Teachers, students, and general readers: This is the first book to explain—in simple, uncomplicated language—the working methods, ideas, and fundamental concepts of the revolutionary developments in modern mathematics.
The Wonderful World of Modern Mathematics

In this era of expanding science, modern mathematics is like a jet plane streaking across the sky to an adventurous destination. But to the average bystander who watches the jet-stream, even its take-off point is a mysterious, hidden secret. The purpose of this book is to help that bystander penetrate the unknown and fascinating realm of numbers—real, imaginary, rational, and complex.

The author maps the routes of advanced theories from their fundamental origins, step by step, and shows how our system has grown from the whole numbers we use in counting to measurements in space that must be denoted by arrows.

Anyone who has a smattering of high-school algebra and geometry can follow the do-it-yourself sections at the end of each chapter and in the supplement. Pencil in hand, he will navigate through old structures into new, and experience the thrill of discovery that awaits him in the field of modern mathematics.
Other Books of Special Interest

**How Life Began by Irving Adler**
A readable account of what science has discovered about the origin of life. Preface by Linus Pauling. Illustrated. (#K369—35¢)

**Magic House of Numbers by Irving Adler**
Mathematical curiosities, riddles, tricks, and games that teach the basic principles of arithmetic. (#K361—35¢)

**The Stars: Steppingstones into Space by Irving Adler**
A clear explanation of the mysteries of the heavens, with photographs and line drawings. (#K364—35¢)

**New Handbook of the Heavens by Hubert J. Bernhard, Dorothy A. Bennett and Hugh S. Rice**
A guide to the stars and planets. (#MD114—50¢)

To Our Readers

We welcome your request for our free catalog of Signet and Mentor Books. If your dealer does not have the books you want, you may order them by mail enclosing the list price plus 5¢ a copy to cover mailing. The New American Library of World Literature, Inc., P.O. Box 2310 Grand Central Station, New York 17, New York.

**THE NEW MATHEMATICS**

*With diagrams by Ruth Adler*

A MENTOR BOOK

Published by THE NEW AMERICAN LIBRARY
Contents

Foreword 7
I. Numbers for Counting 13
II. Number Systems Without "Numbers" 35
III. New Numbers From Old 44
IV. Numbers for Measuring 73
V. Filling Out the Line 90
VI. Spilling Into the Plane 125
VII. The Rank and File: Matrices 148
VIII. Arrows That Are Numbers 160

Bibliography 181
Summary of Basic Definitions 182
Do-It-Yourself Supplement 184
Index 191
Foreword

As we go about our daily business, we make frequent use of whole numbers, like 1, 2, 3, and 4, which arise when we count collections of objects. We also use fractions, like $\frac{1}{2}$ and $\frac{1}{3}$, which arise when measurements are made. These are obviously two different kinds of number, because fractions can never arise as a result of counting alone. In what sense then, do they both deserve to be called numbers? When we say that the fraction $\frac{4}{2}$ is equal to the whole number 2, what does this mean? How can a number of one kind be equal to a number of a totally different kind?

These are among the questions which modern mathematics has explored, and for which it has found answers. Here are others:

We sometimes have occasion to use a number like the square-root of two. It seems like a very elusive number that is reluctant to show its face. Either it hides shyly behind a symbol like $\sqrt{2}$, or it reveals itself only piecemeal as a decimal, 1.4, 1.41, 1.414, in a process that never ends. Why doesn't it behave itself and settle down like a decent ordinary fraction with a definite numerator and denominator that can determine its value once and for all?

In elementary algebra we were introduced to negative numbers, and taught such mysterious rules as that the product of two negative numbers is a positive number. Where does such a rule come from?

The electrical engineer uses the number $\sqrt{-1}$ in the equations that describe the behavior of an alternating cur-
rent. This number is called "imaginary," yet there is nothing imaginary about the electrical current it helps to describe. It is a genuine number, mathematicians assure us, although it is not real. What is the meaning of this paradox?

These are some of the questions that we shall look into in the course of this book as we take a close look at the numbers of everyday life. We shall find the answers in the fact that our number system has not been static, but has been growing, while our conception of what constitutes a number has changed. As we trace this growth, we shall discover the familiar roots of the unfamiliar concepts and terms of modern mathematics.

For mathematics, one of the oldest of the sciences, is growing with the vigor and vitality of youth. It is constantly expanding into new areas of investigation, and works with new concepts that are the fruit of a century-old revolution in mathematical thinking. Associated with the new ideas is a new vocabulary that gives modern mathematical writing its characteristic flavor. To the mathematician, the new ideas expressed by the new words serve as a bright light that penetrates to the core of a problem and helps him see and understand. To the layman, the new vocabulary is often an opaque screen behind which things are going on that he feels he cannot hope to understand. The purpose of this book is to remove that screen, by introducing the reader to the meaning of some of the basic ideas of modern mathematics.

This book is addressed to the average reader who is curious about the new developments in mathematics. It is not a refresher course in high school mathematics. It is not a rehash of old ideas, but an introduction to new ideas, traditionally presented only to the specialist, in advanced mathematics courses on the college senior or graduate level. But, although the ideas are advanced, the presentation is elementary. Anybody who has had high school algebra and geometry will be able to understand and enjoy this book.

A typical text in advanced mathematics today bristles with such terms as group, ring, field, homomorphism, isomorphism, and homeomorphism. These unfamiliar looking words make it seem as though mathematics has abandoned its old subject matter, and is no longer concerned with the study of numbers and space. This, of course, is not true. Numbers and space are still very much at the heart of mathematics. The new ideas and terms have arisen in connection with a more penetrating analysis of their properties.

Underlying the terms group, ring, and field, for example, are the old, familiar, simple operations of addition, subtraction, multiplication, and division. The mathematician has discovered that these operations are not the exclusive property of numbers alone. So he studies them in their most general form, in order to discover rules that will be valid in any context in which the operations are performed.

The outlook of the modern mathematician is indicated in his frequent use of the word stem "morph," meaning form, as in the words homomorphism, isomorphism, and homeomorphism. The mathematician sees the number system as a complex of interrelated structures. He studies these structures separately, and in their relationships to each other. The exploration of these structures has revealed that we have, not a number system, but number systems; not algebra, but algebras; not geometry, but geometries; not space, but spaces. While the properties of numbers and space have been generalized, the subject matter of mathematics has been pluralized.

The central thread around which the book is organized is the expansion of the number system, from natural numbers to integers to rational numbers to real numbers to complex numbers. Although this sequence of steps in the development of the number system parallels very roughly historical stages in the development of the concept of number, the organization of the book is not chronological or historical. It is a logical organization from the modern point of view, showing how the various number systems are related to each other. The development outlined here might be referred to as "operation bootstrap." The system of
natural numbers (the whole numbers used for counting) has defects that limit its usefulness. The story presented here shows how mathematics has lifted itself by its own bootstraps, using the defective system of natural numbers to construct bigger and better number systems that eliminate the defects.

At each stage of the construction of the expanded number systems, we encounter some of the structures such as groups, rings and fields that receive so much attention in modern mathematics. These modern concepts are introduced first by means of familiar examples in the number systems, and then other less familiar examples are given, too. As he reads the sections devoted to these modern concepts, the reader will be aware of the fact that he is merely nibbling at the corner of a great rug that has a beautiful but intricate design woven into it. If what he sees from the corner arouses his curiosity about the main design, it is hoped that he will satisfy this curiosity by systematic study from some of the standard text-books. A bibliography is given at the end of the book.

To get the most value and enjoyment out of this book, read it with pencil and paper in hand. Verify the steps of each argument, work through all examples given, and do other examples like them. A "Do It Yourself" section at the end of each chapter gives you an opportunity to strengthen through use your understanding of the new ideas you will acquire in the book.
Mumhers for Counting

WE ARE thoroughly familiar with the faces of the people with whom we live. Yet we are rarely conscious of the details of their features. If, as we look at a familiar face, we do take particular notice of the details, such as a curve of the lip, or a line in the forehead, it seems as though we are seeing them for the first time. Then, seeing these features that we never notice, we suddenly have the feeling that we are looking at the face of a stranger. We shall have a similar experience with the familiar numbers of everyday life. When we use these numbers, we take advantage of certain properties that they have. However, we are so accustomed to these properties that we are hardly aware of them as we use them. We shall now take particular notice of these properties, and list them explicitly. Looking at the familiar features of ordinary numbers, we shall see the strange new face of modern mathematics.

The first numbers we all learn to use are those we need to answer the question, “How many?” They are the numbers 1, 2, 3, 4, 5, and so on. There is an endless chain of these numbers. We use them for counting, and we perform calculations with them, such as addition and multiplication. Let us take a close look at these simple acts.

Counting

Suppose that on Tuesday evening you want to see how many days are left till the end of the week. It is likely that you will take count in this way: You will call off the names of the days, Wednesday, Thursday, Friday, and Saturday, and, for each day that you name, you will turn down
one finger on your right hand. After completing the list of days, you find that you have turned down all the fingers on your right hand except the thumb. So you conclude that there are four days left till the end of the week. We find hidden in this procedure three important mathematical concepts: the idea of a mapping, the idea of a one-to-one correspondence, and the idea of cardinal number.

A mapping is a matching operation between two sets of objects: to each member of one set a member of the other set is assigned as partner. The two sets in this case are the set of days being counted, and the set of fingers on your hand. You set up a mapping when you single out a finger to turn down for each day you count. The mapping might be summarized in the following table:

<table>
<thead>
<tr>
<th>Day</th>
<th>Finger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday</td>
<td>little finger</td>
</tr>
<tr>
<td>Thursday</td>
<td>ring finger</td>
</tr>
<tr>
<td>Friday</td>
<td>middle finger</td>
</tr>
<tr>
<td>Saturday</td>
<td>index finger</td>
</tr>
</tbody>
</table>

The arrowheads indicate that the mapping has a direction. You select a finger for each day you name. This is not the same as selecting a day for each finger. To specify the direction of the mapping, we say that it is a mapping of the set of days named into the set of fingers. We refer to the finger into which a day is mapped as its image under the mapping.

Another mapping is shown in the diagram below. In this mapping, a set of names of people has been mapped into the set of whole numbers from 20 to 24 by assigning to each name the person's age in years:

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>20</td>
</tr>
<tr>
<td>Richard</td>
<td>21</td>
</tr>
<tr>
<td>William</td>
<td>22</td>
</tr>
<tr>
<td>Mary</td>
<td>23</td>
</tr>
<tr>
<td>Susan</td>
<td>24</td>
</tr>
</tbody>
</table>

This mapping differs from the other one in one important respect. The two names, Richard and William, are both mapped into the same number. This is an example of a many-to-one mapping, in which a single object may be the image of more than one object. In the mapping of days into fingers, however, no two days were mapped into the same finger. This is an example of a one-to-one mapping, in which each object is the image of at most one object.

In the mapping of the set of days into the fingers of the right hand, one of the fingers, the thumb, wasn't used at all. For this reason the mapping of the set of days into the set of fingers on the right hand is not reversible. If we try to reverse it, we find that there is no mapping of the thumb into a day. We do not consider it a mapping then, because a mapping should provide an image for each object in the set on which the mapping is performed. However, if we consider only the set of fingers turned down, then the mapping is reversible. Then, while each day named has a separate finger as its image, in the reverse mapping, each finger has a separate day as its image. In this case we say that the two sets are in one-to-one correspondence. Two sets are in one-to-one correspondence when there is a reversible mapping that assigns each member of one set to one and only one partner in the other. The diagram below, using double-headed arrows, shows the one-to-one correspondence between the set of days and the set of fingers turned down:

| Wednesday | little finger |
| Thursday  | ring finger |
| Friday    | middle finger |
| Saturday  | index finger |

When two sets can be put into one-to-one correspondence by some mapping, we say that they contain the same number of objects, or have the same cardinal number. All sets that have the same cardinal number can be put into one-to-one correspondence with each other. They form a family of sets associated with that cardinal number. Each cardinal number has its own family of sets. For example, sets consisting of single objects only belong to the family of sets associated with the number we call one. Sets of pairs of
objects belong to the family of sets associated with the number we call two. Sets of triples belong to the family of sets associated with the number we call three, and so on.

Any set we ever deal with belongs to one of these families. When we ask the question, “How many objects are there in the set?” it is really like asking, “Which family of sets does it belong to?” To answer the question, we follow this procedure: We pick one set from each family, and use it as a standard set for making comparisons. We match the set we are interested in against these standard sets, until we find one with which it can be put into one-to-one correspondence. In this way we identify the family of sets that it belongs to, and the cardinal number associated with that family. This is precisely what you do when you match days against fingers. You use the set consisting of your little finger alone as a standard set to represent the number one. You use the set consisting of little finger and ring finger as a standard set to represent the number two. You use the set consisting of little finger, ring finger, and middle finger as a standard set to represent the number three. The set consisting of little finger, ring finger, middle finger, and index finger is your standard set representing the number four. That is why you drew the conclusion, in this case, that there are four more days to the end of the week.

On other occasions, we use a method of counting that is more sophisticated but is essentially the same. We count out four objects by saying to ourselves, “one, two, three, four.” As we count, we set up a one-to-one correspondence between the objects we are counting and sets of spoken number-names. The first object is matched with the set consisting of the single word, “one.” The first two are matched with the set consisting of the words, “one, two.” The first three are matched with the set consisting of the words, “one, two, three.” And so on. By using the number standard set step by step. When the count ends, we know that the last number-name used is the cardinal number of the last standard set against which we matched the objects we are counting. So it is also the cardinal number of the counted objects. By using standard sets made up of number names arranged in order we telescope a whole series of matching operations into one, and end up with the answer to the question, “How many?”

Addition

A typical problem in addition is to find the sum of the numbers 2 and 3. The meaning of this problem can be restated in terms of sets of objects in this way: Suppose you have one set of objects whose cardinal number is 2, and another set of objects, different from those in the first set, and whose cardinal number is 3. A larger set is formed when these two sets are united. What is the cardinal number of the united set?

We can answer this question by actually forming such a united set, and then identifying the standard set with which it can be put into one-to-one correspondence. This is the procedure of the beginner in arithmetic, who first turns down two fingers, then turns down three more fingers, and finally matches the set of turned down fingers against the standard set consisting of the spoken words, “one, two, three, four, five.” However, experienced calculators use a short-cut for getting the answer. Having carried out the process of uniting and counting sets of objects many times before, we record the results in an addition table which we memorize. Then, any time we want to find the sum of two numbers, we don’t have to manipulate sets of objects again. We merely consult the table.

Using the addition table instead of adding on our fingers is more than just a time-saving convenience. It is an act of abstraction that has changed the meaning of addition. When we add on our fingers, we are actually working with cardinal numbers, which are properties of sets of objects. When we use the addition table, we are performing an operation on abstract symbols. This operation can now be performed...
We observe, first, that the numbers we are pairing off in our ordered pairs are selected from the list of symbols, 1, 2, 3, 4, etc. To distinguish this set of symbols from the cardinal numbers from which they were derived, let us give it a name. We shall call it the system of natural numbers. We observe next that the number assigned as sum to each ordered pair is selected from the same set, the system of natural numbers. A mapping which assigns to each ordered pair of objects in a set another object selected from the same set is called a binary operation. So addition is an example of a binary operation defined on the system of natural numbers.

If we consult the addition table, we find that \(1 + 4 = 5, 2 + 3 = 5, 3 + 2 = 5, \text{ and } 4 + 1 = 5\). The different ordered pairs, (1, 4), (2, 3), (3, 2), and (4, 1) are all mapped into the same image, 5. So addition is a many-to-one mapping. In particular, an ordered pair like (2, 3) and the pair (3, 2), obtained by having the 2 and 3 change places, both have the same image. We could write \(2 + 3 = 3 + 2\). A similar statement is true for the sum of every ordered pair of natural numbers. We find that \(5 + 2 = 2 + 5, 9 + 16 = 16 + 9\), etc. This characteristic of the addition of natural numbers can be summarized in the following rule: If the letter \(a\) stands for any natural number, and the letter \(b\) stands for any natural number, then \(a + b = b + a\). That is, if the natural numbers being added commute or change places, the sum is still the same. So this rule is known as the commutative law of addition, and we say that addition of natural numbers is a commutative operation.

We are so accustomed to using the commutative law of addition that it may seem to be obvious, and hardly worth mentioning. But it needs special mention because, while some binary operations, like addition of natural numbers, obey a commutative law, there are others that do not. For example, one of the operations we learned in elementary school arithmetic is called division, and is denoted by the symbol \(\div\). It is not a commutative operation, because the
numbers being divided cannot, in general, change places without changing the result. For example, \( 8 \div 2 \) is not equal to \( 2 \div 8 \).

