A FIRST COURSE IN ABSTRACT ALGEBRA

third edition

John B. Fraleigh
Department of Mathematics
University of Rhode Island

ADDISON-WESLEY
PUBLISHING COMPANY
Reading, Massachusetts
Menlo Park, California • London
Amsterdam • Don Mills, Ontario
Sydney

one

Binary Operations

1.1 MOTIVATION

What constitutes the basic ingredient of algebra? The first contact of children with algebra comes when they are taught to add and multiply numbers. Let us try to analyze what really happens here.

Suppose that you are a visitor to a strange civilization in a strange world and you are observing one of the creatures of this world drilling a class of fellow creatures in the addition of numbers. Suppose also that you have not been told that the class is learning to add, but that you were just placed as an observer in the room where this was going on. You are asked to give a report on exactly what happens. The teacher makes noises that sound to you approximately like *gloop, poyt*. The class responds with *bimt*. The teacher then gives *ompt, gaft*, and the class responds with *poyt*. What are they doing? You cannot report that they are adding numbers, for you do not even know that the sounds are representing numbers. Of course, you do realize that there is communication going on. All you can say with any certainty is that these creatures know some rule, so that when certain pairs of things are designated in their language, one after another, like *gloop,*

poyt, they are able to agree on a response, *bimt*. This same procedure goes on in addition drill in our first grade classes where a teacher may say *four*, *seven*, and the class responds with *eleven*.

In our attempt to analyze addition and multiplication of numbers, we are thus led to the idea that addition is basically just a rule that people learn, enabling them to associate, with two numbers in a given order, some number as answer. Multiplication is also such a rule, but a different rule. Note finally that in playing this game with students, teachers have to be a little careful of what two things they give to the class. If a first grade teacher suddenly inserts *ten*, *sky*, the poor class will be very confused. The rule is only defined for pairs of things from some specified set.

1.2 DEFINITION AND PROPERTIES

As mathematicians, let us attempt to collect the core of these basic ideas in a useful definition. As we remarked in the introductory section, we do not attempt to define a set.

Definition A ***binary operation*** $*$ ***on a set*** is a rule that assigns to each ordered pair of elements of the set some element of the set.

The word *ordered* in this definition is very important, for it allows the possibility that the element assigned to the pair (a, b) may be different from the element assigned to the pair (b, a). Also, we were careful not to say that to each ordered pair of elements is assigned *another* or a *third* element, for we wish to permit cases such as occur in addition of numbers where (0, 2) has assigned to it the number 2.

For the first few sections we shall let $a * b$ be the element assigned to the pair (a, b) by $*$. If we have several different binary operations under simultaneous discussion, we shall use subscripts or superscripts on the $*$ to distinguish them. The most important method of describing a particular binary operation $*$ on a given set is to characterize the element $a * b$ assigned to each pair (a, b) by some property defined in terms of a and b.

Example 1.1 On $\mathbf{Z}^+$, define a binary operation $*$ by $a * b$ equals the smaller of a and b or the common value if $a = b$. Thus $2 * 11 = 2$; $15 * 10 = 10$; and $3 * 3 = 3$. ■

Example 1.2 On $\mathbf{Z}^+$, define a binary operation $*'$ by $a *' b = a$. Thus $2 *' 3 = 2$; $25 *' 10 = 25$; and $5 *' 5 = 5$. ■

Example 1.3 On $\mathbf{Z}^+$, define a binary operation $*''$ by $a *'' b = (a * b) + 2$, where $*$ is defined in Example 1.1. Thus $4 *'' 7 = 6$; $25 *'' 9 = 11$; and $6 *'' 6 = 8$. ■

It probably seems to you that these examples are of no importance, but consider for a moment. Suppose you go into a store to buy a nice, large, delicious chocolate bar. Suppose you see two identical bars side by side, the wrapper of one stamped 99¢ and the wrapper of the other stamped 94¢. Of course you pick up the one stamped 94¢. Your knowledge of which one you want depends on the fact that sometime in your life you learned the binary operation $*$ of Example 1.1. *It is a very important operation.* Likewise the binary operation $*'$ of Example 1.2 is clearly dependent on the ability to distinguish order. An often cited illustration of the importance of order is the mess that would result if you tried to put on your shoes first, and then your socks! Thus you should not be hasty about dismissing some binary operation as being of little significance. Of course, our usual operations of addition and multiplication of numbers have a practical importance well known to you.

