

Dr. H. Joseph Straight  
SUNY Fredonia

***Smokin' Joe's Catalog of Groups: Permutation Groups***

Let  $X$  be a nonempty set, and let  $\mathcal{S}(X)$  denote the set of permutations of  $X$ . Then  $(\mathcal{S}(X), \circ)$  is a group, with  $\circ$  denoting the operation of composition. Furthermore, this group is abelian if and only if  $X$  is finite with  $|X| \leq 2$ . Such groups and their subgroups are the object of study in this chapter; they are known as *permutation groups*.

If  $X$  is a finite set with  $n$  elements, then we might as well let  $X = \{1, 2, \dots, n\}$ . In this case, the group  $\mathcal{S}(X)$  is denoted by  $S_n$ , and is called the ***symmetric group of degree  $n$*** . Note that the identity element of  $S_n$  is the *identity permutation*  $\epsilon$ , defined on  $\{1, 2, \dots, n\}$  by  $\epsilon(x) = x$ .

**Example 1:** The only permutation of  $\{1\}$  is  $\epsilon$ ; thus  $S_1 = \{\epsilon\}$  is trivial.

If  $n = 2$ , there are two permutations of  $\{1, 2\}$ :  $\epsilon$ , and the permutation  $\alpha$  defined by  $\alpha(1) = 2$  and  $\alpha(2) = 1$ . Therefore,  $S_2 = \{\epsilon, \alpha\}$  and, since  $|S_2| = 2$ ,  $S_2$  is isomorphic to  $C_2$ .

If  $n = 3$ , there are  $3! = 6$  permutations of  $\{1, 2, 3\}$  (since there are 3 choices for the image of 1; then 2 choices for the image of 2; and finally only one choice for the image of 3).

Besides the identity permutation  $\epsilon$ , an element of  $S_3$  is the permutation  $\alpha$  of  $\{1, 2, 3\}$  defined by  $\alpha(1) = 2$ ,  $\alpha(2) = 3$ , and  $\alpha(3) = 1$ . Using array notation, we denote  $\alpha$  by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

In general, for a permutation  $\alpha$  of  $\{1, 2, \dots, n\}$ , the *array notation* for  $\alpha$  is

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}$$

that is,  $\alpha$  is expressed in array notation as a 2 by  $n$  matrix, where the first row of the matrix is the vector  $[1 \ 2 \ \dots \ n]$  and the second row is the vector  $[\alpha(1) \ \alpha(2) \ \dots \ \alpha(n)]$ .

Given  $\alpha$ , we may compute  $\alpha^2 = \alpha \circ \alpha$ :

$$\alpha^2 = \alpha \circ \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

For example,  $\alpha^2(1) = (\alpha \circ \alpha)(1) = \alpha(\alpha(1)) = \alpha(2) = 3$ . Then  $\alpha^3 = \epsilon$ , so  $\alpha$  has order 3.

Another permutation of  $\{1, 2, 3\}$  is  $\beta$ , with  $\beta(1) = 1$ ,  $\beta(2) = 3$ , and  $\beta(3) = 2$ ;  $\beta$  is expressed in array notation as

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

Note that  $\beta^2 = \beta \circ \beta = \epsilon$ , so that  $|\beta| = 2$ .

Given that  $S_n$  is closed under composition, if  $\alpha \in S_n$  and  $\beta \in S_n$ , then  $\beta \circ \alpha \in S_n$ . We denote the permutation  $\beta \circ \alpha$ , using juxtaposition, by  $\alpha\beta$ , since it is more natural to apply permutations from left to right, rather than from right to left.

In  $S_3$ , for example, we may compute that

$$\begin{aligned} \alpha\beta &= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \\ \alpha^2\beta &= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \end{aligned}$$

For example,  $(\alpha\beta)(1) = (\beta \circ \alpha)(1) = \beta(\alpha(1)) = \beta(2) = 3$ .

Thus,  $S_3 = \{\epsilon, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$  is a group of order 6. We know that there are two groups of order 6, up to isomorphism:  $C_6$  and  $D_3$ . In  $S_3$ , note that

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \alpha^2\beta$$

Thus,  $S_3$  is nonabelian, and has the presentation

$$S_3 = \langle \alpha, \beta \mid |\alpha| = 3, |\beta| = 2, \beta\alpha = \alpha^2\beta \rangle$$

It follows that  $S_3 \cong D_3$ . ■

In general,  $|S_n| = n!$ , as it is a simple combinatorial argument that the number of permutations of  $\{1, 2, \dots, n\}$  is  $n!$ . Thus,  $|S_4| = 4! = 24$ , and  $|S_5| = 5! = 120$ . Furthermore, if  $G = S_n$ ,  $n \geq 2$ , and we consider the subgroup  $H$  of  $G$  defined by

$$H = \{\alpha \in G \mid \alpha(n) = n\}$$

then it is clear that  $H \cong S_{n-1}$ . Thus, we may consider  $S_{n-1}$  to be a subgroup of  $S_n$  for  $n \geq 2$ .

Mathematicians are generally “lazy.” That is, mathematicians want to convey a particular idea or concept in as few symbols as possible. Consider a permutation  $\alpha$  of  $S_n$  that is not the identity permutation. Then, for some  $x \in \{1, 2, \dots, n\}$ ,  $\alpha(x) \neq x$ . Consider the sequence

$$x = \alpha^0(x), \alpha(x) = \alpha^1(x), \alpha(\alpha(x)) = \alpha^2(x), \alpha(\alpha(\alpha(x))) = \alpha^3(x), \dots$$

Since each member of this sequence is an element of  $\{1, 2, \dots, n\}$ , the sequence contains repeated members. In fact, it is an exercise to show that the first element to repeat is  $x$ . Let  $k$  be the minimum exponent such that  $\alpha^k(x) = x$ ; thus,  $k \geq 2$ . The list

$$(x, \alpha(x), \dots, \alpha^{k-1}(x))$$

is called a *cycle of length  $k$* , or  *$k$ -cycle*.

When a permutation  $\alpha$  of  $\{1, 2, \dots, n\}$  is a  $k$ -cycle for some  $k \geq 2$ , say

$$\alpha = (x_1, x_2, \dots, x_k)$$

then  $\alpha(x_i) = x_{i+1}$  for each  $i$ ,  $1 \leq i < k$ , and  $\alpha(x_k) = x_1$ . That is,  $\alpha$  maps each element of the cycle to its successor in the cycle, with the understanding that the successor of the last element in the cycle is the first element. Also, for any element  $y$  not listed in the cycle — that is, for any  $y \in \{1, 2, \dots, n\} - \{x_1, x_2, \dots, x_k\}$  —  $\alpha(y) = y$ .

For example, consider the permutation  $\alpha$  of  $\{1, 2, 3, 4, 5, 6\}$  given in array form by

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

Then  $\alpha$  is a 4-cycle, namely,  $\alpha = (2, 3, 6, 5)$ . Usually, the commas are omitted, and we write  $\alpha = (2365)$ . Note that the expression of  $\alpha$  as a 4-cycle is not unique; here, for example,

$$\alpha = (3652) \quad \text{or} \quad \alpha = (6523) \quad \text{or} \quad \alpha = (5236)$$

However, by convention, the smallest element of a cycle is usually listed first.

Define the permutation  $\beta$  of  $\{1, 2, 3, 4, 5, 6\}$  by

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

Then  $\beta = (14)$  is a 2-cycle. The cycles  $(2365)$  and  $(14)$  are said to be *disjoint cycles* since they have no elements in common. Disjoint cycles commute with each other; for example,  $\alpha\beta = \gamma = \beta\alpha$ , with

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

Thus, we may express  $\gamma$  as a product of disjoint cycles in two ways:

$$\gamma = (14)(2365) \quad \text{or} \quad \gamma = (2365)(14)$$

Again, the convention is to order the disjoint cycles according to the smallest element contained in the cycle.

How should the identity permutation  $\epsilon$  in  $S_n$  be expressed using cycle notation (that is, as a product of disjoint cycles)? Well, if  $\alpha$  is a permutation of  $\{1, 2, \dots, n\}$  and  $\alpha(x) = x$ , for some  $x$ ,  $1 \leq x \leq n$ , then we could use the “1-cycle”  $(x)$  to explicitly indicate that  $\alpha$  fixes  $x$ . For example, for the permutations  $\alpha$  and  $\beta$  above, it would not be incorrect to write

$$\alpha = (1)(2\ 3\ 6\ 5)(4) \quad \text{and} \quad \beta = (1\ 4)(2)(3)(5)(6)$$

The convention, however, is to omit any 1-cycles from the cycle notation. But  $\epsilon$  contains only 1-cycles. If we omitted all the 1-cycles, we would be forced to write “ $\epsilon = .$ ” This would be confusing, to say the least. Therefore, the convention is to write

$$\epsilon = (1)$$

In summary, we have the following result.