Addition, as we have talked about it so far, is an operation performed on a pair of numbers. We can also extend it to three numbers. We can add three numbers by first adding two of them, and then adding the sum to the third. However, for three numbers like 2, 3, and 7, listed in a definite order, we have a choice of two ways of doing it. We might add the sum of 2 and 3 to 7, or we might add 2 to the sum of 3 and 7. These two possibilities can be written down in this form: \((2 + 3) + 7\), and \(2 + (3 + 7)\). In this notation, the parentheses indicate which sum is to be found first. When we carry out these additions, we find that it doesn't make any difference which sum is found first, because the results come out the same: \((2 + 3) + 7 = 5 + 7 = 12\), and \(2 + (3 + 7) = 2 + 10 = 12\). This is a characteristic of the addition of three natural numbers, no matter what numbers are used. It is expressed in the rule, \((a + b) + c = a + (b + c)\), where \(a\), \(b\), and \(c\) stand for any natural numbers. This rule says that in the first step of the addition we are free to associate the middle number either with the number on the left or with the number on the right. So the rule is known as the associative law of addition, and we say that addition of natural numbers is an associative operation. Since it makes no difference which pair of numbers we add first, we may, as well leave out the parentheses altogether, and write the sum of \(a\), \(b\), and \(c\) as \(a + b + c\), where it is understood that \(a + b + c = a + (b + c) = (a + b) + c\).

The associative law, too, deserves special mention because it is a special property of addition of natural numbers, which it shares with some binary operations but not with all. For example, suppose we use the symbol \(\text{av}\) to designate the operation “take the average of.” It is a binary operation that can be performed on the familiar whole numbers and fractions that we use every day. In this notation, \(8\text{ av }16\) means the average of 8 and 16, which is 12. The symbol \(12\text{ av }12\) means the average of 12 and 12, which is also 12. The symbol \(16\text{ av }12\) means 14, and the symbol \(8\text{ av }14\) means 11. This operation does not obey an associative law, because \((8\text{ av }16)\text{ av }12\) is not equal to \(8\text{ av }16\) \(\text{ av }12\). In fact, \((8\text{ av }16)\text{ av }12\) means \(12\text{ av }12\), or 12, while \(8\text{ av }16\) \(\text{ av }12\) means \(8\text{ av }14\), or 11.

By a step-by-step process, the use of the commutative law and the associative law for addition of natural numbers can be extended into a general rule for the sum of any finite selection of natural numbers: When you add a finite selection of natural numbers, you can list them in any order, and group them as you please. The sum will always come out the same.

**Multiplication**

The meaning of multiplication of natural numbers, like the meaning of addition, can be stated first in terms of sets of objects. To multiply 2 times 3, we set up a rectangular array of objects, consisting of two rows, with three objects in each row. Then we find the cardinal number of this set. In general, to multiply the numbers \(a\) and \(b\), we find the cardinal number of a set consisting of \(a\) rows with \(b\) objects in each row. The answer is called the product of \(a\) and \(b\), and is designated by \(a \cdot b\), where we use a dot as the symbol for multiplication. Once we have found the product of two natural numbers, we can record it for future reference in a multiplication table. Then we can separate the operation of multiplication from its original meaning of finding the cardinal number of a rectangular array of objects. We can think of it instead as merely a mapping of ordered pairs of natural numbers into the system of natural numbers. We usually show the mapping by a series of statements like this: \(2 \cdot 3 = 6\), \(2 \cdot 4 = 8\), \(2 \cdot 5 = 10\), etc.
However, as in the case of addition, we can express it with the help of arrows:

\[(2, 3) \rightarrow 6\]
\[(2, 4) \rightarrow 8\]
\[(2, 5) \rightarrow 10\]

etc.

Since the mapping is defined for every ordered pair of natural numbers, and the image under the mapping is always a natural number, multiplication, like addition, is a binary operation on the system of natural numbers. We know from our experience with multiplication of natural numbers that \(2 \cdot 3 = 3 \cdot 2,\ 2 \cdot 4 = 4 \cdot 2,\ 2 \cdot 5 = 5 \cdot 2,\ etc.\) In general, if \(a\) and \(b\) are any natural numbers, \(a \cdot b = b \cdot a.\) This is known as the commutative law of multiplication. Multiplication, like addition, also obeys an associative law: \(a \cdot (b \cdot c) = (a \cdot b) \cdot c.\) This is seen, for example, in the fact that \(2 \cdot (3 \cdot 5) = 2 \cdot 15 = 30,\) and \((2 \cdot 3) \cdot 5 = 6 \cdot 5 = 30.\) Because of this law, we can write the product of three numbers without parentheses, and give it a definite meaning: \(a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c.\) Combining the commutative law and associative law of multiplication leads to the general rule: when you multiply a product of three numbers without parentheses, you can list them in any order, and group them as you please. The product will always come out the same.

There is one more characteristic of the multiplication of natural numbers that links it with addition. We can understand it best by going back to the original meaning of the rectangular array, and the original meaning of addition as finding the cardinal number of a rectangular array of stars, consisting of three rows with nine stars in each row. The number of stars in this rectangular array is \(3 \cdot 9.\) Since a row of nine stars can be thought of as the first five stars united with four other stars, we can write \(9 = 5 + 4.\) So the number of stars in the rectangular array can also be written as \(3 \cdot (5 + 4).\) Now, suppose we move the first five stars in each row over to the left, so that a space separates them from the rest of the stars in the same row. The effect is to split our rectangle into two rectangles. One rectangle has three rows with five stars in each row, so it contains \(3 \cdot 5\) stars. The other rectangle has three rows with four stars in each row, so it contains \(3 \cdot 4\) stars. Since we get the original rectangle by uniting the two smaller rectangles, the number of stars in the original rectangle is the sum of the numbers of stars in the two smaller rectangles. This fact is expressed in the statement that \(3 \cdot (5 + 4) = (3 \cdot 5) + (3 \cdot 4).\) We can verify the correctness of the statement by noting that \(3 \cdot 9 = 27,\) and \(15 + 12 = 27.\) In general, if \(a, b,\) and \(c\) stand for natural numbers, \(a \cdot (b + c) = (a \cdot b) + (a \cdot c).\) Similarly, \((b + c) \cdot a = (b \cdot a) + (c \cdot a).\) This rule is known as the distributive law and expresses the fact that multiplication is distributive with respect to addition. That is, the multiplier can be distributed among the individual terms in the expression it multiplies. In the statement of this law, multiplication and addition cannot change places. While \(3 + (5 \cdot 4) = 3 + 20 = 23,\ (3 + 5) \cdot (3 + 4) = 8 \cdot 7 = 56,\) so that addition is not distributive with respect to multiplication. It is customary, in writing an expression like \((a \cdot b) + (a \cdot c)\) to leave the parentheses out, so that it looks like this: \(a \cdot b + a \cdot c.\) In such an expression, which gives instructions for doing both multiplication and addition of some numbers, it is understood that the multiplications must be done first.

**The Five Laws**

We originally introduced the natural numbers as symbols for the cardinal numbers. Then we made these observations about them: There are two binary operations defined on the natural number system, and we call them addition
and multiplication. The properties of these operations are embodied in the addition and multiplication tables. By examining these tables, we found five laws that are obeyed by the natural number system: the commutative and associative laws of addition, the commutative and associative laws of multiplication, and the distributive law which asserts that multiplication is distributive with respect to addition. These laws have a special significance in the development of our notion of what a number is. We find that when we carry out computations with numbers we do not have to keep in mind their original meaning as cardinal numbers. It is enough to think of them as abstract symbols related to each other by addition and multiplication tables that obey these five laws. This fact suggests that we redefine numbers as follows: A number system is any collection of objects on which two binary operations called addition and multiplication are defined, such that addition is commutative and associative, multiplication is commutative and associative, and multiplication is distributive with respect to addition.

This definition is a declaration of independence for the idea of a number system. It frees it from its cardinal-number ancestry and permits it to lead its own life. It allows it to expand and grow. When a number system is defined in this way, we find that there is not just one number system, but many number systems. We find, too, that it is possible for one number system to be part of a larger number system, which in turn is part of a still larger number system, and so on. In fact, the core of this book is the systematic construction of larger and larger number systems, using the natural numbers as a foundation. At each stage of the construction we shall recognize that we have operations that obey the five laws:

I. \( a + b = b + a \)
II. \( (a + b) + c = a + (b + c) \)
III. \( a \cdot b = b \cdot a \)

IV. \( (a \cdot b) \cdot c = a \cdot (b \cdot c) \)
V. \( a \cdot (b + c) = a \cdot b + a \cdot c \)
or \( (b + c) \cdot a = b \cdot a + c \cdot a \)

Large and Small Numbers

The natural number system has some other important characteristics besides the five laws. One of these is that we can compare any two numbers in it for size. The number 5 is larger than 4, and 4 in turn is larger than 3. The notion of larger and smaller is derived from addition in this way: We say that \( b \) is larger than \( a \) if \( b \) is equal to the sum of \( a \) and some other natural number. For example, 5 is larger than 4, because \( 5 = 4 + 1 \); 5 is larger than 3, because \( 5 = 3 + 2 \).

One System with Many Disguises

There are many different ways of writing the natural numbers. In the system of Arabic numerals that we use every day, the numbers one, two, three, four and five are written as 1, 2, 3, 4, 5. In Roman numerals, still used on clock faces and monuments, they are written as I, II, III, IV, V. In Hebrew they are written as the first five letters of the alphabet. If we think of these different systems of numerals as symbols for the cardinal numbers, then they are different ways of representing one and the same number system. However, we may also think of each system of numerals as a separate number system in its own right, with addition and multiplication defined by its addition and multiplication tables. The Arabic, the Roman, and the Hebrew numerals could then be referred to legitimately as three separate number systems. But they are number systems that can be used interchangeably, so, although they are separate systems, they are still somehow the same. In order to recognize when number systems are interchangeable, and when they are not, we have to define what we mean when we say different systems are the same.
What we have in mind is that they have the same structure. For two number systems to have the same structure, each number in one system must have a counterpart in the other system. We can express this requirement in technical language by saying that there must be a mapping of one system into the other that places them in one-to-one correspondence. But the one-to-one correspondence alone is not enough. We want to be sure, too, that the results of computations in one system will correspond to the results of computations in the other system. So we say that two number systems have the same structure, or are isomorphic, if (1) there is a mapping of one into the other that puts them into one-to-one correspondence, and (2) under this mapping, sums and products are preserved. The requirement can also be stated in this way: Under the mapping, each element in one system has an image in the other. Moreover, the image of the sum of two numbers is the sum of the images; and the image of the product is the product of the images. Comparing Arabic numerals and Roman numerals, for example, we can set up a one-to-one correspondence, shown in part in this table:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>I</th>
<th>II</th>
<th>III</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>II</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>III</td>
<td>IV</td>
<td>V</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>IV</td>
<td>V</td>
<td>VI</td>
</tr>
</tbody>
</table>

Each system has its own addition and multiplication tables, part of which is shown in the customary square arrangements below:

**Addition**

<table>
<thead>
<tr>
<th>+</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

**Multiplication**

<table>
<thead>
<tr>
<th>•</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>•</th>
<th>I</th>
<th>II</th>
<th>III</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>I</td>
<td>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>II</td>
<td>II</td>
<td>IV</td>
<td>VI</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>III</td>
<td>III</td>
<td>VI</td>
<td>IX</td>
</tr>
</tbody>
</table>

Under the mapping the image of 2 is II, and the image of 3 is III. The sum of 2 and 3 is 5. The sum of II and III is V, which is the image of 5. So the sum of the images is the image of the sum. The product of 2 and 3 is 6. The product of II and III is VI, which is the image of 6. So the product of the images is the image of the product. Arabic numerals and Roman numerals, considered as separate number systems, are isomorphic to each other. Although numbers in one system look different from numbers in the other system, the relationships within the systems, as expressed in the addition and multiplication tables, have the same structure. So the two systems are really only one structure appearing in two different styles of dress.

**Zero and One**

Arabic numerals displaced all others because of their great convenience. They are most convenient to use because they give us a way of writing an indefinite amount of numbers while using only a small number of symbols called digits. This feat is accomplished by attaching different meanings to the same digit. In the number 111, three one's are used, and each has a different meaning. The 1 on the extreme right stands for the number one. The 1 in the second column from the right stands for the number ten, and the 1 in the third column stands for the number one hundred. The symbol stands for the sum of one, ten, and one hundred. Because the meaning of a digit depends on its position in the written numeral, we say the Arabic system of numerals is a place value system. To represent three hundreds plus two tens plus five ones, we write 325.
Now suppose we want to write the symbol for three tens. We put a 3 into the second column from the left. But we won't recognize it as the second column unless we write something down in the first column. This makes it necessary to think of three tens as three tens plus no ones, and to introduce a symbol to represent the absence of ones. We use the symbol 0 for this purpose, and call it zero. The concept of a number representing none was first conceived by the Hindus, and was later taken over by the Arabs and built into their system of numerals. Zero became a new number in the natural number system, and had to be incorporated into the addition and multiplication tables in a way which is consistent with the rest of the tables. This was done by using these rules for computation with zero: zero plus any number gives that number again; and zero times any number gives zero. The first of these rules can be written in symbols as follows: \( 0 + x = x \), for any natural number \( x \). In later chapters, we shall be building up some other number systems. It will be necessary for us to find out whether these number systems contain an element that behaves like the zero of the natural number system. In our search for a zero element, we shall use the number \( a \) such that \( a + x = x \), for all numbers \( x \) in that system, then we shall call \( a \) a zero element.

The distinguishing feature of a zero element is that adding it to another number leaves that number unchanged. There is a natural number that has the same relationship to the number one, which obeys the rule: \( 1 \cdot x = x \), for all leaves that number unchanged. In the number systems we explore later, we shall sometimes find an element that has this property, and shall call it a unity element.

When we write out sums, we always use the symbol +; wished, use some other symbol instead, as long as we agreed on its meaning. We might, for example, use the symbol * to represent the operation. In that case, the characteristic property of 0 could be written in this way: \( 0 \ast x = x \). In the same way, we could, if we wished, change the symbol for multiplication. If, temporarily, we used the symbol \( * \) to represent multiplication, then the characteristic property of 1 would be written as follows: \( 1 \ast x = x \).

The similarity in form of these two statements emphasizes the fact that 0 and 1 really both have the same property, except that each has it in relation to another operation. They are both examples of what is known as an identity element. In any system in which a binary operation is defined, and is symbolized by \( \ast \), if there is an element \( e \) that has the property \( e \ast x = x \), for all values \( x \) in the system, then \( e \) is called an identity element. The letter \( e \) is used in this definition of an identity element because it is the initial letter of the German word einheit, which means unity.

Now we can state more precisely how the terms zero element and unity element are used in mathematics today. Whenever a binary operation is denoted by the symbol + and is called “plus,” the identity element for that operation is called a zero element, and is denoted by 0. Whenever a binary operation is denoted by the symbol \( \ast \), and is called “times,” the identity element for that operation is called a unity element and is denoted by 1. We shall use this convention many times in later chapters.

Points on a Line

It is possible to represent the natural numbers as points on a line. On any straight line, choose a point and call it 0. This point divides the line into two half-lines. On one of these half-lines, choose another point and call it 1. Now continue locating points further and further away from 0 by making the distance from each point to the next one the same length as the distance from 0 to 1. Label these points 1, 2, 3, 4, 5.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
</table>
new points successively 2, 3, 4, 5, etc. We then have an endless sequence of points that is in one-to-one correspondence with the natural number system. The number attached to each point is its distance from 0, expressed in terms of the distance from 0 to 1 as the unit of length.

We can define addition and multiplication for these points by means of geometric constructions. Here, for example, is one way of doing it: To add \(a\) and \(b\), measure out from \(a\), in the direction away from 0, a length equal to the distance from 0 to \(b\). The point located in this way has a distance from 0 equal to \(a + b\). To multiply \(a\) and \(b\),

first draw another line intersecting this one at 0. Use the same scheme for assigning numbers to points on this line. Locate points 1', 2', 3', etc., on the line, so that successive points are separated by equal distances, all equal to the distance from 0 to 1'. Join 1' on the new line to \(a\) on the original line. Locate \(b\)' on the new line at a distance from 0 equal to \(b\). Then through \(b\)' draw a line parallel to the line just drawn from 1' to \(a\). It will cross the original line at a point that will represent \(a \cdot b\).

