then

$$\sigma(\tau(a_1)) = \sigma(\tau(a_2)),$$

and since σ is given to be one-to-one, we know that $\tau(a_1) = \tau(a_2)$. But then, since τ is one-to-one, this gives $a_1 = a_2$. Hence $\sigma\tau$ is one-to-one. To show that $\sigma\tau$ is onto A, let $a \in A$. Since σ is onto A, there exists $a' \in A$ such that $\sigma(a') = a$. Since τ is onto A, there exists $a'' \in A$ such that $\tau(a'') = a'$. Thus

$$a = \sigma(a') = \sigma(\tau(a'')) = (\sigma\tau)(a''),$$

so $\sigma\tau$ is onto A.

4.7 Example Suppose that

$$A = \{1, 2, 3, 4, 5\}$$

and that σ is the permutation given by Fig. 4.4. We write σ in a more standard notation, changing the columns to rows in parentheses and omitting the arrows, as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix},$$

so that $\sigma(1) = 4, \sigma(2) = 2$, and so on. Let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

For example, multiplying in right-to-left order,

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5.$$ ▲

HISTORICAL NOTE

One of the earliest recorded studies of permutations occurs in the *Sefer Yetsirah,* or *Book of Creation,* written by an unknown Jewish author sometime before the eighth century. The author was interested in counting the various ways in which the letters of the Hebrew alphabet can be arranged. The question was in some sense a mystical one. It was believed that the letters had magical powers; therefore, suitable arrangements could subjugate the forces of nature. The actual text of the *Sefer Yetsirah* is very sparse: "Two letters build two words, three build six words, four build 24 words, five build 120, six build 720, seven build 5040." Interestingly enough, the idea of counting the arrangements of the letters of the alphabet also occurred in Islamic mathematics in the eighth and ninth centuries. By the thirteenth century, in both the Islamic and Hebrew cultures, the abstract idea of a permutation had taken root so that both Abul-' Abbas ibn al-Banna (1256–1321), a mathematician from Marrakech in what is now Morocco, and Levi ben Gerson, a French rabbi, philosopher, and mathematician, were able to give rigorous proofs that the number of permutations of any set of n elements is $n!$, as well as prove various results about counting combinations.

Levi and his predecessors, however, were concerned with permutations as simply arrangements of a given finite set. It was the search for solutions of polynomial equations that led Lagrange and others in the late eighteenth century to think of permutations as functions from a finite set to itself, the set being that of the roots of a given equation. And it was Augustin-Louis Cauchy (1789–1857) who developed in detail the basic theorems of permutation theory and who introduced the standard notation used in this text.

We now show that the collection of all permutations of a nonempty set A forms a group under this permutation multiplication.

4.8 Theorem Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof We have shown that composition of two permutations of A yields a permutation of A, so S_A is closed under permutation multiplication.

Now permutation multiplication is defined as function composition, and in Section 1, we showed that *function composition is associative*. Hence $\mathscr{G}_1$ is satisfied.

The permutation ι such that $\iota(a) = a$, for all $a \in A$ acts as identity. Therefore $\mathscr{G}_2$ is satisfied.

For a permutation σ, the inverse function, σ^{-1}, is the permutation that reverses the direction of the mapping σ, that is, $\sigma^{-1}(a)$ is the element a' of A such that $a = \sigma(a')$. The existence of exactly one such element a' is a consequence of the fact that, as a function, σ is both one-to-one and onto. For each $a \in A$ we have

$$\iota(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a)) = (\sigma\sigma^{-1})(a)$$

and also

$$\iota(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a'),$$

so that $\sigma^{-1}\sigma$ and $\sigma\sigma^{-1}$ are both the permutation ι. Thus $\mathscr{G}_3$ is satisfied. ◆

Warning: Some texts compute a product $\sigma\mu$ of permutations in left-to-right order, so that $(\sigma\mu)(a) = \mu(\sigma(a))$. Thus the permutation they get for $\sigma\mu$ is the one we would get by computing $\mu\sigma$. Exercise 34 asks us to check in two ways that we still get a group. If you refer to another text on this material, be sure to check its order for permutation multiplication.