Examples 1.1 and 1.2 were chosen to demonstrate that a binary operation may or may not depend on the order of the given pair. Thus in Example 1.1, $a * b = b * a$ for all $a, b \in \mathbf{Z}^+$, and in Example 1.2 this is not the case, for $5 *' 7 = 5$ but $7 *' 5 = 7$.

Now suppose one wishes to consider an expression of the form $a * b * c$. A binary operation $*$ enables you to combine only two elements, and here we have three. The obvious attempts to combine the three elements are to form either $(a * b) * c$ or $a * (b * c)$. With $*$ defined as in Example 1.1, $(2 * 5) * 9$ is computed by $2 * 5 = 2$ and then $2 * 9 = 2$. Likewise $2 * (5 * 9)$ is computed by $5 * 9 = 5$ and then $2 * 5 = 2$. Hence $(2 * 5) * 9 = 2 * (5 * 9)$, and it is easily seen that for this $*$,

$$(a * b) * c = a * (b * c),$$

so there is no ambiguity in writing $a * b * c$. But for $*''$ of Example 1.3,

$$(2 *'' 5) *'' 9 = 4 *'' 9 = 6,$$

while

$$2 *'' (5 *'' 9) = 2 *'' 7 = 4.$$

Thus $(a *'' b) *'' c$ need not equal $a *'' (b *'' c)$ and an expression $a *'' b *'' c$ may be ambiguous.

Definition A binary operation $*$ on a set S is ***commutative*** if (and only if) $a * b = b * a$ for all $a, b \in S$. The operation $*$ is ***associative*** if (and only if) $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

As was pointed out in the introductory section, it is customary in mathematics to omit the words *and only if* from a definition. Definitions are always understood to be if and only if statements. *Theorems are not always if and only if statements, and no such convention is ever used for theorems.*

It is not difficult to show that if $*$ is associative, then longer expressions such as $a * b * c * d$ are not ambiguous. Parentheses may be inserted in any fashion for purposes of computation; the final results of two such computations will be the same.

1.3 TABLES

For a finite set, a binary operation on the set can also be defined by means of a table. The next example shows how this will be done in this text.

Example 1.4 Table 1.1 defines the binary operation $*$ on $S = \{a, b, c\}$ by the rule:

(ith *entry on the left*) $*$ (jth *entry on the top*)
$=$ (*entry in the* ith *row and* jth *column of the table body*).

Thus $a * b = c$ and $b * a = a$, so $*$ is not commutative. ■

Table 1.1

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

The student can easily see that *a binary operation defined by a table is commutative if and only if the entries in the table are symmetric with respect to the diagonal that starts at the upper left corner of the table and terminates at the lower right corner.* We always assume that the elements of the set are listed across the top of a table in the same order as they are listed at the left.

Except for Example 1.4, our examples of binary operations have been defined on sets of numbers. It is important to realize that binary operations may be defined on any sets. Indeed, we shall be studying many important binary operations on sets whose elements are not numbers. Some of the examples to be given in a moment involve sets with *functions* as elements. It is assumed that the student has some familiarity with certain functions from calculus or other courses. We realize that you may not understand the concept of a function at the moment and we shall say more about it later. However, we are anxious to tie in the notions being introduced with the mathematics that you have already had.

1.4 SOME WORDS OF WARNING

The author knows from his own experience the chaos that may result if a student is given a set and asked to define some binary operation on it. Observe that in an attempt to define a binary operation $*$ on a set S you must be sure that

1. *exactly one element is assigned to each possible ordered pair of elements of S,*
2. *for each ordered pair of elements of S, the element assigned to it is again in S.*

Regarding condition 1, a student will often give a rule that assigns an element of S to "most" ordered pairs, but for a few pairs the rule determines no element. In this event, $*$ has **not been defined.** It may also happen that for some pairs, the rule could assign any of several elements of S, that is, there is ambiguity. In any case of ambiguity, $*$ is **not well defined.** If condition 2 is violated, then S is **not closed under** $*$.

We now give several illustrations of attempts to define binary operations on sets. Some of these attempts are worthless, as we point out. Since no comparison between operations will be made, we shall denote them all by $*$.