The construction for addition obviously corresponds to ordinary addition of numbers. The construction for multiplication corresponds to ordinary multiplication for this reason: If we designate by \(x\) the point that we have defined

as the product of \(a\) and \(b\), then \(x\) is its distance from 0. The triangles (0 1' \(a\)) and (0 \(b\)' \(x\)) are similar, so their corresponding sides are proportional. Then \(1 : b = a : x\). From this proportion, we find that \(x = a \cdot b\). With addition and multiplication defined by these constructions, the system of points on the half-line is isomorphic to the natural number system.

After we have assigned numbers in this way to points on a line, we find that there are still many points on the line that do not have numbers. All of our numbers are on one side of 0. There are none on the other side. Moreover, we
A set of elements is called a natural number system if it has the following characteristics:

1. It contains an element called 1.
2. For every member in the system, there is another member (and only one) called its successor.
3. Two distinct members do not have the same successor.
4. There is no member of the system that has 1 as its successor.
5. If a set of elements belonging to the system contains 1, and, for each member that it contains, also contains its successor, then this set contains the whole system.

Notice that addition and multiplication are not mentioned in these axioms at all. Peano defined these operations in terms of his axioms as follows: For any natural numbers $x$ and $y$,

- $x + 1$ = the successor of $x$;
- $x + (\text{the successor of } y) = \text{the successor of } (x + y)$;
- $x \cdot 1 = x$;
- $x \cdot (\text{the successor of } y) = x \cdot y + x$.

With these definitions it is possible to prove that the natural number system obeys the five laws.

What Peano did for the natural number system is typical of the way in which mathematical structures are studied today. In modern mathematics, a mathematical structure is often defined as a set of objects that satisfies a specified set of axioms. If the structure defined is to be unique, the axioms are chosen so that all systems that satisfy the axioms will be isomorphic to each other. Different sets of axioms have been formulated for the various mathematical structures needed in practical applications.

**DO IT YOURSELF**

1. By using double-headed arrows, as on page 26, set up a one-to-one correspondence between the numbers 1, 2,
3, 4, 5 and the letters a, e, i, o, u.

2. An addition operation for the system consisting of two elements, a and b, is defined by the following table:

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
</tr>
</tbody>
</table>

a) Does this system have a zero element?
b) Show that addition is commutative in this system.
c) Verify from the table that \( a + (a + b) = (a + a) + b \).

3. Let the symbol \( M \) stand for the binary operation, “take the maximum of.” For example, \( 5 M 7 \) means 7; \( 8 M 3 \) means 8; \( 6 M 6 \) means 6. Compare \( 8 M 3 \) with \( 3 M 8 \). If \( a \) and \( b \) are any two natural numbers, compare \( a M b \) with \( b M a \). Is the operation \( M \) commutative? Compare \( 8 M (3 M 7) \) with \( (8 M 3) M 7 \). In general, if \( a \), \( b \), and \( c \) are any three natural numbers, compare \( a M (b M c) \) with \( (a M b) M c \). Is the operation \( M \) associative?

4. In Ex. 2, an addition operation is defined for the set whose elements are \( a \) and \( b \). If this operation obeys an associative law, then \( x + (y + z) = (x + y) + z \) for all values of \( x \), \( y \) and \( z \).

a) The associative law stated above is an abbreviated way of making eight separate statements, obtained by replacing \( x \), \( y \) and \( z \) by \( a \) or \( b \). Write these eight statements.
b) Prove the associative law for this system by verifying from the table that all eight statements are true.

**CHAPTER II**

*Number Systems without “Numbers”*

THE word “number,” as we use it in everyday life, refers to a symbol associated with counting or measuring. We have broken away from this usage in the definition of a number system given in Chapter I. We defined a number system as any set of objects on which two binary operations are defined that obey the five laws listed on pages 24-5. In this definition, there is no reference to counting or measuring. The five laws are concerned only with the way in which the numbers are related to each other by the addition and multiplication tables. To emphasize this fact, we separated the concept of natural number from that of cardinal number. While cardinal numbers are properties of actual sets of objects, and are intrinsically related to counting, natural numbers are abstract symbols whose entire meaning lies in the formal rules by which we manipulate them.

Nevertheless, the natural numbers do not convey the full meaning of our break with common usage in the definition of number. Introducing the natural numbers effected a separation from the cardinal numbers, but not a divorce. The cardinal number system is still lurking in the background, because it is isomorphic to the natural number system. This fact may arouse the suspicion that no significant change in the concept of number has really been introduced, and that numbers are still essentially bound up with counting and measuring. However, a real change has been introduced by our definition of number system. The
purpose of this chapter is to demonstrate this fact convincingly by producing some number systems without "numbers." These number systems will consist of elements that have no direct relationship to counting or measuring, and so are not "numbers" in the sense in which the word is commonly used. However, they will be genuine number systems in the sense of our definition.

Subsets of a Set

We shall construct these number systems with the help of the simple notion of a set. A set is any collection of objects. The objects that belong to a set are called its elements. A set is defined by specifying which objects are elements of the set. This may be done by stating some rule by which the elements can be identified, or by actually putting the elements on display. The symbol commonly used for a set is a pair of braces, with the elements of the set on display inside, or with the rule by which they are identified printed inside. For example, here is a set defined by a rule:

{natural numbers larger than 4, but less than 10}

The same set can be represented by putting its elements on display:

{5, 6, 7, 8, 9}

Other sets can be formed from a given set by removing some of its elements. For example, if we remove the elements 5, 7, and 8 from the set shown above, we are left with the set {6, 9}. It is convenient to extend the notion of set to include what is left if we remove all the elements. It is called a "set" with no elements in it, and will be referred to as the empty set. To symbolize it, we shall show a pair by removing none, or some, or all of the elements of a given set A. A set obtained by removing none, or some, or all of the elements of a given set A has eight subsets, listed below:

\{x, y, z\} \{x, y\} \{x, z\} \{y, z\}
\{x\} \{y\} \{z\} \{\}\n
Notice that the given set is one of its own subsets, and the empty set is one of the subsets, too.

Operations on Subsets

To define a number system, we must first specify what the elements of the number system are. We shall use as elements all the subsets of a given set. As a specific example, let us build a number system out of the subsets of the set \{x, y, z\}. For convenience in talking about them, let us assign a name to each of these subsets. We shall use capital letters for their names, as follows:

\[ I = \{x, y, z\} \quad D = \{x\} \]
\[ A = \{x, y\} \quad E = \{y\} \]
\[ B = \{x, z\} \quad F = \{z\} \]
\[ C = \{y, z\} \quad 0 = \{\} \]

The symbols I and 0 are included among the names used for reasons that will become clear later.

The next step is to define two binary operations on these elements. A binary operation is defined when we set up some rule for assigning to each ordered pair of subsets some particular subset in the same list. We define the operation of forming a union of two subsets by means of this rule: The union of two subsets is another subset formed by taking as its elements those elements that are in one or the other of the subsets being united. For example, A contains the elements x and y. B contains the elements x and z. The union of A and B is the set \{x, y, z\}, which we have called I. The union operation will be the "addition" operation of this number system. However, we shall not use the plus sign to represent it. Instead, we shall use the symbol \(\cup\). The union of A and B will be written as \(A \cup B\), and is read as "A union B." We have seen that \(A \cup B = I\). The method
of finding the union of two subsets will be clear from the following examples:

\[
\begin{align*}
I \cup C &= \{x, y, z\} \cup \{y, z\} = \{x, y, z\} = I \\
D \cup E &= \{x\} \cup \{y\} = \{x, y\} = A \\
C \cup 0 &= \{y, z\} \cup \{\} = \{y, z\} = C
\end{align*}
\]

The results of forming all possible unions can be summarized in this table of unions (the addition table for the number system we are constructing):

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>A</td>
<td>I</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td>B</td>
<td>I</td>
<td>B</td>
<td>I</td>
<td>B</td>
<td>I</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>I</td>
<td>AB</td>
<td>I</td>
<td>D</td>
<td>A</td>
<td>B</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>I</td>
<td>C</td>
<td>A</td>
<td>E</td>
<td>C</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>F</td>
<td>I</td>
<td>B</td>
<td>C</td>
<td>B</td>
<td>C</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>0</td>
<td>I</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
</tbody>
</table>

The intersection of two subsets is another subset formed by taking as its elements all those elements that are in both of the subsets being intersected. For example, \(A\) contains the elements \(x\) and \(y\). \(B\) contains the elements \(x\) and \(z\). Only the element \(x\) is in both \(A\) and \(B\). So the intersection of \(A\) and \(B\) is the subset \(\{x\}\), which we have called \(D\). The intersection operation will be the "multiplication" operation of the number system we are constructing. We shall designate it by the symbol \(\cap\).

\[
\begin{align*}
I \cap C &= \{x, y, z\} \cap \{y, z\} = \{y, z\} = C \\
A \cap D &= \{x, y\} \cap \{x\} = \{x\} = D \\
B \cap 0 &= \{x, z\} \cap \{\} = \{\} = 0 \\
E \cap F &= \{y\} \cap \{z\} = \{\} = 0
\end{align*}
\]

The results of forming all possible intersections can be summarized in this table of intersections (the multiplication table for the number system we are constructing):

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>D</td>
<td>B</td>
<td>F</td>
<td>D</td>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>E</td>
<td>F</td>
<td>C</td>
<td>0</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>0</td>
<td>D</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
<td>E</td>
<td>0</td>
<td>E</td>
<td>0</td>
<td>E</td>
<td>0</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>0</td>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
1. The commutative law of addition. Union is our addition operation, so we must see whether \( X \cup Y = Y \cup X \), where \( X \) and \( Y \) represent any subsets of \( I \). \( X \cup Y \) means the set that consists of those elements that are in \( X \) or \( Y \), \( Y \cup X \) means the set that consists of those elements that are in \( Y \) or \( X \). These are obviously the same sets, so law number 1 is obeyed.

2. The associative law for unions. We must see whether \((X \cup Y) \cup Z = X \cup (Y \cup Z)\). The set \((X \cup Y) \cup Z\) is the set consisting of elements that are in \( X \) or \( Y \), or in \( Z \). The set \(X \cup (Y \cup Z)\) is the set consisting of elements that are in \( X \), or in \( Y \) or \( Z \). These are obviously the same sets, so law number 2 is obeyed.

3. The commutative law of multiplication. Intersection is our multiplication operation, so we must see whether \( X \cap Y = Y \cap X \). \( X \cap Y \) means the set consisting of elements that are in both \( X \) and \( Y \). \( Y \cap X \) means the set consisting of elements that are in both \( Y \) and \( X \). These are obviously the same sets, so law number 3 is obeyed.

4. The associative law for intersections. \((X \cap Y) \cap Z\) means the set consisting of elements that are in \( X \) and \( Y \), and also in \( Z \). \( X \cap (Y \cap Z)\) means the set consisting of elements that are in \( X \), and also in \( Y \) and \( Z \). Clearly, then \((X \cap Y) \cap Z = X \cap (Y \cap Z)\), and law number 4 is obeyed.

5. The distributive law. We must see if \( X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \). \( X \cap (Y \cup Z) \) means the set consisting of elements that are in \( X \) and in \( Y \) or \( Z \). \((X \cap Y) \cup (X \cap Z)\) means the set consisting of elements that are in \( X \) and \( Y \), or in \( X \) and \( Z \). These are clearly the same sets, so law number 5 is obeyed.

Since the five laws are obeyed, the system of subsets of \( I \), with the operations union and intersection, forms a number system. Similar number systems can be constructed from the subsets of any given set. In the example just given, we started with a set that contains three elements, and found that it has eight subsets. As a result we obtained a number system that contained exactly eight members. Had we started with a different number of elements, we would have obtained a number system with a different number of members. For example, a set with two elements has four subsets. A set with four elements has sixteen subsets. A set with five elements has thirty-two subsets. In general, a set with \( n \) elements has \( 2^n \) subsets.

Zero and Unity Elements

The number system we have constructed has a zero element and a unity element. Since union is our addition operation, a zero element would have to have the property that when it is united with any element of the system, it leaves that element unchanged. A glance at the union table on page 38 shows that the empty set has this property. That is why we used the symbol 0 to represent it. Since intersection is our multiplication operation, a unity element would have to have the property that when it is intersected with any element of the system, it leaves that element unchanged. A glance at the intersection table on page 39 shows that the original set \( I \) has this property. We chose the symbol 1 to represent it because of its resemblance to the number 1.

Special Properties

The number system we have just constructed out of the subsets of \( \{x, y, z\} \) has, as we have seen, some properties that it shares with the natural number system. These include obedience to the five laws, and possession of a zero element and a unity element. However, it also has some peculiar properties that are entirely unlike the properties of the natural number system. A few of these are noted here.

1. We can see from the tables that for any element \( X \) in the system, \( X \cup X = X \), and \( X \cap X = X \). That is, a subset united with itself yields the same subset, and a subset intersected with itself yields the same subset. In the natural number system, such an outcome is the exception rather than
The rule. 0 + 0 = 0, but 2 + 2 is not 2. 1 • 1 = 1, but 2 • 2 is not 2.

2. We have already observed that intersection is distributive with respect to union. It can also be verified that union is distributive with respect to intersection. That is, in the statement of the distributive law, union and intersection can change places. This, too, is unlike what we found in the natural number system. There, while multiplication is distributive with respect to addition, addition is not distributive with respect to multiplication.

3. For each subset in the system, we can find another one that contains just those elements that the first one does not. We call this second subset the complement of the first one, because, while they do not overlap (their intersection is 0), together they complete the original set (their union is I). If X is any subset in the system, we denote its complement by X'. In the system of subsets of \{x, y, z\}, A = \{x, y\}, so A' = \{z\} = F. Similarly, B' = E, C' = D, and Y' = 0. The operation of "taking the complement" has the following properties:

\[ X \cap X' = 0, \quad X \cup X' = I; \quad (X')' = X. \]

It also obeys the very useful law known as De Morgan's Rule: The complement of a union is the intersection of the complements; and the complement of an intersection is the union of the complements. Written out in symbols, the law says:

\[ (X \cup Y)' = X' \cap Y'; \quad (X \cap Y)' = X' \cup Y'. \]

The truth of the law can be observed by noting that a union consists of elements in one set or the other, an intersection consists of elements in one set and another, and a complement consists of the elements not in a particular set. Then De Morgan's rule says that "not in either X or Y" is the same as "not in X and not in Y"; and that "not in both X and Y" is the same as "not in X or not in Y." A little thought will show that these statements are correct.

The Algebra of Logic

The number system we have constructed in this chapter is only one of a whole family of number systems that have similar properties. They are called Boolean algebras. The type of structure that they represent is not just a mathematical curiosity. It has an important practical application in the study of logic, and in the design of electronic computers. In logic we study relationships among statements. The analysis of these relationships can be carried out in symbols in the following way: Let each proposition or statement be represented by a letter, such as p, q, or r. Use the symbol \( \lor \) for "or," the symbol \( \land \) for "and," and the symbol \( \sim \) for "not," as we already have done in the last paragraph. Use 0 for any statement that is false, and 1 for any statement that is true. With this notation, the class of statements and their logical relations becomes a Boolean algebra. Boolean algebras are named after the English mathematician, George Boole, who pioneered in the study of symbolic logic.

DO IT YOURSELF

1. Assign names to the subsets of the set \{x, y\} as follows:
   \[ I = \{x, y\}, \quad A = \{x\}, \quad B = \{y\}, \quad 0 = \{\} = \text{the empty set}. \]
   a) Construct a table for the union operation for this system of subsets.
   b) Construct a table for the intersection operation.

2. Let I represent the set \{a, b, c, d, e, f, g, h\}.
   Let X represent the subset \{a, b, c, d\}.
   Let Y represent the subset \{a, b, e, f, g\}.
   a) What elements are in X', the complement of X in I?
   b) What elements are in Y', the complement of Y in I?
   c) What elements are in X' \cup Y'?
   d) What elements are in X \cap Y?
   e) What elements are in \( (X \cap Y)' \)?
   f) Compare your answers to c) and e) to show that \( X' \cup Y' = (X \cap Y)' \).

3. List all the sixteen subsets of the set \{a, b, c, d\}.
CHAPTER III

New Numbers from Old

Questions That Have No Answers

IN OUR everyday use of the natural numbers, besides adding them and multiplying them, we sometimes have occasion to subtract them. The operation of subtraction can be defined in terms of addition. The symbol $5 - 3$ really asks us the question, “What natural number added to 3 gives 5?” Since the answer to the question is the number 2, we say $5 - 3 = 2$. We call the answer the difference between 5 and 3. The question can also be written in the form of an equation, $x + 3 = 5$, and the answer to the question is the solution to the equation.

