15. Let $(G, *)$ and $(H, \circ)$ be two distinct groups. Define a binary operation $\cdot$ on the Cartesian product

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

as follows: for

$$(g_1, h_1), (g_2, h_2) \in G \times H,$$

set

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Prove that $(G \times H, \cdot)$ is a group, called the *direct product group* of $(G, *)$ and $(H, \circ)$; show further that this group is commutative whenever the original groups are commutative.

2–3 TWO IMPORTANT GROUPS

This section is devoted to an examination of two important and frequently used groups: the group of integers modulo n and the group of permutations of the elements of a set (the so-called symmetric group). While these groups are of some interest per se, our main purpose in introducing them is to provide two more concrete examples to illustrate concepts which will be developed subsequently.

We begin with an investigation of the notion of congruence, in terms of which the group of integers modulo n will be formulated.

Definition 2–13. Let n be a fixed positive integer. Two integers a and b are said to be *congrent modulo* n, written

$$a \equiv b \pmod{n},$$

if and only if the difference $a - b$ is divisible by n. That is, $a \equiv b \pmod{n}$ if and only if $a - b = kn$ for some integer k.

For instance, if $n = 7$, we have

$$3 \equiv 24 \pmod{7},$$
$$-5 \equiv 2 \pmod{7},$$
$$-8 \equiv -50 \pmod{7}, \quad \text{etc}$$

If $a - b$ is not divisible by n, we say that a is incongruent to b modulo n and, in this case, write $a \not\equiv b \pmod{n}$.

It is noteworthy that every pair of integers are congruent modulo 1, while a pair of integers are congruent modulo 2 provided they are both even or both odd.

Our first theorem provides a useful characterization of congruence modulo n in terms of remainders on division by n.

Theorem 2–9. Let n be a fixed positive integer and a, b be arbitrary integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.

Proof. Suppose first $a \equiv b \pmod{n}$, so that $a = b + kn$ for some integer k. On division by n, b leaves a certain remainder r:

$$b = qn + r, \qquad \text{where} \qquad 0 \leq r < n.$$

Thus, $a = b + kn = (q + k)n + r$, which shows a has the same remainder as b.

On the other hand, let $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n,$$

with $q_1 - q_2$ an integer. Hence, n is a factor of $a - b$ and so $a \equiv b \pmod{n}$.

Congruence may be viewed as a type of equality in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality which also carry over to congruences are listed in the next theorem.

Theorem 2-10. Let n be a fixed positive integer and a, b, c be arbitrary integers. Then

1) $a \equiv a \pmod{n}$,
2) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$,
3) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$,
4) if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$,
   then $a + c \equiv b + d \pmod{n}$, $ac \equiv db \pmod{n}$,
5) if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$,
6) if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for every positive integer k.

Proof. For any integer a, $a - a = 0n$, so that $a \equiv a \pmod{n}$ by Definition 2-13. If $a \equiv b \pmod{n}$, then $a - b = kn$ for some integer k. Hence

$$b - a = (-k)n,$$

where $-k$ is an integer. This yields (2).

To obtain (3), suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then

$$a - b = kn \qquad \text{and} \qquad b - c = hn$$

for some integers k, h. Therefore,

$$a - c = (a - b) + (b - c) = kn + hn = (k + h)n,$$

which implies $a \equiv c \pmod{n}$.

Similarly, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then there exist integers k_1, k_2 such that

$$a - b = k_1 n \qquad \text{and} \qquad c - d = k_2 n.$$

Consequently,

$$(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n$$
$$= (k_1 + k_2)n,$$

or

$$a + c \equiv b + d \pmod{n}.$$

Also,

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Since $bk_2 + dk_1 + k_1 k_2 n$ is an integer, $ac - bd$ is divisible by n, so that

$$ac \equiv bd \pmod{n}.$$

This establishes (4).

Property (5) follows directly from the second part of (4), since $c \equiv c \pmod{n}$.

