CHAPTER 2

GROUP THEORY

2-1 DEFINITION AND EXAMPLES OF GROUPS

In this chapter, and throughout the remainder of the text, we shall deal with mathematical systems which are defined by a prescribed list of properties. Emphasis will be on deriving theorems that follow logically from the postulates and which, at the same time, help to describe the algebraic structure of the particular system under consideration. This axiomatic approach not only permits us to concentrate on essential ideas, but also unifies the presentation by showing the basic similarities of many diverse and apparently unrelated examples.

We first confine our attention to systems involving just one operation, since they are amenable to the simplest formal description. Despite this simplicity, the axioms permit the construction of a profuse and elegant theory in which one encounters many of the fundamental notions common to all algebraic systems.

Before beginning, however, it is necessary to arrive at some understanding concerning the use of the equivalence relation $=$. We will henceforth take the equality sign to mean, intuitively, "is the same as." In other words, the symbol $=$ asserts that the two particular expressions involved are merely different names for, or descriptions of, one and the same object; just one object is being considered, and it is named twice. To indicate that a and b are not the same object we shall, naturally enough, write $a \neq b$.

As a first step in our program, we introduce the concept of a binary operation. This idea is the cornerstone of all that follows.

Definition 2-1. Given a nonempty set S, any function from the Cartesian product $S \times S$ into S is called a *binary operation* on S.

A binary operation on S thus assigns to each ordered pair of elements of S a uniquely determined third element of the same set S. For instance, if $P(A)$ denotes the power set of a fixed set A, then both $\cup$ and $\cap$ are binary operations on $P(A)$. In practice, we shall generally use the symbol $*$ to represent a binary operation and write $a * b$, instead of $*((a, b))$, for its value at the ordered pair $(a, b) \in S \times S$. While this convention is at variance with the functional notation developed in the previous chapter, its use in the present situation is dictated by long-standing mathematical tradition. At the very least, it has the advantage of avoiding some rather clumsy notation.

From time to time, we shall permit ourselves to make such informal statements as "combine a with b" or "form $a * b$." In a precise sense, what is really meant of course is to apply the function $*$ to the ordered pair (a, b). The most useful aspect of a binary operation is that, having once formed the element $a * b$, we may in turn combine it with other members of S; the result of all such calculations again lies in S.

Needless to say, the particular notation used for the abstract product of two elements is of no great importance. On occasions some other symbol, as equally noncommittal as $*$, will be employed. Specifically, we will frequently choose to write $a \circ b$ in place of $a * b$ (in this context, the symbol $\circ$ is not intended to have any special connection with functional composition). In general, a and b will have no numerical value but will simply be arbitrary elements in our underlying set S, whatever this set may be, while $*$ may well be some law of composition which bears no resemblance to the usual operations of elementary algebra.

Closely allied to the notion of a binary operation is the so-called *closure condition*. For a formal statement of this property, suppose that $*$ is a binary operation on the set S and $A \subseteq S$; the subset A is said to be *closed* under the operation $*$ provided $a * b \in A$ whenever a and b are in A. The desirable feature here is that when A is closed under the operation $*$, the restriction of $*$ to the subset A is a binary operation on A as well as S.

Example 2–1. Ordinary subtraction is clearly a binary operation on the set Z of integers; the subset Z_+ of positive integers, however, is not closed under subtraction.

When the set S being considered has a relatively small number of elements, the results of applying the operation $*$ to its members may be conveniently represented in what might be called an *operation* or *multiplication table*. We construct this table by first listing the members of S in the same order both vertically and horizontally. The result $a * b$ then appears in the body of the table at the intersection of the row headed by a and the column headed by b. Conversely, such a table could equally well serve to define a binary operation on S, for the result of combining any pair of elements of S would be displayed somewhere in the table.