**Theorem 1:** Let  $n$  be an integer,  $n \geq 2$ . Then any element of  $S_n$  can be expressed as a cycle, or as a product of disjoint cycles. Furthermore, disjoint cycles commute with each other. ■

**Example 2:** Consider the following two permutations in  $S_8$ :

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

Express, using cycle notation:

- |                   |                   |
|-------------------|-------------------|
| (a) $\alpha$      | (b) $\beta$       |
| (c) $\alpha^2$    | (d) $\beta^{-1}$  |
| (e) $\alpha\beta$ | (f) $\beta\alpha$ |

**Solution:**

- |  |  |
|--|--|
| (a) $\alpha = (1\ 3\ 5\ 7)(2\ 4\ 6)$         | (b) $\beta = (1\ 8)(2\ 7)(3\ 4\ 5\ 6)$       |
| (c) $\alpha^2 = (1\ 5)(2\ 6\ 4)(3\ 7)$       | (d) $\beta^{-1} = (1\ 8)(2\ 7)(3\ 6\ 5\ 4)$  |
| (e) $\alpha\beta = (1\ 4\ 3\ 6\ 7\ 8)(2\ 5)$ | (f) $\beta\alpha = (1\ 8\ 3\ 6\ 5\ 2)(4\ 7)$ |

**Example 3:** There are  $4! = 24$  permutations of  $\{1, 2, 3, 4\}$ ; that is,  $|S_4| = 24$ . List the elements of  $S_4$  using cycle notation.

**Solution:** We list the elements by “type:”

1-cycle:  $\epsilon = (1)$

2-cycle: A 2-cycle has the form  $(ab)$ , and we may assume that  $a < b$ . Since the number of ways to choose two distinct elements  $a$  and  $b$  from  $\{1, 2, 3, 4\}$  is  $C(4, 2) = 6$ , the number of 2-cycles in  $S_4$  is 6. Here they are:

$$(12) \quad (13) \quad (14) \quad (23) \quad (24) \quad (34)$$

3-cycle: A 3-cycle has the form  $(abc)$ , and we may assume that  $a < b$  and  $a < c$ . Since the number of ways to choose three distinct elements  $a, b$ , and  $c$  from  $\{1, 2, 3, 4\}$  is  $C(4, 3) = 4$ , and, once chosen, the largest two of these three elements may be ordered in 2 ways, the number of 3-cycles in  $S_4$  is  $4 \cdot 2 = 8$ . Here they are:

$$(123) \quad (132) \quad (124) \quad (142) \quad (134) \quad (143) \quad (234) \quad (243)$$

4-cycle: A 4-cycle has the form  $(abcd)$ , with  $(b, c, d)$  a permutation of  $\{2, 3, 4\}$ . Since there are  $3! = 6$  permutations of  $\{2, 3, 4\}$ , the number of 4-cycles in  $S_4$  is 6; here they are:

$$(1234) \quad (1243) \quad (1324) \quad (1342) \quad (1423) \quad (1432)$$

product of two disjoint 2-cycles: A product of two disjoint 2-cycles has the form  $(1b)(cd)$ . There are 3 choices for  $b$  and, since  $(cd) = (dc)$ , the choice of  $b$  determines such a permutation. Thus, there are 3 permutations of  $S_4$  that are products of disjoint 2-cycles, and here they are:

$$(12)(34) \quad (13)(24) \quad (14)(23)$$

This accounts for all 24 permutations in  $S_4$ . ■

The fact that any permutation in  $S_n$  can be expressed as a product of disjoint cycles lets us easily compute the order of any such permutation.

**Theorem 2:** Let  $n$  be an integer,  $n \geq 2$ , and let  $\alpha \in S_n$ .

1. If  $\alpha$  is a  $k$ -cycle for some  $k$ ,  $2 \leq k \leq n$ , then  $|\alpha| = k$ .
2. If  $\alpha$  is a product of disjoint cycles, then  $|\alpha|$  is the least common multiple of the cycle lengths.

**Proof:** Let  $n$  be an integer,  $n \geq 2$ , and let  $\alpha \in S_n$ .

First, suppose  $\alpha$  is a  $k$ -cycle for some  $k$ ,  $2 \leq k \leq n$ , say

$$\alpha = (x_0 x_1 \dots x_{k-1})$$

Then, for any integer  $t$ ,  $2 \leq t < k$ , and any  $i$ ,  $0 \leq i < k$ ,  $\alpha^t$  maps  $x_i$  to  $x_{i+t}$ , with the subscripts computed mod  $k$ . Hence, for  $1 \leq t < k$ ,  $\alpha^t(x_0) = x_t \neq x_0$ . Thus,  $\alpha^t \neq \epsilon$  for  $1 \leq t < k$ .

However, when  $t = k$ ,  $\alpha^k(x) = x$  for each  $x \in \{1, 2, \dots, n\}$ . Therefore,  $\alpha^k = \epsilon$ , which shows that  $|\alpha| = k$ .

The second part of the theorem is an immediate consequence of the fact that disjoint cycles commute with each other and the result that, in a finite group  $G$ , if the elements  $x$  and  $y$  commute with each other, then

$$|xy| = \text{lcm}(|x|, |y|)$$

■

It is useful to be able to determine the number of elements of a particular order in a given finite group. For example, given integers  $n$  and  $m$  with  $1 \leq m \leq n$  and  $m$  a factor of  $n$ , the number of elements of order  $m$  in  $C_n$  is  $\phi(m)$ . This fact, along with a basic result concerning orders of elements in direct products (see *Direct Products and Semi-direct Products*), allows us to determine the number of elements of order  $k$  in any finite abelian group  $G$ , once we are able to express  $G$  as a direct product of cyclic groups.

In a similar way, Theorem 2, along with a couple of basic results from combinatorics, allows to determine the number of elements of any particular order in  $S_n$ .

Given a nonempty finite set  $X$ , an *ordered partition of  $X$  into  $m$  parts* is a sequence  $(X_1, X_2, \dots, X_m)$  of subsets of  $X$  such that the subsets are pairwise disjoint and their union is  $X$ . For example, each of  $(\{1, 4, 6\}, \{2, 3, 5, 7\})$  and  $(\{1, 7\}, \{2, 6\}, \{3, 4, 5\})$  is an ordered partition of  $X = \{1, 2, \dots, 7\}$ ; the first ordered partition has 2 parts, and the second has 3 parts.

Obviously, if  $|X| = n$ , then there is only one ordered partition of  $X$  into 1 part —  $(X)$  — and  $n!$  ordered partitions of  $X$  into  $n$  parts, since such ordered partitions correspond to the permutations of  $X$ . In general, we have the following result; for those interested, the proof is considered in Additional Exercise 4.

**Theorem 3:** Let  $k, m$ , and  $n$  be integers with  $1 < k, m < n$ . Then:

1. The number of ordered partitions of  $\{1, 2, \dots, n\}$  into  $m$  parts, with  $n_i$  elements in the  $i$ th part,  $1 \leq i \leq m$ , is  $C(n; n_1, n_2, \dots, n_m)$ , computed as follows:

$$C(n; n_1, n_2, \dots, n_m) = \frac{n!}{n_1! n_2! \cdots n_m!}$$

2. The number of  $k$ -cycles that can be formed from a given  $k$ -element subset of  $\{1, 2, \dots, n\}$  is  $(k - 1)!$ .

3. The number of  $k$ -cycles in  $S_n$  is

$$C(n, k)(k - 1)!$$

■

**Example 4:** Apply Theorem 3 to find the number of elements of each possible order in:

(a)  $S_5$

(b)  $S_6$

**Solution:** Be reminded that any group has a unique element of order 1, namely, the identity element. In particular, the identity permutation  $\epsilon$  is the unique permutation of order 1 in  $S_n$ .

For (a), keep in mind that we have only five numbers to work with: 1, 2, 3, 4, and 5. Thus, the maximum order we can have is 6, and this order is attained for a permutation such as  $(1\ 2)(3\ 4\ 5)$ , which is the disjoint product of a 2-cycle and a 3-cycle.

Any permutation of order 2 in  $S_5$  must be a 2-cycle, or a product of two disjoint 2-cycles. A 2-cycle  $(a\ b)$  is completely determined by the choice of  $a$  and  $b$  (since  $(a\ b) = (b\ a)$ ). Thus, the number of 2-cycles in  $S_5$  is

$$C(5, 2) = \frac{5(5-1)}{2} = 10$$

A product of two disjoint 2-cycles looks like  $(a\ b)(c\ d)$  with  $(\{a, b\}, \{c, d\}, \{e\})$  an ordered partition of  $\{1, 2, 3, 4, 5\}$  into 3 parts of cardinalities 2, 2, and 1, respectively. However, the distinct ordered partitions  $(\{a, b\}, \{c, d\}, \{e\})$  and  $(\{c, d\}, \{a, b\}, \{e\})$  produce the same permutation, since  $(a\ b)(c\ d) = (c\ d)(a\ b)$ . Therefore, the number of distinct permutations of  $S_n$  of the form  $(a\ b)(c\ d)$  is

$$\frac{C(5; 2, 2, 1)}{2} = 15$$

It follows that  $S_n$  contains  $10 + 15 = 25$  permutations of order 2.

