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 with the operation of multiplication:

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

We can now 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 with $a = 5$, -5 played the role of a', and $\frac{1}{2}$ played the role for our multiplicative example with $a = 2$. Finally we need the associative law. The remainder is just computation. A similar analysis shows that in order to solve the equation $x * a = b$ (remember that $a * x$ need not equal $x * a$), we 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. Thus we need an associative binary structure $\langle S, *\rangle$ with an identity element e such that for each $a \in S$, there exists $a' \in S$ such that $a * a' = a' * a = e$. This is precisely the notion of a *group*, which we now define.

Definition and Examples

Rather than describe a *group* using terms defined in Sections 2 and 3 as we did at the end of the preceding paragraph, we give a self-contained definition. This enables a person who picks up this text to discover what a group is without having to look up more terms.

4.1 Definition A **group** $\langle G, *\rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

$\mathscr{G}_1$: For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c). \quad \textbf{associativity of } *$$

$\mathscr{G}_2$: There is an element e in G such that for all $x \in G$,

$$e * x = x * e = x. \quad \textbf{identity element } e \textbf{ for } *$$

$\mathscr{G}_3$: Corresponding to each $a \in G$, there is an element a' in G such that

$$a * a' = a' * a = e. \quad \textbf{inverse } a' \text{ of } a$$ ■

4.2 Example We easily see that $\langle U, \cdot\rangle$ and $\langle U_n, \cdot\rangle$ are groups. Multiplication of complex numbers is associative and both U and U_n contain 1, which is an identity for multiplication. For $e^{i\theta} \in U$, the computation

$$e^{i\theta} \cdot e^{i(2\pi - \theta)} = e^{2\pi i} = 1$$

shows that every element of U has an inverse. For $z \in U_n$, the computation

$$z \cdot z^{n-1} = z^n = 1$$

shows that every element of U_n has an inverse. Thus $\langle U, \cdot\rangle$ and $\langle U_n, \cdot\rangle$ are groups. Because $\langle \mathbb{R}_c, +_c\rangle$ is isomorphic to $\langle U, \cdot\rangle$, we see that $\langle \mathbb{R}_c, +_c\rangle$ is a group for all $c \in \mathbb{R}^+$. Similarly, the fact that $\langle \mathbb{Z}_n, +_n\rangle$ is isomorphic to $\langle U_n, \cdot\rangle$ shows that $\langle \mathbb{Z}_n, +_n\rangle$ is a group for all $n \in \mathbb{Z}^+$. ▲

We point out now that we will sometimes be sloppy in notation. Rather than use the binary structure notation $\langle G, *\rangle$ constantly, we often refer to a group G, with the understanding that there is of course a binary operation on the set G. In the event that clarity demands that we specify an operation $*$ on G, we use the phrase "the group G

▩ HISTORICAL NOTE

There are three historical roots of the development of abstract group theory evident in the mathematical literature of the nineteenth century: the theory of algebraic equations, number theory, and geometry. All three of these areas used group-theoretic methods of reasoning, although the methods were considerably more explicit in the first area than in the other two.

One of the central themes of geometry in the nineteenth century was the search for invariants under various types of geometric transformations. Gradually attention became focused on the transformations themselves, which in many cases can be *thought of as elements of groups.*

In number theory, already in the eighteenth century Leonhard Euler had considered the remainders on division of powers a^n by a fixed prime p. These remainders have "group" properties. Similarly, Carl F. Gauss, in his *Disquisitiones Arithmeticae* (1800), dealt extensively with quadratic forms $ax^2 + 2bxy + cy^2$, and in particular showed that equivalence classes of these forms under composition possessed what amounted to group properties.

Finally, the theory of algebraic equations provided the most explicit prefiguring of the group concept. Joseph-Louis Lagrange (1736–1813) in fact initiated the study of permutations of the roots of an equation as a tool for solving it. These permutations, of course, were ultimately considered as elements of a group.

It was Walter von Dyck (1856–1934) and Heinrich Weber (1842–1913) who in 1882 were able independently to combine the three historical roots and give clear definitions of the notion of an abstract group.

under $*$." For example, we may refer to the *groups* $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ *under addition* rather than write the more tedious $\langle\mathbb{Z}, +\rangle$, $\langle\mathbb{Q}, +\rangle$, and $\langle\mathbb{R}, +\rangle$. However, we feel free to refer to the group $\mathbb{Z}_8$ without specifying the operation.

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

■ Historical Note

Commutative groups are called *abelian* in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829). Abel was interested in the question of solvability of polynomial equations. In a paper written in 1828, he proved that if all the roots of such an equation can be expressed as rational functions $f, g, \ldots, h$ of one of them, say x, and if for any two of these roots, $f(x)$ and $g(x)$, the relation $f(g(x)) = g(f(x))$ always holds, then the equation is solvable by radicals. Abel showed that each of these functions in fact permutes the roots of the equation; hence, these functions are elements of the group of permutations of the roots. It was this property of commutativity in these permutation groups associated with solvable equations that led Camille Jordan in his 1870 treatise on algebra to name such groups *abelian;* the name since then has been applied to commutative groups in general.

Abel was attracted to mathematics as a teenager and soon surpassed all his teachers in Norway. He finally received a government travel grant to study elsewhere in 1825 and proceeded to Berlin, where he befriended August Crelle, the founder of the most influential German mathematical journal. Abel contributed numerous papers to Crelle's *Journal* during the next several years, including many in the field of elliptic functions, whose theory he created virtually single-handedly. Abel returned to Norway in 1827 with no position and an abundance of debts. He nevertheless continued to write brilliant papers, but died of tuberculosis at the age of 26, two days before Crelle succeeded in finding a university position for him in Berlin.

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

4.4 Example The set $\mathbb{Z}^+$ under addition is *not* a group. There is no identity element for $+$ in $\mathbb{Z}^+$. ▲

4.5 Example The set of all nonnegative integers (including 0) under addition is still *not* a group. There is an identity element 0, but no inverse for 2. ▲

4.6 Example The familiar additive properties of integers and of rational, real, and complex numbers show that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups. ▲

4.7 Example The set $\mathbb{Z}^+$ under multiplication is *not* a group. There is an identity 1, but no inverse of 3. ▲

4.8 Example The familiar multiplicative properties of rational, real, and complex numbers show that the sets $\mathbb{Q}^+$ and $\mathbb{R}^+$ of positive numbers and the sets $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ of nonzero numbers under multiplication are abelian groups. ▲

4.9 Example The set of all real-valued functions with domain $\mathbb{R}$ under function addition is a group. This group is abelian. ▲

4.10 Example **(Linear Algebra)** Those who have studied vector spaces should note that the axioms for a vector space V pertaining just to vector addition can be summarized by asserting that V under vector addition is an abelian group. ▲

4.11 Example The set $M_{m \times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a group. The $m \times n$ matrix with all entries 0 is the identity matrix. This group is abelian. ▲

4.12 Example The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is *not* a group. The $n \times n$ matrix with all entries 0 has no inverse. ▲

4.13 Example Show that the subset S of $M_n(\mathbb{R})$ consisting of all *invertible* $n \times n$ matrices under matrix multiplication is a group.