Our success in finding the difference between 5 and 3 tempts us to try to find the difference between any two natural numbers chosen at random. But then we run into trouble. Suppose, for example, we try to find the difference between 3 and 5, written as $3 - 5$. First we have to interpret the symbol as a question. It asks us, “What natural number added to 5 gives 3?” Unfortunately, the answer is that there isn’t any such number. In the natural number system, we cannot subtract any number from any other number. The only time subtraction is possible in that system is when the subtrahend is not larger than the minuend. If $a$ and $b$ stand for any natural numbers, then the expression $a - b$ doesn’t always have a meaning. If we think of it as the question, “What natural number added to $b$ gives $a$?”, then it doesn’t always have an answer. If we use the equation $x + b = a$, a solution. This is a defect of the natural number system that limits its usefulness. Because, although the question $3 - 5$ is meaningless for the natural number system, there are practical problems that lead to just such a question. For example, if the temperature is 3 degrees, what will it be after the mercury drops 5 degrees? It would be useful to have a number system which contains a number that can serve as the answer to this question. The defect of the natural number system that we have observed confronts us with a challenge. Can we construct a number system that does not have this defect? Can we build a number system in which subtraction is always possible for any pair of numbers taken in any order, so that $a - b$ always has a meaning, and $x + b = a$ always has a solution? We find that we can.

Readers who have had high school algebra will remember that a system of numbers that includes “negative” as well as “positive” numbers is supposed to serve this purpose. But in their course in high school algebra, they were given this system as a finished product obeying certain mysterious rules such as, “the product of two negative numbers is a positive number.” In what follows, we do not take the existence of such a number system for granted. We prove it exists by actually constructing it. We also remove the mystery surrounding its rules by actually deriving them from the familiar rules governing the system of natural numbers.

Families of Differences

To construct the improved number system, we use a rather interesting device. The symbol $a - b$ asks us a question which does not always have an answer. To make sure that it will have an answer in the new system, we let the question be its own answer! In effect we say, let each expression like $5 - 3$, or $3 - 5$, or $2 - 7$, represent a number in the new system. To justify calling these strange things numbers we shall have to define addition and multiplication operations for them, and then show that with these operations they really constitute a number system.
However, we run into some complications even before we take our first step in this direction. In the natural number system, $5 - 3$ does have an answer, and the answer is 2. But $2 - 0, 3 - 1, 4 - 2, 6 - 4$, and an endless list of similar symbols also represent 2. So we cannot simply let each such symbol stand for a separate number in the new system. We would want all of these symbols to represent the same number, just as they do in the natural number system. We take care of this difficulty by using as the elements of our new number system, not single symbols written in the form of a “difference” between two natural numbers, but whole families of such differences. The first step is to establish a rule by which we can recognize when two such symbols belong to the same family. We get a clue to the rule we should use by examining the difference symbols that represent the number 2. The difference $3 - 1$ and the difference $6 - 4$ represent the same number. Notice that if we add the left number of each symbol to the right number of the other, we get the same sum: $3 + 4 = 6 + 1$. We shall use this relationship as the criterion for identifying differences that belong to the same family.

Now we are ready to carry out our construction step by step. First we take all possible ordered pairs of natural numbers, such as 7 and 5, 3 and 9, 15 and 1, and so on. Then we write the “difference” of the numbers in the pair, taken in a definite order. Since the difference does not always have a meaning in the natural number system, we shall not use an ordinary minus sign when we write it. We shall use the symbol $\sim$ instead, to remind us that this is really not subtraction of natural numbers, but merely a symbol suggested by subtraction. So we now have symbols like $7 \sim 5$, $3 \sim 9$, $15 \sim 1$, and so on, each of which will be called a “difference” between natural numbers.

Now we associate with each difference a whole family of differences in the following way: The family belonging to a difference $a \sim b$ consists of all those differences $u \sim v$ for which $a + v = u + b$. To designate the family that belongs to a difference we shall write that difference inside parentheses. Thus $(a \sim b)$ means the family of differences that belong to $a \sim b$. The symbol $(3 \sim 1)$ means the family of differences that belong to $3 \sim 1$. We have already seen that the difference $6 \sim 4$ belongs to this family because $3 + 4 = 6 + 1$. We call these families of differences integers. They will be the elements of our new number system.

We observe immediately two characteristics of these families which we call integers:

1) A difference belongs to its own family. For example, $3 \sim 1$ belongs to $(3 \sim 1)$. This follows from the fact that $u \sim v$ belongs to $(a \sim b)$ if $a + v = u + b$. In this case, $a = 3, b = 1, u = 3, v = 1$, and $3 + 1 = 3 + 1$. In general, $a \sim b$ belongs to $(a \sim b)$ because $a + b = a + b$.

2) If one of two differences belongs to the family of the other, then they have the same families. Suppose, for example, that $a \sim b$ belongs to the family $(c \sim d)$. Then we can show that every member of $(a \sim b)$ belongs to $(c \sim d)$, and vice versa. If $p \sim q$ belongs to $(a \sim b)$, then by the criterion for membership in a family, $a + q = p + b$. However, $a \sim b$ belongs to $(c \sim d)$, so $c + b = a + d$. Adding these two equalities, we get $a + b + c + q = a + b + p + d$. Taking away $a + b$ from both sides, we get $c + q = p + d$. But this is equivalent to saying that $p \sim q$ belongs to $(c \sim d)$, according to our criterion for membership in a family. This shows that any member of $(a \sim b)$ also belongs to $(c \sim d)$. A similar argument, going through the same chain of steps in reverse, shows that every member of $(c \sim d)$ also belongs to $(a \sim b)$. So the families $(a \sim b)$ and $(c \sim d)$ have the same memberships, and are therefore the same.

The second characteristic of these families called integers has these consequences: First, each difference $a \sim b$ belongs to one and only one integer. Secondly, an integer may be represented by putting on display inside parentheses any one of the differences that belong to it. So $(3 \sim 1), (4 \sim 2), (5 \sim 3)$ all represent the same integer. Thirdly, the criterion for membership in an integer can also serve as a test for membership in a family.
for equality of integers. That is, the integers \((a \sim b)\) and \((c \sim d)\) are equal if and only if \(a + d = c + b\). For example, to prove that \((3 \sim 1) = (4 \sim 2)\), it is enough to observe that \(3 + 2 = 4 + 1\).

Addition and Multiplication of Integers

Now we define addition and multiplication for the system of integers. We assign a sum to any ordered pair of integers by means of the following defining equation:

\[
(a \sim b) + (c \sim d) = (a + c \sim b + d)
\]

The symbol on the right hand side of this equation represents an integer, because, if \(a\) and \(c\) are natural numbers, \(a + c\) is also a natural number. Similarly, \(b + d\) is a natural number. Then \(a + c \sim b + d\) is a difference of natural numbers, and there is an integer that belongs to it.

We assign a product to any ordered pair of integers by means of the following defining equation:

\[
(a \sim b) \cdot (c \sim d) = (a \cdot c + b \cdot d \sim a \cdot d + b \cdot c)
\]

Here, too, the right hand side represents an integer, because the symbol inside the parentheses represents a difference of two natural numbers.

Notice that to find the sum of two integers, we make use of the natural numbers whose differences are on display inside the parentheses representing these integers. This fact leads to a problem that we have to pay attention to. Each integer is a family of differences. Any member of a family might be put on display to represent it. If we pick another difference to represent each of the integers we are adding, is useless. However, the definition was well chosen. If we follow the directions it gives for finding the sum of two integers, we are used to represent them. We shall verify it for a particular case. Suppose we want to add \((5 \sim 3)\) and \((6 \sim 5)\). Using our definition, we find that

\[
(5 \sim 3) + (6 \sim 5) = (5 + 6 \sim 3 + 5) = (11 \sim 8).
\]

However, \((5 \sim 3)\) could also be represented by \((4 \sim 2)\), because \(5 + 2 = 4 + 3\). Similarly, \((6 \sim 5)\) could also be represented by \((5 \sim 4)\), because \(6 + 4 = 5 + 5\). If we apply our definition to these other representatives of the two integers, we find that

\[
(4 \sim 2) + (5 \sim 4) = (4 + 5 \sim 2 + 4) = (9 \sim 6).
\]

By using different representatives for the two integers we were adding, we got sums that look different. However, although they look different, the sums are the same.

\[
(11 \sim 8) = (9 \sim 6), \text{ because } 11 + 6 = 9 + 8.
\]

The same problem arises in connection with our definition for multiplication of integers. The definition makes use of a particular difference that belongs to each integer. But it can be shown that it does not matter which difference that belongs to an integer is chosen as its representative. They all lead to the same product anyhow. So there is no ambiguity in our definitions of addition and multiplication.

The Integers Form a Number System

We now have a system of elements called integers, with an addition operation and a multiplication operation defined for this system. To show that the integers form a number system, we have to prove that the operations obey the five laws listed on pages 24-5. As an example of how such a proof is carried out, we give the details of the proof for the commutative law of addition. Let \((a \sim b)\) be any integer, and \((c \sim d)\) any other integer. We must show that

\[
(a \sim b) + (c \sim d) = (c \sim d) + (a \sim b).
\]

Applying our definition of addition of integers, we find that

\[
(a \sim b) + (c \sim d) = (a + c \sim b + d), \text{ while } (c \sim d) + (a \sim b) = (c + a \sim d + b).
\]

But natural numbers obey the commutative law for addition, so \(a + c = c + a\), and \(b + d = d + b\). This shows that \((a + c \sim b + d)\) and \((c + a \sim d + b)\) are the same integer. Therefore, \((a \sim b) + (c \sim d) = (c \sim d) + (a \sim b)\), and the commutative law for addition
of integers is true. The other four laws are proved by similar arguments, using the definitions of addition and multiplication of integers, and the fact that natural numbers are known to obey the five laws.

Zero and Unity

Let us add the integer \((0 \sim 0)\) to any other integer \((a \sim b)\). Following the definition of addition, we find that \((0 \sim 0) + (a \sim b) = (0 + a \sim 0 + b) = (a \sim b)\), since \(0 + a = a\) and \(0 + b = b\). In other words, when \((0 \sim 0)\) is added to any other integer, it leaves that integer unchanged. Therefore \((0 \sim 0)\) is a zero element for the system of integers. The integer \((0 \sim 0)\), like any other integer, is a family of differences, and may be represented by any one of these differences. We can identify what these differences look like by using the criterion for belonging to an integer. The difference \(x \sim y\) belongs to the family of differences \((0 \sim 0)\) if and only if \(0 + y = x + 0\), or \(y = x\). That is, a difference belongs to the integer \((0 \sim 0)\) if and only if the left number and the right number are equal. So \((1 \sim 1)\), \((2 \sim 2)\), \((3 \sim 3)\), and so on, are other ways of writing the zero element in the system of integers.

Let us see how the integer \((1 \sim 0)\) behaves under multiplication. Following the definition of multiplication, we find that \((1 \sim 0) \cdot (a \sim b) = (1 \cdot a + 0 \cdot b \sim 1 \cdot b + 0 \cdot a) = (a + 0 \sim b + 0) = (a \sim b)\). In other words, when \((1 \sim 0)\) is multiplied by any other integer, it leaves that integer unchanged. So \((1 \sim 0)\) is a unity element for the system of integers. It may also be written in the form \((a + 1 \sim a)\), where \(a\) is any natural number. This follows from the test for equality of integers, because \(a + 1 + 0 = 1 + a\).

The Negative of an Integer

Our purpose in constructing the system of integers was to find a number system in which an equation of the form \(X + B = A\) always has a solution. To show that we have achieved our purpose, we have to introduce a new concept, the concept of the negative of a number. We say that one number is the negative of another if the sum of the two numbers is zero. In the natural number system, there is only one number that has a negative. That number is \(0\), and it is its own negative, because \(0 + 0 = 0\). No other natural number has a negative, because if a natural number that is different from \(0\) is added to any other natural number, the sum is different from \(0\). However, the system of integers is altogether different in this respect: In the system of integers, every number has a negative. We prove this fact by actually producing the negative of any integer. Let \((a \sim b)\) be any integer. Then \((b \sim a)\) is its negative, because \((a \sim b) + (b \sim a) = (a + b \sim b + a) = \text{the zero integer}\), because, in the difference on display inside the parentheses, the left number is equal to the right number. Because every integer has a negative, we introduce a special symbol to mean "negative of." The minus sign is used for this purpose. If \(A\) stands for an integer, then \(-A\) is used to represent the negative of \(A\).

Now we are prepared to show that the equation \(X + B = A\) always has a solution, if \(X\), \(A\), and \(B\) stand for integers. We have used capital letters here to represent integers, so that we would not confuse them with natural numbers. Each integer is a family of differences of natural numbers, so the equation can also be written in this form: \((x \sim y) + (c \sim d) = (a \sim b)\). We solve the equation by adding the negative of \((c \sim d)\) to both sides. We get

\[
(x \sim y) + (c \sim d) + (d \sim c) = (a \sim b) + (d \sim c).
\]

But the sum of \((c \sim d)\) and \((d \sim c)\) is the zero integer. And the zero integer added to \((x \sim y)\) leaves it unchanged. So we have \((x \sim y) = (a \sim b) + (d \sim c) = (a + d \sim b + c)\). For example, to solve \((x \sim y) + (d \sim c) = (3 \sim 2)\), add \((1 \sim 8)\) to both sides. Then we get \((x \sim y) = (4 \sim 10)\).

On page 44 we saw that solving \(X + B = A\) was another way of saying subtract \(B\) from \(A\). Since, in the system of integers, the equation always has a solution, it means that subtraction is always possible in that system. In fact, our
method for solving the equation suggests an appropriate
definition for the subtraction of integers: To subtract an
integer, means to add its negative. This definition makes
sense in the system of integers, where every number has a
negative. We could not have defined subtraction of natural
numbers in the same way, because in the system of natural
numbers, it is not true that every number has a negative.

We Still Have the Natural Numbers

Among the integers, there are some special integers like
(0 ~ 0), (1 ~ 0), (2 ~ 0), (3 ~ 0), and so on, which are
written by putting on display a difference in which the
number on the right is 0. These special integers are called
positive integers. They can be placed in one-to-one corre-
spondence with the natural numbers by pairing off 0 with
(0 ~ 0), 1 with (1 ~ 0), 2 with (2 ~ 0), and so on. In gen-
eral, in this correspondence, each natural number a is
matched with the positive integer (a ~ 0).

Now let us see what happens when we add or multiply
any two positive integers, (a ~ 0) and (b ~ 0). For the
sum, we get (a ~ 0) + (b ~ 0) = (a + b ~ 0). So the sum
of two positive integers is a positive integer. For the
product, we get (a ~ 0) • (b ~ 0) = (a • b + 0 • 0 ~ a •
0 + 0 • b) = (a • b ~ 0). So the product of two positive
integers is a positive integer. Moreover, the sum of the
integers matched with a and b is the integer matched with
a + b; and the product of the integers matched with a and
b is the integer matched with a • b. That is, under the one-
to-one correspondence the sum of the images of two natural
numbers is the image of their sum; and the product of the
images is the image of the product.

So the positive integers are isomorphic to the natural
numbers. Because of the isomorphism, they can be used in-
stead of the natural numbers, just as Roman numerals
can be used instead of Arabic numerals. In this sense, we say
that the positive integers are the "same" as the natural
numbers. We take advantage of the isomorphism by using
the notation for natural numbers as an abbreviated nota-
tion for the positive integers. In this abbreviated notation
0 represents (0 ~ 0), 1 represents (1 ~ 0), and so on.

Since the system of integers includes the positive integers
which are just "like" the natural numbers, they constitute
an extension of the natural number system. Using the sys-
tem of integers instead of the system of natural numbers
gives us a double advantage: We eliminate a defect of the
natural number system, without losing the natural numbers
themselves.

The Negative Integers

Every integer can be represented by a difference in which
either the left number or the right number is 0. This can be
done by simply subtracting from each of these natural
numbers the smaller of the two. The result will be a differ-
ence that belongs to the integer, and so can be used to
represent it. For example, the integer (8 ~ 3) is equal to
(5 ~ 0). We know they are equal because 8 + 0 = 5 + 3.
The integer (3 ~ 8) is equal to (0 ~ 5), because 3 + 5 =
0 + 8. So every integer may be written in the form (a ~ 0)
or (0 ~ a). Those that can be written in the form (a ~ 0)
are the positive integers. Those that can be written in the
form (0 ~ a) are called negative integers. Each of them is
the negative of a positive integer. Using the symbol for "negative of," we get an abbreviated nota-
tion for them, too, by writing −a for (0 ~ a).

