Exercises

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

Sherlock Holmes, *The Sign of Fou*

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. $(a_1 a_2 \cdots a_k)$

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)

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. Determine whether the following permutations are even or odd.
   a. (135)
   b. (1356)
   c. (13567)
   d. (12)(134)(152)
   e. (1243)(3521)

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. Show that A_8 contains an element of order 15.

11. Find an element in A_{12} of order 30.

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. Suppose that α is a 6-cycle and β is a 5-cycle. Determine whether $\alpha^5\beta^4\alpha^{-1}\beta^{-3}\alpha^5$ is even or odd. Show your reasoning.

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. Complete the following statement: A product of disjoint cycles is even if and only if _____.
22. What cycle is $(a_1a_2 \cdots a_n)^{-1}$?
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. How many elements are there of order 2 in A_8 that have the disjoint cycle form $(a_1a_2)(a_3a_4)(a_5a_6)(a_7a_8)$?
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. Generalize.
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. Let $(a_1a_2a_3a_4)$ and (a_5a_6) be disjoint cycles in S_{10}. Show that there is no element x in S_{10} such that $x^2 = (a_1a_2a_3a_4)(a_5a_6)$.
34. If α and β are distinct 2-cycles, what are the possibilities for $|\alpha\beta|$?
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. In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.
40. In S_3, find elements α and β such that $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

41. Find group elements α and β in S_5 such that $|\alpha| = 3$, $|\beta| = 3$, and $|\alpha\beta| = 5$.
42. Represent the symmetry group of an equilateral triangle as a group of permutations of its vertices (see Example 3).
43. Prove that S_n is non-Abelian for all $n \geq 3$.
44. Prove that A_n is non-Abelian for all $n \geq 4$.
45. 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 $|H|$.
46. Show that in S_7, the equation $x^2 = (1234)$ has no solutions but the equation $x^3 = (1234)$ has at least two.
47. If (ab) and (cd) are distinct 2-cycles in S_n, prove that (ab) and (cd) commute if and only if they are disjoint.
48. Let α and β belong to S_n. Prove that $\beta\alpha\beta^{-1}$ and α are both even or both odd.
49. 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?
50. 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)?
51. 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.
52. Let α_1, α_2 and α_3 be 2-cycles. Prove that $\alpha_1\alpha_2\alpha_3 \neq \epsilon$. Generalize.
53. 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.)
54. Find a cyclic subgroup of A_8 that has order 4. Find a noncyclic subgroup of A_8 that has order 4.
55. Show that a permutation with odd order must be an even permutation.
56. Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?
57. Show that every element in A_n for $n \geq 3$ can be expressed as a 3-cycle or a product of 3-cycles.
58. Show that for $n \geq 3$, $Z(S_n) = \{\varepsilon\}$.
59. 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.

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

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

62. (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?

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

64. Find five subgroups of S_5 of order 24.

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

66. Let α belong to S_n. Prove that $|\alpha|$ divides $n!$

67. Encrypt the message ATTACK POSTPONED using the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{bmatrix}$.

68. The message VAADENWCNHREDEYA was encrypted using the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$. Decrypt it.

Computer Exercises

Computer exercises for this chapter are available at the website:

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

References

1. J. A. Gallian, "The Mathematics of Identification Numbers," *The College Mathematics Journal* 22 (1991): 194–202.
2. J. Verhoeff, *Error Detecting Decimal Codes*, Amsterdam: Mathematisch Centrum, 1969.

and

$$(123)H(321) = \{(1), (1423), (12)(34), (1324), (14)(23), (34), (13)(24), (12)\}$$

of S_4 that are isomorphic to H.