Solution We start by showing that S is closed under matrix multiplication. Let A and B be in S, so that both A^{-1} and B^{-1} exist and $AA^{-1} = BB^{-1} = I_n$. Then

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = I_n,$$

so that AB is invertible and consequently is also in S.

Since matrix multiplication is associative and I_n acts as the identity element, and since each element of S has an inverse by definition of S, we see that S is indeed a group. This group is *not* commutative. It is our first example of a *nonabelian group.* ▲

The group of invertible $n \times n$ matrices described in the preceding example is of fundamental importance in linear algebra. It is the **general linear group of degree** n, and is usually denoted by $GL(n, \mathbb{R})$. Those of you who have studied linear algebra know that a matrix A in $GL(n, \mathbb{R})$ gives rise to an invertible linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$, defined by $T(\mathbf{x}) = A\mathbf{x}$, and that conversely, every invertible linear transformation of $\mathbb{R}^n$ into itself is defined in this fashion by some matrix in $GL(n, \mathbb{R})$. Also, matrix multiplication corresponds to composition of linear transformations. Thus all invertible linear transformations of $\mathbb{R}^n$ into itself form a group under function composition; this group is usually denoted by $GL(\mathbb{R}^n)$. Of course, $GL(n, \mathbb{R}) \simeq GL(\mathbb{R}^n)$.

4.14 Example Let $*$ be defined on $\mathbb{Q}^+$ 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. Computation shows that

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

for all $a \in \mathbb{Q}^+$, 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 $\mathbb{Q}^+$ with the operation $*$ is a group. ▲

Elementary Properties of Groups

As we proceed to prove our first theorem about groups, we must use Definition 4.1, which is the only thing we know about groups at the moment. The proof of a second theorem can employ both Definition 4.1 and the first theorem; the proof of a third theorem can use the definition and the first two theorems, and so on.

Our first theorem will establish cancellation laws. In real arithmetic, we know that $2a = 2b$ implies that $a = b$. We need only divide both sides of the equation $2a = 2b$ by 2, or equivalently, multiply both sides by $\frac{1}{2}$, which is the multiplicative inverse of 2. We parrot this proof to establish cancellation laws for any group. Note that we will also use the associative law.

4.15 Theorem 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 all $a, b, c \in G$.

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

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

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. ◆

Our next proof can make use of Theorem 4.15. We show that a "linear equation" in a group has a *unique* solution. Recall that we chose our group properties to allow us to find solutions of such equations.

4.16 Theorem 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 x and y in G.

Proof First we show the existence of *at least* one solution by just computing that $a' * b$ is a solution of $a * x = b$. 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 uniqueness of y, we use the standard method of assuming that we have two solutions, y_1 and y_2, so that $y_1 * a = b$ and $y_2 * a = b$. Then $y_1 * a = y_2 * a$, and by Theorem 4.15, $y_1 = y_2$. 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; namely, 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.

Because a group is a special type of binary structure, we know from Theorem 3.13 that the identity e in a group is unique. We state this again as part of the next theorem for easy reference.

4.17 Theorem In a group G with binary operation $*$, there is only one element e in G such that

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

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

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

In summary, the identity element and inverse of each element are unique in a group.

Proof Theorem 3.13 shows that an identity element for any binary structure is unique. No use of the group axioms was required to show this.

Turning to the uniqueness of an inverse, suppose that $a \in G$ has inverses a' and a'' so that $a' * a = a * a' = e$ and $a'' * a = a * a'' = e$. Then

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

and, by Theorem 4.15,

$$a'' = a',$$

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

Note that in a group G, we have

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

This equation and Theorem 4.17 show that $b' * a'$ is the unique inverse of $a * b$. That is, $(a * b)' = b' * a'$. We state this as a corollary.

4.18 Corollary Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$.

For your information, we remark that binary algebraic structures with weaker axioms than those for a group 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. A **monoid** is a semigroup that has an identity element for the binary operation. Note that every group is both a semigroup and a monoid.

Finally, it is possible to give axioms for a group $\langle G, *\rangle$ that seem at first glance to be weaker, namely:

1. The binary operation $*$ on G is associative.
2. There exists a **left identity element** 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 element is also a right identity element, 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.

Finite Groups and Group Tables

All our examples after Example 4.2 have been of infinite groups, that is, groups where the set G has an infinite number of elements. We turn to finite groups, starting with the smallest finite sets.

Since a group has to have at least one element, namely, the identity, a minimal 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 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 identity 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 follows, 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 follows:

$*$	e	a
e	e	a
a	a	e

All the group axioms are now satisfied, except possibly the associative property. Checking associativity on a case-by-case basis from a table defining an operation can be a very tedious process. However, we know that $\mathbb{Z}_2 = \{0, 1\}$ under addition modulo 2 is a group, and by our arguments, its table must be the one above with e replaced by 0 and a by 1. Thus the associative property must be satisfied for our table containing e and a.

With this example 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 the identity element. 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 having 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 4.16, 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 each 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 element e appearing first, the table must be shown in Table 4.19. 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 element, a binary operation $*$ on this set has to have a table of the form shown in Table 4.20. This leaves four places to be filled in. You can quickly see that Table 4.20 must be completed as shown in Table 4.21 if each row and each column are to contain each element exactly once. Because there was only one way to complete the table and $\mathbb{Z}_3 = \{0, 1, 2\}$ under addition modulo 3 is a group, the associative property must hold for our table containing e, a, and b.

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. As explained in Section 3, this renaming gives an isomorphism of the group G' with the group G. Definition 3.7 defined the notion of *isomorphism* and of *isomorphic binary structures*. Groups are just certain types of binary structures, so the same definition pertains to them. Thus our work above can be summarized by saying that all groups with a single element are isomorphic, all groups with just two elements are isomorphic, and all groups with just three elements are isomorphic. We use the phrase *up to isomorphism* to express this identification using the equivalence relation $\simeq$. Thus we may say, "There is only one group of three elements, up to isomorphism."

4.19 Table

$*$	e	a
e	e	a
a	a	e

4.20 Table

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

4.21 Table

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

■ EXERCISES 4

Computations

In Exercises 1 through 6, determine whether the binary operation $*$ gives a group structure on the given set. If no group results, give the first axiom in the order $\mathscr{G}_1, \mathscr{G}_2, \mathscr{G}_3$ from Definition 4.1 that does not hold.