A permutation of order 3 in  $S_5$  must be a 3-cycle and, by Theorem 3, part 3, the number of 3-cycles in  $S_5$  is

$$C(5, 3) \cdot 2! = 20$$

A permutation of order 4 in  $S_5$  must be a 4-cycle, and the number of 4-cycles in  $S_5$  is

$$C(5, 4) \cdot 3! = 30$$

Likewise, a permutation of order 5 in  $S_5$  must be a 5-cycle, and the number of 5-cycles in  $S_5$  is

$$C(5, 5) \cdot 4! = 24$$

As mentioned above, the maximum order of any permutation in  $S_5$  is 6, and a permutation of order 6 has the form  $(abc)(de)$ , with  $(\{a, b, c\}, \{d, e\})$  an ordered partition of  $\{1, 2, 3, 4, 5\}$  into 2 parts, with 3 elements in the first part and 2 elements in the second part. Furthermore, each such permutation is uniquely determined by choosing such an ordered partition, and then making the parts into cycles. Therefore, the number of permutations of order 6 in  $S_5$  is

$$C(5; 3, 2) \cdot 2 = 20$$

Our results for  $S_5$  are summarized in the following table:

order	no. of elements
1	1
2	25
3	20
4	30
5	24
6	20
total	$120 = 5!$

(b) **Exercise:** Verify the following table for  $S_6$ :

order	no. of elements
1	1
2	75
3	80
4	180
5	144
6	240
total	$720 = 6!$

■

Among the elements of  $S_n$ , the 2-cycles are especially important. In particular, any element of  $S_n$  can be expressed as a product of 2-cycles; in fact,  $S_n$  is generated by the 2-cycles

$$\delta_2 = (12), \quad \delta_3 = (13), \quad \dots, \quad \delta_n = (1n)$$

To see this, first note that any cycle can be expressed as a product using these 2-cycles:

$$\begin{aligned} (ab) &= (1a)(1b)(1a) \\ (1bc) &= (1b)(1c) \\ (abc) &= (ab)(ac) = (1a)(1b)(1c)(1a) \\ (1bcd) &= (1b)(1c)(1d) \\ (abcd) &= (abc)(ad) = (1a)(1b)(1c)(1d)(1a) \end{aligned}$$

and so on, where  $1 \notin \{a, b, c, d\}$ . Then, since any permutation can be expressed as a product of disjoint cycles, it follows that  $\{\delta_2, \delta_3, \dots, \delta_n\}$  is a generating set for  $S_n$ .

Obviously, the expression of a given permutation as a product of 2-cycles is not unique. Here's another example:

$$\begin{aligned}(1\ 2\ 3\ 4\ 5) &= (1\ 2)(1\ 3)(1\ 4)(1\ 5) \\(1\ 2\ 3\ 4\ 5) &= (1\ 3)(1\ 4)(1\ 3)(3\ 5)(1\ 3)(3\ 2) \\(1\ 2\ 3\ 4\ 5) &= (1\ 3)(1\ 4)(1\ 3)(3\ 5)(2\ 4)(4\ 2)(1\ 3)(3\ 2)\end{aligned}$$

Note that each of the three expressions of  $(1\ 2\ 3\ 4\ 5)$  as a product a 2-cycles uses an even number of 2-cycles; that is, the parity of the number of 2-cycles used is even in each case.

Given an integer  $s$ , the *parity* of  $s$  refers to whether  $s$  is even or odd, and two integers  $s$  and  $t$  are said to have the *same parity* if they are both even or both odd. Although a permutation  $\alpha$  can be expressed as a product of 2-cycles in infinitely many ways, any two such products have the same parity, in terms of the number of 2-cycles used.

**Lemma 4:** Any expression of the identity permutation  $\epsilon$  as a product of 2-cycles uses an even number of 2-cycles.

**Proof:** Let  $n$  be an integer,  $n \geq 2$ , and consider  $S_n$ . Suppose, contrary to the result of the theorem, that  $\epsilon$  can expressed as the product of an odd number 2-cycles, say

$$\epsilon = \beta_1\beta_2 \cdots \beta_t \quad \clubsuit$$

Given the sequence  $\mathcal{L} = (\beta_1, \beta_2, \dots, \beta_t)$  of 2-cycles used in  $\clubsuit$ , we are interested in three numbers: (1) its length  $t$ ; (2) the maximum number,  $k$ , that appears among the 2-cycles; and (3) the rightmost index,  $j$ , among those 2-cycles in which  $k$  appears (that is, the maximum index  $j$  for which  $\beta_j(k) \neq k$ ). By the principle of well-ordering, we may assume that we have chosen a counterexample  $\mathcal{L}$  so that (1)  $t$  is a minimum; (2) among all counterexamples with length  $t$ ,  $k$  is a minimum, and (3) among all counterexamples with length  $t$  for which the maximum value used is  $k$ ,  $j$  is a minimum.

It must be that  $k \geq 3$ , since, if  $k = 2$ , then  $\beta_1 = \beta_2 = \cdots = \beta_t = (1\ 2)$ , which forces  $t$  to be even.

Note that  $k$  must appear in at least two of the  $\beta$ s, since, if some  $\beta_i$  is the only 2-cycle in which  $k$  appears, then the product of the  $\beta$ s does not map  $k$  to  $k$ , and hence is not equal to  $\epsilon$ . This forces  $j$  to be at least 2.

Consider the product  $\beta_{j-1}\beta_j$ . Based on the form of this product, we shall determine a revised product of 2-cycles equal to  $\epsilon$ :

$$\epsilon = \beta'_1\beta'_2 \cdots \beta'_t \quad \blacklozenge$$

and, equivalently, a revised sequence  $\mathcal{L}' = (\beta'_1, \beta'_2, \dots, \beta'_t)$  of the 2-cycles used in  $\diamond$ . So  $\mathcal{L}'$  has odd length  $t'$ ; let  $k'$  be the maximum number that appears in  $\mathcal{L}'$ , and let  $j'$  be the rightmost index such that  $\beta_{j'}(k') \neq k'$ .

*Case 1:*  $\beta_{j-1} = \beta_j$ . Then  $\beta_{j-1}\beta_j = \epsilon$ , and so we define the sequence  $\mathcal{L}'$  by deleting  $\beta_{j-1}$  and  $\beta_j$  from  $\mathcal{L}$ . In this case, however,  $t' = t - 2 < t$ . This contradicts the choice of  $\mathcal{L}$ .

*Case 2:*  $\beta_{j-1} \neq \beta_j$  and  $k$  appears in  $\beta_{j-1}$ . Then, for some  $1 \leq a, b < k$  with  $a \neq b$ ,

$$\beta_{j-1}\beta_j = (a k)(b k) = (b k)(a b)$$

Thus, we obtain the sequence  $\mathcal{L}'$  from  $\mathcal{L}$  by replacing  $\beta_{j-1}$  by  $\beta'_{j-1} = (b k)$  and  $\beta_j$  by  $\beta'_j = (a b)$ . This results in  $\mathcal{L}'$  having  $t' = t$  and  $k' = k$ , but with  $j' = j - 1 < j$ . This again contradicts the choice of  $\mathcal{L}$ .

*Case 3:*  $\beta_{j-1} \neq \beta_j$ , and  $k$  does not appear in  $\beta_{j-1}$ , yet some other element  $a$  does appear in both  $\beta_{j-1}$  and  $\beta_j$ . Then, for some  $1 \leq a, b < k$ ,

$$\beta_{j-1}\beta_j = (a b)(a k) = (b k)(a b)$$

Thus, we obtain the sequence  $\mathcal{L}'$  from  $\mathcal{L}$  by replacing  $\beta_{j-1}$  by  $\beta'_{j-1} = (b k)$  and  $\beta_j$  by  $\beta'_j = (a b)$ . This results in  $\mathcal{L}'$  having  $t' = t$  and  $k' = k$ , but with  $j' = j - 1 < j$ . This again contradicts the choice of  $\mathcal{L}$ .

*Case 4:*  $\beta_{j-1}$  and  $\beta_j$  are disjoint 2-cycles. Thus, we obtain the sequence  $\mathcal{L}'$  from  $\mathcal{L}$  by replacing  $\beta_{j-1}$  by  $\beta_j$  and  $\beta_j$  by  $\beta_{j-1}$ . This results in  $\mathcal{L}'$  having  $t' = t$  and  $k' = k$ , but with  $j' = j - 1 < j$ . This contradicts the choice of  $\mathcal{L}$ .

In any case, we obtain a contradiction to the assumption that  $\epsilon$  can be expressed as a product of an odd number of 2-cycles, thus proving the lemma. ■

**Theorem 5:** Let  $\alpha \in S_n$ , and suppose  $\alpha$  can be expressed as the product of  $s$  2-cycles and also as the product of  $t$  2-cycles. Then  $s$  and  $t$  have the same parity.