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 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 $H \approx G$
   $G \approx H$ 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. Given that ϕ is a isomorphism from a group G under addition to a group $\overline{G}$ under addition, convert property 2 of Theorem 6.2 to additive notation.
11. Let G be a group under multiplication, $\overline{G}$ be a group under addition and ϕ be an isomorphism from G to $\overline{G}$. If $\phi(a) = \overline{a}$ and $\phi(b) = \overline{b}$, find an expression for $\phi(a^3b^{-2})$ in terms of $\overline{a}$ and $\overline{b}$.
12. 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.
13. If g and h are elements from a group, prove that $\phi_g\phi_h = \phi_{gh}$.

14. Find two groups G and H such that $G \not\approx H$, but $\text{Aut}(G) \approx \text{Aut}(H)$.

15. Prove the assertion in Example 14 that the inner automorphisms ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, and ϕ_D of D_4 are distinct.

16. Find $\text{Aut}(Z_6)$.

17. If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups. (This exercise is referred to in this chapter.)

18. If a group G is isomorphic to H, prove that $\text{Aut}(G)$ is isomorphic to $\text{Aut}(H)$.

19. Suppose ϕ belongs to $\text{Aut}(Z_n)$ and a is relatively prime to n. If $\phi(a) = b$, determine a formula for $\phi(x)$.

20. 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.)

21. 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 $n \geq 3$?

22. Show that Z has infinitely many subgroups isomorphic to Z.

23. Let n be an even integer greater than 2 and let ϕ be an automorphism of D_n. Determine $\phi(R_{180})$.

24. Let ϕ be an automorphism of a group G. Prove that $H = \{x \in G \mid \phi(x) = x\}$ is a subgroup of G.

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

26. Suppose that $\phi: Z_{20} \to Z_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

27. Identify a group G that has subgroups isomorphic to Z_n for all positive integers n.

28. Prove that the mapping from $U(16)$ to itself given by $x \to x^3$ is an automorphism.

29. 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.)

30. 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 $\mathbf{R}$?

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

32. Suppose that $\phi: Z_{50} \to Z_{50}$ is an automorphism with $\phi(7) = 13$. Determine a formula for $\phi(x)$.

33. Prove property 1 of Theorem 6.3.
34. Prove property 4 of Theorem 6.3.
35. Referring to Theorem 6.1, prove that T_g is indeed a permutation on the set G.
36. Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.
37. 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.)
38. 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.)
39. Prove that Z under addition is not isomorphic to Q under addition.
40. Explain why S_8 contains subgroups isomorphic to Z_{15}, $U(16)$, and D_8.
41. 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.
42. 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.
43. 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.
44. 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.

45. 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).

46. Prove that $\mathbf{R}$ under addition is not isomorphic to $\mathbf{R}^*$ under multiplication.

47. Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

48. Combine the results of Exercises 45 and 47 into a single "if and only if" theorem.

49. If α and β are elements in S_n $(n \geq 3)$,prove that $\phi_\alpha = \phi_\beta$ implies that $\alpha = \beta$. (Here, ϕ_α is the inner automorphism of S_n induces by α.)

50. Prove or disprove that the mapping ϕ from Q^+, the positive rational numbers under multiplication, to itself given by $\phi(x) = x^2$ is an automorphism.

51. 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.

52. Let G be a group. Complete the following statement: $|\text{Inn}(G)| = 1$ if and only if _____.

53. 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.

54. Let ϕ be an automorphism of D_8. What are the possibilities for $\phi(R_{45})$?

55. Let ϕ be an automorphism of $\mathbf{C}^*$, the group of nonzero complex numbers under multiplcation. Determine $\phi(-1)$. Determine the possibilities for $\phi(i)$.

56. Let $G = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Prove that G and H are isomorphic groups under addition by defining a mapping that has the required properties. 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.

57. Give three examples of groups of order 120, no two of which are isomophic. Explain why they are not isomorphic.

58. Let ϕ be an automorphism of D_4 such that $\phi(H) = D$. Find $\phi(V)$.

59. Suppose that ϕ is an automorphism of D_4 such that $\phi(R_{90}) = R_{270}$ and $\phi(V) = V$. Determine $\phi(D)$ and $\phi(H)$.