1. Let $*$ be defined on $\mathbb{Z}$ by letting $a * b = ab$.
2. Let $*$ be defined on $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ by letting $a * b = a + b$.
3. Let $*$ be defined on $\mathbb{R}^+$ by letting $a * b = \sqrt{ab}$.
4. Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$.
5. Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by letting $a * b = a/b$.
6. Let $*$ be defined on $\mathbb{C}$ by letting $a * b = |ab|$.
7. Give an example of an abelian group G where G has exactly 1000 elements.
8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4(7) + 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.
9. Show that the group $\langle U, \cdot \rangle$ is not isomorphic to either $\langle \mathbb{R}, + \rangle$ or $\langle \mathbb{R}^*, \cdot \rangle$. (All three groups have cardinality $|\mathbb{R}|$.)
10. Let n be a positive integer and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.
    - **a.** Show that $\langle n\mathbb{Z}, + \rangle$ is a group.
    - **b.** Show that $\langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$.

In Exercises 11 through 18, determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group. Recall that a **diagonal matrix** is a square matrix whose only nonzero entries lie on the **main diagonal,** from the upper left to the lower right corner. An **upper-triangular matrix** is a square matrix with only zero entries below the main diagonal. Associated with each $n \times n$ matrix A is a number called the determinant of A, denoted by $\det(A)$. If A and B are both $n \times n$ matrices, then $\det(AB) = \det(A)\det(B)$. Also, $\det(I_n) = 1$ and A is invertible if and only if $\det(A) \neq 0$.

11. All $n \times n$ diagonal matrices under matrix addition.

12. All $n \times n$ diagonal matrices under matrix multiplication.

13. All $n \times n$ diagonal matrices with no zero diagonal entry under matrix multiplication.

14. All $n \times n$ diagonal matrices with all diagonal entries 1 or -1 under matrix multiplication.

15. All $n \times n$ upper-triangular matrices under matrix multiplication.

16. All $n \times n$ upper-triangular matrices under matrix addition.

17. All $n \times n$ upper-triangular matrices with determinant 1 under matrix multiplication.

18. All $n \times n$ matrices with determinant either 1 or -1 under matrix multiplication.

19. 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.

20. This exercise shows that there are two nonisomorphic group structures on a set of 4 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 4.22. The square indicated by the question mark cannot be filled in with a. It must be filled in either with the identity element 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 isomorphic groups. Determine which two tables these are, and give the one-to-one onto renaming function which is an isomorphism.

a. Are all groups of 4 elements commutative?

b. Which table gives a group isomorphic to the group U_4, so that we know the binary operation defined by the table is associative?

c. Show that the group given by one of the other tables is structurally the same as the group in Exercise 14 for one particular value of n, so that we know that the operation defined by that table is associative also.

21. According to Exercise 12 of Section 2, 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?

Concepts

22. 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 are not acceptable, and why? (Remember this. Most instructors ask the student to define a group on at least one test.)

4.22 Table

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

23. The following "definitions" of a group are taken verbatim, including spelling and punctuation, from papers of students who wrote a bit too quickly and carelessly. 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

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

24. 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 $\mathscr{G}_1$.

25. 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.** Every group is a binary algebraic structure.

Proof synopsis

We give an example of a proof synopsis. Here is a one-sentence synopsis of the proof that the inverse of an element a in a group $\langle G, *\rangle$ is unique.

Assuming that $a * a' = e$ and $a * a'' = e$, apply the left cancellation law to the equation $a * a' = a * a''$.

Note that we said "the left cancellation law" and not "Theorem 4.15." We always suppose that our synopsis was given as an explanation given during a conversation at lunch, with no reference to text numbering and as little notation as is practical.

26. Give a one-sentence synopsis of the proof of the left cancellation law in Theorem 4.15.

27. Give at most a two-sentence synopsis of the proof in Theorem 4.16 that an equation $ax = b$ has a unique solution in a group.

Theory

28. From our intuitive grasp of the notion of isomorphic groups, it should be clear that if $\phi : G \to G'$ is a group isomorphism, then $\phi(e)$ is the identity e' of G'. Recall that Theorem 3.14 gave a proof of this for isomorphic binary structures $\langle S, *\rangle$ and $\langle S', *'\rangle$. Of course, this covers the case of groups.

It should also be intuitively clear that if a and a' are inverse pairs in G, then $\phi(a)$ and $\phi(a')$ are inverse pairs in G', that is, that $\phi(a)' = \phi(a')$. Give a careful proof of this for a skeptic who can't see the forest for all the trees.

29. 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 $a * a = e$.

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

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

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

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

d. Explain the significance of this exercise.

31. 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.)

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

33. Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

34. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$. See Exercise 33 for the meaning of a^n. [*Hint:* Consider $e, a, a^2, a^3, \ldots, a^m$, where m is the number of elements in G, and use the cancellation laws.]

35. Show that if $(a * b)^2 = a^2 * b^2$ for a and b in a group G, then $a * b = b * a$. See Exercise 33 for the meaning of a^2.

36. Let G be a group and let $a, b \in G$. Show that $(a * b)' = a' * b'$ if and only if $a * b = b * a$.

37. Let G be a group and suppose that $a * b * c = e$ for $a, b, c \in G$. Show that $b * c * a = e$ also.

38. Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given on page 43, is a group.

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

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

is a group. [*Hint:* Use Exercise 38.]

40. Let $\langle G, \cdot \rangle$ be a group. Consider the binary operation $*$ on the set G defined by

$$a * b = b \cdot a$$

for $a, b \in G$. Show that $\langle G, * \rangle$ is a group and that $\langle G, * \rangle$ is actually isomorphic to $\langle G, \cdot \rangle$. [*Hint:* Consider the map ϕ with $\phi(a) = a'$ for $a \in G$.]

41. Let G be a group and let g be one fixed element of G. Show that the map i_g, such that $i_g(x) = gxg'$ for $x \in G$, is an isomorphism of G with itself.

SECTION 5 Subgroups

Notation and Terminology

It is time to explain some conventional notation and terminology used in group theory. Algebraists as a rule do not use a special symbol $*$ to denote a binary operation different from the usual addition and multiplication. They stick with the conventional additive or multiplicative notation and even call the operation *addition* or *multiplication,* depending on the symbol used. The symbol for addition is, of course, $+$, and usually multiplication is denoted by juxtaposition without a dot, if no confusion results. Thus in place of the notation $a * b$, we shall be using either $a + b$ to be read "the *sum* of a and b," or ab to be read "the *product* of a and b." There is a sort of unwritten agreement that the symbol $+$ should be used only to designate commutative operations. Algebraists feel very uncomfortable when they see $a + b \neq b + a$. For this reason, when developing our theory in a general situation where the operation may or may not be commutative, we shall always use multiplicative notation.