Example 1.5 On $\mathbf{Q}$, "define" $*$ by $a * b = a/b$. Here $*$ is *not defined*, for no rational number is assigned by this rule to the pair $(2, 0)$. ■

Example 1.6 On $\mathbf{Q}^+$, define $*$ by $a * b = a/b$. Here both conditions 1 and 2 are satisfied and $*$ is a binary operation on $\mathbf{Q}^+$. ■

Example 1.7 On $\mathbf{Z}^+$, "define" $*$ by $a * b = a/b$. Here condition 2 is violated, for $1 * 3$ is not in $\mathbf{Z}^+$. Thus $*$ is not a binary operation on $\mathbf{Z}^+$, since $\mathbf{Z}^+$ is *not closed under* $*$. ■

Example 1.8 Let S be the set of all real-valued functions defined for all real numbers. Define $*$ to give the usual sum of two functions, that is, $f * g = h$, where $h(x) = f(x) + g(x)$ for $f, g \in S$ and $x \in \mathbf{R}$. This definition of $*$ satisfies conditions 1 and 2 and gives a binary operation on S. ■

Example 1.9 Let S be as in Example 1.8 and define $*$ to give the usual product of two functions, that is, $f * g = h$, where $h(x) = f(x)g(x)$. Again this definition is a good one and gives a binary operation on S. ■

Example 1.10 Let S be as in Example 1.8 and "define" $*$ to give the usual quotient of f by g, that is, $f * g = h$, where $h(x) = f(x)/g(x)$. Here condition 2 is violated, for the functions in S were to be defined for *all* real numbers, and for some $g \in S$, $g(x)$ will be zero for some values of x in $\mathbf{R}$ and $h(x)$ would not be defined at those numbers in $\mathbf{R}$. For example, if $f(x) = \cos x$ and $g(x) = x^2$, then $h(0)$ is undefined, so $h \notin S$. ■

Example 1.11 Let S be as in Example 1.8 and "define" $*$ by $f * g = h$, where h is the function greater than both f and g. This "definition" is completely worthless. In the first place, we have not defined what it means for one function to be greater than another. Even if we had, any sensible definition would result in there being many functions greater than both f and g, and $*$ would still be *not well defined.* ■

Example 1.12 Let S be a set consisting of twenty people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the tallest person among the twenty in S. This is a perfectly good binary operation on the set, although not a particularly interesting one. ■

Example 1.13 Let S be as in Example 1.12 and "define" $*$ by $a * b = c$, where c is the shortest person in S who is taller than both a and b. This $*$ is *not defined*, since if either a or b is the tallest person in the set, $a * b$ is not determined. ■

Exercises

1.1 Let the binary operation $*$ be defined on $S = \{a, b, c, d, e\}$ by means of Table 1.2.

a) Compute $b * d$, $c * c$ and $[(a * c) * e] * a$ from the table.

b) Compute $(a * b) * c$ and $a * (b * c)$ from the table. Can you say on the basis of this computation whether $*$ is associative?

c) Compute $(b * d) * c$ and $b * (d * c)$ from the table. Can you say on the basis of this computation whether $*$ is associative?

d) Is $*$ commutative? Why?

Table 1.2

$*$	a	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

1.2 Complete Table 1.3 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d\}$.

Table 1.3

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

1.3 Table 1.4 may be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries.

Table 1.4

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

1.4 Determine whether each of the definitions of $*$ given below does give a binary operation on the given set. In the event that $*$ is not a binary operation, state whether condition 1, condition 2, or both of these conditions from Section 1.4 are violated.

a) On $\mathbf{Z}^+$, define $*$ by $a * b = a - b$.

b) On $\mathbf{Z}^+$, define $*$ by $a * b = a^b$.

c) On $\mathbf{R}$, define $*$ by $a * b = a - b$.

d) On $\mathbf{Z}^+$, define $*$ by $a * b = c$, where c is the smallest integer greater than both a and b.

e) On $\mathbf{Z}^+$, define $*$ by $a * b = c$, where c is at least 5 more than $a + b$.

f) On $\mathbf{Z}^+$, define $*$ by $a * b = c$, where c is the largest integer less than the product of a and b.

†**1.5** Prove that if $*$ is an associative and commutative binary operation on a set S, then

$$(a * b) * (c * d) = [(d * c) * a] * b$$

for all $a, b, c, d \in S$. Assume the associative law only for triples as in the definition, that is, assume only

$$(x * y) * z = x * (y * z)$$

for all $x, y, z \in S$.

1.6 For each binary operation $*$ defined, determine whether $*$ is commutative and whether $*$ is associative.

a) On $\mathbf{Z}$, define $*$ by $a * b = a - b$.

b) On $\mathbf{Q}$, define $*$ by $a * b = ab + 1$.

c) On $\mathbf{Q}$, define $*$ by $a * b = ab/2$.

d) On $\mathbf{Z}^+$, define $*$ by $a * b = 2^{ab}$.

e) On $\mathbf{Z}^+$, define $*$ by $a * b = a^b$.