**Proof:** Let  $\alpha \in S_n$ , and suppose  $\alpha$  can be expressed as the product  $s$  2-cycles and also as the product of  $t$  2-cycles, say

$$\beta_1\beta_2 \cdots \beta_s = \alpha = \gamma_1\gamma_2 \cdots \gamma_t$$

Then

$$\begin{aligned} \epsilon &= (\beta_1\beta_2 \cdots \beta_s)(\gamma_1\gamma_2 \cdots \gamma_t)^{-1} \\ &= (\beta_1\beta_2 \cdots \beta_s)(\gamma_t^{-1} \cdots \gamma_2^{-1}\gamma_1^{-1}) \\ &= (\beta_1\beta_2 \cdots \beta_s)(\gamma_t \cdots \gamma_2\gamma_1) \end{aligned}$$

using the fact that any 2-cycle is its own inverse. Thus, we have  $\epsilon$  expressed as a product of  $s + t$  2-cycles. By the lemma, this means that  $s + t$  is even, which in turn implies that  $s$  and  $t$  are either both odd or both even. ■

In view of Theorem 5, we have the following definition.

**Definition 1:** Let  $\alpha \in S_n$ . If any expression of  $\alpha$  as a product of 2-cycles uses an even number of 2-cycles, then  $\alpha$  is called an **even permutation**; otherwise,  $\alpha$  is called an **odd permutation**. The subset of  $S_n$  consisting of the even permutations is denoted by  $A_n$ . ■

**Theorem 6:** For  $n \geq 2$ ,  $A_n$  is a subgroup of  $S_n$ . Moreover,  $|A_n| = |S_n|/2$ , and hence  $A_n$  is a normal subgroup of  $S_n$ .

**Proof:** First, to show that  $A_n$  is a subgroup of  $S_n$ , we apply SJST.

By Lemma 4,  $\epsilon \in A_n$ . Let  $\alpha_1, \alpha_2 \in A_n$ . Then each of  $\alpha_1$  and  $\alpha_2$  can be expressed as an even number of 2-cycles, say

$$\alpha_1 = \beta_1\beta_2 \cdots \beta_s \quad \text{and} \quad \alpha_2 = \gamma_1\gamma_2 \cdots \gamma_t$$

Thus,

$$\begin{aligned} \alpha_1\alpha_2 &= \beta_1\beta_2 \cdots \beta_s\gamma_1\gamma_2 \cdots \gamma_t \\ \alpha_1^{-1} &= (\beta_1\beta_2 \cdots \beta_s)^{-1} = \beta_s \cdots \beta_2\beta_1 \end{aligned}$$

Hence,  $\alpha_1\alpha_2$  can be expressed as a product of  $s + t$  2-cycles, and  $\alpha_1^{-1}$  can be expressed as a product of  $s$  2-cycles, and both  $s + t$  and  $s$  are even. Therefore,  $\alpha_1\alpha_2 \in A_n$  and  $\alpha_1^{-1} \in A_n$ , which shows that  $A_n$  is closed under products and inverses. Therefore,  $A_n \leq S_n$ .

Next, to show that half the permutations of  $\{1, 2, \dots, n\}$  are even and half are odd, it suffices to construct a bijection  $f : A_n \rightarrow S_n - A_n$  (note that  $S_n - A_n$  is the subset of  $S_n$  consisting of the odd permutations).

Note that the 2-cycle  $(1\ 2)$  is odd, and the product of an even permutation and an odd permutation is odd (see Additional Exercise 6). Thus, we may define  $f : A_n \rightarrow S_n - A_n$  by

$$f(\alpha) = (1\ 2)\alpha$$

Clearly,  $f$  is onto, for if  $\beta$  is an odd permutation, then  $(1\ 2)\beta$  is an even permutation, and

$$f((1\ 2)\beta) = (1\ 2)(1\ 2)\beta = \beta$$

Moreover,  $f$  is one-to-one, for if  $\alpha_1, \alpha_2 \in A_n$ , then

$$f(\alpha_1) = f(\alpha_2) \rightarrow (1\ 2)\alpha_1 = (1\ 2)\alpha_2 \rightarrow \alpha_1 = \alpha_2$$

by cancellation. ■

As noted above, a  $k$ -cycle is even if and only if  $k$  is odd. This yields the following result.

**Theorem 7:** For  $\alpha \in S_n$ ,  $\alpha \in A_n$  if and only if any expression of  $\alpha$  as a product of disjoint cycles has an even number of cycles of even length. ■

**Example 5:** Note that  $A_2 = \{\epsilon\}$  is trivial. Find:

(a)  $A_3$

(b)  $A_4$

**Solution:** For (a), note that every nonidentity element of  $S_3$  is a 2-cycle or a 3-cycle. By the result of Theorem 7, 2-cycles are odd and 3-cycles are even. Therefore,

$$A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$$

For (b), refer to Example 3. There, we note that each nonidentity element of  $S_4$  is either: (2) a 2-cycle, which is odd; (3) a 3-cycle, which is even; (4) a 4-cycle, which is odd; or (5) a product of two disjoint 2-cycles, which is even. Therefore,  $A_4$  consists of the identity permutation, 3-cycles, and products of two disjoint 2-cycles:

$$A_4 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

**Example 6:** Note that  $|A_5| = 5!/2 = 60$ . Also, note that the maximum order of any element of  $S_5$  is 6, which is attained only by the disjoint product of a 2-cycle and a 3-cycle, which is odd. Thus, the maximum order of any element in  $A_5$  is 5. The identity permutation is the unique element of order 1. For each  $k$ ,  $2 \leq k \leq 5$ , find the number of elements of  $A_5$  of order  $k$ .

**Solution:** For  $k = 2$ ,  $\alpha \in A_5$  has order 2 if and only if  $\alpha$  is the product of two disjoint 2-cycles,  $(a\ b)(c\ d)$ . To determine  $\alpha$  uniquely, we can: (1) choose the unique element  $x \in \{1, 2, 3, 4, 5\}$  such that  $\alpha(x) = x$ ; (2) for any  $y \in \{1, 2, 3, 4, 5\} - \{x\}$ , choose its image  $\alpha(y)$ . Since (1) can be done in 5 ways and (2) can be done in  $C(3, 1) = 3$  ways, this yields 15 elements of  $A_5$ .

For  $k = 3$  or 5, any element of order  $k$  in  $S_5$  is a  $k$ -cycle, which is even. By Example 4, part (a),  $S_5$  has 20 3-cycles and 24 5-cycles.

The other nonidentity elements of  $S_5$  have order 4 and are 4-cycles, which are odd.

In conclusion,  $A_5$  has 1 element of order 1, 15 elements of order 2, 20 elements of order 3, and 24 elements of order 5, for a total of 60 elements. ■

Subgroups of some symmetric group often occur as the group of symmetries of some mathematical object in the plane or in space. For the basics, refer to *Dihedral Groups*.

In that chapter, we considered the group of symmetries for a regular  $n$ -pyramid and for a regular  $n$ -prism. In this chapter, we consider the regular polyhedra. A *regular polyhedron* is a polyhedron each of whose faces is congruent to a given regular polygon. One of the most famous results in mathematics is that there are exactly five regular polyhedra:

1. the *tetrahedron*, which has four vertices, six edges, and four faces, each congruent to the same equilateral triangle;
2. the *cube*, which has eight vertices, twelve edges, and six faces, each congruent to the same square;
3. the *octahedron*, which has six vertices, twelve edges, and eight faces, each congruent to the same equilateral triangle;
4. the *dodecahedron*, which has twenty vertices, thirty edges, and twelve faces, each of which is congruent to the same regular pentagon;
5. the *icosahedron*, which has twelve vertices, thirty edges, and twenty faces, each congruent to the same equilateral triangle.

The cube and octahedron are *dual* polyhedra, and this implies that they have the same group of symmetries. Likewise, the dodecahedron and icosahedron are dual and have the same symmetry group.

Thus, for the regular polyhedra, it suffices to determine the group of symmetries for the tetrahedron, the cube, and the icosahedron.

**Example 7:** Determine the group  $\mathcal{G}$  of symmetries of the (regular) tetrahedron  $\mathcal{T}$ .

**Solution:** Without loss of generality, we place  $\mathcal{T}$  in  $\mathbb{R}^3$  so that its four vertices are

$$A = (1, 1, 1), \quad B = (1, -1, -1), \quad C = (-1, 1, -1), \quad D = (-1, -1, 1)$$

Note that  $AB = AC = AD = BC = BD = CD = 2\sqrt{2}$ . Also note that, with  $Z = (0, 0, 0)$ , we have  $AZ = BZ = CZ = DZ = \sqrt{3}$ . Thus, the origin  $Z$  is the center of  $\mathcal{T}$ .