There was nothing in our definition of a permutation to require that the set A be finite. However, most of our examples of permutation groups will be concerned with permutations of finite sets. Note that the *structure* of the group S_A is concerned only with the number of elements in the set A, and not what the elements in A are. If sets A and B have the same cardinality, then $S_A \simeq S_B$. To define an isomorphism $\phi : S_A \to S_B$, we let $f : A \to B$ be a one-to-one function mapping A onto B, which establishes that A and B have the same cardinality. For $\sigma \in S_A$, we let $\phi(\sigma)$ be the permutation $\bar{\sigma} \in S_B$ such that $\bar{\sigma}(f(a)) = f(\sigma(a))$ for all $a \in A$. To illustrate this for $A = \{1, 2, 3\}$ and $B = \{\#, \$, \%\}$ and the function $f : A \to B$ defined as

$$f(1) = \#, \quad f(2) = \$, \quad f(3) = \%,$$

ϕ maps

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ into } \begin{pmatrix} \# & \$ & \% \\ \% & \$ & \# \end{pmatrix}.$$

We simply rename the elements of A in our two-row notation by elements in B using the renaming function f, thus renaming elements of S_A to be those of S_B. We can take $\{1, 2, 3, \cdots, \mathrm{n}\}$ to be a prototype for a finite set A of n elements.

4.9 Definition Let A be the finite set $\{1, 2, \cdots, n\}$. The group of all permutations of A is the **symmetric group on n letters**, and is denoted by S_n. ■

Note that S_n has $n!$ elements, where

$$n! = n(n-1)(n-2)\cdots(3)(2)(1).$$

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then

$$\sigma\tau(1) = \sigma(1) = 2$$

and

$$\tau\sigma(1) = 3$$

which says that $\sigma\tau \neq \tau\sigma$. Therefore S_3 is not abelian. We have seen that any group with at most four elements is abelian. Furthermore we will see later that up to isomorphism, the abelian group $\mathbb{Z}_5$ is the only group of order 5. Thus S_3 is the smallest group which is not abelian.

4.10 Example Suppose that $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}$. We find the inverse σ^{-1}. We saw in the proof of Theorem 4.8 that the inverse function of a permutation is the group inverse. So it is easy to find inverses for permutations, we simply turn the tables! That is, we switch the top and bottom rows and sort the columns so the top row is in order:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 6 & 3 \end{pmatrix}. \quad \blacktriangle$$

Disjoint Cycles

There is a more efficient way of specifying the action of a permutation. In the two-row notation that we have been using, we list each number 1 through n twice, once in the top row and once in the bottom row. Disjoint cycle notation allows us to write the permutation using each number only once. We illustrate with an example. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$. To write in disjoint cycle notation we start by writing

$$(1$$

We see that $\sigma(1) = 3$, so we place 3 just to the right of 1:

$$(1, 3$$

Now we see that σ maps 3 to 6, so we write:

$$(1, 3, 6$$

Our permutation maps 6 to 1, but there is no reason to write 1 again, so we just place a parenthesis after the 6 to indicate that 6 maps back to the first element listed:

$$(1, 3, 6)$$

This is called a **cycle** because when we apply σ repeatedly, we cycle through the numbers 1, 3, and 6. A cycle containing exactly k numbers is called a ***k*-cycle**. So the cycle $(1, 3, 6)$ is a 3-cycle. This is not the end of the story for σ because we have not indicated that 2 maps to 4. So we start another cycle and write

$$(1, 3, 6)(2, 4$$

to indicate that σ maps 2 to 4. Since 4 maps back to 2, we obtain a 2-cycle:

$$(1, 3, 6)(2, 4)$$

We still have not indicated what σ does to 5. We can write $(1, 3, 6)(2, 4)(5)$ to indicate that 5 maps to itself, but usually we will simply leave out 1-cycles with the understanding that any number not listed maps to itself. So in disjoint cycle notation

$$\sigma = (1, 3, 6)(2, 4).$$