15. Consider the set G consisting of the four permutations

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

Show that $(G, \circ)$ constitutes a commutative group.

16. Form the set $G = \{f, f^2, f^3, f^4, f^5, f^6\}$, where f is the permutation

$$f = \begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix},$$

and prove that the pair $(G, \circ)$ is a commutative group.

2–4 SUBGROUPS

There are two standard techniques in attacking the problem of the structure of a particular group. One method calls for finding all the subgroups of the group, with the hope of gaining information about the parent group through its local structure. The other approach is to determine all homomorphisms from the given group into a more familiar group; the idea here is that the images will reflect some of the algebraic properties of the original group. On closer scrutiny, we shall see that while these lines of investigation aim in different directions, they are not entirely unrelated, but rather aspects of the same problem. For the moment, however, our attention is focused on analyzing a group by means of its subgroups; the question of structure-preserving mappings is a more subtle matter and will be deferred to a later section.

From various examples and exercises, the reader may have noticed that certain subsets of the elements of a group lead to new groups when one restricts the group operation to these subsets. It is this situation in which we shall be primarily interested.

Definition 2–19. Let $(G, *)$ be a group and $H \subseteq G$ be a nonempty subset of G. The pair $(H, *)$ is said to be a *subgroup* of $(G, *)$ if $(H, *)$ is itself a group.

Each group $(G, *)$ has two obvious subgroups. For, if $e \in G$ is the identity element of the group $(G, *)$, then both $(\{e\}, *)$ and $(G, *)$ are subgroups of $(G, *)$. These two subgroups are often referred to as the *trivial* subgroups of $(G, *)$; all subgroups between these two extremes are called nontrivial subgroups. Any subgroup different from $(G, *)$ is termed *proper*.

Example 2–28. If Z_e and Z_o denote the sets of even and odd integers, respectively, then $(Z_e, +)$ is a subgroup of the group $(Z, +)$, while $(Z_o, +)$ is not.

Example 2–29. Consider $(Z_6, +_6)$, the group of integers modulo 6. If

$$H = \{0, 2, 4\},$$

then $(H, +_6)$, whose operation table is given below, is a subgroup of $(Z_6, +_6)$.

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Example 2–30. Let $(G, *)$ be the group of symmetries of the square (see Example 2–24), where $G = \{R_{90}, R_{180}, R_{270}, R_{360}, H, V, D_1, D_2\}$ and the operation $*$ consists of following one motion by another. This group contains eight nontrivial subgroups. We leave it to the reader to verify that the following sets comprise the elements of these subgroups:

$$\{R_{90}, R_{180}, R_{270}, R_{360}\}, \quad \{R_{180}, R_{360}, H, V\},$$
$$\{R_{180}, R_{360}, D_1, D_2\}, \quad \{R_{180}, R_{360}\}, \quad \{R_{360}, D_1\},$$
$$\{R_{360}, D_2\}, \quad \{R_{360}, H\}, \quad \{R_{360}, V\}.$$

Suppose $(H, *)$ is a subgroup of the group $(G, *)$. Since the identity element of $(H, *)$ satisfies the equation $x * x = x$, it must be the same as the identity of the parent group $(G, *)$, for otherwise we would have two idempotent elements in G, contrary to Theorem 2–5. The identity element of a group thus also serves as the identity element for any of its subgroups. Moreover, the uniqueness of the inverse elements in a group implies the inverse of an element $h \in H$ in the subgroup $(H, *)$ is the same as its inverse in the whole group $(G, *)$.

To establish that a given subset H of G, along with the induced operation of $(G, *)$, constitutes a subgroup, we must verify that all the conditions of Definition 2–11 are satisfied. However, the associativity of the operation $*$ in H is an immediate consequence of its associativity in G, since $H \subseteq G$. It is necessary then to show only the following:

1) $a, b \in H$ implies $a * b \in H$ (closure),

2) $e \in H$, where e is the identity element of $(G, *)$,

3) $a \in H$ implies $a^{-1} \in H$.

Needless to say, the saving in not having to check the associative law can prove to be considerable.

A theorem which establishes a single convenient criterion for determining subgroups is given below.

Theorem 2–17. Let $(G, *)$ be a group and $\emptyset \neq H \subseteq G$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if $a, b \in H$ implies $a * b^{-1} \in H$.