Any symmetry of  $\mathcal{T}$  must permute  $\{A, B, C, D\}$ ; thus, the group of symmetries of  $\mathcal{T}$  is a subgroup of  $\mathcal{S}(\{A, B, C, D\}) \cong S_4$ . In fact, any permutation of  $\{A, B, C, D\}$  defines a symmetry of  $\mathcal{T}$ , since the vertices of  $\mathcal{T}$  are equidistant from each other. Therefore, the group  $\mathcal{G}$  of symmetries of  $\mathcal{T}$  is isomorphic to  $S_4$ .

We note that each of the lines  $\overleftrightarrow{AZ}$ ,  $\overleftrightarrow{BZ}$ ,  $\overleftrightarrow{CZ}$ , and  $\overleftrightarrow{DZ}$  is an axis of 3-fold rotational symmetry of  $\mathcal{T}$ , meaning that, if  $\mathbb{R}^3$  is rotated  $(360/3)^\circ = 120^\circ$  about any one of these lines, then  $\mathcal{T}$  is mapped to  $\mathcal{T}$ . It follows that each of the following is a symmetry of  $\mathcal{T}$ :

$$\begin{aligned}
 \rho_1 &= \text{rotation, } 120^\circ, \overleftrightarrow{AZ} = (BCD) \\
 \rho_1^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{AZ} = (BDC) \\
 \rho_2 &= \text{rotation, } 120^\circ, \overleftrightarrow{BZ} = (ACD) \\
 \rho_2^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{BZ} = (ADC) \\
 \rho_3 &= \text{rotation, } 120^\circ, \overleftrightarrow{CZ} = (ABD) \\
 \rho_3^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{CZ} = (ADB) \\
 \rho_4 &= \text{rotation, } 120^\circ, \overleftrightarrow{DZ} = (ABC) \\
 \rho_4^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{DZ} = (ACB)
 \end{aligned}$$

Next, let the points  $E, F, G, H, I,$  and  $J$  be the midpoints of the edges of  $\mathcal{T}$ ; that is, let

$$\begin{aligned}
 E &= \text{midpoint of } \overline{AB} = (1, 0, 0) & F &= \text{midpoint of } \overline{AC} = (0, 1, 0) \\
 G &= \text{midpoint of } \overline{AD} = (0, 0, 1) & H &= \text{midpoint of } \overline{BC} = (0, 0, -1) \\
 I &= \text{midpoint of } \overline{BD} = (0, -1, 0) & J &= \text{midpoint of } \overline{CD} = (-1, 0, 0)
 \end{aligned}$$

Note that a line through the midpoint of any edge and the midpoint of the opposite edge (which also contains  $Z$ ) is an axis of 2-fold rotational symmetry of  $\mathcal{T}$ ; that is, if  $\mathbb{R}^3$  is rotated  $(360/2)^\circ = 180^\circ$  about any one of these lines, then  $\mathcal{T}$  is mapped to  $\mathcal{T}$ . It follows that each of the following is a symmetry of  $\mathcal{T}$ :

$$\begin{aligned}
 \rho_5 &= \text{rotation, } 180^\circ, \overleftrightarrow{EJ} = (AB)(CD) \\
 \rho_6 &= \text{rotation, } 180^\circ, \overleftrightarrow{FI} = (AC)(BD) \\
 \rho_7 &= \text{rotation, } 180^\circ, \overleftrightarrow{GH} = (AD)(BC)
 \end{aligned}$$

We note that the rotational symmetries of  $\mathcal{T}$  (including the identity symmetry  $\epsilon$ ) form a subgroup of the group of all symmetries of  $\mathcal{T}$ . In fact, as a permutation of the set  $\{A, B, C, D\}$  of vertices of  $\mathcal{T}$ , each of the rotational symmetries is an even permutation, and there are exactly 12 of them. Hence, the subgroup  $\mathcal{H}$  of rotational symmetries of  $\mathcal{T}$  is isomorphic to  $A_4$ .

The tetrahedron  $\mathcal{T}$  also has reflective symmetry. The plane through any two vertices of  $\mathcal{T}$  and the midpoint of the opposite edge is a mirror of reflective symmetry. This observation yields the following symmetries of  $\mathcal{T}$ :

$$\begin{aligned}
 \sigma_1 &= \text{reflection, } y + z = 0; \sigma_1 = (AB) \\
 \sigma_2 &= \text{reflection, } x + z = 0; \sigma_2 = (AC) \\
 \sigma_3 &= \text{reflection, } x + y = 0; \sigma_3 = (AD) \\
 \sigma_4 &= \text{reflection, } x = y; \sigma_4 = (BC) \\
 \sigma_5 &= \text{reflection, } x = z; \sigma_5 = (BD) \\
 \sigma_6 &= \text{reflection, } y = z; \sigma_6 = (CD)
 \end{aligned}$$

The remaining six symmetries of  $\mathcal{T}$  are the permutations of  $\{A, B, C, D\}$  that are 4-cycles. Each of these can be expressed as the composition of a 2-fold rotational symmetry and a reflective symmetry, as follows:

$$\begin{aligned}\rho_5\sigma_2 &= (A B C D) \\ \rho_5\sigma_3 &= (A B D C) \\ \rho_6\sigma_1 &= (A C B D) \\ \rho_5\sigma_4 &= (A C D B) \\ \rho_6\sigma_6 &= (A D B C) \\ \rho_5\sigma_5 &= (A D C B)\end{aligned}$$

■

**Example 8:** Refer to Example 8 and to Theorem 2 in *Dihedral Groups*.

**Exercise:** Apply Theorem 2 to show that:

$$\begin{array}{lll}\epsilon(x, y, z) = (x, y, z), & \rho_1(x, y, z) = (z, x, y), & \rho_1^2(x, y, z) = (y, z, x) \\ \rho_2(x, y, z) = (-y, z, -x), & \rho_2^2(x, y, z) = (-z, -x, y), & \rho_3(x, y, z) = (z, -x, -y) \\ \rho_3^2(x, y, z) = (-y, -z, x), & \rho_4(x, y, z) = (y, -z, -x), & \rho_4^2(x, y, z) = (-z, x, -y) \\ \rho_5(x, y, z) = (x, -y, -z), & \rho_6(x, y, z) = (-x, y, -z), & \rho_7(x, y, z) = (-x, -y, z) \\ \sigma_1(x, y, z) = (x, -z, -y), & \sigma_2(x, y, z) = (-z, y, -x) & \sigma_3(x, y, z) = (-y, -x, z) \\ \sigma_4(x, y, z) = (y, x, z), & \sigma_5(x, y, z) = (z, y, x) & \sigma_6(x, y, z) = (x, z, y) \\ (\rho_5\sigma_2)(x, y, z) = (z, -y, -x), & (\rho_5\sigma_3)(x, y, z) = (y, -x, -z), & (\rho_6\sigma_1)(x, y, z) = (-x, z, -y) \\ (\rho_5\sigma_4)(x, y, z) = (-y, x, -z), & (\rho_6\sigma_6)(x, y, z) = (-x, -z, y), & (\rho_5\sigma_5)(x, y, z) = (-z, -y, x)\end{array}$$

■

Next, we turn to the cube  $\mathcal{C}$ . Let's place  $\mathcal{C}$  in  $\mathbb{R}^3$  so that its vertices are:

$$\begin{array}{llll}A = (1, 1, 1), & B = (-1, 1, 1), & C = (-1, -1, 1), & D = (1, -1, 1) \\ E = (1, 1, -1), & F = (-1, 1, -1), & G = (-1, -1, -1), & H = (1, -1, -1)\end{array}$$

Any symmetry of  $\mathcal{C}$  must fix  $Z = (0, 0, 0)$  and permute the vertices; hence, the group of symmetries of  $\mathcal{C}$  is a subgroup of  $S(\{A, B, \dots, H\}) \cong S_8$ . To begin, let's obtain an upper bound on the number of symmetries of  $\mathcal{C}$ .

In general, let  $X'$  denote the image of the vertex of  $X$  under an arbitrary symmetry of  $\mathcal{C}$ . Assume that  $A'$  can be any element of  $\{A, B, \dots, H\}$ . Thus, there are 8 possibilities for  $A'$ . Given  $A'$ , there are 3 choices for  $B'$ , since  $\overline{A'B'}$  must be an edge of  $\mathcal{C}$ . Then, given  $A'$  and  $B'$ , there are 2 choices for  $D'$ , since  $\overline{A'D'}$  must be an edge of the cube, and  $D' \neq B'$ . The choices for  $A'$ ,  $B'$ , and  $D'$  completely determine the symmetry, since  $ZABD$  is a (non-regular) tetrahedron. Therefore,  $\mathcal{C}$  has at most  $8(3)(2) = 48$  symmetries.