This is the form in which students are introduced to them
for the first time in courses in elementary algebra. The fa-
familiar rules for calculating with these symbols can all be
derived from our definitions for the addition and multi-
plication of integers. For example, the rule that the product
of two negative integers is a positive integer can be proved
as follows: (0 ~ a) • (0 ~ b) = (0 • 0 + a • b ~ 0 • b +
a • 0) = (a • b ~ 0), which is positive.

The positive integers, being essentially carbon copies of
the natural numbers, can be represented as the natural
numbers were on page 29, by points on the half-line that
lies to the right of the 0. We can represent the negative
numbers pictorially, too, by putting them on the other half of the line, on the other side of 0. Arranging them on a line suggests that we can talk about larger and smaller integers, just as we were able to talk about larger and smaller natural numbers. We give a meaning to the term larger as applied to integers by agreeing that one integer will be considered larger than another if it lies to the right of it on the line on which the integers are represented as points in the diagram below. The term can also be defined without reference to the picture. If \( a \) and \( b \) are two different integers, we say that \( a \) is larger than \( b \) if \( a - b \) is positive. It is understood here that \( a - b \) means \( a + \) the negative of \( b \), in accordance with the definition of subtraction of integers given on page 52. On the basis of this definition, 2 is larger than \(-7\), because \( 2 - (-7) = 2 + 7 = 9 \), which is positive. The integer \(-4\) is larger than \(-5\), because \( -4 - (-5) = -4 + 5 = 1 \), which is positive.

The Integers Form a Group

Before we proceed to any further extension of our number system, let us stay with the system of integers for a while to observe some of its properties. We shall find within the system of integers examples of some of the structures that form the typical subject matter of modern mathematics.

We have two binary operations defined for the system of integers, addition and multiplication. Let us disregard multiplication, and list some of the properties the system has in relation to the operation of addition alone. We observe these characteristics: 1) The operation of addition is associative. 2) The system contains an identity element, \( e \), with the property that \( 0 + x = x + 0 = x \). 3) For every element \( a \) in the system, its inverse \( a^{-1} \) is also in the system, with the property that \( a * a^{-1} = e \). The word “negative” is used for an inverse only in the special case where the operation is designated by \(+\) and is called “addition.”

Another Example of a Group

The type of structure known as a group has been singled out for special study by mathematicians because it is found in many places. The system of integers is only one of a multitude of systems that have a group structure. It happens to be a group that contains an infinite number of elements. But there are also groups that contain a finite number of elements. As an example of a finite group, let us examine the group of “symmetries” of an equilateral triangle.

An equilateral triangle has equal sides and equal angles. The symmetries of the triangle are motions that bring it into coincidence with itself. To get acquainted with these motions, it is best to see them in action as applied to a model. So, before reading the paragraphs that follow, cut
an equilateral triangle out of paper, and label its vertices A, B, and C, as shown in the diagram. Enter the labels on the reverse side of the paper, too, so that the vertices can be identified even when the triangle is turned over.

Let us begin with the triangle placed on a level surface so that one side, say BC, is horizontal, and the opposite vertex A lies above BC, as shown in the diagram below.

Now, as we discover motions that bring the triangle into coincidence with itself, we shall assign a name to each one. One motion that will qualify is a clockwise rotation of 120 degrees around the center of the triangle. The result of such a rotation is to put B in the place of A, A in the place of C, and C in the place of B. Let us call this rotation P. Another motion that qualifies is a clockwise rotation of 240 degrees. It puts C in the place of A, B in the place of C, and A in the place of B. Let us call it Q. Another "motion" that qualifies is a clockwise rotation of 0 degrees. This, of course, involves no movement of the triangle at all, and leaves A in the place of A, B in the place of B and C in the place of C. We shall call it I.

Before we go any further, let us make an agreement. We shall consider two motions as being the "same" if they have the same effect. A clockwise rotation of 360 degrees has the same effect as a rotation of 0 degrees, so it, too, will be called I. A counterclockwise rotation of 120 degrees has the same effect as a clockwise rotation of 240 degrees, so it, too, will be called Q. Similarly, a counterclockwise rotation of 240 degrees is the same as P.

There are three more motions that can bring the triangle into coincidence with itself. In one of them, we flip the triangle over to bring the bottom face up, while leaving the top vertex where it is. If we start with A at the top, B at the left, and C at the right, this motion puts A in its own place, and makes B and C change places. Let us call this motion R. A similar motion that keeps the vertex on the left fixed,
while the top vertex and the vertex on the right change places, will be called $S$. One which keeps the vertex on the right fixed, while the top vertex and the vertex on the left change places, will be called $T$.

We now have a system consisting of six elements, $I$, $P$, $Q$, $R$, $S$, and $T$. We define a binary operation $\ast$ for this system as follows: If $A$ and $B$ represent any two of these motions, the product $A \ast B$ is the motion that results when the two motions are performed one right after the other, with $B$ performed first, and $A$ taking over where $B$ leaves off. For example, $P \ast R$ means first perform $R$, then $P$. If we start with vertex $A$ at the top, $B$ at the left, and $C$ at the right, motion $R$ leaves $A$ at the top, and makes $B$ and $C$ change places. Then, from this position, motion $P$ rotates the triangle 120 degrees clockwise. As a result, $A$ moves to the position on the right, $B$ moves to the position on the left, and $C$ moves to the top. The effect is the same as if only the single motion $S$ had been used. So $P \ast R = S$. If we pick any two of the six motions at random, and perform one after the other, we find that the result is always one of the original six motions. The results of performing the operation $\ast$ can be summarized in the multiplication table shown below, where the motion that is performed first, and is written on the right hand side in a product, is listed at the top of the table, and the motion that is performed second, and is written on the left hand side in a product, is written at the side.

### Multiplication Table for Symmetries of the Triangle

<table>
<thead>
<tr>
<th></th>
<th>$I$</th>
<th>$P$</th>
<th>$Q$</th>
<th>$R$</th>
<th>$S$</th>
<th>$T$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I$</td>
<td>$I$</td>
<td>$P$</td>
<td>$Q$</td>
<td>$R$</td>
<td>$S$</td>
<td>$T$</td>
</tr>
<tr>
<td>$P$</td>
<td>$P$</td>
<td>$Q$</td>
<td>$I$</td>
<td>$S$</td>
<td>$T$</td>
<td>$R$</td>
</tr>
<tr>
<td>$Q$</td>
<td>$Q$</td>
<td>$I$</td>
<td>$P$</td>
<td>$T$</td>
<td>$R$</td>
<td>$S$</td>
</tr>
<tr>
<td>$R$</td>
<td>$R$</td>
<td>$T$</td>
<td>$S$</td>
<td>$I$</td>
<td>$Q$</td>
<td>$P$</td>
</tr>
<tr>
<td>$S$</td>
<td>$S$</td>
<td>$R$</td>
<td>$T$</td>
<td>$P$</td>
<td>$I$</td>
<td>$Q$</td>
</tr>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$S$</td>
<td>$R$</td>
<td>$Q$</td>
<td>$P$</td>
<td>$I$</td>
</tr>
</tbody>
</table>

To show that the symmetries of the triangle form a group, we have to prove that the three requirements for a group are satisfied. 1) The operation $\ast$ is associative. That is, if $A$, $B$, and $C$ are any three motions in the system, $A \ast (B \ast C) = (A \ast B) \ast C$. This can be verified from the table, or from the fact that both symbols, $A \ast (B \ast C)$, and $(A \ast B) \ast C$ require that $C$ be performed first, $B$ second, and $A$ third, so that both lead to the same result. The parentheses here signify no more than a pause between motions. 2) The system has an identity element. In fact $I$ is the identity element, because the table shows that if $X$ stands for any element, $I \ast X = X \ast I = X$. 3) For every element in the system, there is an inverse element that is also in the system. The inverse of $P$ is $Q$, and the inverse of $Q$ is $P$, because $P \ast Q = Q \ast P = I$. Each of the elements, $I$, $R$, $S$, and $T$ is its own inverse, because $I \ast I = I$, $R \ast R = I$, $S \ast S = I$, and $T \ast T = I$. 
$S \ast S = I$, and $T \ast T = I$. Therefore the symmetries of the triangle, with the operation $\ast$ as defined, form a group.

Not All Groups Are Commutative

We see from the multiplication table for the group of symmetries that $P \ast R = S$, and that $R \ast P = T$. Therefore $P \ast R$ is not equal to $R \ast P$. The operation $\ast$ in this group does not obey the commutative law. On the other hand, in the system of integers, which forms a group with the operation $+$, the operation is commutative. A group which obeys the commutative law is called a commutative group. It is also called an abelian group in honor of one of the pioneers in the study of groups, Niels Henrik Abel, who died at the age of 27 in 1829. It is now the custom to use the symbol $+$ to represent the binary operation in a group only if it is a commutative or abelian group. If the plus sign is used to designate the operation, then the word zero is used instead of identity, and the word negative is used instead of inverse.

Although the system of integers is the most commonly used system that has a group structure, it was not the first system to have its group structure analyzed. The first groups that were studied extensively were finite groups, like the group of symmetries of the triangle. They came up in the theory of equations, as studied by the methods of the French mathematician Evariste Galois. Galois recorded his findings in 1832 in a paper that he wrote the night before he was killed in a duel at the age of 21. After being neglected for about thirty years, they were saved from obscurity and extended by other mathematicians. Since then, the concept of a group has invaded every branch of mathematics.

The Integers Form a Ring

To observe the group structure of the system of integers, we disregarded the operation of multiplication. Now, if we put multiplication back into the picture, we find in the system of integers an example of another structure that plays an important part in modern mathematics, a ring. A system of elements is called a ring if there are two binary operations defined for the system, and they have these properties: 1) Both operations are associative. 2) The system is an abelian group with respect to one of the operations. This operation is designated by $+$, and is called addition. 3) The other operation is distributive with respect to addition. If we call it multiplication, and represent it by the usual symbol for "times," then the distributive law takes this form: $a \cdot (b + c) = a \cdot b + a \cdot c$; and $(b + c) \cdot a = b \cdot a + c \cdot a$. It is necessary to state the distributive law in two parts in this way, because the multiplication operation need not be commutative, so multiplication by $a$ from the left is not the same as multiplication by $a$ from the right.

The fact that the system of integers is a ring follows from the properties of the system that we have already seen.

Multiplication by Zero

One of the familiar rules of arithmetic that we use every day when we work with natural numbers is that zero times any number gives a product equal to zero. This rule turns out to be true in the system of integers as well. In fact, we can show that it has to be true in any system that has a ring structure. In any ring, if $x$ is any element, and $0$ is its zero element, $x + 0 = x$. Now multiply both sides of this equation by any other element in the ring, say $y$. Then we have $y \cdot (x + 0) = y \cdot x$. By the distributive law in the ring, we can replace $y \cdot (x + 0)$ by $y \cdot x + y \cdot 0$, so we get $y \cdot x + y \cdot 0 = y \cdot x$. Since the ring is a group with respect to addition, the element $y \cdot x$ has a negative, $-(y \cdot x)$. Let us add this negative to both sides of the equation. We get $-(y \cdot x) + y \cdot x + y \cdot 0 = -(y \cdot x) + y \cdot x$. But $-(y \cdot x) + y \cdot x = 0$, from the definition of a negative. So we now have $0 + y \cdot 0 = 0$. But since $0$ is a zero element for addition, $0 + y \cdot 0$ can be replaced by $y \cdot 0$. This leads to the conclusion that $y \cdot 0 = 0$. 

60
Hidden Groups and Rings

The group structure and ring structure that we have observed so far in the system of integers lie on the surface, we might say, because they embrace the system as a whole. However, there are more group and ring structures hidden within the system of integers as substructures. We shall produce some examples for examination.

Suppose we divide the integer 6 by 3. The quotient is 2, which is also an integer. Then 6 can be written as $2 \cdot 3$. There are other integers that can also be written as some integer times 3. For example, $-9 = -3 \cdot 3$. All such integers are called integral multiples of 3. The integral multiples of 3 form the set \{0, 3, -3, 6, -6, 9, -9, 12, -12, \ldots \}. The dots inside the brace indicate that there are many more members of the set besides those that are listed. A characteristic of all integral multiples of 3 is that when we divide them by 3, the remainder is 0.

The integers which are not multiples of 3 can be divided into two families. One family consists of those that are 1 more than an integral multiple of 3. For example, $7 = 6 + 1$, and $-5 = -6 + 1$, so 7 and $-5$ both belong to this family. Members of this family have the characteristic that when we divide them by 3, the remainder is 1. The other family consists of those integers that are 2 more than an integral multiple of 3. For example, $8 = 6 + 2$, and $-4 = -6 + 2$, so 8 and $-4$ belong to this family. Members of this family have the characteristic that when we divide them by 3, the remainder is 2. All integers therefore fall into one of three classes, depending on whether the remainder, when we divide by 3, is 0, 1, or 2. We call these classes residue classes modulo 3. For convenience in talking about them, we shall designate each class by the remainder which is characteristic of it. Here, then, are the three classes:

- 0 class: \{0, 3, 6, 9, 12, \ldots \}
- 1 class: \{1, 4, 7, 10, 13, \ldots \}
- 2 class: \{-1, -4, -7, -10, -13, \ldots \}

The 0 class has some interesting properties. Notice first that if we add any two members of the 0 class, the sum is itself a member of the 0 class. For example, $3 + (-6) = -3$. This is not true of the other two classes. For example, although 1 and 4 belong to the 1 class, their sum, $1 + 4 = 5$, which is not in the 1 class. Similarly, although 2 and 5 belong to the 2 class, their sum, $2 + 5 = 7$, which is not in the 2 class. Therefore, addition is a binary operation for the 0 class, but not for the 1 class or the 2 class. (Recall that a binary operation is defined for a set only by a mapping that associates with each pair of elements in the set another element in the same set.) Since addition is associative for the whole system of integers, it is surely associative when used with the members of the 0 class alone.

Notice, secondly, that the 0 class contains the identity element for addition, namely, 0. Moreover, for every element in the 0 class, its negative also belongs to the class. Therefore the 0 class satisfies all the requirements for being a group in its own right. In fact, since addition is commutative, it is even an abelian group. Because it is a group that is a subset of the larger group of integers, it is called a subgroup of the group of integers. The other two residue classes modulo 3 cannot qualify as subgroups with respect to addition, because, as we have seen, addition is not even a binary operation for them.

We can say even more about the 0 class. If we multiply any two members of the 0 class, the product is itself a member of the 0 class. So that multiplication is also a binary operation for this class. Moreover, it obeys the distributive law, so the 0 class satisfies all the requirements for being a ring in its own right. It is called a subring of the ring of integers.

We can say still more about the 0 class. If we multiply any member of the 0 class by any integer, whether it is in the class or not, the product is a member of the 0 class. For
example, \(4 \cdot 3 = 12\), which is in the 0 class, although 4 is not. A subring which has this property is called an ideal, so the 0 class modulo 3 is an ideal in the ring of integers.

The 0 class, considered as a ring, differs in one very important way from the ring of integers. It does not contain the number 1, which is the unity element for multiplication. So we see it is possible for a ring to be with or without a unity element.

**The Arithmetic of Residue Classes**

We are now going to construct a new number system whose elements are the residue classes modulo 3. To do so, we must define what we mean by addition and multiplication of these classes. We define addition as follows: To add two residue classes, pick one member from each class, and add these members. The class to which the sum belongs will be called the sum of those residue classes. For example, to add the 1 class and the 2 class, we might add 1 (chosen from the 1 class) to 2 (chosen from the 2 class). The sum is 3, which belongs to the 0 class. Therefore the 1 class plus the 2 class equals the 0 class. Our definition allows us a free choice in picking the numbers in each class that we will add. However, it makes no difference which ones we choose, because all members of the same class have the same remainder when divided by 3. Adding a representative from each of two classes is like adding their remainders, and the result is the same no matter which representative is chosen.