1.7 Mark each of the following true or false.

___ a) If $*$ is any binary operation on any set S, then $a * a = a$ for all $a \in S$.

___ b) If $*$ is any commutative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

___ c) If $*$ is any associative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

— d) The only binary operations of any importance are those defined on sets of numbers.

— e) A binary operation $*$ on a set S is commutative if there exist $a, b \in S$ such that $a * b = b * a$.

— f) Every binary operation defined on a set having exactly one element is both commutative and associative.

— g) A binary operation on a set S assigns at least one element of S to each ordered pair of elements of S.

— h) A binary operation on a set S assigns at most one element of S to each ordered pair of elements of S.

— i) A binary operation on a set S assigns exactly one element of S to each ordered pair of elements of S.

— j) A binary operation on a set S may assign more than one element of S to some ordered pair of elements of S.

1.8 Give a set different from any of those described in the examples of the text and not a set of numbers. Define two different binary operations $*$ and $*'$ on this set. Be sure that your set is *well defined.*

1.9 Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.

1.10 How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements?

1.11 Observe that the binary operations $*$ and $*'$ on the set $\{a, b\}$ given by the tables

$*$	a	b
a	a	a
b	a	b

and

$*'$	a	b
a	a	b
b	b	b

provide the *same type of algebraic structure* on $\{a, b\}$, in the sense that if the table for $*'$ is rewritten

$*'$	b	a
b	b	b
a	b	a

this table for $*'$ looks just like that for $*$ with the roles of a and b interchanged.

a) Try to give a natural definition of a concept of two binary operations $*$ and $*'$ on the same set giving *algebraic structures of the same type,* which generalizes this observation.

b) How many different types of algebraic structures are given by the 16 possible different binary operations on a set of 2 elements?

two

Groups

2.1 MOTIVATION

Let us continue the analysis of our past experience with algebra. Once we had mastered the computational problems of addition and multiplication of numbers, we were ready to apply these binary operations to the solution of problems. Often problems lead to equations involving some unknown number x, which is to be determined. The simplest equations are the linear ones of the forms $a + x = b$ for the operation of addition, and $ax = b$ for multiplication. The additive linear equation always has a numerical solution, and so has the multiplicative one, provided $a \neq 0$. Indeed, the need for solutions of additive linear equations such as $5 + x = 2$ is a very good motivation for the negative numbers. Similarly, the need for rational numbers is shown by equations such as $2x = 3$, and the need for the complex number i is shown by the equation $x^2 = -1$.

It is desirable for us to be able to solve linear equations involving our binary operations. This is not possible for every binary operation, however. For example, the equation $a * x = a$ has no solution in $S = \{a, b, c\}$ for the

operation $*$ of Example 1.4. Let us see just what properties of the operation of addition on the integers $\mathbf{Z}$ enable us to solve the equation $5 + x = 2$ in $\mathbf{Z}$. We must not refer to subtraction, for we are concerned with the solution phrased in terms of a single binary operation, in this case addition. The steps in the solution are as follows:

$$\begin{aligned} 5 + x &= 2, && \text{given,} \\ -5 + (5 + x) &= -5 + 2, && \text{adding } -5, \\ (-5 + 5) + x &= -5 + 2, && \text{associative law,} \\ 0 + x &= -5 + 2, && \text{computing } -5 + 5, \\ x &= -5 + 2, && \text{property of 0,} \\ x &= -3, && \text{computing } -5 + 2. \end{aligned}$$

Strictly speaking, we have not shown here that -3 is a solution, but rather that it is the only possibility for a solution. To show that -3 is a solution, one merely computes $5 + (-3)$. A similar analysis could be made for the equation $2x = 3$ in the rational numbers:

$$\begin{aligned} 2x &= 3, && \text{given,} \\ \tfrac{1}{2}(2x) &= \tfrac{1}{2}(3), && \text{multiplying by } \tfrac{1}{2}, \\ (\tfrac{1}{2} \cdot 2)x &= \tfrac{1}{2}3, && \text{associative law,} \\ 1 \cdot x &= \tfrac{1}{2}3, && \text{computing } \tfrac{1}{2}2, \\ x &= \tfrac{1}{2}3, && \text{property of 1,} \\ x &= \tfrac{3}{2}, && \text{computing } \tfrac{1}{2}3. \end{aligned}$$