Proof. If $(H, *)$ is a subgroup and $a, b \in H$, then $b^{-1} \in H$, and so $a * b^{-1} \in H$ by the closure condition. Conversely, suppose H is a nonempty subset of G

which contains the element $a * b^{-1}$ whenever $a, b \in H$. Since H contains at least one element b, we may take $a = b$ to see that $b * b^{-1} = e \in H$. Also, $b^{-1} = e * b^{-1} \in H$ for every b in H, applying the hypothesis to the pair e, $b \in H$. Finally, if a and b are any two members of the set H, then by what was just proved b^{-1} also belongs to H, so that $a * b = a * (b^{-1})^{-1} \in H$; in other words, the set H is closed with respect to the operation $*$. Because $*$ is an associative operation in G, H inherits the associative law as a subset of G. All the group axioms are satisfied and the system $(H, *)$ is therefore a subgroup of $(G, *)$.

Definition 2–20. The *center* of a group $(G, *)$, denoted by cent G, is the set

$$\text{cent } G = \{c \in G \mid c * x = x * c \text{ for all } x \in G\}.$$

Thus cent G consists of those elements which commute with every element of G. For example, in the group of symmetries of the square,

$$\text{cent } G = \{R_{180}, R_{360}\}.$$

The reader may already have deduced that a group $(G, *)$ is commutative if and only if cent $G = G$.

As illustrations of the use of Theorem 2–17 in determining when a subset of the elements of a group is the set of elements of a subgroup, we present the following two theorems.

Theorem 2–18. The pair (cent G, $*$) is a subgroup of each group $(G, *)$.

Proof. We first observe that cent G is nonempty, for at the very least $e \in$ cent G. Now consider any two elements $a, b \in$ cent G. By the definition of center, we know that $a * x = x * a$ and $b * x = x * b$ for every element x of G. Thus, if $x \in G$,

$$\begin{aligned}(a * b^{-1}) * x &= a * (b^{-1} * x) \\ &= a * (x^{-1} * b)^{-1} \\ &= a * (b * x^{-1})^{-1} \\ &= a * (x * b^{-1}) \\ &= (a * x) * b^{-1} \\ &= (x * a) * b^{-1} = x * (a * b^{-1}),\end{aligned}$$

which implies $a * b^{-1} \in$ cent G. According to Theorem 2–17, this is a sufficient condition for (cent G, $*$) to be a subgroup of $(G, *)$.

Theorem 2–19. If $(H_i, *)$ is an arbitrary indexed collection of subgroups of the group $(G, *)$, then $(\cap H_i, *)$ is also a subgroup.

Proof. Since the sets H_i all contain the identity element of $(G, *)$, the intersection $\cap H_i \neq \emptyset$. Next, suppose a and b are any two elements of $\cap H_i$; then

$a, b \in H_i$, where i ranges over the index set. The pair $(H_i, *)$ being a subgroup, it follows that the product $a * b^{-1}$ also belongs to H_i. As this is true for every index i, $a * b^{-1} \in \cap H_i$, which implies $(\cap H_i, *)$ is a subgroup of $(G, *)$.

In regard to the group of symmetries of the square, we could take

$$H_1 = \{R_{90}, R_{180}, R_{270}, R_{360}\},$$
$$H_2 = \{R_{180}, R_{360}, D_1, D_2\}.$$

The system $(H_1 \cap H_2, *) = (\{R_{180}, R_{360}\}, *)$ is obviously a subgroup of this group, for its elements comprise the center of the group.

In general, without further restriction on the subgroups $(H_i, *)$, it is not true that the pair $(\cup H_i, *)$ will again be a subgroup of $(G, *)$. One simply cannot guarantee that $\cup H_i$ will contain products whose factors come from different H_i. To give a concrete illustration, both $(\{0, 6\}, +_{12})$ and $(\{0, 4, 8\}, +_{12})$ are subgroups of $(Z_{12}+_{12})$, yet on taking the union, $(\{0, 4, 6, 8\}, +_{12})$ fails to be so. The difficulty in this case is that the modular sums $4 +_{12} 6$ and $6 +_{12} 8$ do not belong to the set $\{0, 4, 6, 8\}$.

By the way of an analog to Theorem 2–19, we have:

Theorem 2–20. Let $(H_i, *)$ be an indexed collection of subgroups of the group $(G, *)$. Suppose the family of subsets $\{H_i\}$ has the property that for any two of its members H_i and H_j there exists a set H_k (depending on i and j) in $\{H_i\}$ such that $H_i \subseteq H_k$ and $H_j \subseteq H_k$. Then $(\cup H_i, *)$ is also a subgroup of $(G, *)$.