Algebraists frequently use the symbol 0 to denote an additive identity element and the symbol 1 to denote a multiplicative identity element, even though they may not be actually denoting the integers 0 and 1. Of course, if they are also talking about numbers at the same time, so that confusion would result, symbols such as e or u are used as

5.1 Table

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

identity elements. Thus a table for a group of three elements might be one like Table 5.1 or, since such a group is commutative, the table might look like Table 5.2. In general situations we shall continue to use e to denote the identity element of a group.

It is customary to denote the inverse of an element a in a group by a^{-1} in multiplicative notation and by $-a$ in additive notation. From now on, we shall be using these notations in place of the symbol a'.

Let n be a positive integer. If a is an element of a group G, written multiplicatively, we denote the product $aaa \dots a$ for n factors a by a^n. We let a^0 be the identity element e, and denote the product $a^{-1}a^{-1}a^{-1} \dots a^{-1}$ for n factors by a^{-n}. It is easy to see that our usual law of exponents, $a^m a^n = a^{m+n}$ for $m, n \in \mathbb{Z}$, holds. For $m, n \in \mathbb{Z}^+$, it is clear. We illustrate another type of case by an example:

$$a^{-2}a^5 = a^{-1}a^{-1}aaaaa = a^{-1}(a^{-1}a)aaaa = a^{-1}eaaaa = a^{-1}(ea)aaa$$
$$= a^{-1}aaaa = (a^{-1}a)aaa = eaaa = (ea)aa = aaa = a^3.$$

5.2 Table

+	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

In additive notation, we denote $a + a + a + \cdots + a$ for n summands by na, denote $(-a) + (-a) + (-a) + \cdots + (-a)$ for n summands by $-na$, and let $0a$ be the identity element. Be careful: In the notation na, the number n is in $\mathbb{Z}$, not in G. One reason we prefer to present group theory using multiplicative notation, even if G is abelian, is the confusion caused by regarding n as being in G in this notation na. No one ever misinterprets the n when it appears in an exponent.

Let us explain one more term that is used so often it merits a special definition.

5.3 Definition If G is a group, then the **order** $|G|$ of G is the number of elements in G. (Recall from Section 0 that, for any set S, $|S|$ is the cardinality of S.) ■

Subsets and Subgroups

You may have noticed that we sometimes have had groups contained within larger groups. For example, the group $\mathbb{Z}$ under addition is contained within the group $\mathbb{Q}$ under addition, which in turn is contained in the group $\mathbb{R}$ under addition. When we view the group $\langle \mathbb{Z}, + \rangle$ as contained in the group $\langle \mathbb{R}, + \rangle$, it is very important to notice that the operation $+$ on integers n and m as elements of $\langle \mathbb{Z}, + \rangle$ produces the same element $n + m$ as would result if you were to think of n and m as elements in $\langle \mathbb{R}, + \rangle$. Thus we should *not* regard the group $\langle \mathbb{Q}^+, \cdot \rangle$ as contained in $\langle \mathbb{R}, + \rangle$, even though $\mathbb{Q}^+$ is contained in $\mathbb{R}$ as a set. In this instance, $2 \cdot 3 = 6$ in $\langle \mathbb{Q}^+, \cdot \rangle$, while $2 + 3 = 5$ in $\langle \mathbb{R}, + \rangle$. We are requiring not only that the set of one group be a subset of the set of the other, but also that the group operation on the subset be the *induced operation* that assigns the same element to each ordered pair from this subset as is assigned by the group operation on the whole set.

5.4 Definition If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup of** G. We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G, and $H < G$ or $G > H$ shall mean $H \leq G$ but $H \neq G$. ■

Thus $\langle \mathbb{Z}, +\rangle < \langle \mathbb{R}, +\rangle$ but $\langle \mathbb{Q}^+, \cdot\rangle$ is *not* a subgroup of $\langle \mathbb{R}, +\rangle$, even though as sets, $\mathbb{Q}^+ \subset \mathbb{R}$. Every group G has as subgroups G itself and $\{e\}$, where e is the identity element of G.

5.5 Definition If G is a group, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups are **proper subgroups.** The subgroup $\{e\}$ is the **trivial subgroup** of G. All other subgroups are **nontrivial.** ■

We turn to some illustrations.

5.6 Example Let $\mathbb{R}^n$ be the additive group of all n-component row vectors with real number entries. The subset consisting of all of these vectors having 0 as entry in the first component is a subgroup of $\mathbb{R}^n$. ▲

5.7 Example $\mathbb{Q}^+$ under multiplication is a proper subgroup of $\mathbb{R}^+$ under multiplication. ▲

5.8 Example The nth roots of unity in $\mathbb{C}$ form a subgroup U_n of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication. ▲

5.9 Example There are two different types of group structures of order 4 (see Exercise 20 of Section 4). We describe them by their group tables (Tables 5.10 and 5.11). The group V is the **Klein 4-group,** and the notation V comes from the German word *Vier* for four. The group $\mathbb{Z}_4$ is isomorphic to the group $U_4 = \{1, i, -1, -i\}$ of fourth roots of unity under multiplication.

The only nontrivial proper subgroup of $\mathbb{Z}_4$ is $\{0, 2\}$. Note that $\{0, 3\}$ is *not* a subgroup of $\mathbb{Z}_4$, since $\{0, 3\}$ is *not closed* under $+$. For example, $3 + 3 = 2$, and $2 \notin \{0, 3\}$. However, the group V has three nontrivial proper subgroups, $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$. Here $\{e, a, b\}$ is *not* a subgroup, since $\{e, a, b\}$ is not closed under the operation of V because $ab = c$, and $c \notin \{e, a, b\}$. ▲

5.10 Table

$\mathbb{Z}_4$:

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

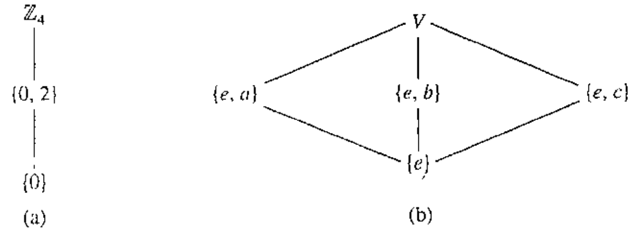
5.11 Table

V:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It is often useful to draw a *subgroup diagram* of the subgroups of a group. In such a diagram, a line running downward from a group G to a group H means that H is a subgroup of G. Thus the larger group is placed nearer the top of the diagram. Figure 5.12 contains the subgroup diagrams for the groups $\mathbb{Z}_4$ and V of Example 5.9.

Note that if $H \leq G$ and $a \in H$, then by Theorem 4.16, the equation $ax = a$ must have a unique solution, namely the identity element of H. But this equation can also be viewed as one in G, and we see that this unique solution must also be the identity element e of G. A similar argument then applied to the equation $ax = e$, viewed in both H and G, shows that the inverse a^{-1} of a in G is also the inverse of a in the subgroup H.