**Example 9:** Show that  $\mathcal{C}$  has exactly 24 rotational symmetries.

**Solution:** Consider any face of  $\mathcal{C}$  and its opposite face. The line through the centers of these faces is an axis of 4-fold rotational symmetry. This observation yields the following rotational symmetries of  $\mathcal{C}$ :

$$\begin{aligned}\rho_1 &= \text{rotation, } 90^\circ, z\text{-axis; } \rho_1 = (A B C D)(E F G H) \\ \rho_1^2 &= \text{rotation, } 180^\circ, z\text{-axis; } \rho_1^2 = (A C)(B D)(E G)(F H) \\ \rho_1^3 &= \text{rotation, } 270^\circ, z\text{-axis; } \rho_1^3 = (A D C B)(E H G F) \\ \rho_2 &= \text{rotation, } 90^\circ, y\text{-axis; } \rho_2 = (A B F E)(C G H D) \\ \rho_2^2 &= \text{rotation, } 180^\circ, y\text{-axis; } \rho_2^2 = (A F)(B E)(C H)(D G) \\ \rho_2^3 &= \text{rotation, } 270^\circ, y\text{-axis; } \rho_2^3 = (A E F B)(C D H G) \\ \rho_3 &= \text{rotation, } 90^\circ, x\text{-axis; } \rho_3 = (A D H E)(B C G F) \\ \rho_3^2 &= \text{rotation, } 180^\circ, x\text{-axis; } \rho_3^2 = (A H)(B G)(C F)(D E) \\ \rho_3^3 &= \text{rotation, } 270^\circ, x\text{-axis; } \rho_3^3 = (A E H D)(B F G C)\end{aligned}$$

Next, the line through any two opposite vertices of  $\mathcal{C}$  is an axis of 3-fold rotational symmetry. This observation yields the following rotational symmetries of  $\mathcal{C}$ :

$$\begin{aligned}\rho_4 &= \text{rotation, } 120^\circ, \overleftrightarrow{AG}; \rho_4 = (B D E)(C H F) \\ \rho_4^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{AG}; \rho_4^2 = (B E D)(C F H) \\ \rho_5 &= \text{rotation, } 120^\circ, \overleftrightarrow{BH}; \rho_5 = (A C F)(D G E) \\ \rho_5^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{BH}; \rho_5^2 = (A F C)(D E G) \\ \rho_6 &= \text{rotation, } 120^\circ, \overleftrightarrow{CE}; \rho_6 = (A F H)(B G D) \\ \rho_6^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{CE}; \rho_6^2 = (A H F)(B D G) \\ \rho_7 &= \text{rotation, } 120^\circ, \overleftrightarrow{DF}; \rho_7 = (A C H)(B G E) \\ \rho_7^2 &= \text{rotation, } 240^\circ, \overleftrightarrow{DF}; \rho_7^2 = (A H C)(B E G)\end{aligned}$$

Lastly, consider any edge of  $\mathcal{C}$ . The line through  $Z$  and the midpoint of this edge (which contains the midpoint of the opposite edge of  $\mathcal{C}$ ) is an axis of 2-fold rotational symmetry. This observation yields the following rotational symmetries of  $\mathcal{C}$ :

$$\begin{aligned}\rho_8 &= \text{rotation, } 180^\circ, x = 0 \text{ and } z = y; \rho_8 = (A B)(C E)(D F)(G H) \\ \rho_9 &= \text{rotation, } 180^\circ, z = x \text{ and } y = 0; \rho_9 = (A D)(B H)(C E)(F G) \\ \rho_{10} &= \text{rotation, } 180^\circ, y = x \text{ and } z = 0; \rho_{10} = (A E)(B H)(C G)(D F) \\ \rho_{11} &= \text{rotation, } 180^\circ, z = -x \text{ and } y = 0; \rho_{11} = (A G)(B C)(D F)(E H) \\ \rho_{12} &= \text{rotation, } 180^\circ, y = -x \text{ and } z = 0; \rho_{12} = (A G)(B F)(C E)(D H) \\ \rho_{13} &= \text{rotation, } 180^\circ, x = 0 \text{ and } z = -y; \rho_{13} = (A G)(B H)(C D)(E F)\end{aligned}$$

■

It can be shown that the set  $\mathcal{H}$  of rotational symmetries of a cube is a subgroup of the group  $\mathcal{G}$  of all the symmetries, and that this subgroup is isomorphic to  $S_4$ . For the particular cube  $\mathcal{C}$  described above, it can be shown that  $\mathcal{H}$  is generated by  $\rho_1$  and  $\rho_4$ , and that the isomorphism with  $S_4$  is provided by the function that maps  $\rho_1$  to  $(1\ 2\ 3\ 4)$  and  $\rho_4$  to  $(2\ 4\ 3)$  — see Exercise 10.

In Example 7, we showed that the group of rotational symmetries of a regular tetrahedron is isomorphic to  $A_4$ . Also, as noted, the group of rotational symmetries of a cube is isomorphic to  $S_4$ . In general, we have the following result.

**Theorem 8 (Auguste Bravais, 1849):** For any polyhedron  $\mathcal{P}$  in  $\mathbb{R}^3$ , the rotational symmetries of  $\mathcal{P}$  form a group (under composition), and this group is cyclic, dihedral, or is isomorphic to one of  $A_4$ ,  $S_4$ , or  $A_5$ . ■

Back to the symmetries of the cube  $\mathcal{C}$ . So far, we have found 24 rotational symmetries of  $\mathcal{C}$ . There are at most 48 symmetries total, and  $\mathcal{C}$  clearly has some non-rotational symmetries. It follows that there are exactly 48 symmetries of  $\mathcal{C}$ . Furthermore, since the rotational symmetries make up exactly half the total number, the subgroup  $\mathcal{H}$  of rotational symmetries is a normal subgroup of the group  $\mathcal{G}$  of all symmetries. Letting  $\sigma$  be any non-rotational symmetry of  $\mathcal{C}$ , the non-rotational symmetries of  $\mathcal{C}$  are the elements in the coset  $\sigma\mathcal{H}$ .

**Example 10:** With the vertices of  $\mathcal{C}$  defined as above, we can now complete our list of the symmetries of  $\mathcal{C}$ , as follows:

$$\begin{aligned} \sigma &= (AE)(BF)(CG)(DH) = \text{reflection, } z = 0 \\ \sigma\rho_1 &= (AFCH)(BGDE); (\sigma\rho_1)(x, y, z) = (-y, x, -z) \\ \sigma\rho_1^2 &= (AG)(BH)(CE)(DF); (\sigma\rho_1^2)(x, y, z) = (-x, -y, -z) \\ \sigma\rho_1^3 &= (AHC F)(BEDG); (\sigma\rho_1^3)(x, y, z) = (y, -x, -z) \\ \sigma\rho_2 &= (BE)(CH) = \text{reflection, } z = x \\ \sigma\rho_2^2 &= (AB)(CD)(EF)(GH) = \text{reflection, } x = 0 \\ \sigma\rho_2^3 &= (AF)(DG) = \text{reflection, } z = -x \\ \sigma\rho_3 &= (CF)(DE) = \text{reflection, } z = y \\ \sigma\rho_3^2 &= (AD)(BC)(EH)(FG) = \text{reflection, } y = 0 \\ \sigma\rho_3^3 &= (AH)(BG) = \text{reflection, } z = -y \end{aligned}$$

**Exercise:** Determine each of the symmetries,  $\sigma\rho_4$ ,  $\sigma\rho_4^2$ ,  $\sigma\rho_5$ ,  $\sigma\rho_5^2$ ,  $\sigma\rho_6$ ,  $\sigma\rho_6^2$ ,  $\sigma\rho_7$ , and  $\sigma\rho_7^2$  (both analytically and as a permutation of  $\{A, B, C, D, E, F, G, H\}$ ). Note that each of these symmetries has order 6, with

$$\sigma\rho_4^2 = (\sigma\rho_6)^{-1}, \quad \sigma\rho_6^2 = (\sigma\rho_4)^{-1}, \quad \sigma\rho_7 = (\sigma\rho_5)^{-1}, \quad \sigma\rho_7^2 = (\sigma\rho_5^2)^{-1}$$

**Exercise:** Determine each of the symmetries,  $\sigma\rho_8, \sigma\rho_9, \sigma\rho_{10}, \sigma\rho_{11}, \sigma\rho_{12}$ , and  $\sigma\rho_{13}$  (both analytically and as a permutation of  $\{A, B, C, D, E, F, G, H\}$ ). In particular, show that

$$\sigma\rho_{10} = \text{reflection, } y = x, \quad \sigma\rho_{12} = \text{reflection, } y = -x \quad \sigma\rho_{11} = (\sigma\rho_9)^{-1}, \quad \sigma\rho_{13} = (\sigma\rho_8)^{-1}$$



The icosahedron and the dodecahedron are dual polyhedra, so, as mentioned earlier, they have the same group of symmetries. It can be shown that an icosahedron has 60 rotational symmetries and 60 non-rotational symmetries, for a total of 120. As with the tetrahedron and the cube, the rotational symmetries form a normal subgroup of the group of all symmetries, and this subgroup is isomorphic to  $A_5$ . Details are left to the additional exercises.