Proof. By now the pattern of proof should be clear. We assume that a and b are arbitrary elements of $\cup H_i$ and show that $a * b^{-1} \in \cup H_i$. If $a, b \in \cup H_i$, then there exist subsets H_i, H_j containing a and b, respectively. According to our hypothesis, $H_i \subseteq H_k$ and $H_j \subseteq H_k$ for some choice of H_k in $\{H_i\}$. Since $(H_k, *)$ is a subgroup and both $a, b \in H_k$, it follows that the product $a * b^{-1}$ belongs to H_k. Accordingly, $a * b^{-1} \in \cup H_i$ as was claimed at the beginning.

As a particular case of the foregoing result, consider just two subgroups $(H_1, *)$ and $(H_2, *)$. Theorem 2–20 may be interpreted as asserting that $(H_1 \cup H_2*)$ will again be a subgroup of $(G, *)$ provided either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. What is rather interesting is that this condition is necessary, as well as sufficient. The next theorem gives the details.

Theorem 2–21. Let $(H_1, *)$ and $(H_2, *)$ be subgroups of the group $(G, *)$. The pair $(H_1 \cup H_2,)$ is also a subgroup if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof. In view of the preceding remarks, it is enough to show that if $(H_1 \cup H_2, *)$ is a subgroup, then one of the sets H_1 or H_2 must be contained in the other. Suppose to the contrary that this assertion were false: that is, $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$. Then there would exist elements $a \in H_1 - H_2$ and $b \in H_2 - H_1$.

Now, if the product $a * b$ were a member of the set H_1, we could infer that

$$b = a^{-1} * (a * b) \in H_1,$$

which is clearly not true. On the other hand, the possibility $a * b \in H_2$ yields the equally false conclusion

$$a = (a * b) * b^{-1} \in H_2.$$

That is, the elements $a, b \in H_1 \cup H_2$, but $a * b \notin H_1 \cup H_2$. This conclusion is obviously untenable, for it contradicts the fact $(H_1 \cup H_2, *)$ is a group. Having arrived at a contradiction, the proof is complete.

The next topic of interest concerns cyclic subgroups. To facilitate this discussion, we first introduce some special notation.

Definition 2–21. If $(G, *)$ is an arbitrary group and $\emptyset \neq S \subseteq G$, then the symbol (S) will represent the set

$$(S) = \cap\{H \mid S \subseteq H;\ (H, *) \text{ is a subgroup of } (G, *)\}.$$

The set (S) clearly exists, for G itself is a member of the family appearing on the right; that is, $(G, *)$ is a (trivial) subgroup of $(G, *)$ and $S \subseteq G$. In addition, since S is contained in each of the sets being intersected, we always have the inclusion $S \subseteq (S)$.

Theorem 2–22. The pair $((S), *)$ is a subgroup of $(G, *)$, known either as the *enveloping subgroup* for S or the *subgroup generated by the set* S.

Proof. The proof is an immediate consequence of Theorem 2–19.

Definition 2–21 implies that whenever $(H, *)$ is a subgroup of the group $(G, *)$ with $S \subseteq H$, then $(S) \subseteq H$. For this reason, one speaks informally of $((S), *)$ as being the smallest subgroup which contains the set S. Of course, it may well happen that $(S) = G$, and in such a situation, the group $(G, *)$ is said to be *generated* by the subset S. For example, it is easy to see that the group $(Z, +)$ is generated by Z_o, the set of odd integers.

We shall give an alternative description of the subset (S) which is frequently easier to work with than Definition 2–21. In what follows, the symbol S^{-1} is used to indicate the collection of inverses of elements in S: $S^{-1} = \{a^{-1} \mid a \in S\}$. The result we propose to obtain is that

$$(S) = \{a_1 * a_2 * \cdots * a_n \mid a_1, \ldots, a_n \in S \cup S^{-1};\ n \in Z_+\}.$$

Although the notation is self explanatory, it would be helpful to explicitly point out that the set on the right consists of all finite products whose factors are either elements in S or inverses of elements in S. Let us temporarily designate this set of products by $[S]$.

An abbreviated proof of the assertion above might run as follows: The system $([S], *)$ is a subgroup of the group $(G, *)$ with the property $S \subseteq [S]$. As $((S), *)$ is the smallest such subgroup, it follows that $(S) \subseteq [S]$. The reverse inclusion is justified by the fact that any subgroup which contains the set S must necessarily contain all the elements of $[S]$.

A case of special importance arises when S consists of a single element a. In this situation, it is usual to write (a) instead of $(\{a\})$ and refer to the associated subgroup $((a), *)$ as the *cyclic subgroup generated by* a. The subset (a) is rather easy to describe; as all its products involve the element a or its inverse, (a) simply reduces to the integral powers of a:

$$(a) = \{a^n \mid n \in Z\}.$$

It is entirely possible that the group $(G, *)$ is equal to one of its cyclic subgroups, that is, for some choice of $a \in G$, $(a) = G$. Under these circumstances, the group $(G, *)$ is referred to as a *cyclic group* with *generator* a. Thus, to say a group is cyclic means that each of its members can be expressed as an integral power of some fixed element of the group.