Let us see what properties a set S and a binary operation $*$ on S would have to have to permit imitation of this procedure for an equation $a * x = b$ for $a, b \in S$. Basic to the procedure is the existence of an element e in S with the property that $e * x = x$ for all $x \in S$. For our additive example, 0 played the role of e, and 1 played the role for our multiplicative example. Then we need an element a' in S that has the property that $a' * a = e$. For our additive example, -5 played the role of a', and $\frac{1}{2}$ played the role for our multiplicative example. Finally we need the associative law. The remainder is just computation. The student will easily see that in order to solve the equation $x * a = b$ (remember that $a * x$ need not equal $x * a$) one would like to have an element e in S such that $x * e = x$ for all $x \in S$ and an a' in S such that $a * a' = e$. With all of these properties of $*$ on S, we could be sure of being able to solve linear equations. These are precisely the properties of a *group*.

2.2 DEFINITION AND ELEMENTARY PROPERTIES

Definition A ***group*** $\langle G, * \rangle$ is a set G, together with a binary operation $*$ on G, such that the following axioms are satisfied:

$\mathscr{G}_1$. The binary operation $*$ is associative.

$\mathscr{G}_2$. There is an element e in G such that $e * x = x * e = x$ for all $x \in G$. (This element e is an ***identity element*** for $*$ on G.)[†]

$\mathscr{G}_3$. For each a in G, there is an element a' in G with the property that $a' * a = a * a' = e$. (The element a' is an ***inverse of a with respect to $*$***.)

Many books have another axiom for a group, namely that G is **closed under the operation** $*$, that is $(a * b) \in G$ for all $a, b \in G$. For us, this is a consequence of our *definition* of a binary operation on G.

We should point out right now that we are going to be sloppy in notation. Observe that a group is not just a set G. Rather, a group $\langle G, * \rangle$ is made up of two entities, the set G and the binary operation $*$ on G. There are *two* ingredients involved. Denoting the group by the single set symbol G is logically incorrect. Nevertheless, as you get further into the theory, the logical extensions of the notation $\langle G, * \rangle$ become so unwieldy as to actually make the exposition hard to read. At some point, all authors give up and become sloppy, denoting the group by the single letter G. We choose to recognize this and be sloppy from the start. We emphasize, however, that when you are speaking of a specific group G, you must make it clear what the group operation on G is to be, since a set could conceivably have a variety of binary operations defined on it, all giving different groups. We shall sometimes resort to the notation $\langle G, * \rangle$ for reasons of clarity in our discussions.

Theorem 2.1 *If G is a group with binary operation $*$, then the **left and right cancellation laws** hold in G, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for $a, b, c \in G$.*

Proof. Suppose $a * b = a * c$. Then by $\mathscr{G}_3$, there exists a', and

$$a' * (a * b) = a' * (a * c).$$

By the associative law,

$$(a' * a) * b = (a' * a) * c.$$

By the definition of a' in $\mathscr{G}_3$, $a' * a = e$, so

$$e * b = e * c.$$

[†] Remember that boldface type indicates that a term is being defined. See the last paragraph of Section 0.1. Thus an **identity element** for a binary operation $*$ on a set S is any element e satisfying $e * x = x * e = x$ for all $x \in S$.

By the definition of e in $\mathscr{G}_2$,

$$b = c.$$

Similarly, from $b * a = c * a$ one can deduce that $b = c$ upon multiplication on the right by a' and use of the axioms for a group. ■

Note how we had to use the definition of a group to prove this theorem.

Theorem 2.2 *If G is a group with binary operation $*$, and if a and b are any elements of G, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions in G.*

Proof. Note that

$$\begin{aligned} a * (a' * b) &= (a * a') * b, && \text{associative law,} \\ &= e * b, && \text{definition of } a', \\ &= b, && \text{property of } e. \end{aligned}$$

Thus $x = a' * b$ is a solution of $a * x = b$. In a similar fashion, $y = b * a'$ is a solution of $y * a = b$.

To show that y is unique, suppose that $y * a = b$ and $y_1 * a = b$. Then $y * a = y_1 * a$ and, by Theorem 2.1, $y = y_1$. The uniqueness of x follows similarly. ■

Of course, to prove the uniqueness in the last theorem we could have followed the procedure we used in motivating the definition of a group, showing that if $a * x = b$, then $x = a' * b$. However, we chose to illustrate the standard way to prove an object is unique. Suppose you have two such objects, and then prove they must be the same. Note that the solutions $x = a' * b$ and $y = b * a'$ need not be the same unless $*$ is commutative.