Example 2–2. A binary operation $*$ may be defined on the three-element set $S = \{1, 2, 3\}$ by means of the operation table below:

*	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

According to the table, the product $2 * 3$, for instance, is equal to the element 2, located at the intersection of the row marked 2 and the column marked 3.

Given an arbitrary binary operation $*$, there is certainly no reason to expect that $a * b$ will be the same as $b * a$ for all a and b. In fact, it can be seen in the above example that $1 * 2 = 2$, whereas $2 * 1 = 3$. One must consequently take care to refer to $a * b$ as the product of a and b and to $b * a$ as the product of b and a; the distinction is quite important. We should also point out that it is obviously possible to combine an element with itself. That is to say, $a * a$ can be defined.

Definition 2-2. By a *mathematical system* (or *mathematical structure*), we shall mean a nonempty set of elements together with one or more binary operations defined on this set.

A mathematical system consisting of the set S and a single binary operation $*$ will be denoted by the ordered pair $(S, *)$; analogously, a system consisting of the set S and two operations $*$ and $\circ$ will be represented by the ordered triple $(S, *, \circ)$.

Example 2-3. The pair $(S, \cdot)$, where the set $S = \{1, -1, i, -i\}$ and the operation is that of ordinary multiplication, is a mathematical system provided one defines $i^2 = -1$.

Example 2-4. If Z_e and Z_o denote the even and odd integers, respectively, then $(Z_e, +, \cdot)$ constitutes a mathematical system, while $(Z_o, +, \cdot)$ does not. In the latter case, the set Z_o is not closed under addition, since the sum of two odd integers is necessarily even.

The systems to be studied subsequently are classified according to the properties they possess or, to put it another way, according to the axioms they satisfy. Our object will be to present a sequential development of the principal mathematical systems of modern algebra, beginning with those involving relatively few axioms and progressing to systems satisfying more detailed hypotheses.

The axioms which form the starting point of the abstract theory can be, by nature, rather varied. The growing tendency of modern mathematics is to isolate almost any convenient set of properties from its original context, to define a particular system, and to develop the corresponding abstract theory through logical deduction. Some of these formal axiomatic theories, such as the notion of a group, have a fundamental importance to the whole of mathematics and have been instrumental in unifying various apparently unrelated branches; other theories, while satisfying the esthetic and inquisitive needs of the mathematician, are limited in the extent of their applicability. We do not mean to create the impression that it is the usual practice for one to define a new system by arbitrarily (apart from logical considerations) writing down axioms. Although there is no particular necessity for the model to precede the theoretical development, in most cases the axioms are the abstract realization of the properties common to a variety of specific examples. With these general remarks out of the way, let us get down to work.

A set on which a single unrestricted binary operation is defined does not by itself yield a structure rich enough for our purposes; the concept, being too general, is poor in content. Certain reasonable limitations must be imposed on the operation if one is to obtain useful results. In the following paragraphs, some of the more basic requirements are named and briefly examined. For conciseness, we shall hereafter omit the word "binary" inasmuch as every operation to be considered will necessarily be binary.

Given a mathematical system $(S, *)$, the symbol $a * b * c$ is at the moment completely meaningless, since the operation $*$ has only been defined for pairs of elements of S. If, however, we make the stipulation that whenever quantities are enclosed in parentheses these are to be evaluated first, then both the expressions $a * (b * c)$ and $(a * b) * c$ make sense. Namely, $a * (b * c)$ is to be interpreted as: combine a with what results from combining b with c; while $(a * b) * c$ is to be interpreted as: first combine a with b and then combine the result with c. Of course, the resulting elements $a * (b * c)$ and $(a * b) * c$ will not necessarily be the same.

Definition 2–3. The operation $*$ defined on the set S is said to be ***associative*** if

$$a * (b * c) = (a * b) * c \qquad \text{(associative law)},$$

for every triple, distinct or not, of elements a, b, and c of S.