A theme of this chapter is that many groups are permutation groups. Again, a permutation group is any group that is isomorphic to a subgroup of  $(\mathcal{S}(X), \circ)$  for some nonempty set  $X$ . For example, the dihedral group  $D_n$  of order  $2n$ , which is the abstract group of order  $2n$  having the presentation

$$\langle r, s \mid |r| = n, |s| = 2, s \notin \langle r \rangle, sr = r^{n-1}s \rangle$$

is seen to be isomorphic to the subgroup of  $S_n$  generated by

$$\alpha = (1\ 2\ \cdots\ n) \quad \text{and} \quad \beta = \begin{cases} (2\ n)\cdots(n/2\ (n+4)/2), & \text{if } n \text{ is even} \\ (2\ n)\cdots((n+1)/2\ (n+3)/2), & \text{if } n \text{ is odd} \end{cases}$$

In fact, every group is a permutation group! This fact was first proved by Arthur Cayley in 1854.

**Theorem 9 (Cayley):** Every group is a permutation group. In fact, given a group  $G$ ,  $G$  is isomorphic to a subgroup of  $(\mathcal{S}(G), \circ)$ .

**Proof:** Given an arbitrary group  $(G, *)$ , we want to show that it is isomorphic to some subgroup of the group of permutations of  $G$  under the operation of composition. To that end, we ask: Given an element  $g$  in  $G$ , is there a permutation of  $G$  that can be naturally associated with  $g$ ? In fact, there is! In Theorem 2.1, we show that the function  $f_g$ , defined on  $G$  by

$$f_g(x) = g * x$$

is a permutation of  $G$ . (Note that, if  $G$  is finite, then  $f_g$  is simply the permutation of  $G$  given by the row corresponding to  $g$  in the operation table for  $(G, *)$ .)

Thus, we define  $\theta : G \rightarrow \mathcal{S}(G)$  by

$$\theta(g) = f_g$$

We claim that  $G \cong \text{im}(G)$ , which is a subgroup of  $S(G)$  by Chapter 5, Notebook Exercise 16. To verify this, it suffices to show that  $\theta$  is a homomorphism and that  $\theta$  is one-to-one.

Clearly,  $\theta$  is one-to-one. In fact, if  $g_1$  and  $g_2$  are arbitrary elements of  $G$  with  $g_1 \neq g_2$ , and  $e$  is the identity of  $G$ , then  $f_{g_1}(e) = g_1 * e = g_1 \neq g_2 = g_2 * e = f_{g_2}(e)$ .

To verify that  $\theta$  is a homomorphism, let  $g_1, g_2 \in G$ . Then, for any  $x \in G$ ,

$$\begin{aligned} \theta(g_1 * g_2)(x) &= f_{g_1 * g_2}(x) \\ &= (g_1 * g_2) * x \\ &= g_1 * (g_2 * x) \\ &= f_{g_1}(g_2 * x) \\ &= f_{g_1}(f_{g_2}(x)) \\ &= (f_{g_1} \circ f_{g_2})(x) \\ &= (\theta(g_1) \circ \theta(g_2))(x) \end{aligned}$$

It follows that, for arbitrary elements  $g_1, g_2 \in G$ , that

$$\theta(g_1 * g_2) = \theta(g_1) \circ \theta(g_2)$$

Therefore,  $\theta$  is a homomorphism, as we wanted to show. ■

An interesting general problem is the following: Given a finite group  $G$  of order  $n$ , find the minimum positive integer  $n'$  such that  $G$  is isomorphic to a subgroup of  $S_{n'}$ . Cayley's Theorem asserts that  $n' \leq n$ .

For example,  $D_4$  has order 8, and so Cayley's Theorem asserts that  $D_4$  is isomorphic to a subgroup of  $S_8$ . In fact, we know that we can do better than this — since  $D_4$  is isomorphic to the group of symmetries of a square,  $D_4$  is isomorphic to a subgroup of  $S_4$ .

### Additional Exercises

1. Considering  $A_4$  as a subgroup of  $S_4$ , let  $\alpha = (1\ 2\ 3)$  and  $\beta = (1\ 2)(3\ 4)$ . Construct the Cayley digraph for  $A_4$  using the generating set  $\{\alpha, \beta\}$ . Compare with Figure 5.2.
2. Consider a permutation  $\alpha$  of  $S_n$  that is not the identity permutation. Then, for some  $x \in \{1, 2, \dots, n\}$ ,  $\alpha(x) \neq x$ . Consider the sequence

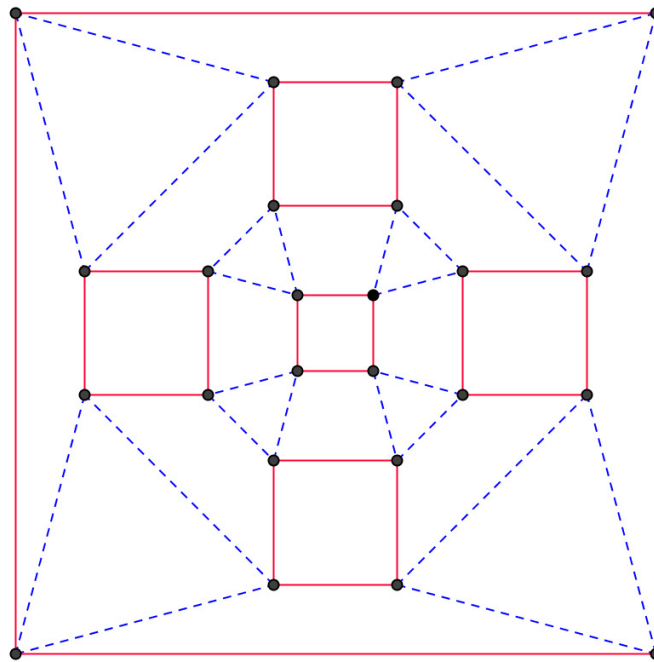
$$x = \alpha^0(x), \alpha(x) = \alpha^1(x), \alpha(\alpha(x)) = \alpha^2(x), \alpha(\alpha(\alpha(x))) = \alpha^3(x), \dots$$

Since each member of this sequence is an element of  $\{1, 2, \dots, n\}$ , the sequence contains repeated members. Show that, in fact, the first element to repeat is  $x$ .

3. In  $S_4$ , let  $\alpha = (1\ 2\ 3\ 4)$ ,  $\beta = (2\ 3\ 4)$ ,  $\delta_2 = (1\ 2)$ ,  $\delta_3 = (1\ 3)$ , and  $\delta_4 = (1\ 4)$ . Construct the Cayley digraph for  $S_4$  using generating set:

- (a)  $\{\alpha, \beta\}$
- (b)  $\{\alpha, \delta_2\}$
- (c)  $\{\delta_2, \delta_3, \delta_4\}$

Figure 1 provides a hint for part (a).



**Figure 1** Hint for Exercise 3, part (a)

4. Prove Theorem 7.3.

5. Complete the following table for  $S_7$ :

order	no. of elements
1	1
2	
3	
4	
5	
6	
7	
10	
12	
total	$5040 = 7!$

6. Let  $n$  be an integer,  $n \geq 3$ , and let  $\alpha, \beta \in S_n$ . If  $\alpha$  and  $\beta$  are both even, then  $\alpha\beta$  and  $\alpha^{-1}$  are even; this was shown in the proof of Theorem 7.6. Show that:

- (a) If  $\alpha$  and  $\beta$  have opposite parity, then  $\alpha\beta$  is odd.
- (b) If  $\alpha$  and  $\beta$  are both odd, then  $\alpha\beta$  is even.
- (c) If  $\alpha$  is odd, then  $\alpha^{-1}$  is odd.

7. Consider the group  $A_6$ .

- (a) Show that  $A_6$  contains no elements of order 6.
- (b) Complete the following table for  $A_6$ :

order	no. of elements
1	1
2	
3	
4	
5	
total	$360 = 6!/2$

8. Show that the group of rotational symmetries of a cube is isomorphic to  $S_4$ . Hint: Refer to Example 9; show that the group  $H$  of rotational symmetries of  $\mathcal{C}$  is generated by  $\rho_1$  and  $\rho_4$ , and define  $\phi : H \rightarrow S_4$  by  $\phi(\rho_1) = (1\ 2\ 3\ 4)$  and  $\phi(\rho_4) = (2\ 4\ 3)$ .

9. Consider the group  $A_7$ .

- (a) Show that  $A_7$  contains no elements of order 10.
- (b) Show that  $A_7$  contains no elements of order 12.

