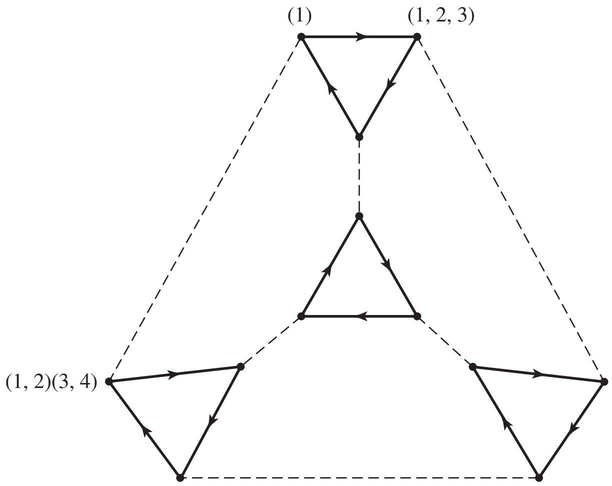

8.26 Figure

30. Before the proof of Cayley's Theorem, it is shown that λ_x is one-to-one. In the proof, one-to-one is shown again. Is it necessary to show one-to-one twice? Explain.

31. Determine whether each of the following is true or false.

a. Every permutation is a cycle.
b. Every cycle is a permutation.
c. The definition of even and odd permutations could have been given equally well before Theorem 8.19.
d. Every nontrivial subgroup H of S_9 containing some odd permutation contains a transposition.
e. A_5 has 120 elements.
f. S_n is not cyclic for any $n \geq 1$.
g. A_3 is a commutative group.
h. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 8 fixed.
i. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 5 fixed.
j. The odd permutations in S_8 form a subgroup of S_8.
k. Every group G is isomorphic with a subgroup of S_G.

32. The dihedral group is defined to be permutations with certain properties. Use the usual notation involving μ and ρ for elements in D_n.

a. Identify which elements in D_3 are even. Do the even elements form a cyclic group?
b. Identify which of elements of D_4 are even. Do the even elements form a cyclic group?
c. For which values of n do the even permutations of D_n form a cyclic group?

Proof Synopsis

33. Give a two-sentence synopsis of the proof of Cayley's Theorem.

34. Give a two-sentence synopsis of the proof of Theorem 8.19.

Theory

35. Suppose that $\phi : G \to G'$ is a group homomorphism and $a \in \text{Ker}\phi$. Show that for any $g \in G$, $gag^{-1} \in \text{Ker}\phi$.

36. Prove that a homomorphism $\phi : G \to G'$ is one-to-one if and only if $\text{Ker}(\phi)$ is the trivial subgroup of G.

37. Let $\phi : G \to G'$ be a group homomorphism. Show that $\phi(a) = \phi(b)$ if and only if $a^{-1}b \in \text{Ker}\phi$.

38. Use Exercise 37 to prove that if $\phi : G \to G'$ is a group homomorphism mapping onto G' and G is a finite group, then for any $b, c \in G'$, $|\phi^{-1}[\{b\}]| = |\phi^{-1}[\{c\}]|$. Conclude that if $|G|$ is a prime number, then either ϕ is an isomorphism or else G' is the trivial group.

39. Show that if $\phi : G \to G'$ and $\gamma : G' \to G''$ are group homomorphisms, then $\gamma \circ \phi : G \to G''$ is also a group homomorphism.

40. Let $\phi : G \to G'$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$ for all $x, y \in G$.

41. Prove the following about S_n if $n \geq 3$.

a. Every permutation in S_n can be written as a product of at most $n - 1$ transpositions.

b. Every permutation in S_n that is not a cycle can be written as a product of at most $n - 2$ transpositions.

c. Every odd permutation in S_n can be written as a product of $2n + 3$ transpositions, and every even permutation as a product of $2n + 8$ transpositions.

42. a. Draw a figure like Fig. 8.20 to illustrate that if i and j are in different orbits of σ and $\sigma(i) = i$, then the number of orbits of $(i, j)\sigma$ is one less than the number of orbits of σ.

b. Repeat part (a) if $\sigma(j) = j$ also.

43. Show that for every subgroup H of S_n for $n \geq 2$, either all the permutations in H are even or exactly half of them are even.

44. Let σ be a permutation of a set A. We shall say "σ **moves** $a \in A$" if $\sigma(a) \neq a$. If A is a finite set, how many elements are moved by a cycle $\sigma \in S_A$ of length n?

45. Let A be an infinite set. Let H be the set of all $\sigma \in S_A$ such that the number of elements moved by σ (see Exercise 44) is finite. Show that H is a subgroup of S_A.

46. Let A be an infinite set. Let K be the set of all $\sigma \in S_A$ that move (see Exercise 44) at most 50 elements of A. Is K a subgroup of S_A? Why?

47. Consider S_n for a fixed $n \geq 2$ and let σ be a fixed odd permutation. Show that every odd permutation in S_n is a product of σ and some permutation in A_n.