We can prove this fact for the illustration being given in this way: Any number in the 1 class is of the form \(3a + 1\). Any number in the 2 class is of the form \(3b + 2\). When we add them, we get \(3a + 1 + 3b + 2 = 3a + 3b + 3 = 3(a + b + 1)\), that is a multiple of 3, which is in the 0 class. For the sake of brevity, let us now drop the word class from the name of each class, and simply refer to them as 0, 1, and 2. Then we get the following addition table for residue classes modulo 3:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

We define multiplication in the same way: To find the product of two residue classes, multiply any member of one class by any member of the other. The class to which the product belongs is the product of the classes. For example, to multiply the 2 class by the 2 class, multiply 2 (chosen from the 2 class) by 5 (chosen from the 2 class). The product is 10, which belongs to the 1 class. So the 2 class times the 2 class equals the 1 class. As in the case of addition, it makes no difference which member of each class is chosen for carrying out the operation. Here, too, we drop the word class from the name of each class, and record the products in the following multiplication table for residue classes modulo 3:

<table>
<thead>
<tr>
<th>.</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

With these tables for addition and multiplication, the residue classes modulo 3 obey the five laws. Therefore they make up a number system consisting of only 3 elements. This number system is also both a group and a ring. It is a group with respect to addition, because 1) it contains a zero element, viz., the 0 class, and 2) for every element in the system, there is a negative in the system, too. The 0
class is a zero element, because, as the addition table shows, that class added to any other class leaves it unchanged: 0 + 0 = 0, 0 + 1 = 1, and 0 + 2 = 2. The negative of 0 is 0. The negative of 1 is 2, and vice versa, because 1 + 2 = 2 + 1 = 0. The group is abelian, because the addition operation is commutative. The system is also a ring, because, besides being an abelian group, it has a multiplication operation which is distributive with respect to addition. For example, 2 (1 + 2) = 2 (0) = 0, and 2 \cdot 1 + 2 \cdot 2 = 2 + 1 = 0. Therefore 2 (1 + 2) = 2 \cdot 1 + 2 \cdot 2.

Quotient Groups

The group that we have just observed contained as its elements a subgroup of the system of integers (the 0 class), and certain companion sets, the 1 class and the 2 class. The companion sets can be obtained from the subgroup by adding to each member of the subgroup some element that is not in it. For example, by adding 1 to each of the elements in the 0 class, we get all the elements of the 1 class. In fact, if we add any single member of the 1 class to each of the elements in the 0 class, we get all the members of the 1 class. Similarly, if we add any member of the 2 class to each of the elements of the 0 class, we get all the members of the 2 class. Companion classes that have this relationship to a subgroup are called its cosets. When a subgroup and its cosets are themselves elements of a group, the group they form is called a quotient group.

If we look back to the table for multiplication of the symmetries of a triangle (page 59), we shall find another example of a subgroup, its cosets, and a quotient group that they form. Here, of course, the group operation will be * instead of +. Notice, first, that when \( I, P, \) and \( Q \) are multiplied among themselves, the product is always \( I, \) or \( P, \) or \( Q. \) Therefore the operation * is a binary operation for the subset \( \{I, P, Q\}. \) The identity element \( I \) is in this subset, and the inverse of every element in the subset is also in the subset. In fact, the inverse of \( I \) is \( I, \) the inverse of \( P \) is \( Q, \) and the inverse of \( Q \) is \( P. \) Therefore the subset \( \{I, P, Q\} \) forms a subgroup with the operation * . Its coset is the set \( \{R, S, T\}. \)

Now let us assign a short name to each of these sets, by writing \( G = \{I, P, Q\}, \) and \( H = \{R, S, T\}. \) We can define an operation * on the system whose elements are \( G \) and \( H \) as follows. To multiply one set by another, pick an element from each set, and multiply them. For example, take \( P \) (from \( G \)) * \( S \) (from \( H \)). The product is \( T, \) which is in \( H. \) The set to which the product belongs will be called the product of the sets. Therefore \( G * H = H. \) As in the case of residue classes, it turns out that the product comes out the same no matter which representative we choose from each class to carry out the operation. The products we get can be summarized in this multiplication table:

\[
\begin{array}{c|cc}
* & G & H \\
\hline
G & G & H \\
H & H & G \\
\end{array}
\]

In this system of two elements, \( G \) is an identity element for the operation *, because \( G * G = G, \) and \( G * H = H * G = H. \) Also, there is an inverse for every element. In fact, each element is its own inverse, because \( G * G = G, \) and \( H * H = G, \) which is the identity element. Therefore the subgroup \( G \) and the coset \( H \) form a quotient group of the group of symmetries of the triangle. In this case, we can see why it is called a quotient group. The group of symmetries has 6 elements, the subgroup \( G \) has 3 elements, and the quotient group has \( 6 \div 3 = 2 \) elements. Not every subgroup, together with its cosets, will form a quotient group. Galois was the first to identify the special kind of subgroups that have this property. They are known as normal subgroups. In an abelian group all subgroups are normal.

We saw that the residue classes modulo 3 form a ring as well as a group. It is an example of a quotient ring. Just as in a group, a special kind of subgroup with cosets forms a
quotient group, in a ring, a special kind of ideal with its cosets form a quotient ring. In a ring in which the multiplication is commutative, all ideals have this property.

Residue Classes Modulo 6

We formed the residue classes modulo 3 by classifying the integers by the remainder you get when you divide by 3, using for this purpose only positive remainders that are less than 3, viz., 0, 1 and 2. If we use any other integer as divisor, we can divide the system of integers into residue classes modulo that integer in the same way. For example, when an integer is divided by 6, the remainder may be 0, 1, 2, 3, 4, or 5. This gives us six residue classes modulo 6. As we did in the case of residue classes modulo 3, let us use the remainder associated with each class as the name of the class. If we define addition and multiplication of residue classes the same way we did before, we get these addition and multiplication tables:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>.</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

With these tables, the residue classes modulo 6 form a ring. This ring has a peculiar feature that it does not share with the ring of integers. In the ring of integers, the only time a product of two elements equals 0 is when one of the multipliers is itself 0. On the other hand, in the ring of residue classes modulo 6, \(2 \cdot 3 = 0\), and neither 2 nor 3 is itself zero. Non-zero elements, like 2 and 3, which when multiplied give a zero product are called zero divisors. The ring of integers has no zero divisors, but the ring of residue classes modulo 6 does have zero divisors.

The absence of zero divisors in the ring of integers is the basis for one of the very important rules we all learned in elementary high school algebra, the cancellation law of multiplication. We learned that if \(2 \cdot x = 2 \cdot 3\), we may cancel the 2 on both sides of the equation, and conclude that \(x = 3\). The argument that proves this is correct proceeds as follows: Add the negative of \(2 \cdot 3\) to both sides of the equation. This gives us \(2 \cdot x - 2 \cdot 3 = 0\). By using the distributive law, we get \(2 \cdot (x - 3) = 0\). This statement tells us that the product of two integers equals 0. This can happen only if one of the multipliers is 0. Since 2 is not 0, the other multiplier, \(x - 3\), must be 0. Therefore \(x\) has to be 3. In the ring of residue classes modulo 6, this whole argument breaks down, because there are zero divisors in the system. That is, a product can be equal to 0, without either of the multipliers being equal to 0. Consequently, the cancellation law of multiplication is not obeyed in this system. In fact, in this system, if \(2 \cdot x = 2\), we cannot conclude that \(x = 1\). The multiplication table shows that while \(x = 1\) is one possible solution to the equation, \(x = 4\) is another solution, because \(2 \cdot 4 = 2\).

Mapping Group into Group

We can set up a mapping of the group of integers into the group of residue classes modulo 3 by assigning to each integer in the system of integers the residue class that it belongs to, as shown in the table:

\[
\begin{align*}
0 & \rightarrow 0 \\
1 & \rightarrow 1 \\
2 & \rightarrow 2 \\
3 & \rightarrow 0 \\
4 & \rightarrow 1 \\
5 & \rightarrow 2 \\
6 & \rightarrow 0
\end{align*}
\]
By this mapping, 0, 3, 6, 9, and 12, for example, have the 0 class as their image; 1, 4, 7, 10, and 13 have the 1 class as their image; and 2, 5, 8, and 14 have the 2 class as their image. The mapping is clearly a many-to-one mapping. It has the interesting property of preserving the operation that is defined for the group. That is, the image of a sum is the sum of the images. For example, the image of 3 is 0, and the image of 4 is 1. The sum of 3 and 4 is 7, and its image is 1, which is the sum of the images 0 and 1. A mapping like this, of one group into another, which preserves the group operation is called a group homomorphism. Where it is a many-to-one mapping it is like collapsing or telescoping the group to make it fit into a smaller one. If we consider the system of integers and the system of residue classes modulo 3 as rings, the same mapping preserves not only the group operation of addition, but also the other ring operation, multiplication. For this reason, it is also an example of a ring homomorphism (one which preserves the operations in the ring).

When a group homomorphism of one group into another is a one-to-one correspondence, then it is a group isomorphism. Each element in one group is then paired off with one and only one element in the other. In that case, we say that the two groups are isomorphic to each other, or have the same structure. Two groups that are isomorphic to each other are really the same group structure dressed up in different clothes. We have an example of isomorphic groups in the group of residue classes modulo 3, and the subgroup \{I, P, Q\} of the group of symmetries of the triangle. A mapping which matches them one-to-one, and preserves the group operation is shown below:

\[
\begin{align*}
0 & \leftrightarrow I \\
1 & \leftrightarrow P \\
2 & \leftrightarrow Q \\
* & \leftrightarrow *
\end{align*}
\]

If we take any true statement in one system, such as \(1 + 2 = 0\), and replace each symbol by its image under the mapping, we get a true statement in the other system. In the example shown, we get \(P \ast Q = I\). In other words, the symbols used in the two systems are like two different languages that may be used for expressing the same ideas. The isomorphism printed above is the dictionary that allows us to translate from one language into the other.

**DO IT YOURSELF**

1. Using the definition of multiplication of integers given on page 48, prove that multiplication of integers is commutative by showing that

\[(a \sim b) \cdot (c \sim d) = (c \sim d) \cdot (a \sim b).
\]

2. Using \((0 \sim a)\) and \((0 \sim b)\) to represent any two negative integers, prove that the sum of two negative integers is a negative integer.

3. Using \((0 \sim a)\) to represent any negative integer, and \((b \sim 0)\) to represent any positive integer, prove that the product of a negative integer and a positive integer is a negative integer.

4. A rearrangement of the numbers 1, 2, 3 is called a permutation of these numbers. Each rearrangement has the effect of replacing one number by another. For example, if the arrangement 123 is changed to 312, 1 is replaced by 3, 2 is replaced by 1, and 3 is replaced by 2. This permutation can be represented as a mapping:

\[
\begin{align*}
1 & \rightarrow 3 \\
2 & \rightarrow 1 \\
3 & \rightarrow 2
\end{align*}
\]

There are six possible permutations of three numbers. Call them \(I, A, B, C, D, E\) as follows:

\[
\begin{align*}
I & \quad A \quad B \\
1 \rightarrow 1 & \quad 1 \rightarrow 2 & \quad 1 \rightarrow 3 \\
2 \rightarrow 2 & \quad 2 \rightarrow 3 & \quad 2 \rightarrow 1 \\
3 \rightarrow 3 & \quad 3 \rightarrow 1 & \quad 3 \rightarrow 2
\end{align*}
\]
Define the product of two permutations $X \times Y$ as the result of performing $Y$ first and $X$ afterwards on the result of $Y$. How a product is identified is shown in the following example: To find $A \times B$:

<table>
<thead>
<tr>
<th>$C$</th>
<th>$D$</th>
<th>$E$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 $\rightarrow$ 1</td>
<td>1 $\rightarrow$ 3</td>
<td>1 $\rightarrow$ 2</td>
</tr>
<tr>
<td>2 $\rightarrow$ 3</td>
<td>2 $\rightarrow$ 2</td>
<td>2 $\rightarrow$ 1</td>
</tr>
<tr>
<td>3 $\rightarrow$ 2</td>
<td>3 $\rightarrow$ 1</td>
<td>3 $\rightarrow$ 3</td>
</tr>
</tbody>
</table>

Therefore $A \times B = I$.

a) Construct the multiplication table for the permutations $I, A, B, C, D, E$.

b) Prove that they form a group with the operation $\times$.

c) Identify the subgroups of this group.

d) Show that this group of permutations is isomorphic to the group of symmetries of the triangle.

5. Use the associated remainders, 0, 1, 2, 3, 4 as the names of the residue classes modulo 5. Use the definitions of addition and multiplication given on pages 64-5 to construct addition and multiplication tables for these residue classes. Use the tables to verify that $2 \cdot (1 + 2) = 2 \cdot 1 + 2 \cdot 2$ in this system. Does this system have zero divisors?

6. Show that the set of all even integers is a subgroup of the group of integers with respect to the operation $\times$. Show that it is a subring of the ring of integers. Show that it is an ideal of the ring of integers. (See definitions, pages 63-4.)

### Numbers for Measuring

**Another Defect to Overcome**

The natural number system has the defect that subtraction is not always possible in that system. To overcome this defect, we constructed the system of integers, an enlarged number system that includes the natural numbers, and in which subtraction is always possible. In this chapter we undertake another extension of the number system for a similar purpose. We find that the system of integers has the defect that division is not always possible within the system. To overcome this defect, we shall construct an enlarged number system that includes the integers, and in which division is (almost) always possible. The word "almost" has to be included in the statement of our goal, because, in the enlarged system, there will still be one number whose use as a divisor will be forbidden.

Just as subtraction of natural numbers was defined in terms of addition, division of integers may be defined in terms of multiplication. The symbol $\frac{-6}{2}$ really asks us the question, "What integer multiplied by 2 gives $-6$ as the product?" Since the answer to the question is $-3$, we say $\frac{-6}{2} = -3$. We call the symbol $\frac{-6}{2}$ the *quotient* of $-6$ and 2. We also refer to it as a *fraction*, and in this case it has meaning as another symbol for the integer $-3$. The question asked by the fraction $\frac{-6}{2}$ can also be written in the form of
an equation, \(2 \cdot x = -6\), and the answer to the question is the solution to the equation.

However, some fractions ask us a question that we cannot answer in the system of integers. For example, the fraction \(\frac{2}{3}\) asks the question, “What number, when multiplied by 3, gives 2 as the product?” In the system of integers there isn’t any such number. So, in the system of integers, the fraction \(\frac{2}{3}\) has no meaning, and the equation \(3 \cdot x = 2\) has no solution. This situation offers us a challenge similar to the one we faced in the last chapter. Can we build a number system in which division is always possible for any pair of numbers, so that \(\frac{a}{b}\) always has a meaning, and \(b \cdot x = a\) always has a solution?

Zero Is an Exception

We find that we can, provided that we agree not to use zero as a divisor. We can see the reason for this exclusion if we try to answer the question that is asked by a fraction that has 0 in the denominator. If the numerator is not 0, as in the fraction \(\frac{2}{0}\), the fraction asks, “What number multiplied by 0 gives 2 as the product?” We hope to make the enlarged number system a ring. And in a ring, as we saw on page 61, zero times any other number gives a product equal to zero. Then the answer to the question will have to be “No number.” On the other hand, if the numerator of the fraction is 0, the situation is even worse. Then the fraction \(\frac{0}{0}\) asks, “What number multiplied by 0 will give 0 as a product?” The answer to this question would be, “any number.” In fact, even in the system of integers, this would be the answer. We would like the fractions in our expanded number system not to overreach themselves. We want each fraction to stand for one and only one number. Since the fraction \(\frac{2}{0}\) stands for no number, and the fraction \(\frac{0}{0}\) stands for too many numbers, we exclude them as legitimate fractions. So, from now on, whenever we talk about a fraction, it will be understood that the denominator may not be 0.

Families of Fractions

To construct the new number system, we use the same device that was employed in the last chapter. To be sure that the question asked by the fraction \(\frac{a}{b}\) (where \(b\) is not 0) always has an answer, we shall let the question be its own answer. We shall let each fraction represent a number in the new system. However, the numbers in this system will not be single fractions. Just as each number in the system of integers is a family of differences of natural numbers, each number in the system we are now constructing will be a family of fractions or quotients of integers. This is made necessary by the fact that, even among fractions that have a meaning in the system of integers, many fractions can represent the same number. For example, \(\frac{3}{6} = \frac{9}{12}\), and many others represent the number 3, so we shall have to put them together into one family. In fact, we can obtain from this example the criterion we shall use for deciding when two fractions belong to the same family. Notice that \(\frac{6}{2}\) and \(\frac{9}{3}\) which belong to the same family, have the property that the numerator of each times the denominator of the other gives the same product, that is, \(6 \cdot 3 = 9 \cdot 2\).

