power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]
5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]
6. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).
7. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]
8. Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 27 of Section 1).

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

9. Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.
10. Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.
11. Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.
12. Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.
13. Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.
14. Find a set of generators for $\mathbb{Z}$.
15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.
16. Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1 \rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). [Show that the last relation is the same as: $x_1y_1 = y_1x_1^{-1}$.]
17. Let X_{2n} be the group whose presentation is displayed in (1.2).
    (a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.
    (b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [Use the facts that $x^n = 1$ and $x^3 = 1$.]
18. Let Y be the group whose presentation is displayed in (1.3).
    (a) Show that $v^2 = v^{-1}$. [Use the relation: $v^3 = 1$.]
    (b) Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use part (a).]
    (c) Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]
    (d) Show that $uv = 1$. [Use part (c) and the last relation.]
    (e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $u^4v^3 = 1$.]

1.3 SYMMETRIC GROUPS

Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself (i.e., the set of all permutations of Ω). The set S_Ω is a group under function composition: $\circ$. Note that $\circ$ is a binary operation on S_Ω since if $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$ are both bijections, then $\sigma \circ \tau$ is also a bijection from Ω to Ω. Since function composition is associative in general, $\circ$ is associative. The identity of S_Ω is the permutation 1 defined by $1(a) = a$, for all $a \in \Omega$. For every permutation σ there is a (2-sided) inverse function, $\sigma^{-1} : \Omega \to \Omega$ satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Thus, all the group axioms hold for $(S_\Omega, \circ)$. This group is called the *symmetric group on the set* Ω. It is important to recognize that the elements of S_Ω are the *permutations* of Ω, not the elements of Ω itself.

In the special case when $\Omega = \{1, 2, 3, \dots, n\}$, the symmetric group on Ω is denoted S_n, the *symmetric group of degree* n.[1] The group S_n will play an important role throughout the text both as a group of considerable interest in its own right and as a means of illustrating and motivating the general theory.

First we show that the order of S_n is $n!$. The permutations of $\{1, 2, 3, \dots, n\}$ are precisely the injective functions of this set to itself because it is finite (Proposition 0.1) and we can count the number of injective functions. An injective function σ can send the number 1 to any of the n elements of $\{1, 2, 3, \dots, n\}$; $\sigma(2)$ can then be any one of the elements of this set except $\sigma(1)$ (so there are $n - 1$ choices for $\sigma(2)$); $\sigma(3)$ can be any element except $\sigma(1)$ or $\sigma(2)$ (so there are $n - 2$ choices for $\sigma(3)$), and so on. Thus there are precisely $n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1 = n!$ possible injective functions from $\{1, 2, 3, \dots, n\}$ to itself. Hence there are precisely $n!$ permutations of $\{1, 2, 3, \dots, n\}$ so there are precisely $n!$ elements in S_n.

We now describe an efficient notation for writing elements σ of S_n which we shall use throughout the text and which is called the *cycle decomposition*.

A *cycle* is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The cycle $(a_1\ a_2\ \dots\ a_m)$ is the permutation which sends a_i to a_{i+1}, $1 \le i \le m-1$ and sends a_m to a_1. For example $(2\,1\,3)$ is the permutation which maps 2 to 1, 1 to 3 and 3 to 2. In general, for each $\sigma \in S_n$ the numbers from 1 to n will be rearranged and grouped into k cycles of the form

$$(a_1\ a_2 \dots a_{m_1})(a_{m_1+1}\ a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1}\ a_{m_{k-1}+2} \dots a_{m_k})$$

from which the action of σ on any number from 1 to n can easily be read, as follows. For any $x \in \{1, 2, 3, \dots, n\}$ first locate x in the above expression. If x is not followed immediately by a right parenthesis (i.e., x is not at the right end of one of the k cycles), then $\sigma(x)$ is the integer appearing immediately to the right of x. If x is followed by a right parenthesis, then $\sigma(x)$ is the number which is at the start of the cycle ending with x (i.e., if $x = a_{m_i}$, for some i, then $\sigma(x) = a_{m_{i-1}+1}$ (where m_0 is taken to be 0)). We can represent this description of σ by

[1] We shall see in Section 6 that the structure of S_Ω depends only on the cardinality of Ω, not on the particular elements of Ω itself, so if Ω is any finite set with n elements, then S_Ω "looks like" S_n.

$$a_1 \to a_2 \to \cdots \to a_{m_1}$$

$$a_{m_1+1} \to a_{m_1+2} \to \cdots \to a_{m_2}$$

$$\vdots$$

$$a_{m_{k-1}+1} \to a_{m_{k-1}+2} \to \cdots \to a_{m_k}$$

The product of all the cycles is called the *cycle decomposition* of σ.