Example 2–5. The operation of subtraction on the set $R^{\#}$ of real numbers is not associative, since in general

$$a - (b - c) \neq (a - b) - c.$$

Example 2–6. An associative operation $*$ may be defined on Z, the set of integers, by taking $a * b = a + b + ab$. (We shall frequently delete the dot and write the product of a and b under ordinary multiplication simply as ab.) Then

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc), \end{aligned}$$

while

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c. \end{aligned}$$

The equality of these two expressions follows in part from the fact that addition and multiplication are themselves associative in Z.

When dealing with a system whose operation is defined by a multiplication table rather than a formula, it is generally quite tedious to establish the associativity of the operation, for one must compute all possible threefold products. On the other hand, it may be far easier to show that the operation is not associative, as all we need do in this case is find three particular elements from the underlying set for which the associative law fails.

Example 2-7. Consider the operation $*$ defined on the set $S = \{1, 2, 3\}$ by the operation table:

$*$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

From this table, we see that $2 * (1 * 3) = 2 * 3 = 2$, whereas $(2 * 1) * 3 = 3 * 3 = 1$; that is,

$$2 * (1 * 3) \neq (2 * 1) * 3.$$

The associative law thus fails to hold in the system $(S, *)$.

The mathematical system which we shall use to build up more complicated algebraic structures is known as a semigroup.

Definition 2-4. A *semigroup* is a pair $(S, *)$ consisting of a nonempty set S together with an associative (binary) operation $*$ defined on S.

Let us stress that it is an abuse of language to say a certain set alone is a semigroup without also specifying the operation involved, as it may be quite possible to equip the same set with several associative operations. For this reason, we have utilized the ordered pair notation to indicate both the operation and the underlying set of elements.

Observe that since any three elements from the set of a semigroup always associate, there is no particular reason for parentheses. Consequently, when dealing with such a system, the symbol $a * b * c$ has meaning in the sense that we are free to interpret it either as $a * (b * c)$ or as $(a * b) * c$. More generally, the notation $a_1 * a_2 * \cdots * a_m$ is unambiguous, for it can be shown that all ways of inserting parentheses so as to give this expression a value yield the same result (Theorem 2-4). An operation which is not associative has the decided disadvantage that the notation for multiple-factored products can become quite unwieldy as a result of the constant need for parentheses.

In order to solidify the notion of a semigroup, we present several examples.

Example 2-8. There are several semigroups with which the reader is already familiar. If, for instance, Z_+ denotes the set of all positive integers, then both the pairs $(Z_+, +)$ and $(Z_+, \cdot)$ form semigroups. Similar statements hold for the sets Z, Q, and $R^\#$.

Example 2-9. Define the operation $*$ on the real numbers by the rule

$$a * b = \max\{a, b\}, \qquad a, b \in R^{\prime}.$$

That is, $a * b$ is the larger of the two numbers a and b, or either one if $a = b$. Here, we have

$$a * (b * c) = \max\{a, b, c\} = (a * b) * c,$$

so that $(R^{\prime}, *)$ satisfies the requirements of a semigroup.

Example 2-10. For any set X, each of the systems $(P(X), \cup)$ and $(P(X), \cap)$ constitutes a semigroup (Theorem 1-2).

Example 2-11. Let X be a nonempty set and S be the collection of all functions $f: X \to X$. If $\circ$ denotes functional composition, then the pair $(S, \circ)$ provides another illustration of a semigroup (Problem 5, Section 1-2).

As we shall subsequently see, the relevance of the semigroup concept lies in the fact that many important systems contain the semigroup structure as a subsystem.

We have already indicated that the order in which elements occur in a product is quite essential. If it is possible to interchange the order of combining any two elements from our set without affecting the result, then the operation is termed commutative.

Definition 2-5. The operation $*$ defined on the set S is called *commutative* if

$$a * b = b * a \qquad \text{(commutative law)},$$

for every pair of elements $a, b \in S$.