We are now ready to start building up the new number system. First, we take all possible ordered pairs of integers, such as 6 and 2, 5 and 7, -2 and 3, or -3 and -9, in which the second number in the pair is not zero. Then we write the “quotients” of the numbers in the pair, using the first number as numerator. So we now have a collection of fractions or quotients like \(\frac{6}{2}, \frac{5}{7}, \frac{-2}{3}, \text{ and } \frac{-3}{-9}\). Next, we associate
with each fraction a family of fractions according to the following rule: The family of fractions belonging to $\frac{a}{b}$, where $b$ is not zero, consists of all those fractions $\frac{u}{v}$ for which $a \cdot v = u \cdot b$. To designate the family, we shall write the fraction $\frac{a}{b}$ inside parentheses. Thus, $\left(\frac{a}{b}\right)$ means the family of fractions belonging to $\frac{a}{b}$. We call such a family of fractions a rational number.

The rational numbers have some properties analogous to those of integers. First, a fraction belongs to its own family. Secondly, if one of two fractions belongs to the family of the other, then they have the same family. Because of these properties, each fraction belongs to one and only one rational number. A rational number can be represented by putting on display inside parentheses any one of the fractions that belongs to it. For example, since $\frac{9}{3}$ belongs to the rational number \(\left(\frac{6}{2}\right)\), \(\left(\frac{6}{2}\right) = \left(\frac{9}{3}\right)\). Finally, the criterion for membership in a rational number also serves as a test for equality of rational numbers. That is, the rational numbers $\left(\frac{a}{b}\right)$ and $\left(\frac{c}{d}\right)$ are equal if and only if $a \cdot d = c \cdot b$. For example, we know that $\left(\frac{6}{2}\right) = \left(\frac{9}{3}\right)$ because $6 \cdot 3 = 9 \cdot 2$.

Addition and Multiplication of Rational Numbers

Addition and multiplication of rational numbers are defined by the following equations:

$$\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right) = \left(\frac{a \cdot d + b \cdot c}{b \cdot d}\right)$$

$$\left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right) = \left(\frac{a \cdot c}{b \cdot d}\right)$$

For example,

$$\left(\frac{2}{3}\right) + \left(\frac{3}{5}\right) = \left(\frac{2 \cdot 5 + 3 \cdot 3}{3 \cdot 5}\right) = \left(\frac{19}{15}\right),$$

and

$$\left(\frac{2}{3}\right) \left(\frac{3}{5}\right) = \left(\frac{2 \cdot 3}{3 \cdot 5}\right) = \left(\frac{6}{15}\right).$$

To carry out the addition or multiplication of rational numbers, we apply these definitions to whatever fractions are on display inside the parentheses to represent the rational numbers. Since each rational number may be represented by any one of its members, the addition or multiplication may be carried out in many ways. The definitions make sense only if the result comes out the same no matter which member of a rational number is used to represent it. This turns out to be so. For example, we just obtained as the sum of $\left(\frac{2}{3}\right)$ and $\left(\frac{3}{5}\right)$ the rational number $\left(\frac{19}{15}\right)$. But $\left(\frac{2}{3}\right) = \left(\frac{4}{6}\right)$, since $2 \cdot 6 = 4 \cdot 3$; and $\left(\frac{3}{5}\right) = \left(\frac{12}{20}\right)$, since $3 \cdot 20 = 12 \cdot 5$.

So we can add $\left(\frac{2}{3}\right)$ and $\left(\frac{3}{5}\right)$ by applying the definition to $\left(\frac{4}{6}\right)$ and $\left(\frac{12}{20}\right)$. We get the sum $\left(\frac{4 \cdot 20 + 6 \cdot 12}{6 \cdot 20}\right) = \left(\frac{152}{120}\right)$. But this is the same answer we got before, because $152 \cdot 15 = 19 \cdot 120$, showing that $\left(\frac{152}{120}\right) = \left(\frac{19}{15}\right)$.

With addition and multiplication defined in this way, the rational numbers form a number system, because they obey the five laws. We prove this fact here only for the commutative law of addition:

$$\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right) = \left(\frac{a \cdot d + b \cdot c}{b \cdot d}\right)$$
But the $a$, $b$, $c$, and $d$ appearing in these symbols are integers, and integers obey the commutative laws for addition and multiplication. Therefore $b \cdot d = d \cdot b$, showing that the two results have the same denominator; and $a \cdot d + b \cdot c = c \cdot b + d \cdot a$, showing that the two results have the same numerator. Therefore the two sums are the same and $(\frac{a}{b}) + (\frac{c}{d}) = (\frac{c}{d}) + (\frac{a}{b})$. A similar proof can be given for each of the other four laws.

Zero, Unity and Negatives

Like the natural number system and the system of integers, the rational number system has a zero element and a unity element. The rational number $\left(\frac{0}{1}\right)$ is the zero element, because $\left(\frac{0}{1}\right) + \left(\frac{x}{y}\right) = \left(\frac{0 \cdot y + 1 \cdot x}{1 \cdot y}\right) = \left(\frac{0 + x}{y}\right) = \left(\frac{x}{y}\right)$. The zero element can also be written in the form $\left(\frac{0}{b}\right)$, where $b$ is any integer different from zero. This is proved by the test for equality of rational numbers, because $0 \cdot 1 = 0 \cdot b$. Where there is no danger of confusion with the zero of the system of integers, we use the symbol 0 for the zero element of the rational numbers, too.

The rational number $\left(\frac{1}{1}\right)$ is the unity element, because $\left(\frac{1}{1}\right) \cdot \left(\frac{x}{y}\right) = \left(\frac{1 \cdot x}{1 \cdot y}\right) = \left(\frac{x}{y}\right)$. The unity element can also be written in the form $\left(\frac{b}{b}\right)$, where $b$ is any integer different from zero. This is proved by the fact that $1 \cdot b = b \cdot 1$. So $\left(\frac{3}{2}\right)$, $\left(\frac{4}{3}\right)$, and $\left(-\frac{5}{-5}\right)$ are all legitimate ways of representing the unity element. A rational number is the unity element if it is represented by a fraction whose numerator and denominator are equal. Where there is no danger of confusion with the unity element of the system of integers, we let the symbol 1 stand for the unity element of the rational numbers, too.

The system of integers has one important property that the natural number system does not have: every number in the system has a negative. The system of rational numbers has this property, too. In fact, if $\left(\frac{a}{b}\right)$ is any rational number, then $\left(-\frac{a}{b}\right)$ is its negative. To prove this fact, we must show that their sum is the zero element:

$$\left(\frac{a}{b}\right) + \left(-\frac{a}{b}\right) = \left(\frac{a \cdot b + b \cdot (-a)}{b \cdot b}\right).$$

The numerator of the fraction on display for the sum is $a \cdot b + b \cdot (-a)$. By the commutative law for multiplication of integers, $a \cdot b$ can be replaced by $b \cdot a$, so the numerator is equal to $b \cdot a + b \cdot (-a)$. By the distributive law for integers, this sum is equal to $b \cdot (a + (-a))$. But $a + (-a) = 0$, so we finally have that the numerator is equal to $b \cdot 0 = 0$. Therefore $\left(\frac{a}{b}\right) + \left(-\frac{a}{b}\right) = \left(\frac{0}{b \cdot b}\right)$ the zero element in the rational number system.

The Reciprocal of a Rational Number

The negative of a number was defined in terms of addition: one number is the negative of another if the sum of the two numbers is zero. The analogous concept in relation to multiplication is that of the reciprocal. One number is called the reciprocal of another if the product of the two numbers is the unity element. In the natural number system, 1 is the only number that has a reciprocal. In fact, it is its own reciprocal, since $1 \cdot 1 = 1$. In the system of integers, there are only two numbers that have reciprocals. They are 1 and $-1$. Each of them is its own reciprocal, because $1 \cdot 1 = 1$, and $(-1) \cdot (-1) = 1$. But in the rational number system, the existence of reciprocals becomes the rule rather than the exception. Every rational number except the zero element in that system has a reciprocal. In fact, if $\left(\frac{a}{b}\right)$
is any rational number that is not the zero element, then \( a \) is not 0. Consequently, \( \left( \frac{b}{a} \right) \) is also a rational number, and it is the reciprocal of \( \left( \frac{a}{b} \right) \). To prove that it is, we multiply them. The product \( \left( \frac{a}{b} \right) \cdot \left( \frac{b}{a} \right) = \left( \frac{a \cdot b}{b \cdot a} \right) \) is the unity element, since the numerator and the denominator of the fraction on display are equal.

Since every rational number except the zero element has a reciprocal, it is convenient to introduce a special symbol to mean "the reciprocal of." If \( A \) stands for any rational number that is different from zero, we write \( \frac{1}{A} \) for the reciprocal of \( A \). Then, by the definition of reciprocal, we know that \( A \cdot \frac{1}{A} = \frac{1}{A} \cdot A = 1 \).

We undertook the construction of the system of rational numbers for the purpose of finding a number system in which the equation \( B \cdot X = A \) always has a solution, as long as \( B \) is not zero. We can now show that we have achieved our purpose. If \( B \) and \( A \) are rational numbers, and \( B \) is not zero, then \( B \) has a reciprocal, \( \frac{1}{B} \). If we multiply both sides of the equation by \( \frac{1}{B} \), we get \( \frac{1}{B} \cdot B \cdot X = \frac{1}{B} \cdot A \). But \( \frac{1}{B} \cdot B = 1 \), so we have \( 1 \cdot X = \frac{1}{B} \cdot A \). But \( 1 \cdot X = X \), because of the characteristic property of a unity element. Therefore we have found a solution to the equation. In fact, we know that \( X \) must be equal to \( \frac{1}{B} \cdot A \). Since solving the equation \( B \cdot X = A \) is another way of saying divide \( A \) by \( B \), our result suggests a definition of division that is appropriate for rational numbers. To divide by a rational number means to multiply by its reciprocal. In the system of rational numbers, division is always possible as long as the divisor is different from 0.

**We Still Have the Integers**

By constructing the rational number system, we have gained something, in that every number in it except 0 has a reciprocal. At the same time, we have lost nothing, because we still have the original system of integers hidden within the rational number system in disguise. That is, there is a subset of the rational number system that is isomorphic to the system of integers, and therefore can take its place for all practical purposes. This subset consists of all rational numbers of the form \( \left( \frac{a}{1} \right) \), where \( a \) is any integer, positive, negative, or 0. In fact, suppose we set up a mapping which matches each integer \( a \) with the rational number \( \left( \frac{a}{1} \right) \). This mapping turns out to be an isomorphism, because, under this mapping, the image of a product is the product of the images, and the image of a sum is the sum of the images. The proof of this fact is seen in the following equations obtained by merely applying the definitions of addition and multiplication of rational numbers to the numbers \( \left( \frac{a}{1} \right) \) and \( \left( \frac{b}{1} \right) \):

\[
\left( \frac{a}{1} \right) + \left( \frac{b}{1} \right) = \left( \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} \right) = \left( \frac{a + b}{1} \right)
\]

\[
\left( \frac{a}{1} \right) \cdot \left( \frac{b}{1} \right) = \left( \frac{a \cdot b}{1 \cdot 1} \right) = \left( \frac{a \cdot b}{1} \right).
\]

Because of this isomorphism, the rational number \( \left( \frac{a}{1} \right) \) may be thought of as being the "same" as the integer \( a \), and we use the symbol for the integer as an abbreviated notation for the corresponding rational number. So, from now on,
we shall write 0 instead of \( \left( \frac{0}{1} \right) \), and 1 instead of \( \left( \frac{1}{1} \right) \), as already agreed. But we shall also write 2 instead of \( \left( \frac{2}{1} \right) \), \(-2\) instead of \( \left( \frac{-2}{1} \right) \), and so on. We shall also drop the parentheses in writing a rational number, so that, when we write the fraction \( \frac{1}{3} \) we shall mean the whole family of fractions of which \( \frac{1}{3} \) is only a representative. With these conventions, we have the familiar notation for rational numbers that is used in everyday life. A rational number is called positive if it can be written as a fraction with positive numerator and denominator. It is called negative, if, when its denominator is positive, its numerator is negative.

The Rational Points on a Line

On page 29, we saw how we could represent the natural numbers as points on a line, spaced at equal intervals on one side of the point called 0. This procedure assigned numbers to only some of the points on the line. On page 54, we saw that we could represent the integers as points on a line, too. We equated the positive integers with the natural numbers already associated with points on one side of the 0. Then we placed the negative integers on the other side of the 0. In this way we assigned numbers to more of the points on the line. Now we can continue the process and assign numbers to many of the points that lie between those that represent the integers.

There is a point that divides the distance between 0 and 1 into two equal parts. We call that point \( \frac{1}{2} \). There are two points that divide the distance between 0 and 1 into three equal parts. We call those points \( \frac{1}{3} \) and \( \frac{2}{3} \). By a similar procedure, we can put \( -\frac{1}{2} \), \( -\frac{1}{3} \) and \( -\frac{2}{3} \) between 0 and \(-1\).

\[
-1 -\frac{3}{2} -\frac{3}{4} -\frac{3}{8} 0 \frac{1}{2} \frac{1}{4} \frac{1}{8} 1
\]

This process can be extended so that we can find a point on the line for every rational number, positive or negative. The arrangement on the line makes it possible to talk about larger or smaller rational numbers in the same way that we could talk about larger or smaller integers. Of any two distinct rational numbers, the one that is further to the right is the larger one. Or, as in the case of integers, we can define the meaning of "larger" in this way: If \( a \) and \( b \) are rational numbers, \( a \) is larger than \( b \) if \( a - b \) is positive.

The rational numbers are quite densely distributed over the whole line. Between any two points that represent rational numbers, there is at least another one that also represents a rational number. In fact, if \( a \) and \( b \) are two rational numbers, their average, \( \frac{a + b}{2} \), is also a rational number, and lies between them. The fact that we can always find "in between" numbers makes the rational number system the appropriate one to use to represent measurements where subdivisions of the unit may be needed. By using as many "in between" numbers as we wish, we can refine a scale of measurement as much as we like, and make measurements as precise as the physical limitations of our equipment and our senses will allow us to.

Since the rational numbers are distributed densely over the line, we may guess that we now have a number assigned to every point on the line. But this guess turns out to be false, as we shall see. In fact, the lack of numbers for some points on the line is the next defect in the number system that we shall try to eliminate by expanding it once more.

The Rational Numbers Form a Field

The rational number system, like the system of integers, is an example of a group structure and a ring structure.
Addition of rational numbers is associative. There is an identity element for addition (the zero), and each element has an inverse with respect to addition (the negative). So the rational number system meets all the requirements for being a group with respect to addition. In fact, since addition of rational numbers is commutative, it is an abelian group, and we are conforming to custom by using a plus sign for the group operation. The operation of multiplication in the rational number system is associative, and it is also distributive with respect to addition. With these further properties, the rational number system meets the requirements for being a ring. In fact, since multiplication is commutative, it is a commutative ring. Moreover, it contains a unity element.

In the transition from integers to rational numbers, something new has been added. Every rational number except 0 has a reciprocal. But a reciprocal is simply an inverse with respect to the operation of multiplication. So the rational number system with zero omitted meets all the requirements for being a group with respect to multiplication. It therefore has a double group structure, one for addition, and one for multiplication. A system of this kind, that has a double group structure, is called a field. A field is defined as a ring in which a unity element exists, and which has a reciprocal for every element except zero. The presence of these reciprocals makes it possible to carry out division by any element except zero.

The way in which groups, rings, and fields differ from each other may be expressed briefly, though crudely, as follows: A group is a system in which we can perform addition and subtraction. A ring is a system in which we can perform addition, subtraction, and multiplication. A field is a system in which we can perform addition, subtraction, multiplication, and division, except that division by 0 is excluded.

Finite Fields

The rational number system is a field that contains an infinite number of elements. There are also fields that have only a finite number of elements. In fact, we have already encountered some in earlier sections of this book. In the last chapter, we found that the system of residue classes of integers modulo 3 has a ring structure. The elements in the ring are classes called 0, 1, and 2. The multiplication table in this ring is as follows:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

We see from this table that every element in the ring except zero has a reciprocal. In fact, the reciprocal of 1 is 1, because \(1 \cdot 1 = 1\); and the reciprocal of 2 is 2, because \(2 \cdot 2 = 1\). So the system of residue classes of integers modulo 3 is a field.

If you did exercise 5 in the "Do It Yourself" section at the end of Chapter III, you have met another finite field. The residue classes of integers modulo 5 constitute a ring with this multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

This table shows that every element except zero in this system has a reciprocal. In fact, the reciprocal of 1 is 1; the reciprocal of 2 is 3; the reciprocal of 3 is 2; and the reciprocal of 4 is 4.