5.12 Figure (a) Subgroup diagram for $\mathbb{Z}_4$. (b) Subgroup diagram for V.

5.13 Example Let F be the group of all real-valued functions with domain $\mathbb{R}$ under addition. The subset of F consisting of those functions that are continuous is a subgroup of F, for the sum of continuous functions is continuous, the function f where $f(x) = 0$ for all x is continuous and is the additive identity element, and if f is continuous, then $-f$ is continuous. ▲

It is convenient to have routine steps for determining whether a subset of a group G is a subgroup of G. Example 5.13 indicates such a routine, and in the next theorem, we demonstrate carefully its validity. While more compact criteria are available, involving only one condition, we prefer this more transparent theorem for a first course.

5.14 Theorem A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G,
2. the identity element e of G is in H,
3. for all $a \in H$ it is true that $a^{-1} \in H$ also.

Proof The fact that if $H \leq G$ then Conditions 1, 2, and 3 must hold follows at once from the definition of a subgroup and from the remarks preceding Example 5.13.

Conversely, suppose H is a subset of a group G such that Conditions 1, 2, and 3 hold. By 2 we have at once that $\mathscr{G}_2$ is satisfied. Also $\mathscr{G}_3$ is satisfied by 3. It remains to check the associative axiom, $\mathscr{G}_1$. But surely for all $a, b, c \in H$ it is true that $(ab)c = a(bc)$ in H, for we may actually view this as an equation in G, where the associative law holds. Hence $H \leq G$. ◆

5.15 Example Let F be as in Example 5.13. The subset of F consisting of those functions that are differentiable is a subgroup of F, for the sum of differentiable functions is differentiable, the constant function 0 is differentiable, and if f is differentiable, then $-f$ is differentiable. ▲

5.16 Example Recall from linear algebra that every square matrix A has associated with it a number $\det(A)$ called its determinant, and that A is invertible if and only if $\det(A) \neq 0$. If A and B are square matrices of the same size, then it can be shown that $\det(AB) = \det(A) \cdot \det(B)$. Let G be the multiplicative group of all invertible $n \times n$ matrices with entries in $\mathbb{C}$ and let T be the subset of G consisting of those matrices with determinant 1. The equation $\det(AB) = \det(A) \cdot \det(B)$ shows that T is closed under matrix multiplication. Recall that the identity matrix I_n has determinant 1. From the equation $\det(A) \cdot \det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1$, we see that if $\det(A) = 1$, then $\det(A^{-1}) = 1$. Theorem 5.14 then shows that T is a subgroup of G. ▲

Cyclic Subgroups

Let us see how large a subgroup H of $\mathbb{Z}_{12}$ would have to be if it contains 3. It would have to contain the identity element 0 and $3 + 3$, which is 6. Then it has to contain $6 + 3$, which is 9. Note that the inverse of 3 is 9 and the inverse of 6 is 6. It is easily checked that $H = \{0, 3, 6, 9\}$ is a subgroup of $\mathbb{Z}_{12}$, and it is the smallest subgroup containing 3.

Let us imitate this reasoning in a general situation. As we remarked before, for a general argument we always use multiplicative notation. Let G be a group and let $a \in G$. A subgroup of G containing a must, by Theorem 5.14, contain a^n, the result of computing products of a and itself for n factors for every positive integer n. These positive integral powers of a do give a set closed under multiplication. It is possible, however, that the inverse of a is not in this set. Of course, a subgroup containing a must also contain a^{-1}, and, in general, it must contain a^{-m} for all $m \in \mathbb{Z}^+$. It must contain the identity element $e = a^0$. Summarizing, *a subgroup of G containing the element a must contain all elements a^n (or na for additive groups) for all $n \in \mathbb{Z}$.* That is, a subgroup containing a must contain $\{a^n | n \in \mathbb{Z}\}$. Observe that these powers a^n of a need not be distinct. For example, in the group V of Example 5.9,

$$a^2 = e, \quad a^3 = a, \quad a^4 = e, \quad a^{-1} = a, \qquad \text{and so on.}$$

We have almost proved the next theorem.

5.17 Theorem Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest[†] subgroup of G that contains a, that is, every subgroup containing a contains H.

[†] We may find occasion to distinguish between the terms *minimal* and *smallest* as applied to subsets of a set S that have some property. A subset H of S is minimal with respect to the property if H has the property, and no subset $K \subset H$, $K \neq H$, has the property. If H has the property and $H \subseteq K$ for every subset K with the property, then H is the smallest subset with the property. There may be many minimal subsets, but there can be only one smallest subset. To illustrate, $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$ are all minimal nontrivial subgroups of the group V. (See Fig. 5.12.) However, V contains no smallest nontrivial subgroup.

Proof We check the three conditions given in Theorem 5.14 for a subset of a group to give a subgroup. Since $a^r a^s = a^{r+s}$ for $r, s \in \mathbb{Z}$, we see that the product in G of two elements of H is again in H. Thus H is closed under the group operation of G. Also $a^0 = e$, so $e \in H$, and for $a^r \in H$, $a^{-r} \in H$ and $a^{-r}a^r = e$. Hence all the conditions are satisfied, and $H \leq G$.

Our arguments prior to the statement of the theorem showed that any subgroup of G containing a must contain H, so H is the smallest subgroup of G containing a. ◆

5.18 Definition Let G be a group and let $a \in G$. Then the subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of G, characterized in Theorem 5.17, is called the **cyclic subgroup of G generated by a**, and denoted by $\langle a \rangle$. ■

5.19 Definition An element a of a group G **generates** G and is a **generator for** G if $\langle a \rangle = G$. A group G is **cyclic** if there is some element a in G that generates G. ■

5.20 Example Let $\mathbb{Z}_4$ and V be the groups of Example 5.9. Then $\mathbb{Z}_4$ is cyclic and both 1 and 3 are generators, that is,

$$\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4.$$

However, V is *not* cyclic, for $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are proper subgroups of two elements. Of course, $\langle e \rangle$ is the trivial subgroup of one element. ▲

5.21 Example The group $\mathbb{Z}$ under addition is a cyclic group. Both 1 and -1 are generators for this group, and they are the only generators. Also, for $n \in \mathbb{Z}^+$, the group $\mathbb{Z}_n$ under addition modulo n is cyclic. If $n > 1$, then both 1 and $n - 1$ are generators, but there may be others. ▲

5.22 Example Consider the group $\mathbb{Z}$ under addition. Let us find $\langle 3 \rangle$. Here the notation is additive, and $\langle 3 \rangle$ must contain

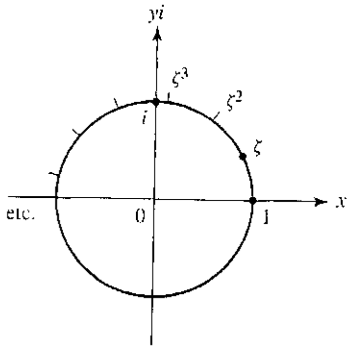
$$\begin{array}{lllll} & 3, & 3+3=6, & 3+3+3=9, & \text{and so on,} \\ 0, & -3, & -3+-3=-6, & -3+-3+-3=-9, & \text{and so on.} \end{array}$$