Finally, we prove (6) by an inductive argument. The statement is certainly true for $k = 1$. Assuming it holds for an arbitrary k, we must show that it also holds for $k + 1$. But this is immediate from (4), since $a^k \equiv b^k \pmod{n}$ and $a \equiv b \pmod{n}$ imply $a^k a \equiv b^k b \pmod{n}$, or $a^{k+1} \equiv b^{k+1} \pmod{n}$.

In the foregoing theorem we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. It is interesting to note that the converse of this statement fails to be true. For instance, $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, yet $4 \not\equiv 1 \pmod{6}$. To put it another way, one cannot unrestrictedly apply the cancellation law in the algebra of congruences. The only positive assertion that can be made in this regard is embodied in the following theorem.

Theorem 2–11. If $ca \equiv cb \pmod{n}$ and c is relatively prime to n, then $a \equiv b \pmod{n}$.

Proof. By hypothesis, $c(a - b) = kn$ for some integer k. Since c is prime to n, it follows that n must divide $a - b$ [Theorem 1–14]; hence, $a \equiv b \pmod{n}$.

Definition 2–14. For an arbitrary integer a, let $[a]$ denote the set of all integers congruent to a modulo n:

$$[a] = \{x \in Z \mid x \equiv a \pmod{n}\}$$
$$= \{x \in Z \mid x = a + kn \text{ for some integer } k\}.$$

We call $[a]$ the *congruence class*, modulo n, determined by a and refer to a as a *representative* of this class.

By way of illustration, suppose that we are dealing with congruence modulo 3. Then

$$[0] \quad \{x \in Z \mid x = 3k \text{ for some } k \in Z\}$$
$$\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

Also

$$\begin{aligned}[1] &= \{x \in Z \mid x = 1 + 3k \text{ for some } k \in Z\} \\ &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.\end{aligned}$$

Similarly,

$$[2] = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Observe that every integer lies in one of these three classes. Integers in the same congruence class are congruent modulo 3, while integers in different classes are incongruent modulo 3.

A particular congruence class may be designated in a variety of ways by merely changing its representative. In the above illustration, for instance,

$$[-7] = [2] = [11] = [35] = \cdots$$

It suffices to remark that the characteristic feature of these various representatives is that, in this case, they all differ from each other by multiples of 3, and in general, differ by multiples of n. For convenience, one often selects the smallest nonnegative integer from each congruence class to represent it; in practice, we shall adhere to this notational convention.

To return to the general case of congruence modulo n, let

$$Z_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Several properties of the collection Z_n which we shall later require appear in the next theorem.

Theorem 2–12. Let n be a positive integer and Z_n be as defined above. Then

1) for each $[a] \in Z_n$, $[a] \neq \emptyset$,
2) if $[a] \in Z_n$ and $b \in [a]$, then $[b] = [a]$; that is, any element of the congruence class $[a]$ determines the class,
3) for any $[a], [b] \in Z_n$ where $[a] \neq [b]$, $[a] \cap [b] = \emptyset$,
4) $\cup\{[a] \mid a \in Z\} = Z$.

Proof. The first three assertions of Theorem 2–10 indicate that the relation $a \equiv b \pmod{n}$ forms an equivalence relation in the set Z of integers. Indeed, the congruence classes as defined in Definition 2–14 are simply the equivalence classes for this equivalence relation. Viewed in this light, the statement of Theorem 2–12 is a translation of Theorem 1–5 into the language of "congruence modulo n."

The set Z_n, whose elements are the congruence classes modulo n, is traditionally known as the set of *integers modulo n*. It may strike the reader that this terminology is somewhat inappropriate for, precisely speaking, the elements of Z_n are not single integers, but rather infinite sets of integers. Moreover, the set Z_n is not infinite, like the integers, but is a finite set with n elements. While

this is not quite in accord with our intuition, we bow to long-standing custom and shall continue to refer to Z_n as the integers modulo n.

By a partition of the set S, we mean a family of nonempty subsets of S which are pairwise disjoint and whose union is all of S. It follows from Theorem 2–12 that, for each $n \in Z_+$, the integers modulo n constitute a partition of the set Z.