48. Show that if σ is a cycle of odd length, then σ^2 is a cycle.

49. Following the line of thought opened by Exercise 48, complete the following with a condition involving n and r so that the resulting statement is a theorem:

If σ is a cycle of length n, then σ^r is also a cycle if and only if . . .

50. Show that S_n is generated by $\{(1, 2), (1, 2, 3, \cdots, n)\}$. [*Hint:* Show that as r varies, $(1, 2, 3, \cdots, n)^r(1, 2)(1, 2, 3, \cdots, n)^{n-r}$ gives all the transpositions $(1, 2), (2, 3), (3, 4), \cdots, (n - 1, n), (n, 1)$. Then show that any transposition is a product of some of these transpositions and use Theorem 8.15.]

51. Let $\sigma \in S_n$ and define a relation on $\{1, 2, 3, \ldots, n\}$ by $i \sim j$ if and only if $j = \sigma^k(i)$ for some $k \in \mathbb{Z}$.

1. Prove that $\sim$ is an equivalence relation.

2. Prove that for any $1 \leq i \leq n$, the equivalence class of i is the orbit of i.

52. The usual definition for the determinant of an $n \times n$ matrix $A = (a_{i,j})$ is

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)}$$

where $\text{sgn}(\sigma)$ is the sign of σ. Using this definition, prove the following properties of determinants.

a. If a row of matrix A has all zero entries, then $\det(A) = 0$.

b. If two different rows of A are switched to obtain B, then $\det(B) = -\det(A)$.

c. If r times one row of A is added to another row of A to obtain a matrix B, then $\det(A) = \det(B)$

d. If a row of A is multiplied by r to obtain the matrix B, then $\det(B) = r\det(A)$.

53. Prove that any finite group G is isomorphic with a subgroup of $\text{GL}(n, \mathbb{R})$ for some n. [Hint: For each $\sigma \in S_n$, find a matrix in $\text{GL}(n, \mathbb{R})$ that sends each basis vector e_i to $e_{\sigma(i)}$. Use this to show that S_n is isomorphic with a subgroup of $\text{GL}(n, \mathbb{R})$.]

54. Prove Cayley's Theorem using the right regular representation rather than the left regular representation.

55. Let $\sigma \in S_n$. An inversion is a pair (i, j) such that $i < j$ and $\sigma(i) > \sigma(j)$. Prove Theorem 8.19 by showing that multiplying a permutation by a transposition changes the number of inversions by an odd number.

56. The sixteen puzzle consists of 15 tiles numbered 1 through 15 arranged in a four-by-four grid with one position left blank. A move is sliding a tile adjacent to the blank position into the blank position. The goal is to arrange the numbers in order by a sequence of moves. Is it possible to start with the configuration pictured in Figure 8.27(a) and solve the puzzle as indicated in Figure 8.27(b)? Prove your answer by finding a sequence of moves to solve the puzzle or by proving that it is impossible to solve.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

a.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

b.

8.27 Figure

SECTION 9 FINITELY GENERATED ABELIAN GROUPS

Direct Products

Let us take a moment to review our present stockpile of groups. Starting with finite groups, we have the cyclic group $\mathbb{Z}_n$, the symmetric group S_n, and the alternating group A_n for each positive integer n. We also have the dihedral groups D_n and the Klein 4-group V. Of course we know that subgroups of these groups exist. Turning to infinite groups, we have groups consisting of sets of numbers under the usual addition or multiplication, as, for example, $\mathbb{Z}, \mathbb{R}$, and $\mathbb{C}$ under addition, and their nonzero elements under multiplication. We have the group U of complex numbers of magnitude 1 under multiplication, which is isomorphic to each of the groups $\mathbb{R}_c$ under addition modulo c, where $c \in \mathbb{R}^+$. We also have the group S_A of all permutations of an infinite set A, as well as various groups formed from matrices such as GL(n, $\mathbb{R}$).

One purpose of this section is to show a way to use known groups as building blocks to form more groups. The Klein 4-group will be recovered in this way from the cyclic groups. Employing this procedure with the cyclic groups gives us a large class of abelian groups that can be shown to include all possible structure types for a finite abelian group. We start by generalizing Definition 0.4.

9.1 Definition The **Cartesian product of sets** $B_1, B_2, \cdots, B_n$ is the set of all ordered n-tuples $(b_1, b_2, \cdots, b_n)$, where $b_i \in B_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$B_1 \times B_2 \times \cdots \times B_n$$

or by

$$\prod_{i=1}^{n} B_i.$$ ■

We could also define the Cartesian product of an infinite number of sets, but the definition is considerably more sophisticated and we shall not need it.

Now let $G_1, G_2, \cdots, G_n$ be groups, and let us use multiplicative notation for all the group operations. Regarding the G_i as sets, we can form $\prod_{i=1}^{n} G_i$. Let us show that we can make $\prod_{i=1}^{n} G_i$ into a group by means of a binary operation of *multiplication by components*. Note again that we are being sloppy when we use the same notation for a group as for the set of elements of the group.