Examples 2-8, 2-9 and 2-10 are of *commutative semigroups* (semigroups whose operation is commutative), while in Example 2-11 functional composition is not, in general, a commutative operation. Although the commutative law may fail to hold throughout an entire system, it may still be valid for particular pairs of elements; accordingly, it will be convenient to make the following definition.

Definition 2-6. Two elements a and b are said to *commute* or *permute* (with each other) provided $a * b = b * a$.

Employing this terminology, we observe that the operation of the system $(S, *)$ is commutative if and only if every pair of elements of S commute.

Once an operation has been defined on a set, one finds that certain elements play special roles; there may exist identity elements and inverse elements.

Definition 2-7. The system $(S, *)$ is said to have a (two-sided) identity element for the operation $*$ if there exists an element e in S such that

$$a * e = e * a = a$$

for every $a \in S$. An element e having this property is called an *identity element* (unit element, neutral element) for $(S, *)$.

An identity element thus causes each element of the set S to remain stationary under the operation. In particular, notice that $e * e = e$. Of course, for a given system, an identity element may or may not exist; in case an identity does exist, it must be unique, as the theorem below shows.

Theorem 2–1. A mathematical system $(S, *)$ has at most one identity element.

Proof. For the proof, let us suppose that $(S, *)$ has two identity elements e and e'. Since $e * a = a$ for each $a \in S$, then in particular $e * e' = e'$. But on the other hand, e' is also an identity element, so we must have $e * e' = e$. We thus obtain $e = e * e' = e'$ and consequently $e = e'$; that is, if the system actually has an identity, then there is precisely one element with this property.

It follows from Theorem 2–1 that, whenever $(S, *)$ has an identity, we are justified in using the expression "the identity element of $(S, *)$"; the symbol e will be reserved exclusively for this identity.

Definition 2–8. A semigroup $(S, *)$ is said to be a *semigroup with identity* if there exists a (unique) identity element for $(S, *)$.

Example 2–12. The semigroup $(Z_+, \cdot)$ possesses an identity element, namely, the positive integer 1. On the other hand, the semigroup $(Z_+, +)$ has none, since $0 \notin Z_+$.

Example 2–13. Both the semigroups $(P(X), \cup)$ and $(P(X), \cap)$ have identities. Here, the empty set $\emptyset$ is the identity element for the union operation, since

$$A \cup \emptyset = \emptyset \cup A = A \qquad \text{for each set} \quad A \subseteq X.$$

As is easy to see, the universal set X acts as the identity element for the operation of intersection, since

$$A \cap X = X \cap A = A \qquad \text{for each set} \quad A \subseteq X.$$

Example 2–14. To record one more example of a semigroup with identity, consider the set of numbers

$$S = \{a + b\sqrt{2} \mid a, b \in Z\},$$

and the operation of ordinary multiplication. First, one is obliged to check that S is actually closed under multiplication; this is fairly clear, for if $a + b\sqrt{2}$ and $c + d\sqrt{2}$ are arbitrary members of S, then

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ad + 2bd) + (ad + bc)\sqrt{2} \in S.$$

It is not particularly difficult to establish that the pair $(S, \cdot)$ is a commutative semigroup with identity element $1 = 1 + 0\sqrt{2}$; we omit the argument.

When working with an operation which has an identity element, it is natural to inquire which elements of the underlying set, if any, have inverses.

Definition 2-9. Let $(S, *)$ be a mathematical system with identity element e. An element $a \in S$ is said to have a (two-sided) inverse under the operation $*$ if there exists some member a' of S such that

$$a * a' = a' * a = e.$$

An element a' having this property is called an *inverse* of a and is customarily denoted by a^{-1}.

An inverse has the effect of reducing a given element, under the operation, to the identity element. In particular, since $e * e = e$, we may infer that $e^{-1} = e$.

It will be established shortly that, for a semigroup with identity, each element has at most one inverse relative to the unique identity element. (The reader might try to work out the proof for himself.) Thus, when dealing with such a system, there is no ambiguity of meaning in the symbol a^{-1} and, if it exists, we are free to speak of "the inverse of an element."