60. 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, $\alpha_2 = (0)(124875)(36)$.]

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

62. Show that every automorphism ϕ of the rational numbers Q under addition to itself has the form $\phi(x) = x\phi(1)$.
63. Prove that Q^+, the group of positive rational numbers under multiplication, is isomorphic to a proper subgroup of itself.
64. Prove that Q, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.
65. 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.
66. Prove that Q^*, the group of nonzero rational numbers under multiplication, is not isomorphic to Q, the group of rational numbers under addition.
67. Give a group theoretic proof that Q under addition is not isomorphic to $\mathbf{R}^+$ under multiplication.

Reference

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

Computer Exercises

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

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

An Application of Cosets to the Rubik's Cube

Recall from Chapter 5 that in 2010 it was proved via a computer computation, which took 35 CPU-years to complete, that every Rubik's cube could be solved in at most 20 moves. To carry out this effort, the research team of Morley Davidson, John Dethridge, Herbert Kociemba, and Tomas Rokicki applied a program of Rokicki, which built on early work of Kociemba, that checked the elements of the cosets of a subgroup H of order $(8! \cdot 8! \cdot 4!)/2 = 19{,}508{,}428{,}800$ to see if each cube in a position corresponding to the elements in a coset could be solved within 20 moves. In the rare cases where Rokicki's program did not work, an alternate method was employed. Using symmetry considerations, they were able to reduce the approximately 2 billion cosets of H to about 56 million cosets for testing. Cosets played a role in this effort because Rokicki's program could handle the 19.5+ billion elements in the same coset in about 20 seconds.

Exercises

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

Homer Simpson

1. Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in Z.
2. Rewrite the condition $a^{-1}b \in H$ given in property 6 of the lemma on page 139 in additive notation. Assume that the group is Abelian.
3. Let H be as in Exercise 1. Use Exercise 2 to decide whether or not the following cosets of H are the same.
   a. $11 + H$ and $17 + H$
   b. $-1 + H$ and $5 + H$
   c. $7 + H$ and $23 + H$
4. Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in Z. How many are there?
5. Find all of the left cosets of $\{1, 11\}$ in $U(30)$.
6. Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.
7. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.
8. Give an example of a group G and subgroups H and K such that $HK = \{h \in H, k \in K\}$ is not a subgroup of G.
9. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (see Table 5.1 on page 105). How many left cosets of H in S_4 are there? (Determine this without listing them.)

10. Let a and b be elements of a group G and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.
11. If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.
12. Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.
13. Let H be a subgroup of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication. If $\mathbf{R}^+ \subseteq H \subseteq \mathbf{R}^*$, prove that $H = \mathbf{R}^+$ or $H = \mathbf{R}^*$.
14. Let $\mathbf{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbf{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.
15. Let G be a group of order 60. What are the possible orders for the subgroups of G?
16. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?
17. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.
18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \bmod n = 1$.
19. Compute $5^{15} \bmod 7$ and $7^{13} \bmod 11$.
20. Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.
21. Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.
22. Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.
23. For any integer $n \geq 3$, prove that D_n has a subgroup of order 4 if and only if n is even.
24. Let p be a prime and k a positive integer such that $a^k \bmod p = a \bmod p$ for all integers a. Prove that $p - 1$ divides $k - 1$.
25. Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.
26. Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

27. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.
28. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?
29. Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.
30. Let $|G| = 8$. Show that G must have an element of order 2.
31. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.
32. Determine all finite subgroups of $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication.
33. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K|\,|K:H|$.
34. Suppose that a group contains elements of orders 1 through 10. What is the minimum possible order of the group?
35. Give an example of the dihedral group of smallest order that contains a subgroup isomorphic to Z_{12} and a subgroup isomorphic to Z_{20}. No need to prove anything, but explain your reasoning.
36. Let G be a group and $|G| = 21$. If $g \in G$ and $g^{14} = e$, what are the possibilities for $|g|$?
37. Suppose that a finite Abelian group G has at least three elements of order 3. Prove that 9 divides $|G|$.
38. Prove that if G is a finite group, the index of $Z(G)$ cannot be prime.
39. Suppose that H and K are subgroups of a group with $|H| = 24$, $|K| = 20$. Prove that $H \cap K$ Abelian.
40. Prove that a group of order 63 must have an element of order 3.
41. Let G be a group of order 100 that has a subgroup H of order 25. Prove that every element of G of order 5 is in H.
42. Let G be a group of order n and k be any integer relatively prime to n. Show that the mapping from G to G given by $g \to g^k$ is one-to-one. If G is also Abelian, show that the mapping given by $g \to g^k$ is an automorphism of G.
43. Let G be a group of permutations of a set S. Prove that the orbits of the members of S constitute a partition of S. (This exercise is referred to in this chapter and in Chapter 29.)
44. Prove that every subgroup of D_n of odd order is cyclic.

45. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.
- **a.** Find the stabilizer of 1 and the orbit of 1.
- **b.** Find the stabilizer of 3 and the orbit of 3.
- **c.** Find the stabilizer of 5 and the orbit of 5.

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

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

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

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

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

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

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

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

54. Suppose that G is a group of order 105 with the property that G has exactly one subgroup for each divisor of 105. Prove that G is cyclic.

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

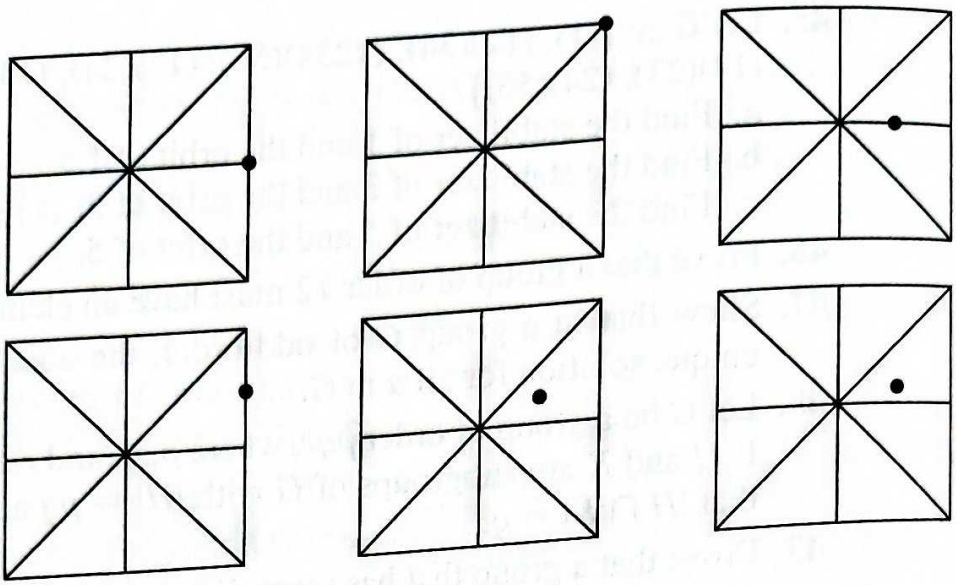
56. Why does the fact that A_4 has no subgroup of order 6 imply that $|Z(A_4)| = 1$?

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

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

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

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



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

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

a. The group of rotations of a regular tetrahedron (a solid with four congruent equilateral triangles as faces)

b. The group of rotations of a regular octahedron (a solid with eight congruent equilateral triangles as faces)

c. The group of rotations of a regular dodecahedron (a solid with 12 congruent regular pentagons as faces)

d. The group of rotations of a regular icosahedron (a solid with 20 congruent equilateral triangles as faces)