Definition 2–15. A binary operation $+_n$ may be defined on Z_n as follows: for each $[a], [b] \in Z_n$, let $[a] +_n [b] = [a + b]$.

Definition 2–15 asserts that the modular sum of two congruence classes $[a]$ and $[b]$ is the unique member of Z_n which contains the ordinary sum $a + b$. However, there is a subtle problem connected with this definition. Inasmuch as addition of congruence classes in Z_n is defined in terms of representatives from these classes, we must show that the operation $+_n$ does not depend on the two representatives chosen. It must be proved formally, that if $[a'] = [a]$ and $[b'] = [b]$, then $[a'] +_n [b'] = [a] +_n [b]$, or rather, $[a' + b'] = [a + b]$. Now $a' \in [a'] = [a]$ and $b' \in [b'] = [b]$, which implies

$$a' \equiv a \pmod{n} \qquad \text{and} \qquad b' \equiv b \pmod{n}.$$

By virtue of Theorem 2–10(4), it follows that

$$a' + b' \equiv a + b \pmod{n}, \qquad \text{or} \qquad a' + b' \in [a + b].$$

Theorem 2–12(2) then indicates that $[a' + b'] = [a + b]$, as desired. Thus the operation $+_n$ is unambiguously defined, independent of the arbitrary choice of representatives.

Example 2–26. Suppose we consider congruence modulo 7 and the typical addition

$$[3] +_7 [6] = [3 + 6] = [9].$$

Since $[3] = [10]$ and $[6] = [-15]$, the same answer should be obtained if one used

$$[10] +_7 [-15] = [10 - 15] = [-5].$$

While these results appear superficially different, both congruence classes $[9]$ and $[-5]$ may be expressed more simply as $[2]$. Thus, although written in terms of different representatives, either modular addition gives the same sum, $[2]$. Other possible choices $[-4] +_7 [-8] = [-12]$, $[17] +_7 [6] = [23]$, $[3] +_7 [13] = [16]$, also yield the sum $[2]$.

We are now in a position to prove one of the principal theorems of this section.

Theorem 2–13. For each positive integer n, the mathematical system $(Z_n, +_n)$ forms a commutative group, known as the *group of integers modulo n*.

Proof. The associativity and commutativity of the operation $+_n$ are a direct consequence of the same properties of the integers under ordinary addition.

Indeed, if $[a], [b], [c] \in Z_n$, then

$$\begin{aligned}[a] +_n ([b] +_n [c]) &= [a] +_n [b + c] \\ &= [a + (b + c)] \\ &= [(a + b) + c] \\ &= [a + b] +_n [c] \\ &= ([a] +_n [b]) +_n [c].\end{aligned}$$

Similarly,

$$[a] +_n [b] = [a + b] = [b + a] = [b] +_n [a].$$

By definition of $+_n$, it is clear that $[0]$ is the identity element. Finally, if $[a] \in Z_n$, then $[n - a] \in Z_n$ and

$$[a] +_n [n - a] = [a + (n - a)] = [n] = [0],$$

so that $[a]^{-1} = [n - a]$. This completes the proof that $(Z_n, +_n)$ is a commutative group.

Incidentally, Theorem 2–13 also shows that for every positive integer n there exists at least one commutative group with n elements.

If we adopt the convention of designating each congruence class by its smallest nonnegative representative, then the operation table for, say $(Z_4, +_4)$, looks like

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

For simplicity, it is convenient to remove the brackets in the designation of the congruence classes of Z_n. Thus we often write $Z_n = \{0, 1, 2, \ldots, n - 1\}$. With this notation, the above operation table assumes the form

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

For the second of our two examples, let us turn to the study of permutation groups. To this end, suppose that N is a finite set having n elements which, for simplicity, we take to be the first n natural numbers; that is to say,

$$N = \{1, 2, \ldots, n\}.$$

Definition 2–16. By a *permutation* of the set N is meant any one-to-one mapping of N onto itself.