We now give an algorithm for computing the cycle decomposition of an element σ of S_n and work through the algorithm with a specific permutation. We defer the proof of this algorithm and full analysis of the uniqueness aspects of the cycle decomposition until Chapter 4.

Let $n = 13$ and let $\sigma \in S_{13}$ be defined by

$$\begin{array}{lllll} \sigma(1) = 12, & \sigma(2) = 13, & \sigma(3) = 3, & \sigma(4) = 1, & \sigma(5) = 11, \\ \sigma(6) = 9, & \sigma(7) = 5, & \sigma(8) = 10, & \sigma(9) = 6, & \sigma(10) = 4, \\ \sigma(11) = 7, & \sigma(12) = 8, & \sigma(13) = 2. & & \end{array}$$

Cycle Decomposition Algorithm

Method	**Example**
To start a new cycle pick the smallest element of $\{1, 2, \ldots, n\}$ which has not yet appeared in a previous cycle — call it a (if you are just starting, $a = 1$); begin the new cycle: $(a$	$(1$
Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: $(a\ b$	$\sigma(1) = 12 = b$, $12 \neq 1$ so write: $(1\ 12$
Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: $(a\ b\ c$ Repeat this step using the number c as the new value for b until the cycle closes.	$\sigma(12) = 8$, $8 \neq 1$ so continue the cycle as: $(1\ 12\ 8$

Naturally this process stops when all the numbers from $\{1, 2, \ldots, n\}$ have appeared in some cycle. For the particular σ in the example this gives

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9).$$

The *length* of a cycle is the number of integers which appear in it. A cycle of length t is called a *t-cycle*. Two cycles are called *disjoint* if they have no numbers in common.

Thus the element σ above is the product of 5 (pairwise) disjoint cycles: a 5-cycle, a 2-cycle, a 1-cycle, a 3-cycle, and another 2-cycle.

Henceforth we adopt the convention that 1-cycles will not be written. Thus if some integer, i, does not appear in the cycle decomposition of a permutation τ it is understood that $\tau(i) = i$, i.e., that τ fixes i. The identity permutation of S_n has cycle decomposition $(1)(2)\dots(n)$ and will be written simply as 1. Hence the final step of the algorithm is:

Cycle Decomposition Algorithm (cont.)

Final Step: Remove all cycles of length 1	

The cycle decomposition for the particular σ in the example is therefore

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$$

This convention has the advantage that the cycle decomposition of an element τ of S_n is also the cycle decomposition of the permutation in S_m for $m \geq n$ which acts as τ on $\{1, 2, 3, \dots, n\}$ and fixes each element of $\{n+1, n+2, \dots, m\}$. Thus, for example, $(1\ 2)$ is the permutation which interchanges 1 and 2 and fixes all larger integers whether viewed in S_2, S_3 or S_4, etc.

As another example, the 6 elements of S_3 have the following cycle decompositions:

The group S_3

Values of σ_i	**Cycle Decomposition of σ_i**
$\sigma_1(1) = 1, \sigma_1(2) = 2, \sigma_1(3) = 3$	1
$\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$	$(2\ 3)$
$\sigma_3(1) = 3, \sigma_3(2) = 2, \sigma_3(3) = 1$	$(1\ 3)$
$\sigma_4(1) = 2, \sigma_4(2) = 1, \sigma_4(3) = 3$	$(1\ 2)$
$\sigma_5(1) = 2, \sigma_5(2) = 3, \sigma_5(3) = 1$	$(1\ 2\ 3)$

For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order. For example, if $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ is the element of S_{13} described before then

$$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6).$$

Computing products in S_n is straightforward, keeping in mind that when computing $\sigma \circ \tau$ in S_n one reads the permutations from *right to left*. One simply "follows" the elements under the successive permutations. For example, in the product $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$ the number 1 is sent to 2 by the first permutation, then 2 is sent to 3 by the second permutation, hence the composite maps 1 to 3. To compute the cycle decomposition of the product we need next to see what happens to 3. It is sent first to 4,