A cyclic group may possess several different generators; indeed, one always has $(a) = (a^{-1})$. Notice in addition that, as a consequence of the law of exponents, any cyclic group must be commutative.

To make these notions clearer, let us pause to examine several examples.

Example 2–31. First consider the group of integers $(Z, +)$. In this case, since the group operation is that of addition, the abstract product $a * a * \cdots * a$ is replaced by the ordinary sum $a + a + \cdots + a$. Accordingly, the subset generated by the element a takes the form

$$(a) = \{na \mid n \in Z\}.$$

Using this notation, $\{0\} = (0)$, $Z = (1)$, while $Z_e = (2)$. We may thus conclude that both the groups $(Z, +)$ and $(Z_e, +)$ are cyclic, with the integers 1 and 2 as their respective generators.

Example 2–32. Another illustration is furnished by $(Z_{12}, +_{12})$, the group of integers modulo 12. Note that we now write $a +_{12} a +_{12} \cdots +_{12} a$ for $a * a * \cdots * a$. The cyclic subgroup generated by, say 3, is $(\{0, 3, 6, 9\}, +_{12})$, for here,

$$(3) = \{3n \pmod{12} \mid n \in Z\} = \{0, 3, 6, 9\}.$$

As $(1) = Z_{12}$, the group $(Z_{12}, +_{12})$ is itself cyclic; other possible generators of $(Z_{12}, +_{12})$ are 5, 7 and 11. It is not difficult to see that, in general, the group of integers modulo n is cyclic with 1 as a generator.

Example 2–33. The group of symmetries of the square is not cyclic, for cyclic groups are necessarily commutative. Save for the identity, the distinct

powers of any of its elements comprise the members of a nontrivial cyclic subgroup. The rotation R_{90}, in particular, generates the subgroup whose elements are $\{R_{90}, R_{180}, R_{270}, R_{360}\}$.

By a *finite group*, we mean any group whose underlying set of elements is a finite set. The *order* of a finite group is defined to be the number of its elements. Analogously, a group with an infinite number of elements is said to have infinite order.

In the following theorems, we shall see that finite cyclic groups have a particularly simple structure. For one thing, the elements of a finite cyclic group with generator a are just $e, a, a^2, \ldots, a^{n-1}$, where n is the order of the group. All other powers of a are superfluous, since they merely repeat these.

Theorem 2–23. If $((a), *)$ is a finite cyclic group of order n, then

$$(a) = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Proof. As the set (a) is finite, not all the powers of the generator a are distinct. There must be some repetition $a^i = a^j$ with $i < j$. On multiplying this equation by $a^{-i} = (a^i)^{-1}$, it follows that $a^{j-i} = e$. Thus the set of positive integers k for which $a^k = e$ is nonempty. Suppose m is the smallest positive integer with this property; that is, $a^m = e$, while $a^k \neq e$ for $0 < k < m$.

The set $S = \{e, a, a^2, \ldots, a^{m-1}\}$ consists of distinct elements of (a). For $a^r = a^s$, with $0 \leq r < s \leq m - 1$, implies that $a^{s-r} = e$, contrary to the minimality of m. To complete the proof, it remains to show each member a^k of the group $((a), *)$ is equal to an element of S. Now, by the division algorithm, we may write $k = qm + r$ for some integers q and r with $0 \leq r < m$. Hence,

$$a^k = (a^m)^q * a^r = e * a^r = a^r \in S.$$

This means the set $(a) \subseteq S$, yielding $(a) = \{e, a, a^2, \ldots, a^{m-1}\}$ and the subsequent equality $m = n$.

If a is an element of the group $(G, *)$, we define the *order of* a to be the order of the cyclic subgroup $((a), *)$ generated by a. The last result permits an alternative viewpoint: the order of a is the least positive integer n, provided it exists, such that $a^n = e$. Of course, if no such integer exists, a is of infinite order. As an illustration, consider the group $(Z_4, +_4)$; here, the element 0 has order 1, 1 has order 4, 2 has order 2, while 3 has order 4.

In certain cases (unfortunately, far too few), it is possible to characterize completely the subgroups of a given group. To cite one instance, in the additive group of integers $(Z, +)$, the subgroups are all of the form $((n), +)$ for some nonnegative integer n. Actually, the situation is somewhat more general, for it can be shown that any subgroup of a cyclic group is again cyclic; we shall discuss this next.