Definition A group G is ***abelian*** if its binary operation $*$ is commutative.

Let us give some examples of some sets with binary operations that give groups and also of some that do not give groups.

Example 2.1 The set $\mathbf{Z}^+$ with operation $+$ is *not* a group. There is no identity element for $+$ in $\mathbf{Z}^+$. ■

Example 2.2 The set of all nonnegative integers (including 0) with operation $+$ is still *not* a group. There is an identity element 0, but no inverse for 2. ■

Example 2.3 The set $\mathbf{Z}$ with operation $+$ *is* a group. All conditions of the definition are satisfied. The group is abelian. ■

Example 2.4 The set $\mathbf{Z}^+$ with operation multiplication is *not* a group. There is an identity 1, but no inverse of 3. ■

Example 2.5 The set $\mathbf{Q}^+$ with operation multiplication *is* a group. All conditions of the definition are satisfied. The group is abelian. ■

Example 2.6 Define $*$ on $\mathbf{Q}^+$ by $a * b = ab/2$. Then

$$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4},$$

and likewise

$$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{4}.$$

Thus $*$ is associative. Clearly,

$$2 * a = a * 2 = a$$

for all $a \in \mathbf{Q}^+$, so 2 is an identity element for $*$. Finally,

$$a * \frac{4}{a} = \frac{4}{a} * a = 2,$$

so $a' = 4/a$ is an inverse for a. Hence $\mathbf{Q}^+$ with the operation $*$ is a group. ■

There is one other result about groups we would like to prove in this section.

Theorem 2.3 *In a group G with operation $*$, there is only one identity e such that*

$$e * x = x * e = x$$

for all $x \in G$. Likewise for each $a \in G$, there is only one element a' such that

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

In summary, the identity and inverses are unique in a group.

Proof. Suppose $e * x = x * e = x$ and also $e_1 * x = x * e_1 = x$ for all $x \in G$. We let e and e_1 compete. Now regarding e as identity, $e * e_1 = e_1$. But regarding e_1 as identify, $e * e_1 = e$. Thus

$$e_1 = e * e_1 = e,$$

and the identify of a group is unique.

Now suppose $a' * a = a * a' = e$ and $a'' * a = a * a'' = e$. Then

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

and, by Theorem 2.1,

$$a'' = a',$$

so the inverse of a in a group is unique. ■

For the student's information, we remark that algebraic structures consisting of sets with binary operations for which not all of the group axioms

hold have also been studied quite extensively. Of these weaker structures, the **semigroup,** a set with an associative binary operation, has perhaps had the most attention. Recently, nonassociative structures have also been studied.

Finally, it is possible to give formally weaker axioms for a group $\langle G, * \rangle$, namely:

1. The binary operation $*$ on G is associative.
2. There exists a **left identity** e in G such that $e * x = x$ for all $x \in G$.
3. For each $a \in G$, there exists a **left inverse** a' in G such that $a' * a = e$.

From this *one-sided definition,* one can prove that the left identity is also a right identity and a left inverse is also a right inverse for the same element. Thus these axioms should not be called weaker, since they result in exactly the same structures being called groups. It is conceivable that it might be easier in some cases to check these *left axioms* than to check our *two-sided axioms.* Of course, by symmetry it is clear that there are also *right axioms* for a group.

2.3 FINITE GROUPS AND GROUP TABLES

Thus far all our examples have been of infinite groups, that is, groups where the set G has an infinite number of elements. The student may wonder whether there can be a group structure on some finite set. The answer is yes, and indeed such structures are very important.

Since a group has to have at least one element, namely the identity, a smallest set that might give rise to a group is a one-element set $\{e\}$. The only possible binary operation $*$ on $\{e\}$ is defined by $e * e = e$. The student can check at once that the three group axioms hold. The identity element is always its own inverse in every group.

Let us try to put a group structure on a set of two elements. Since one of the elements must play the role of identity element, we may as well let the set be $\{e, a\}$. Let us attempt to find a table for a binary operation $*$ on $\{e, a\}$ that gives a group structure on $\{e, a\}$. When giving a table for a group operation, we shall always list the elements in the same order across the top as down the left side, with the identity listed first, as in the following table.

$*$	e	a
e		
a		

Since e is to be the identity, so

$$e * x = x * e = x$$

for all $x \in \{e, a\}$, we are forced to fill in the table as shown below, if $*$ is to give a group.