In what follows, the totality of all permutations of the set N will be denoted by the symbol S_n. Since the number of different permutations of n objects is $n!$, the first thing to note is that S_n is itself a finite set with $n!$ distinct elements. Next, any permutation $f \in S_n$ may be described by

$$f = \{(1, f(1)), (2, f(2)), \ldots, (n, f(n))\}.$$

While this is the acceptable functional notation, it will prove to be more convenient to represent f in a *two-line form*

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix},$$

where the corresponding images appear below each integer. Clearly, the order of the elements in the top row of this symbol is immaterial, for the columns may be rearranged without affecting the nature of the function. Precisely speaking, if g is an arbitrary permutation of the integers, $1, 2, \ldots, n$, then f could equally well be given by

$$f = \begin{pmatrix} g(1) & g(2) & \ldots & g(n) \\ f(g(1)) & f(g(2)) & \ldots & f(g(n)) \end{pmatrix}.$$

From this, we infer that each of the $n!$ permutations in S_n may be written in $n!$ different ways. For instance, the following two symbols both represent the same element of S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Permutations, being functions, may be *multiplied* under the operation of functional composition. Thus, for permutations $f, g \in S_n$,

$$\begin{aligned} f \circ g &= \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \\ g(1) & g(2) & \ldots & g(n) \end{pmatrix} \\ &= \begin{pmatrix} g(1) & g(2) & \ldots & g(n) \\ f(g(1)) & f(g(2)) & \ldots & f(g(n)) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \\ g(1) & g(2) & \ldots & g(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \ldots & n \\ f(g(1)) & f(g(2)) & \ldots & f(g(n)) \end{pmatrix}. \end{aligned}$$

What we have done is to rearrange the columns of the first (left) permutation until its top row is the same as the bottom row of the second (right) permutation; the product $f \circ g$ is then the permutation whose top row is the top row of the second factor and whose bottom row is the bottom row of the first factor. With a little practice one can evaluate products without having to write out this intermediate preparation. Many authors prefer to carry out the multiplication of permutations in the opposite order (that is, they apply the factors in a product from left to right), and the reader should be particularly watchful for this.

Before stating a theorem which indicates the algebraic nature of S_n under this method of composition, we hope to clarify some of the foregoing points with an example.

Example 2-27. If the set N consists of the integers 1, 2, 3, then there are $3!$ 6 permutations in S_3, namely,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

A typical multiplication, say $f_4 \circ f_6$, proceeds as follows:

$$\begin{aligned} f_4 \circ f_6 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_2. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} f_6 \circ f_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_3, \end{aligned}$$

so that multiplication of permutations is not commutative.

Theorem 2-14. The pair $(S_n, \circ)$ forms a group, known as the *symmetric group on n symbols*, which is noncommutative for $n \geq 3$.

The proof of this fact is omitted inasmuch as a more general version of the theorem will be given shortly. In passing, it is only necessary to note that the

identity element for $(S_n, \circ)$ is the permutation

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

while the multiplicative inverse of any permutation $f \in S_n$ is described by

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Parenthetically, we might observe that the group of symmetries of the square (Example 2–24) can be subsumed under the theory of permutation groups, for these symmetries really do nothing more than map the four vertices of the square in a one-to-one fashion onto themselves. This particular group is obviously not equal to the symmetric group $(S_4, \circ)$, since the set S_4 must contain $4! = 24$ elements; indeed, one can easily find permutations in S_4 which do not correspond to any symmetry of the square. Rather, we have an example of what is called a subgroup of the group $(S_4, \circ)$.

In the following somewhat technical definition, we introduce a special type of permutation called a cycle.

Definition 2–17. Let $n_1, n_2, \dots, n_k$ be k distinct integers between 1 and n. If a permutation $f \in S_n$ is such that

$$\begin{aligned} f(n_i) &= n_{i+1} \quad \text{for} \quad 1 \leq i < k, \\ f(n_k) &= n_1, \quad \text{and} \\ f(n) &= n \quad \text{for} \quad n \notin \{n_1, n_2, \dots, n_k\}, \end{aligned}$$

then f is said to be a *k-cycle*, or a *cycle of length k*.