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

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

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

Computer Exercises

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

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

just use strings of 0's, 1's, 2's, and 3's and add componentwise modulo 4. A DNA molecule is composed of two long strands in the form of a double helix. Each strand is made up of strings of the four nitrogen bases adenine (A), thymine (T), guanine (G), and cytosine (C). Each base on one strand binds to a complementary base on the other strand. Adenine always is bound to thymine, and guanine always is bound to cytosine. To model this process, we identify A with 0, T with 2, G with 1, and C with 3. Thus, the DNA segment ACGTAACAGGA and its complement segment TGCATTGTCCT are denoted by 03120030110 and 21302212332. Noting that in Z_4, $0 + 2 = 2$, $2 + 2 = 0$, $1 + 2 = 3$, and $3 + 2 = 1$, we see that adding 2 to elements of Z_4 interchanges 0 and 2 and 1 and 3. So, for any DNA segment $a_1a_2 \cdots a_n$ represented by elements of $Z_4 \oplus Z_4 \oplus \cdots \oplus Z_4$, we see that its complementary segment is represented by $a_1a_2 \cdots a_n + 22 \cdots 2$.

Electric Circuits

Many homes have light fixtures that are operated by a pair of switches. They are wired so that when either switch is thrown, the light changes its status (from on to off or vice versa). Suppose the wiring is done so that the light is on when both switches are in the up position. We can conveniently think of the states of the two switches as being matched with the elements of $Z_2 \oplus Z_2$, with the two switches in the up position corresponding to (0, 0) and the two switches in the down position corresponding to (1, 1). Each time a switch is thrown, we add 1 to the corresponding component in the group $Z_2 \oplus Z_2$. We then see that the lights are on when the switches correspond to the elements of the subgroup $\langle(1, 1)\rangle$ and are off when the switches correspond to the elements in the coset $(1, 0) + \langle(1, 1)\rangle$. A similar analysis applies in the case of three switches, with the subgroup $\{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$ corresponding to the lights-on situation.

Exercises

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

1. Prove that the external direct product of any finite number of groups is a group. (This exercise is referred to in this chapter.)
2. Prove that (1,1) is an element of largest order in $Z_{n_1} \oplus Z_{n_2}$. State the general case.

3. Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.
4. Show that $G \oplus H$ is Abelian if and only if G and H are Abelian. State the general case.
5. Prove that $Z \oplus Z$ is not cyclic. Does your proof work for $Z \oplus G$ where G is any group with more than one element?
6. Prove, by comparing orders of elements, that $Z_8 \oplus Z_2$ is not isomorphic to $Z_4 \oplus Z_4$.
7. Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$. State the general case.
8. Is $Z_3 \oplus Z_9$ isomorphic to Z_{27}? Why?
9. Give an example of a group of order 12 that has more than one subgroup of order 6.
10. How many elements of order 9 does $Z_3 \oplus Z_9$ have? (Do not do this exercise by brute force.)
11. How many elements of order 4 does $Z_4 \oplus Z_4$ have? (Do not do this by examining each element.) Explain why $Z_4 \oplus Z_4$ has the same number of elements of order 4 as does $Z_{8000000} \oplus Z_{400000}$. Generalize to the case $Z_m \oplus Z_n$.
12. Give examples of four groups of order 12, no two of which are isomorphic. Give reasons why no two are isomorphic.
13. For each integer $n > 1$, give examples of two nonisomorphic groups of order n^2.
14. The dihedral group D_n of order $2n$ ($n \geq 3$) has a subgroup of n rotations and a subgroup of order 2. Explain why D_n cannot be isomorphic to the external direct product of two such groups.
15. Prove that the group of complex numbers under addition is isomorphic to $\mathbf{R} \oplus \mathbf{R}$.
16. Suppose that $G_1 \approx G_2$ and $H_1 \approx H_2$. Prove that $G_1 \oplus H_1 \approx G_2 \oplus H_2$. State the general case.
17. If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.
18. Find a cyclic subgroup of $Z_{40} \oplus Z_{30}$ of order 12 and a non-cyclic subgroup of $Z_{40} \oplus Z_{30}$ of order 12.
19. If r is a divisor of m and s is a divisor of n, find a subgroup of $Z_m \oplus Z_n$ that is isomorphic to $Z_r \oplus Z_s$.
20. Find a subgroup of $Z_{12} \oplus Z_{18}$ that is isomorphic to $Z_9 \oplus Z_4$.
21. Let G and H be finite groups and $(g, h) \in G \oplus H$. State a necessary and sufficient condition for $\langle (g, h) \rangle = \langle g \rangle \oplus \langle h \rangle$.
22. Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $Z_{30} \oplus Z_{20}$.