In other words, the cyclic subgroup generated by 3 consists of all multiples of 3, positive, negative, and zero. We denote this subgroup by $3\mathbb{Z}$ as well as $\langle 3 \rangle$. In a similar way, we shall let $n\mathbb{Z}$ be the cyclic subgroup $\langle n \rangle$ of $\mathbb{Z}$. Note that $6\mathbb{Z} < 3\mathbb{Z}$. ▲

5.23 Example For each positive integer n, let U_n be the multiplicative group of the nth roots of unity in $\mathbb{C}$. These elements of U_n can be represented geometrically by equally spaced points on a circle about the origin, as illustrated in Fig. 5.24. The heavy point represents the number

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

The geometric interpretation of multiplication of complex numbers, explained in Section 1, shows at once that as ζ is raised to powers, it works its way counterclockwise around the circle, landing on each of the elements of U_n in turn. Thus U_n under multiplication is a cyclic group, and ζ is a generator. The group U_n is the cyclic subgroup $\langle \zeta \rangle$ of the group U of all complex numbers z, where $|z| = 1$, under multiplication. ▲



5.24 Figure

EXERCISES 5

Computations

In Exercises 1 through 6, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. $\mathbb{R}$ **2.** $\mathbb{Q}^+$ **3.** $7\mathbb{Z}$

4. The set $i\mathbb{R}$ of pure imaginary numbers including 0

5. The set $\pi\mathbb{Q}$ of rational multiples of π **6.** The set $\{\pi^n \mid n \in \mathbb{Z}\}$

7. Which of the sets in Exercises 1 through 6 are subgroups of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication?

In Exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

8. The $n \times n$ matrices with determinant 2

9. The diagonal $n \times n$ matrices with no zeros on the diagonal

10. The upper-triangular $n \times n$ matrices with no zeros on the diagonal

11. The $n \times n$ matrices with determinant -1

12. The $n \times n$ matrices with determinant -1 or 1

13. The set of all $n \times n$ matrices A such that $(A^T)A = I_n$. [These matrices are called **orthogonal.** Recall that A^T, the *transpose* of A, is the matrix whose jth column is the jth row of A for $1 \le j \le n$, and that the transpose operation has the property $(AB)^T = (B^T)(A^T)$.]

54. For sets H and K, we define the **intersection** $H \cap K$ by

$$H \cap K = \{x \mid x \in H \text{ and } x \in K\}.$$

Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$. (Remember: $\leq$ denotes "is a subgroup of," not "is a subset of.")

55. Prove that every cyclic group is abelian.

56. Let G be a group and let $G_n = \{g^n \mid g \in G\}$. Under what hypothesis about G can we show that G_n is a subgroup of G?

57. Show that a group with no proper nontrivial subgroups is cyclic.

SECTION 6 Cyclic Groups

Recall the following facts and notations from Section 5. If G is a group and $a \in G$, then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G (Theorem 5.17). This group is the **cyclic subgroup $\langle a \rangle$ of G generated by a.** Also, given a group G and an element a in G, if

$$G = \{a^n \mid n \in \mathbb{Z}\},$$

then a is a **generator of** G and the group $G = \langle a \rangle$ is **cyclic.** We introduce one new bit of terminology. Let a be an element of a group G. If the cyclic subgroup $\langle a \rangle$ of G is finite, then the **order of** a is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that a is of **infinite order.** We will see in this section that if $a \in G$ is of finite order m, then m is the smallest positive integer such that $a^m = e$.

The first goal of this section is to describe all cyclic groups and all subgroups of cyclic groups. This is not an idle exercise. We will see later that cyclic groups serve as building blocks for all sufficiently small abelian groups, in particular, for all finite abelian groups. Cyclic groups are fundamental to the understanding of groups.

Elementary Properties of Cyclic Groups

We start with a demonstration that cyclic groups are abelian.

6.1 Theorem Every cyclic group is abelian.

Proof Let G be a cyclic group and let a be a generator of G so that

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1,$$

so G is abelian. ◆

We shall continue to use multiplicative notation for our general work on cyclic groups, even though they are abelian.

3.1 Table

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

3.2 Table

$*'$	#	$	&
#	&	#	$
$	#	$	&
&	$	&	#

3.3 Table

$*''$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

3.4 Table

$*''$	y	x	z
y	z	y	x
x	y	x	z
z	x	z	y

3.5 Table

$\bar{*}$	a	b	c
a	b	b	b
b	b	b	b
c	b	b	b

3.6 Table

$\hat{*}$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

names (un, deux, trois, $\cdots$ versus ein, zwei, drei $\cdots$) for the numbers, but they are learning the same binary structure. (In this case, they are also using the same symbols for the numbers, so their addition tables would appear the same if they list the numbers in the same order.)

We are interested in studying the different types of *structures* that binary operations can provide on sets having the same number of elements, as typified by Tables 3.4, 3.5, and 3.6. Let us consider a **binary algebraic structure**[†] $\langle S, *\rangle$ to be a set S together with a binary operation $*$ on S. In order for two such binary structures $\langle S, *\rangle$ and $\langle S', *'\rangle$ to be structurally alike in the sense we have described, we would have to have a one-to-one correspondence between the elements x of S and the elements x' of S' such that

$$\text{if}\quad x \leftrightarrow x' \quad\text{and}\quad y \leftrightarrow y', \quad\text{then}\quad x * y \leftrightarrow x' *' y'. \tag{1}$$

A one-to-one correspondence exists if the sets S and S' have the same number of elements. It is customary to describe a one-to-one correspondence by giving a *one-to-one* function ϕ mapping S *onto* S' (see Definition 0.12). For such a function ϕ, we regard the equation $\phi(x) = x'$ as reading the one-to-one pairing $x \leftrightarrow x$ in left-to-right order. In terms of ϕ, the final $\leftrightarrow$ correspondence in (1), which asserts the algebraic structure in S' is the same as in S, can be expressed as

$$\phi(x * y) = \phi(x) *' \phi(y).$$

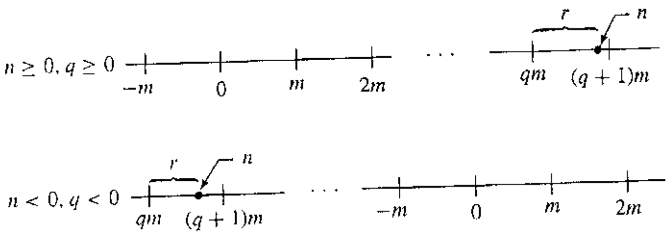
Such, a function showing that two algebraic systems are structurally alike is known as an *isomorphism*. We give a formal definition.