$*$	e	a
e	e	a
a	a	

Also, a must have an inverse a' such that

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

In our case, a' must be either e or a. Since $a' = e$ obviously does not work, we must have $a' = a$, so we have to complete the table as below.

$*$	e	a
e	e	a
a	a	e

All the group axioms are now satisfied except possibly the associative law. We will see later in a more general situation that this operation $*$ is associative. You are asked either to accept it here or to go through the tedious chore of checking various cases.

With these examples as background, we should be able to list some necessary conditions that a table giving a binary operation on a finite set must satisfy for the operation to give a group structure on the set. There must be one element of the set, which we may as well denote by e, that acts as identity. The condition $e * x = x$ means that the row of the table opposite e at the extreme left must contain exactly the elements appearing across the very top of the table in the same order. Similarly, the condition $x * e = x$ means that the column of the table under e at the very top must contain exactly the elements appearing at the extreme left in the same order. The fact that every element a has a right and a left inverse means that in the row opposite a at the extreme left, the element e must appear, and in the column under a at the very top, the e must appear. Thus e must appear in each row and in each column. We can do even better than this, however. By Theorem 2.2, not only the equations $a * x = e$ and $y * a = e$ have unique solutions, but also the equations $a * x = b$ and $y * a = b$. By a similar argument, this means that *each element b of the group must appear once and only once in each row and column of the table.*

Suppose conversely that a table for a binary operation on a finite set is such that there is an element acting as identity and that in each row and each column each element of the set appears exactly once. Then it can be seen that the structure is a group structure if and only if the associative law holds. If a binary operation $*$ is given by a table, the associative law is usually messy to check. If the operation $*$ is defined by some characterizing property of $a * b$, the associative law is often easy to check. Fortunately this second case turns out to be the one usually encountered.

We saw that there was essentially only one group of two elements in the sense that if the elements are denoted by e and a with the identity e appearing first, the table must be as follows.

$*$	e	a
e	e	a
a	a	e

Suppose that a set has three elements. As before, we may as well let the set be $\{e, a, b\}$. For e to be an identity, a binary operation $*$ on this set has to have a table of the form shown in Table 2.1. This leaves four places to be filled in. The student can quickly see that Table 2.1 must be completed as shown in Table 2.2 if each row and each column are to contain each element exactly once. Again you are asked to accept without proof the fact that this operation is associative, so that $*$ does give a group structure on $G = \{e, a, b\}$.

Table 2.1

$*$	e	a	b
e	e	a	b
a	a		
b	b		

Table 2.2

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Now suppose that G' is any other group of three elements and imagine a table for G' with identity element appearing first. Since our filling out of the table for $G = \{e, a, b\}$ could be done in only one way, we see that if we take the table for G' and rename the identity e, the next element listed a, and the last element b, the resulting table for G' must be the same as the one we had for G. In other words, the *structural* features are the same for the two groups, and one group can be made to look exactly like the other by a renaming of the elements. *Thus any two groups of three elements are structurally the same.* This is our introduction to the concept of *isomorphism.* The groups G and G' are *isomorphic.* This concept is sometimes a bit sticky for the student. We say no more about it now, but we shall make it more precise later.

Exercises

2.1 For each binary operation $*$ defined on a set below, say whether $*$ gives a group structure on the set. If no group results, give the first axiom in the order $\mathscr{G}_1, \mathscr{G}_2, \mathscr{G}_3$ from Section 2.2 that does not hold.

a) Define $*$ on $\mathbf{Z}$ by $a * b = ab$.

b) Define $*$ on $\mathbf{Z}$ by $a * b = a - b$.

c) Define $*$ on $\mathbf{R}^+$ by $a * b = ab$.

d) Define $*$ on $\mathbf{Q}$ by $a * b = ab$.

e) Define $*$ on the set of all nonzero real numbers by $a * b = ab$.

f) Define $*$ on $\mathbf{C}$ by $a * b = a + b$.

2.2 Consider our axioms $\mathscr{G}_1, \mathscr{G}_2$, and $\mathscr{G}_3$ for a group. We gave them in the order $\mathscr{G}_1\mathscr{G}_2\mathscr{G}_3$. Conceivable other orders to state the axioms are $\mathscr{G}_1\mathscr{G}_3\mathscr{G}_2$, $\mathscr{G}_2\mathscr{G}_1\mathscr{G}_3$, $\mathscr{G}_2\mathscr{G}_3\mathscr{G}_1$, $\mathscr{G}_3\mathscr{G}_1\mathscr{G}_2$, and $\mathscr{G}_3\mathscr{G}_2\mathscr{G}_1$. Of these six possible orders, exactly three are acceptable for a definition. Which orders aren't acceptable, and why? (Remember this. Most instructors ask the student to define a group on at least one test.)