(c) Complete the following table for  $A_7$ :

order	no. of elements
1	1
2	
3	
4	
5	
6	
7	
total	$2520 = 7!/2$

10. Consider the cube  $\mathcal{C}$  as in Examples 9 and 10. Number the faces  $ABCD$ ,  $ADEH$ ,  $CDGH$ ,  $ABEF$ ,  $BCFG$ , and  $EFGH$  of the cube 1, 2, 3, 4, 5, and 6, respectively (like a die).

(a) Provide a face-based argument that the cube has at most 48 symmetries of  $\mathcal{C}$ . Hint: Let  $F'$  denote the image of face  $F$  under an arbitrary symmetry. Then there are 6 choices for  $1'$ . Given  $1'$ , how many choices are there for  $2'$ ? Given  $1'$  and  $2'$ , how many choices are there for  $4'$ ?

(b) Express each of the 48 symmetries of  $\mathcal{C}$  as a permutation of the faces. This describes the group of symmetries of  $\mathcal{C}$  as a subgroup of  $S_6$ , rather than as a subgroup of the group of permutations of the 8 vertices of  $\mathcal{C}$ .

11. Consider the following elements of  $S_8$ , expressed in array notation:

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

Express each of the following in cycle notation (that is, as a product of disjoint cycles):

- (a)  $\alpha$
- (b)  $\beta$
- (c)  $\alpha\beta$
- (d)  $\beta\alpha$
- (e)  $\alpha^2$
- (f)  $\beta^2$
- (g)  $\alpha^{-1}$
- (h)  $\beta^{-1}$

12. Consider the group  $\mathcal{G}$  of symmetries of a cube  $\mathcal{C}$  and the subgroup  $\mathcal{H}$  of rotational symmetries of  $\mathcal{C}$ , as described in Examples 9 and 10.

(a) Show that  $\mathcal{H} = \langle \rho_1, \rho_{10} \rangle$ .

(b) Show that

$$\sigma\rho_1 = \rho_1\sigma \quad \text{and} \quad \sigma\rho_{10} = \rho_{10}\sigma$$

(c) Show that  $\mathcal{G} \cong S_4 \times \mathbb{Z}_2$ .

13. For the permutations  $\alpha$  and  $\beta$  given in Exercise 11, find:

(a)  $|\alpha|$  (b)  $|\beta|$

14. Note that  $C_1 \cong S_1$  and  $C_2 \cong S_2$ . Given a positive integer  $n \geq 3$ , determine the minimum  $m$  such that  $C_n$  is isomorphic to a subgroup of  $S_m$ . Hint: Consider the canonical factorization of  $n$  — hey, it ain't called the “fundamental theorem of arithmetic” for nothin'!

15. For each of the following groups of order 8, find the minimum  $n'$  such that the group is isomorphic to a subgroup of  $S_{n'}$ . (Refer to *Groups of Order 8*.)

(a)  $\mathbb{Z}_8$  (b)  $\mathbb{Z}_4 \times \mathbb{Z}_2$   
 (c)  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  (d)  $Q$  (the quaternion group)

16. The purpose of this exercise is to describe the group  $\mathcal{G}$  of symmetries of an icosahedron  $\mathcal{I}$ .

Let  $A$  denote one vertex of  $\mathcal{I}$ . Then  $A$  is adjacent to five other vertices, and these five vertices form a regular pentagon.

(a) Use this observation to argue that  $\mathcal{I}$  has at most 120 symmetries.

Let  $Z$  denote the center of  $\mathcal{I}$ . The line  $\overleftrightarrow{ZA}$  is an axis of 5-fold rotational symmetry of  $\mathcal{I}$ .

(b) Considering all such axes — that is, any axis of the form  $\overleftrightarrow{ZX}$ , with  $X$  a vertex of  $\mathcal{I}$  — how many (nonidentity) rotational symmetries of  $\mathcal{I}$  are accounted for?

Let  $P$  denote the center of one face of  $\mathcal{I}$ . The line  $\overleftrightarrow{ZP}$  is an axis of 3-fold rotational symmetry of  $\mathcal{I}$ .

(c) Considering all such axes — that is, any axis of the form  $\overleftrightarrow{ZX}$ , with  $X$  the center of some face of  $\mathcal{I}$  — how many rotational symmetries of  $\mathcal{I}$  are accounted for?

Let  $M$  denote the midpoint of some edge of  $\mathcal{I}$ . The line  $\overleftrightarrow{ZM}$  is an axis of 2-fold rotational symmetry of  $\mathcal{I}$ .

(d) Considering all such axes — that is, any axis of the form  $\overleftrightarrow{ZX}$ , with  $X$  the midpoint of some edge of  $\mathcal{I}$  — how many rotational symmetries of  $\mathcal{I}$  are accounted for?

Parts (b), (c), and (d) account for all 60 rotational symmetries of  $\mathcal{I}$ . Let  $\mathcal{H}$  denote the subgroup of rotational symmetries.

(e) Show that  $\mathcal{H}$  has the same “order profile” as the group  $A_5$ . In fact,  $\mathcal{H} \cong A_5$ .

Let  $\sigma$  be any non-rotational symmetry of  $\mathcal{I}$ . Then  $\mathcal{G} = \mathcal{H} \cup \sigma\mathcal{H}$ , so that  $|\mathcal{G}| = 120$ , and  $\mathcal{H} \triangleleft \mathcal{G}$ . The group  $\mathcal{G}$  is known as the *Coxeter group*  $G_3$ .

17. For each of the following groups of order 12, determine the minimum  $n'$  such that the group is isomorphic to a subgroup of  $S_{n'}$ . (Refer to *Groups of Order 12*.)

(a)  $\mathbb{Z}_6 \times \mathbb{Z}_2$  (b)  $T$

18. Give an example of  $\alpha, \beta \in \mathcal{S}(\mathbb{Z})$  such that both  $\alpha$  and  $\beta$  have order 2, but  $\alpha\beta$  has infinite order. This example shows that, if an infinite group, the subset of elements with finite order is not necessarily closed.

19. Let  $n$  be an integer,  $n \geq 3$ . Show that the center  $\mathcal{C}$  of  $S_n$  contains only the identity permutation  $\epsilon$ .

20. Let  $X$  be a nonempty set and let  $Y$  be a nonempty subset of  $X$ . Define the subset  $F_Y$  of  $\mathcal{S}(X)$  by

$$F_Y = \{\alpha \in \mathcal{S}(X) \mid \alpha(y) = y \text{ for every } y \in Y\}$$

that is,  $F_Y$  consists of those permutations of  $X$  that fix every element of  $Y$ .

(a) Show that  $F_Y$  is a subgroup of  $\mathcal{S}(X)$ .

(b) Prove or disprove:  $F_Y$  is a normal subgroup of  $\mathcal{S}(X)$ .

(c) In the case when  $X = \{1, 2, \dots, n\}$  and  $|Y| = m$ ,  $1 \leq m < n$ ,  $F_Y$  is isomorphic to a well-known group. What group?

21. Let  $H$  be a subgroup of  $S_n$ . Show that either  $H$  is a subgroup of  $A_n$  or  $|A_n \cap H| = 2$  (that is, exactly half of the elements of  $H$  are even).

22. Let  $a, b, c$ , and  $d$  be real numbers such that  $ad - bc \neq 0$ . Define the function  $f : \mathbb{R} \rightarrow \mathbb{R}$  as follows:

$$f(x) = \begin{cases} \frac{ax + b}{d}, & \text{if } c = 0 \\ \begin{cases} \frac{a}{c}, & cx = -d \\ \frac{ax + b}{cx + d}, & cx \neq -d \end{cases}, & \text{if } c \neq 0 \end{cases}$$

(a) Show that  $f$  is a permutation of  $\mathbb{R}$ .

(b) Show that the set  $\mathcal{H}$  of all such functions is a subgroup of  $\mathcal{S}(\mathbb{R})$ .

23. In the group  $S_7$ , determine all possibilities for the permutation  $\alpha$  given the information that:

(a)  $\alpha^3 = (1\ 2\ 3\ 4\ 5)$

(b)  $\alpha^2 = (1\ 2\ 3)(4\ 5\ 6)$

(c)  $\alpha^3 = (1\ 2)(3\ 4\ 5\ 6)$

(d)  $\alpha^5 = (1\ 2)$

(e)  $\alpha^4 = (1\ 2\ 3\ 4\ 5\ 6\ 7)$

(f)  $\alpha^6 = (4\ 5)(6\ 7)$

24. Every element of  $S_n$  can be expressed as a product of 2-cycles. Prove or disprove: Every element of  $S_n$  can be expressed as a product of 3-cycles.

25. Let  $k$  and  $n$  be integers with  $1 < k \leq n$ , and let  $\alpha \in S_n$  be a  $k$ -cycle. For which integers  $t$ ,  $2 \leq t \leq n$ , is  $\alpha^t$  a  $k$ -cycle?

26. For  $n \geq 3$ , show that every element of  $A_n$  can be expressed as a product of 3-cycles.

27. Let  $\alpha \in S_n$ . Prove: If  $|\alpha|$  is odd, then  $\alpha \in A_n$ .