3.7 Definition Let $\langle S, *\rangle$ and $\langle S', *'\rangle$ be binary algebraic structures. An **isomorphism of** S with S' is a one-to-one function ϕ mapping S onto S' such that

$$\begin{gathered}\phi(x * y) = \phi(y) *' \phi(y) \text{ for all } x, y \in S.\\ \textit{homomorphism property}\end{gathered} \tag{2}$$

[†] Remember that boldface type indicates that a term is being defined.

The *division algorithm* that follows is a seemingly trivial, but very fundamental tool for the study of cyclic groups.



6.2 Figure

6.3 Division Algorithm for $\mathbb{Z}$ If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$

Proof We give an intuitive diagrammatic explanation, using Fig. 6.2. On the real x-axis of analytic geometry, mark off the multiples of m and the position of n. Now n falls either on a multiple qm of m and r can be taken as 0, or n falls between two multiples of m. If the latter is the case, let qm be the first multiple of m to the left of n. Then r is as shown in Fig. 6.2. Note that $0 \leq r < m$. Uniqueness of q and r follows since if n is not a multiple of m so that we can take $r = 0$, then there is a unique multiple qm of m to the left of n and at distance less than m from n, as illustrated in Fig. 6.2. ◆

In the notation of the division algorithm, we regard q as the **quotient** and r as the nonnegative **remainder** when n is divided by m.

6.4 Example Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solution The positive multiples of 7 are 7, 14, 21, 28, 35, 42, $\cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$38 = 35 + 3 = 7(5) + 3$$

so the quotient is $q = 5$ and the remainder is $r = 3$. ▲

6.5 Example Find the quotient q and remainder r when -38 is divided by 7 according to the division algorithm.

Solution The negative multiples of 7 are $-7, -14, -21, -28, -35, -42, \cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$-38 = -42 + 4 = 7(-6) + 4$$

so the quotient is $q = -6$ and the remainder is $r = 4$. ▲

We will use the division algorithm to show that a subgroup H of a cyclic group G is also cyclic. Think for a moment what we will have to do to prove this. We will have to

31. Function subtraction $-$ on F is associative.

32. Function multiplication $\cdot$ on F is commutative.

33. Function multiplication $\cdot$ on F is associative.

34. Function composition $\circ$ on F is commutative.

35. If $*$ and $*'$ are any two binary operations on a set S, then

$$a * (b *' c) = (a * b) *' (a * c) \quad \text{for all} \quad a, b, c \in S.$$

36. Suppose that $*$ is an *associative binary* operation on a set S. Let $H = \{a \in S \mid a * x = x * a \text{ for all } x \in S\}$. Show that H is closed under $*$. (We think of H as consisting of all elements of S that *commute* with every element in S.)

37. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that $H = \{a \in S \mid a * a = a\}$ is closed under $*$. (The elements of H are **idempotents** of the binary operation $*$.)

SECTION 3 Isomorphic Binary Structures

Compare Table 3.1 for the binary operation $*$ on the set $S = \{a, b, c\}$ with Table 3.2 for the binary operation $*'$ on the set $T = \{\#, \$, \&\}$.

Notice that if, in Table 3.1, we replace all occurrences of a by #, every b by \$, and every c by & using the one-to-one correspondence

$$a \leftrightarrow \# \qquad b \leftrightarrow \$ \qquad c \leftrightarrow \&$$

we obtain precisely Table 3.2. The two tables differ only in the symbols (or names) denoting the elements and the symbols $*$ and $*'$ for the operations. If we rewrite Table 3.3 with elements in the order y, x, z, we obtain Table 3.4. (Here we did not set up any one-one-correpondence; we just listed the same elements in different order outside the heavy bars of the table.) Replacing, in Table 3.1, all occurrences of a by y, every b by x, and every c by z using the one-to-one correspondence

$$a \leftrightarrow y \qquad b \leftrightarrow x \qquad c \leftrightarrow z$$

we obtain Table 3.4. We think of Tables 3.1, 3.2, 3.3, and 3.4 as being *structurally alike*. These four tables differ only in the names (or symbols) for their elements and in the order that those elements are listed as heads in the tables. However, Table 3.5 for binary operation $\bar{*}$ and Table 3.6 for binary operation $\hat{*}$ on the set $S = \{a, b, c\}$ are *structurally different* from each other and from Table 3.1. In Table 3.1, each element appears three times in the body of the table, while the body of Table 3.5 contains the single element b. In Table 3.6, for all $s \in S$ we get the same value c for $s \mathbin{\hat{*}} s$ along the upper-left to lower-right diagonal, while we get three different values in Table 3.1. Thus Tables 3.1 through 3.6 give just three structurally different binary operations on a set of three elements, provided we disregard the names of the elements and the order in which they appear as heads in the tables.

The situation we have just discussed is somewhat akin to children in France and in Germany learning the operation of addition on the set $\mathbb{Z}^+$. The children have different use the *definition* of a cyclic group since we have proved little about cyclic groups yet. That is, we will have to use the fact that G has a generating element a. We must then exhibit, in terms of this generator a, some generator $c = a^m$ for H in order to show that H is cyclic. There is really only one natural choice for the power m of a to try. Can you guess what it is before you read the proof of the theorem?

6.6 Theorem A subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group generated by a and let H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

We claim that $c = a^m$ generates H; that is,

$$H = \langle a^m \rangle = \langle c \rangle.$$

We must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some n. Find q and r such that

$$n = mq + r \qquad \text{for} \qquad 0 \leq r < m$$

in accord with the division algorithm. Then

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

so

$$a^r = (a^m)^{-q} a^n.$$

Now since $a^n \in H$, $a^m \in H$, and H is a group, both $(a^m)^{-q}$ and a^n are in H. Thus

$$(a^m)^{-q} a^n \in H; \qquad \text{that is,} \qquad a^r \in H.$$

Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus $n = qm$ and

$$b = a^n = (a^m)^q = c^q,$$

so b is a power of c. ◆

As noted in Examples 5.21 and 5.22, $\mathbb{Z}$ under addition is cyclic and for a positive integer n, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$ under addition, the cyclic subgroup generated by n. Theorem 6.6 shows that these cyclic subgroups are the only subgroups of $\mathbb{Z}$ under addition. We state this as a corollary.

6.7 Corollary The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.

This corollary gives us an elegant way to define the *greatest common divisor* of two positive integers r and s. Exercise 45 shows that $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of the group $\mathbb{Z}$ under addition. Thus H must be cyclic and have a generator d, which we may choose to be positive.

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

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

23. Let H be the subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. Is H closed under

a matrix addition? **b** matrix multiplication?

24. 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.

25. 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.*

Theory

26. 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 $x, y, z \in S$.

In Exercises 27 and 28, either prove the statement or give a counterexample.