Simply put, a cycle replaces n_1 by n_2, n_2 by $n_3, \dots$, and finally n_k by n_1, while leaving all other elements fixed. For cycles, a more condensed notation than the usual two-line form is to write $(n_1, n_2, \dots, n_k)$, indicating that each integer is to be replaced by its successor on the right and the last integer by the first. In the symmetric group $(S_5, \cdot)$, for example, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2 \quad 5 \quad 3).$$

Of course, each integer which is omitted in this cycle notation is presumed to map onto itself under the permutation. A given cycle may clearly be represented in more than one way, since any of its elements can be put in the first position of the one-line form, as with

$$(2 \quad 5 \quad 3) = (5 \quad 3 \quad 2) = (3 \quad 2 \quad 5).$$

A final comment, before we formulate a significant result on the factorization of permutations, is that one multiplies cycles by multiplying the permutations they represent. Thus, in $(S_5, \circ)$ again,

$$(2\ \ 5\ \ 3) \circ (1\ \ 2\ \ 4\ \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

Theorem 2–15. Every permutation $f \in S_n$ can be written as a commutative product of cycles, no two of which have an element in common.

Proof. First, consider the set of images of the integer 1 under successive powers of f: $\{f(1), f^2(1), f^3(1), \ldots\}$. As usual, by f^m we mean $f \circ f \circ \cdots \circ f$, m times. Since the domain of f is finite, $f^i(1) = f^j(1)$ for some $i < j$, whence $f^{j-i}(1) = 1$. This in turn implies that there exists a least positive integer k $(1 \leq k \leq n)$ for which $f^k(1) = 1$. Let $(1, f(1), f^2(1), \cdots, f^{k-1}(1))$ be the first cycle of the permutation f. If the element 2 is not found in this cycle, repeat the foregoing argument to obtain another cycle $(2, f(2), f^2(2), \ldots, f^{j-1}(2))$, where j is the smallest positive integer such that $f^j(2) = 2$. In at most n such steps, this procedure must terminate. The order of multiplication of the resulting cycles is immaterial, for they clearly have no elements in common.

To illustrate Theorem 2–15, let us return momentarily to the permutation considered above; in this case,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1\ \ 5\ \ 3) \circ (2\ \ 4),$$

since

$$f(1) = 5, \qquad f^2(1) = f(5) = 3, \qquad f^3(1) = f(3) = 1,$$

and

$$f(2) = 4, \qquad f^2(2) = f(4) = 2.$$

The simplest of permutations are undoubtably the 2-cycles, for they just interchange two elements and leave all others fixed. It is customary to refer to such cycles as *transpositions*.

Corollary. Every permutation may be expressed as the product of transpositions.

Proof. In light of the preceding result, it suffices to write any k-cycle as a product of transpositions. A direct computation shows that this can be done rather simply in the following manner:

$$(1\ \ 2\ \ \ldots\ \ k) = (1\ \ k) \circ (1\ \ k-1) \circ \cdots \circ (1\ \ 2).$$

As the above transpositions have an integer in common, they do not, in general, commute. Furthermore, the decomposition is by no means unique. For instance,

$$(1\ \ 2\ \ 3) = (1\ \ 3) \circ (1\ \ 2) = (2\ \ 1) \circ (2\ \ 3).$$

While a given permutation may be factored into a product of transpositions in a variety of ways, the number of transpositions involved will always have the same parity. That is, if one factorization has an even (odd) number of transpositions, then every factorization must have an even (odd) number of transpositions.

The notion of permutation as presented in Definition 2–16 is not sufficiently general for all our purposes, since it restricts us to finite sets only. It would seem more natural to define this concept for arbitrary sets, finite or infinite, as follows.

Definition 2–18. If G is any nonempty set, then a *permutation* of G is a one-to-one function from the set G onto itself.

We represent the set of all permutations of G by the symbol, sym G (the reason for this choice will be clear in a moment). To be sure, if G is a finite set having n elements, then sym $G = S_n$.