23. How many subgroups of order 3 are there in $Z_3 \oplus Z_3$? What about $Z_3 \oplus Z_3 \oplus Z_3$? What about $Z_3 \oplus Z_3 \oplus \cdots \oplus Z_3$ (n copies)?

24. Let $m > 2$ be an even integer and let $n > 2$ be an odd integer. Find a formula for the number of elements of order 2 in $D_m \oplus D_n$.

25. Let M be the group of all real 2×2 matrices under addition. Let $N = \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R}$ under componentwise addition. Prove that M and N are isomorphic. What is the corresponding theorem for the group of $m \times n$ matrices under addition?

26. The group $S_3 \oplus Z_2$ is isomorphic to one of the following groups: Z_{12}, $Z_6 \oplus Z_2$, A_4, D_6. Determine which one by elimination.

27. Let G be a group, and let $H = \{(g, g) \mid g \in G\}$. Show that H is a subgroup of $G \oplus G$. (This subgroup is called the *diagonal* of $G \oplus G$.) When G is the set of real numbers under addition, describe $G \oplus G$ and H geometrically.

28. List six examples of non-Abelian groups of order 24.

29. Find all subgroups of order 3 in $Z_9 \oplus Z_3$.

30. Find all subgroups of order 4 in $Z_4 \oplus Z_4$.

31. What is the order of the largest cyclic subgroup of $Z_6 \oplus Z_{10} \oplus Z_{15}$? What is the order of the largest cyclic subgroup of $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$?

32. How many elements of order 2 are in $Z_{2000000} \oplus Z_{4000000}$? Generalize.

33. Find a subgroup of $Z_{800} \oplus Z_{200}$ that is isomorphic to $Z_2 \oplus Z_4$.

34. Find a subgroup of $Z_{12} \oplus Z_4 \oplus Z_{15}$ that has order 9.

35. Prove that $\mathbf{R}^* \oplus \mathbf{R}^*$ is not isomorphic to $\mathbf{C}^*$. (Compare this with Exercise 15.)

36. Let

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

(See Exercise 46 in Chapter 2 for the definition of multiplication.) Show that H is an Abelian group of order 9. Is H isomorphic to Z_9 or to $Z_3 \oplus Z_3$?