27. Every binary operation on a set consisting of a single element in both commutative and associative.

28. Every commutative binary operation on a set having just two elements is associative.

Let F be the set of all real-valued functions having as domain the set $\mathbb{R}$ of all real numbers. Example 2.7 defined the binary operations $+$, $-$, $\cdot$, and $\circ$ on F. In Exercises 29 through 35, either prove the given statement or give a counterexample.

29. Function addition $+$ on F is associative.

30. Function subtraction $-$ on F is commutative

6.8 Definition Let r and s be two positive integers. The positive generator d of the cyclic group

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor** (abbreviated gcd) of r and s. We write $d = \gcd(r, s)$. ■

Note from the definition that d is a divisor of both r and s since both $r = 1r + 0s$ and $s = 0r + 1s$ are in H. Since $d \in H$, we can write

$$d = nr + ms$$

for some integers n and m. We see that every integer dividing both r and s divides the right-hand side of the equation, and hence must be a divisor of d also. Thus d must be the largest number dividing both r and s; this accounts for the name given to d in Definition 6.8.

6.9 Example Find the gcd of 42 and 72.

Solution The positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, and 42. The positive divisors of 72 are 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, and 72. The greatest common divisor is 6. Note that $6 = (3)(72) + (-5)(42)$. There is an algorithm for expressing the greatest common divisor d of r and s in the form $d = nr + ms$, but we will not need to make use of it here. ▲

Two positive integers are **relatively prime** if their gcd is 1. For example, 12 and 25 are relatively prime. Note that they have no prime factors in common. In our discussion of subgroups of cyclic groups, we will need to know the following:

> If r and s are relatively prime and if r divides sm, then r must divide m. (1)

Let's prove this. If r and s are relatively prime, then we may write

$$1 = ar + bs \qquad \text{for some} \qquad a, b \in \mathbb{Z}.$$

Multiplying by m, we obtain

$$m = arm + bsm.$$

Now r divides both arm and bsm since r divides sm. Thus r is a divisor of the right-hand side of this equation, so r must divide m.

The Structure of Cyclic Groups

We can now describe all cyclic groups, up to an isomorphism.

6.10 Theorem Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, +\rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n\rangle$.

Proof **Case I** *For all positive integers m, $a^m \neq e$.* In this case we claim that no two distinct exponents h and k can give equal elements a^h and a^k of G. Suppose that $a^h = a^k$ and say $h > k$. Then

$$a^h a^{-k} = a^{h-k} = e,$$

contrary to our Case I assumption. Hence every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$. The map $\phi : G \to \mathbb{Z}$ given by $\phi(a^i) = i$ is thus well defined, one to one, and onto $\mathbb{Z}$. Also,

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j),$$

so the homomorphism property is satisfied and ϕ is an isomorphism.

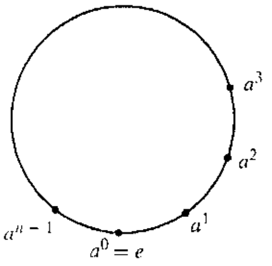
Case II *$a^m = e$ for some positive integer m.* Let n be the smallest positive integer such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. As in Case 1, if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting our choice of n. Thus the elements

$$a^0 = e, a, a^2, a^3, \cdots, a^{n-1}$$

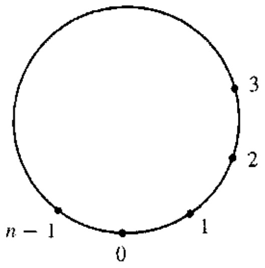
are all distinct and comprise all elements of G. The map $\psi : G \to \mathbb{Z}_n$ given by $\psi(a^i) = i$ for $i = 0, 1, 2, \cdots, n-1$ is thus well defined, one to one, and onto $\mathbb{Z}_n$. Because $a^n = e$, we see that $a^i a^j = a^k$ where $k = i +_n j$. Thus

$$\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j),$$

so the homomorphism property is satisfied and ψ is an isomorphism. ◆



6.11 Figure



6.12 Figure

6.13 Example Motivated by our work with U_n, it is nice to visualize the elements $e = a^0, a^1, a^2, \cdots, a^{n-1}$ of a cyclic group of order n as being distributed evenly on a circle (see Fig. 6.11). The element a^h is located h of these equal units counterclockwise along the circle, measured from the bottom where $e = a^0$ is located. To multiply a^h and a^k diagrammatically, we start from a^h and go k additional units around counterclockwise. To see arithmetically where we end up, find q and r such that

$$h + k = nq + r \qquad \text{for} \qquad 0 \leq r < n.$$

The nq takes us all the way around the circle q times, and we then wind up at a^r. ▲

Figure 6.12 is essentially the same as Fig. 6.11 but with the points labeled with the exponents on the generator. The operation on these exponents is *addition modulo n*.

Subgroups of Finite Cyclic Groups

We have completed our description of cyclic groups and turn to their subgroups. Corollary 6.7 gives us complete information about subgroups of infinite cyclic groups. Let us give the basic theorem regarding generators of subgroups for the finite cyclic groups.

6.14 Theorem Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = gcd(t, n)$.

Proof That b generates a cyclic subgroup H of G is known from Theorem 5.17. We need show only that H has n/d elements. Following the argument of Case II of Theorem 6.10, we see that H has as many elements as the smallest positive power m of b that gives the identity. Now $b = a^s$, and $b^m = e$ if and only if $(a^s)^m = e$, or if and only if n divides ms. What is the smallest positive integer m such that n divides ms? Let d be the gcd of n and s. Then there exists integers u and v such that

$$d = un + vs.$$

Since d divides both n and s, we may write

$$1 = u(n/d) + v(s/d)$$

where both n/d and s/d are integers. This last equation shows that n/d and s/d are relatively prime, for any integer dividing both of them must also divide 1. We wish to find the smallest positive m such that

$$\frac{ms}{n} = \frac{m(s/d)}{(n/d)} \text{ is an integer.}$$

From the boxed division property (1), we conclude that n/d must divide m, so the smallest such m is n/d. Thus the order of H is n/d.

Taking for the moment $\mathbb{Z}_n$ as a model for a cyclic group of order n, we see that if d is a divisor of n, then the cyclic subgroup $\langle d \rangle$ of $\mathbb{Z}_n$ had n/d elements, and contains all the positive integers m less than n such that $\gcd(m, n) = d$. Thus there is only one subgroup of $\mathbb{Z}_n$ of order n/d. Taken with the preceding paragraph, this shows at once that if a is a generator of the cyclic group G, then $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$. ◆

6.15 Example For an example using additive notation, consider $\mathbb{Z}_{12}$, with the generator $a = 1$. Since the greatest common divisor of 3 and 12 is 3, $3 = 3 \cdot 1$ generates a subgroup of $\frac{12}{3} = 4$ elements, namely

$$\langle 3 \rangle = \{0, 3, 6, 9\}.$$