In this general framework, it is possible to prove a structure theorem from which Theorem 2–14 will follow as a special case.

Theorem 2–16. For a nonempty set G, the pair (sym G, $\circ$) constitutes a group, called the *symmetric group* of G.

Proof. The first thing to be done is to show that $\circ$ is actually a binary operation on sym G. Given arbitrary permutations f, $g \in$ sym G, the composition $f \circ g$ is obviously a function from G into G. If the element $c \in G$, then there exists some $b \in G$ such that $f(b) = c$; similarly, there is an element a in G for which $g(a) = b$. Hence,

$$(f \circ g)(a) = f(g(a)) = f(b) = c,$$

which shows that $f \circ g$ is an onto function.

By definition, both f and g are one-to-one functions; we would like to conclude that the composition $f \circ g$ also has this property. For this purpose, consider arbitrary elements a, $b \in G$ with $a \neq b$. Since g is one-to-one, the images $g(a)$ and $g(b)$ are necessarily distinct in G. But then, the one-to-one character of f implies $f(g(a)) \neq f(g(b))$. In other words, $(f \circ g)(a) \neq (f \circ g)(b)$, which establishes the desired one-to-oneness of $f \circ g$. From the preceding remarks, we infer that $f \circ g \in$ sym G whenever f and g are in sym G, making $\circ$ a binary operation of the set sym G.

The associativity of functional composition follows from Theorem 1–7. Plainly, the identity function i_G is a permutation of G and is such that

$$f \circ i_G = f = i_G \circ f,$$

for any $f \in \text{sym } G$, showing i_G to be an identity element for the system (sym G, $\circ$). If $f \in \text{sym } G$, the inverse function f^{-1} exists, is a one-to-one function, and maps the set G onto itself. Moreover, f^{-1} is the inverse of f with respect to composition. All of which justifies the statement that (sym G, $\circ$) is a group.

PROBLEMS

1. Prove that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{cn}$.
2. a) Find all solutions x, where $0 \leq x < 15$, of the equation $3x \equiv 6 \pmod{15}$.
   b) Prove that $6^n \equiv 6 \pmod{10}$ for any $n \in Z_+$.
3. Describe the partition of Z determined by the integers modulo 5.
4. Let $P(x)$ be a polynomial in x with integral coefficients. If n is a solution of the equation $P(x) \equiv 0 \pmod{n}$, and $a \equiv b \pmod{n}$, prove that b is also a solution.
5. Show that the pair $(\{0, 4, 8, 12\}, +_{16})$ is a group.
6. Use the fact that $10 \equiv 1 \pmod{9}$ to prove that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. [*Hint:* Express the integer in decimal form as a sum of powers of 10.]
7. For any integer n, prove that either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.
8. a) Determine solutions of the congruence equations $x^2 \equiv -1 \pmod{5}$ and $x^2 \equiv -1 \pmod{13}$. This shows, loosely speaking, that the square of an integer in Z_n may be negative.
   b) If the equation $x^2 \equiv a \pmod{n}$ has a solution x_1, show $x_2 = n - x_1$ is also a solution.
9. Suppose $a^2 \equiv b^2 \pmod{n}$, where n is a prime number. Prove that either $a \equiv b \pmod{n}$ or $a \equiv -b \pmod{n}$.
10. a) Prove the symmetric group on two symbols, $(S_2, \circ)$, is commutative.
    b) Demonstrate that the group $(S_3, \circ)$, and hence any larger symmetric group, is noncommutative by considering the permutations

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

11. Express the following permutations as (a) products of cycles having no elements in common, (b) products of transpositions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 3 & 4 \end{pmatrix}$$

12. Show that the cycle (1 2 3 4 5) may be written as a product of 3-cycles.
13. Verify the relation $(1\ 2\ 3\ \ldots\ n)^{-1} = (n\ n-1\ \ldots\ 2\ 1)$; in particular deduce that every transposition is its own inverse.
14. The symmetries of the square (Example 2–24) may be interpreted as permutations of the vertices. Represent each of these symmetries by a corresponding permutation.