langle 6\rangle$ is not a subgroup of $\langle 10\rangle$.

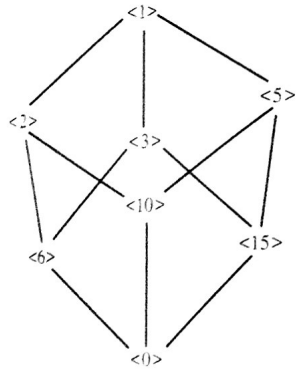


Figure 4.2 Subgroup lattice of Z_{30}.

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. 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 $|a|$ ....
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 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

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.[†]

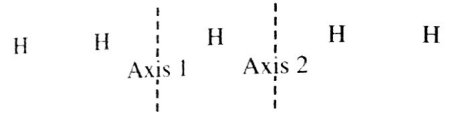
3. Let G be a group. For each $a \in G$, define $\text{cl}(a) = \{xax^{-1} \mid x \in G\}$. Prove that these subsets of G partition G. [$\text{cl}(a)$ is called the *conjugacy class* of a.]

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.

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 $H_1 \subset H_2 \subset H_3 \cdots$.

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 $2n - 1$.

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) Copyright © Piet Hein Grooks. Reprinted with kind permission from Piet Hein a/s, DK-5500 Middelfart, 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 four 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.

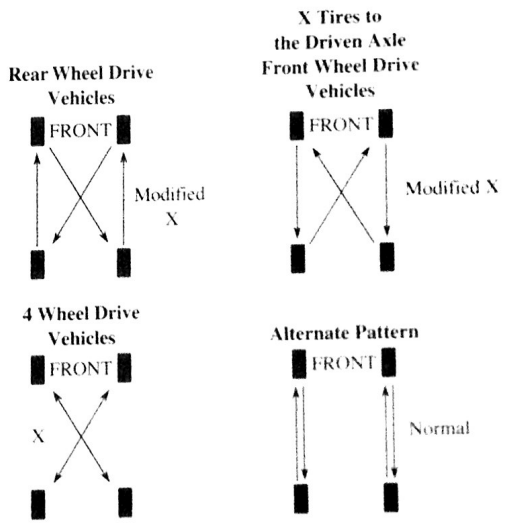
77. Why does the fact that the orders of the elements of A_4 are 1, 2, and 3 imply that $|Z(A_4)| = 1$?

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?

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 $G \neq H$, but $\text{Aut}(G) = \text{Aut}(H)$.
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

Cayley Tables

Cayley Table for the Alternating Group A_4 of Even Permutations of $\{1, 2, 3, 4\}$

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3\,\alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

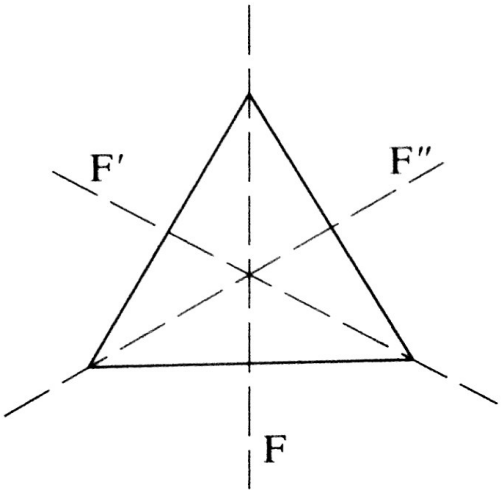
Cayley Table for the Quaternion Group

	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

Cayley Tables

Cayley Table for the Dihedral Group of Order 6

	R_0	R_{120}	R_{240}	F	F'	F''
R_0	R_0	R_{120}	R_{240}	F	F'	F''
R_{120}	R_{120}	R_{240}	R_0	F'	F''	F
R_{240}	R_{240}	R_0	R_{120}	F''	F	F'
F	F	F''	F'	R_0	R_{240}	R_{120}
F'	F'	F	F''	R_{120}	R_0	R_{240}
F''	F''	F'	F	R_{240}	R_{120}	R_0



Cayley Table for the Dihedral Group of Order 8

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0