Example 2-15. Let S be the set of all ordered pairs of nonzero real numbers and $*$ the binary operation defined by

$$(a, b) * (c, d) = (ac, bd).$$

Then the system $(S, *)$ forms a (commutative) semigroup with identity, with the pair $(1, 1)$ serving as its identity element. For $(a, b) \in S$, we evidently have $(a, b)^{-1} = (1/a, 1/b)$, since

$$(a, b) * (1/a, 1/b) = \big(a(1/a), b(1/b)\big) = (1, 1).$$

Example 2-16. Let X be a nonempty set and S be the collection of all functions $f\colon X \to X$. It is easy to see that the system $(S, \circ)$ is a semigroup with identity, having as its identity the identity map i_X. A function $f \in S$ will possess an inverse relative to the operation of composition if and only if f is a one-to-one mapping from X onto itself; in this event, the inverse of f (under $\circ$) is the usual inverse function f^{-1}:

$$f \circ f^{-1} = i_X = f^{-1} \circ f.$$

Example 2-17. As a further illustration of these ideas, let us return to the semigroup $(P(X), \cup)$ of Example 2-13. In this case, just the empty set $\emptyset$ possesses an inverse; for if $A \in P(X)$, with $A \neq \emptyset$, there is no subset A^{-1} of X such that $A \cup A^{-1} = \emptyset$. Likewise, in regard to the semigroup $\big(P(X), \cap\big)$, the only member of $P(X)$ which has an inverse is the universal set X.

There is a mathematical system, known as a group, which displays most of the properties we have so far discussed.

Definition 2-10. The pair $(G, *)$ is a *group* if and only if $(G, *)$ is a semigroup with identity in which each element of G has an inverse.

While the above definition is perfectly acceptable, we prefer to rephrase it in the following more detailed form, merely as a matter of convenience.

Definition 2-11. A group is a pair $(G, *)$ consisting of a nonempty set G and a binary operation $*$ defined on G, satisfying the four requirements:

1) G is closed under the operation $*$,
2) the operation $*$ is associative,
3) G contains an identity element e for the operation $*$, and
4) each element a of G has an inverse $a^{-1} \in G$, relative to $*$.

This definition calls for several remarks. For one thing, the first of the requirements cited above could easily have been omitted, since any set is closed with respect to a binary operation defined on it. (We merely wish to emphasize that one must always check the closure condition.) Observe particularly that commutativity is not required in the definition. If it happens that the group operation satisfies this additional hypothesis, then $(G, *)$ is referred to as a *commutative* or *abelian group*. Let us also point out that it is possible to give a less redundant version of the group axioms from which the present axioms follow as logical consequences; for this, we refer the reader to Problem 14 at the end of the section.

When the group operation is clearly understood, one often identifies the group with its underlying set of elements and refers to the group as G rather than as $(G, *)$. For further simplicity, many authors drop the star notation and write ab in place of $a * b$. While we shall continue to adhere to the $a * b$ convention, we will nonetheless adopt some of the terminology of ordinary multiplication and talk of forming products, multiplying elements together, etc. At times, we shall also be somewhat imprecise and speak loosely about the elements of the group $(G, *)$, when we really mean the elements of the underlying set G; however, this should cause no particular confusion.

In order that the reader fully appreciate the generality of the concept of a group and at the same time gain some familiarity with this idea, we pause to offer a selection of examples. Further examples appear in the exercises.

Example 2-18. Let a be any nonzero real number and consider the set G of integral multiples of a:

$$G = \{na \mid n \in Z\}.$$

The pair $(G, +)$, where, as usual, $+$ indicates ordinary addition, forms a commutative group. In this case, the identity is $0 = 0a \in G$, while the inverse of an arbitrary element na of G is $-(na) = (-n)a \in G$.