2.3 Show by computation and by Theorem 2.3 that if G is a group with binary operation $*$, then for all $a, b \in G$, we have $(a * b)' = b' * a'$. What is a similar expression for $(a * b' * c)'$?

2.4 Proceed as follows to show that there are two possible different types of group structures on a set of four elements. Let the set be $\{e, a, b, c\}$, with e the identity element for the group operation. A group table would then have to start in the manner shown in Table 2.3. The square indicated by the question mark can't be filled in with a. It must be filled in either with the identity e or with an element different from both e and a. In this latter case, it is no loss of generality to assume that this element is b. If this square is filled in with e, the table can then be completed in two ways to give a group. Find these two tables. (You need not check the associative law.) If this square is filled in with b, then the table can only be completed in one way to give a group. Find this table. (Again you need not check the associative law.) Of the three tables you now have, two give the same type of group structure. Determine which two tables these are, and show how the elements in one table would have to be renamed for these two tables to be the same. Are all groups of 4 elements commutative?

Table 2.3

$*$	e	a	b	c
e	e	a	b	c
a	a	?		
b	b			
c	c			

†**2.5** Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.

2.6 Mark each of the following true or false.

___ a) A group may have more than one identity element.

___ b) Any two groups of three elements are isomorphic.

___ c) In a group, each linear equation has a solution.

___ d) The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.

___ e) Any definition a person gives for a group is correct provided that everything that is a group by that person's definition is also a group by the definition in the text.

___ f) Any definition a person gives for a group is correct provided he or she can show that everything that satisfies the definition satisfies the one in the text and conversely.

___ g) Every finite group of at most three elements is abelian.

___ h) An equation of the form $a * x * b = c$ always has a unique solution in a group.

___ i) The empty set can be considered a group.

___ j) The text has as yet given no examples of groups that are not abelian.

2.7 Give a table for a binary operation on the set $\{e, a, b\}$ of three elements satisfying axioms $\mathscr{G}_2$ and $\mathscr{G}_3$ for a group but not axiom $\mathscr{G}_1$.

2.8 According to Exercise 1.9, there are 16 possible binary operations on a set of 2 elements. How many of these give a structure of a group? How many of the 19,683 possible binary operations on a set of 3 elements give a group structure?

2.9 Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab.$$

a) Show that $*$ gives a binary operation on S.

b) Show that $\langle S, * \rangle$ is a group.

c) Find the solution of the equation $2 * x * 3 = 7$ in S.

2.10 Let $\mathbf{R}^*$ be the set of all real numbers except 0. Define $*$ on $\mathbf{R}^*$ by $a * b = |a|b$.

a) Show that $*$ gives an associative binary operation on $\mathbf{R}^*$.

b) Show that there is a left identity for $*$ and a right inverse for each element in $\mathbf{R}^*$.

c) Is $\mathbf{R}^*$ with this binary operation a group?

d) Explain the significance of this exercise.

2.11 If $*$ is a binary operation on a set S, an element x of S is an **idempotent for** $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

2.12 Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian. [*Hint:* Consider $(ab)^2$.]

2.13 Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given at the end of Section 2.2, is a group.

2.14 Prove that a nonempty set G, together with an associative binary operation $*$ on G such that equations

$$a * x = b \text{ and } y * a = b \text{ have solutions in } G \text{ for all } a, b \in G,$$

is a group [*Hint:* Use Exercise 2.13.]

2.15 The following "definitions" of a group are taken verbatim, including spelling and punctuation, from students' examination papers. Criticize them.

a) A group G is a set of elements together with a binary operation $*$ such that the following conditions are satisfied

$*$ is associative

There exists $e \in G$ such that

$$e * x = x * e = x = \text{identity.}$$

For every $a \in G$ there exists an a' (inverse) such that

$$a \cdot a' = a' \cdot a = e$$

b) A group is a set G such that

The operation on G is associative.

there is an identity element (e) in G.

for every $a \in G$, there is an a' (inverse for each element)

c) A group is a set with a binary operation such

the binary operation is defined

an inverse exists

an identity element exists

d) A set G is called a group over the binery operation $*$ such that for all $a, b \in G$

Binary operation $*$ is associative under addition

there exist an element $\{e\}$ such that

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

Fore every element a there exists an element a' such that

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