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

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

39. Compare the number of elements of each order in D_6 with the number for each order in $D_3 \oplus Z_2$.

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

41. List the elements in the groups $U_5(35)$ and $U_7(35)$.
42. Prove or disprove that $U(40) \oplus Z_6$ is isomorphic to $U(72) \oplus Z_4$.
43. Prove or disprove that C^* has a subgroup isomorphic to $Z_2 \oplus Z_2$.
44. Let G be a group isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$. Let x be the product of all elements in G. Describe all possibilities for x.
45. If a group has exactly 24 elements of order 6, how many cyclic subgroups of order 6 does it have?
46. Give an example of an infinite group that has both a subgroup isomorphic to D_4 and a subgroup isomorphic to A_4.
47. Express $\text{Aut}(U(25))$ in the form $Z_m \oplus Z_n$.
48. Determine $\text{Aut}(Z_2 \oplus Z_2)$.
49. Suppose that $n_1, n_2, \ldots, n_k$ are positive even integers. How many elements of order 2 does $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ have ? How many are there if we drop the requirement that $n_1, n_2, \ldots, n_k$ must be even?
50. Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{60} \oplus Z_6 \oplus Z_2$? Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{15} \oplus Z_4 \oplus Z_{12}$?
51. a. How many isomorphisms are there from Z_{18} to $Z_2 \oplus Z_9$?
    b. How many isomorphisms are there from Z_{18} to $Z_2 \oplus Z_3 \oplus Z_3$?
52. Suppose that ϕ is an isomorphism from $Z_3 \oplus Z_5$ to Z_{15} and $\phi((2, 3)) = 2$. Find the element in $Z_3 \oplus Z_5$ that maps to 1.
53. If ϕ is an isomorphism from $Z_4 \oplus Z_3$ to Z_{12}, what is $\phi((2, 0))$? What are the possibilities for $\phi((1, 0))$? Give reasons for your answer.
54. Find a subgroup of $U(140)$ isomorphic to $Z_4 \oplus Z_6$.
55. Let (a, b) belong to $Z_m \oplus Z_n$. Prove that $|(a, b)|$ divides $\text{lcm}(m, n)$.
56. Let $G = \{ax^2 + bx + c \mid a, b, c \in Z_3\}$. Add elements of G as you would polynomials with integer coefficients, except use modulo 3 addition. Prove that G is isomorphic to $Z_3 \oplus Z_3 \oplus Z_3$. Generalize.
57. Determine all cyclic groups that have exactly two generators.
58. Explain a way that a string of length n of the four nitrogen bases A, T, G, and C could be modeled with the external direct product of n copies of $Z_2 \oplus Z_2$.
59. Let p be a prime. Prove that $Z_p \oplus Z_p$ has exactly $p + 1$ subgroups of order p.
60. Give an example of an infinite non-Abelian group that has exactly six elements of finite order.
61. Give an example to show that there exists a group with elements a and b such that $|a| = \infty$, $|b| = \infty$, and $|ab| = 2$.
62. Express $U(165)$ as an external direct product of cyclic groups of the form Z_n.

63. Express $U(165)$ as an external direct product of U-groups in four different ways.

64. If n is an integer at least 3, determine the number of elements of order 2 in $U(2^n)$.

65. Without doing any calculations in $\text{Aut}(Z_{105})$, determine how many elements of $\text{Aut}(Z_{105})$ have order 6.

66. Without doing any calculations in $U(27)$, decide how many subgroups $U(27)$ has.

67. What is the largest order of any element in $U(900)$?

68. Let p and q be odd primes and let m and n be positive integers. Explain why $U(p^m) \oplus U(q^n)$ is not cyclic.

69. Use the results presented in this chapter to prove that $U(55)$ is isomorphic to $U(75)$.

70. Use the results presented in this chapter to prove that $U(144)$ is isomorphic to $U(140)$.

71. Find a subgroup of order 4 in $U(1000)$.

72. Find an integer n such that $U(n)$ is isomorphic to $Z_2 \oplus Z_4 \oplus Z_9$.

73. What is the smallest positive integer k such that $x^k = e$ for all x in $U(7 \cdot 17)$? Generalize to $U(pq)$ where p and q are distinct primes.

74. Prove that $U_{50}(200)$ is not isomorphic to $U(4)$. Why does this not contradict Theorem 8.3?

75. Prove or disprove: $U(200) \approx U(50) \oplus U(4)$.

76. Find the smallest positive integer n such that $x^n = 1$ for all x in $U(100)$. Show your reasoning.

77. Which of the following groups are cyclic?

a. $U(35)$

b. $U_5(40)$

c. $U_8(40)$

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

79. Using the RSA scheme with $p = 37$, $q = 73$, $e = 5$, and replacing the letters A, B, ..., Z by 01, 02, ..., 26, what number would be sent for the messsage "RL"?

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

81. Explain why the message YES cannot be sent using RSA scheme with $p = 31$ and $q = 73$ using blocks of length 4.