On the other hand, the residue classes of integers modulo
6 constitute a ring that is not a field. The multiplication table for this system, printed on page 68, shows that some of its elements which are not zero do not have a reciprocal. In fact, there is no element whose product with 2, 3, or 4 is equal to 1. So the elements 2, 3, and 4 in this system do not have reciprocals. The reason for this failure is that the number 6 has positive integer divisors besides itself and the number 1. These divisors are 2 and 3. Any integer which is also divisible by 2 or 3 belongs to a residue class that cannot have a reciprocal. Let us prove this fact for an integer divisible by 2.

Suppose that such an integer belongs to residue class $a$, and we multiply by any other residue class $x$. We shall show that the product $a \cdot x$ cannot be equal to 1, and so $a$ cannot have a reciprocal. To identify the product of $a$ and $x$, we follow the directions given on page 65. We pick any member of $a$ and any member of $x$, multiply them, and then identify the residue class of the product. Identifying the residue class of the product means finding its remainder when it is divided by 6. As the representative of $a$ let us use the member that we know is in it that is divisible by 2. Since it is divisible by 2 we may represent it as $2 \cdot m$, where $m$ is some other integer. Let us designate by $k$ the member we select from class $x$. Then the product of the two representatives of their classes is $2 \cdot m \cdot k$. Now we divide this product by 6, and obtain a quotient and a remainder, both of which are integers. Let us call the quotient $q$, and the remainder $r$. Then, from the fact that a dividend is equal to the divisor times the quotient plus the remainder, we can say that $2 \cdot m \cdot k = 6 \cdot q + r$. Therefore $r = 2 \cdot m \cdot k - 6 \cdot q$. By the distributive law, $r = 2 \cdot (m \cdot k - 3 \cdot q)$. That is, the remainder is divisible by 2. Therefore it cannot be 1. Therefore the residue class to which $2 \cdot m \cdot k$ belongs cannot be class 1, no matter what class $x$ may be.

By means of a similar proof, it can be shown that, in general, the ring of residue classes modulo $n$ is not a field if $n$ has positive integer divisors besides itself and the number 1. An integer that has positive integer divisors other than itself and 1 is called factorable. An integer that is not factorable is called prime. It can also be shown that if $n$ is a prime integer, the ring of residue classes modulo $n$ is a field. The integers 3 and 5 are both prime. That is why the ring of residue classes modulo 3 and the ring of residue classes modulo 5 both turned out to be fields.

No Zero Divisors

In the system of integers, we found that the cancellation law for multiplication was a consequence of the fact that the ring of integers has no zero divisors. Since this law is a great convenience in solving equations, it would be useful if it turned out to be true in the rational number system, too. Fortunately, it does, because the rational number system is a field, and a field cannot have zero divisors. The proof of this fact flows directly from the definition of zero divisors and the definition of a field. If a field did have zero divisors, there would be two elements in the field, say $a$ and $b$, both not zero, but whose product is zero. So we could write $a \cdot b = 0$. Since $a$ is not zero, and the system is a field, it has a reciprocal, $\frac{1}{a}$. Multiplying both sides by $\frac{1}{a}$ we get

$$\frac{1}{a} \cdot a \cdot b = \frac{1}{a} \cdot 0.$$ But $\frac{1}{a} \cdot a = 1$, and $\frac{1}{a} \cdot 0 = 0$, so we have

$$1 \cdot b = 0,$$ or $b = 0$, contradicting the assumption that $a$ and $b$ are both not zero. Therefore it is impossible for a field to have zero divisors.

Ideals in a Field

The special properties of a field also impose some restrictions on the ideals that it may contain. To get acquainted with these restrictions, let us first recall the definition of an ideal, and note some facts about the ideals of rings in general. We defined an ideal as a subring of a ring that has the property that if we multiply any member of the subring by any member of the ring, whether it is in the subring or not, the product turns out to be in the subring. For example,
the set of all even integers is an ideal in the ring of integers because, first, it is a subring, and secondly, the product of an even integer and any integer is an even integer.

Every ring contains at least two ideals. One of them is the subset consisting of only one element, the 0 of the ring. The other is the entire ring itself.

To show that the subset that contains only the 0 element is an ideal, we check to see if it fits the definition of an ideal. Notice first that addition within this subset is associative and commutative because it is in the ring as a whole. Multiplication within the subset is associative, and is distributive with respect to addition because it is in the ring as a whole. We observe next that the subset \{0\} contains the zero element, and also the negative of each of its elements, since 0 is its own negative. Moreover, 0 + 0 = 0, so the sum of elements in the subset is in the subset. Therefore the subset meets all the requirements for being an abelian group. The product 0 · 0 = 0, and so is a member of the subset. And, since multiplication in it is associative and distributive with respect to addition, the subset meets all the requirements for being a subring. Now we observe that any element in the ring times 0 gives a product equal to 0, so that this product is also in the subring. This last property makes the subring an ideal. Similarly, checking the requirements one by one, we see that the original ring is one of its ideals.

The ideal that consists of the zero element alone is called the zero ideal. We shall also assign a special name to the original ring when viewed as one of its own ideals. We call it the unit ideal. The reason for this name is seen in the following considerations. Suppose the ring we are talking about has a unity element. (This is not true of all rings, as we saw on page 64, but it is true of all fields.) Let us take a close look at any ideal that contains the unity element 1. The characteristic property of an ideal is that when we multiply a member of the ideal by any member of the ring, the product is a member of the ideal. Let us, then, multiply 1 by any element \(x\) in the ring. The product, \(1 \cdot x = x\) is therefore in the ideal. In other words, every element in the

ring is in the ideal. So, if an ideal contains the unity element, it contains all the elements of the ring, and therefore must be the whole ring. That is why the ideal that consists of the whole ring is called the unit ideal. We have in this fact and in this name a test for recognizing when an ideal is the unit ideal. To show that an ideal is the unit ideal of a ring, it suffices to show that the ideal contains the element 1.

Since a field is a ring, it has these two special ideals, the zero ideal and the unit ideal. Now we show that a field has no other ideals besides these two. Suppose we examine any ideal of a field. Since the ideal is a subring, it must contain the 0 element. If it contains no other elements, then it is the zero ideal. If it contains some other element, say \(b\), then \(b\) is different from zero, and therefore has a reciprocal \(\frac{1}{b}\) in the field. If we multiply the element \(b\) of the ideal by \(\frac{1}{b}\), the product is a member of the ideal. But this product is 1. Therefore the ideal contains 1, and must be the unit ideal. This concludes the proof.

**DO IT YOURSELF**

1. Separate all integers into residue classes modulo 7, by putting into one class all the integers that have the same remainder when you divide by 7. By using the remainder as the name for the class associated with it, we get seven classes called 0, 1, 2, 3, 4, 5, and 6. Construct the multiplication table for these residue classes (see page 65). Verify from the table that each element in this system except 0 has a reciprocal. What are the reciprocals of 2, 3, 4, 5, and 6 in this system?
2. Construct the multiplication table for residue classes modulo 12. Which elements are zero divisors in this system?
3. Prove that multiplication of rational numbers is commutative.
4. Prove that addition of rational numbers is associative.
More Questions to Be Answered

So far we have expanded the number system twice, from natural numbers to integers, and then from integers to rational numbers. In each case, the purpose of the expansion was to have a number system in which a certain type of equation would always have a solution. The first type of equation we tried to solve was one that included only a single step of addition. This was the equation of the form \( b + x = a \). The second type of equation we tried to solve included only a single step of multiplication. This was the equation of the form \( b \cdot x = a \). It was natural to consider these equations first, because addition and multiplication are the operations that are built into the structure of a number system.

It is just as natural now to go beyond these simplest equations, and consider others that may include both operations, or may use an operation more than once. For example, we might examine equations like \( 2 \cdot x + 5 = 11 \), or \( 3 \cdot (x + 2) = 7 \) which involve both addition and multiplication. We could also consider an equation like \( 3 \cdot x \cdot x \cdot x - 5 \cdot x \cdot x = 2 \cdot x + 9 \) where the operation of multiplication is repeated several times. Such equations, in which only addition and multiplication may be employed, are known as algebraic equations.

For a systematic survey of these equations, we first rewrite them in standard form. Wherever the unknown \("x"\) is multiplied by itself several times, we use the abbreviated power notation, writing \( x^2 \) for \( x \cdot x \), \( x^3 \) for \( x \cdot x \cdot x \), and so on. We eliminate parentheses by using the distributive law.

For example, \( 3 \cdot (x + 2) \) can be replaced by \( 3 \cdot x + 6 \). We reduce one side of the equation to 0 by adding negatives where necessary. For example, in the equation \( x^2 - 3x = x + 6 \), if we add \( -x - 6 \) to both sides of the equation, we get \( x^2 - 3x - x - 6 = 0 \). Finally, we combine like terms, and arrange all terms in descending powers of \( x \), getting \( x^2 - 4x - 6 = 0 \).

Here are some typical equations, written in standard form, using numbers that belong to the rational number system:

\[
\begin{align*}
2 \cdot x - 5 &= 0, \\
3 \cdot x^2 + \frac{5}{3} \cdot x - \frac{1}{2} &= 0, \\
x^3 - 2 \cdot x^2 + \frac{1}{3} \cdot x - 5 &= 0
\end{align*}
\]

The highest power of \( x \) that appears in an algebraic equation in standard form is called the degree of the equation. In the rational number system, an equation of the first degree always has a solution. The typical first degree equation has the form \( a \cdot x + b = 0 \), where \( a \) and \( b \) are rational numbers, and \( a \) is different from 0. To solve it, we take advantage of the fact that every rational number has a negative, and every rational number that is different from 0 has a reciprocal. First we add to both sides of the equation the number \( -b \), which is the negative of \( b \). This gives us \( a \cdot x = -b \). Then we multiply both sides of the equation by \( \frac{1}{a} \), which is the reciprocal of \( a \), and we find that \( x = \frac{1}{a} \cdot (-b) \). This result tells us that if there is a solution to the equation, it must be equal to \( \frac{1}{a} \cdot (-b) \). We verify that it is indeed a solution by substituting into the equation. For example, to solve the equation \( \frac{2}{3} \cdot x - \frac{5}{2} = 0 \), first add \( \frac{5}{2} \) to
both sides of the equation. Then multiply both sides by \( \frac{3}{2} \). The result asserts that if there is a solution, it must be equal to \( \frac{3}{2} \cdot \frac{5}{2} \) or \( \frac{15}{4} \). If we substitute \( \frac{15}{4} \) for \( x \) in the equation, it then says \( \frac{2}{3} \cdot \frac{15}{4} - \frac{5}{2} = 0 \). Calculation shows that this statement is true, so that \( \frac{15}{4} \) really is a solution to the equation.

However, we have less luck when we try to solve equations of the second degree. In the rational number system, we can solve some of them, but we cannot solve others. For example, we can solve without any difficulty the equation \( x^2 - 1 = 0 \). First add 1 to both sides and we get \( x^2 = 1 \). In this form, the equation asks, "What number, when multiplied by itself, gives 1 as the product?" The number 1 is obviously an answer to this question, because \( 1 \cdot 1 = 1 \). In fact, the number -1 is also a good answer to the question, because \((-1) \cdot (-1) = 1\). So we have found two solutions to the equation. The equation \( x^2 - 2 = 0 \) looks as though it ought to be just as easy to solve, but it isn't. If we add 2 to both sides, we get \( x^2 = 2 \). In this form, the equation asks, "What number, when multiplied by itself, gives 2 as the product?"

We may be tempted to say that the answer is \( \sqrt{2} \), or the square root of 2. But this is really not an answer to the question. It is only a restatement of the question. When we write the symbol \( \sqrt{2} \), it signifies, "that number (if it exists) which when multiplied by itself gives 2 as the product." But the question still remains, "Does it exist?"

We shall soon see that it does not exist in the rational number system. We shall prove that there is no rational number whose square is equal to 2.

Before giving the proof, let us approach the question in another way. We find that the question we are trying to answer is one that comes up in a simple problem in geometry. Suppose we construct a square whose sides are one unit long, and then draw the diagonal of the square. The diagonal has a definite length. To calculate it, we use the Pythagorean theorem that states that the square of the hypotenuse of a right triangle is equal to the sum of the squares of the legs. In this case the theorem leads to the equation \( x^2 = 1^2 + 1^2 \), or \( x^2 = 2 \), which is precisely the equation that we are trying to solve. So, when we prove that there is no rational number whose square is equal to 2, we shall be proving at the same time that no rational number can represent the length of the diagonal of a square whose side has length 1.

The proof makes use of some simple facts about rational numbers and integers that we shall take note of first. 1) Every rational number can be represented by a fraction that is "reduced to lowest terms." 2) If a fraction is reduced to lowest terms, then its numerator and denominator cannot both be even numbers. For, if they were, it would mean that the fraction can be reduced further by dividing numerator and denominator by 2. For example, \( \frac{6}{8} \) is not in lowest terms.

It can be reduced to \( \frac{3}{4} \). 3) The square of an even integer is an even integer, and the square of an odd integer is an odd integer. For example, \( 6 \cdot 6 = 36 \), which is an even integer; \( 7 \cdot 7 = 49 \), which is an odd integer. From this fact, it follows that if the square of an integer is even, then the integer itself is even.

We prove that there is no rational number whose square is equal to 2 by showing that the assumption that there is one leads to a contradiction. Suppose there is a rational number whose square is equal to 2. Then it can be repre-
sented by a fraction that is reduced to lowest terms. Let \( \frac{a}{b} \)
represent this fraction, where \( a \) and \( b \) are both integers. Since
the fraction is in lowest terms, \( a \) and \( b \) are not both even
integers. Since the square of this fraction is supposed to be
equal to 2, we can write \( \frac{a^2}{b^2} = 2 \). Multiplying both sides by
\( b^2 \), we find that \( a^2 = 2 \cdot b^2 \). This equation tells us that \( a^2 \)
is double the integer \( b^2 \), so \( a^2 \) is an even integer. But if \( a^2 \) is
even, then \( a \) must be even, that is, it is double some other
integer. If we call that other integer \( k \), then \( a = 2 \cdot k \). In
that case, \( a^2 = (2 \cdot k)(2 \cdot k) = 4 \cdot k^2 \). If we substitute this
expression for \( a^2 \) in the equation \( a^2 = 2 \cdot b^2 \), we get \( 4 \cdot k^2 = 2 \cdot b^2 \).
Dividing both sides by 2, we see that \( 2 \cdot k^2 = b^2 \). In
other words, \( b^2 \) is double the integer \( k^2 \), or \( b^2 \) is an even
integer. But if \( b^2 \) is even, then \( b \) must be even. We began by
observing that \( a \) and \( b \) are not both even, and end up by
concluding that they are both even. We were led to this
contradiction by the assumption that there is a rational
number whose square is equal to 2. Therefore we are com-
pelled to reject the assumption.

The proof given above is a very old one. It was first
worked out about 2500 years ago by the Greek mathe-
matician Pythagoras. The philosophers of Greece were so
pleased to discover that there were lengths that could not
be represented by rational numbers, that they celebrated
the discovery, we are told, by sacrificing one hundred oxen
to the gods.

In Chapter IV we represented the rational numbers as
points on a line. In this representation, wherever a positive
number is attached to a point, the number represents the
distance of that point from 0, if we use the distance from 0
to 1 as the unit of length. Suppose, now, we measure out
to the right of 0 a length equal to the length of the diagonal
of a square whose side has length 1 (see diagram on page
102). In this way we locate a definite point whose distance
from 0 is equal to the length of the diagonal. But we have
just proved that there is no rational number that can repre-

---

Decimal Fractions

There are many ways of approaching the problem of filling
the gaps between the rational numbers. We shall use here an
approach that grows naturally out of the custom of writing
numbers as "decimals." Decimals are more correctly de-
scribed as decimal fractions. The decimal .2 is an abbrevi-
ated way of writing the fraction \( \frac{2}{10} \). The decimal .23 is an ab-
reviated way of writing the fraction \( \frac{23}{100} \). In each case, the
denominator is understood to be a power of 10, and we
identify the power by counting the number of digits to the
right of the decimal point. Thus, since .235 has three digits
after the decimal point, we know the denominator is \( 10^3 \) or
1000, and the decimal .235 represents the fraction \( \frac{235}{1000} \).

So we see that each decimal represents a fraction, and there-
fore is simply another way of writing some of the numbers
in the rational number system. This observation immediately
suggests the question, "Can every rational number be
written as a decimal?" We are led to a rather interesting
problem when we try to answer this question.

In elementary school we learned that we can convert a
fraction into a decimal by using the process of long division.
For example, to get the decimal equivalent of \( \frac{1}{4} \), we divide
4 into 1, using the following form:
The long division terminates after two steps because in the last subtraction the remainder is zero. The conclusion is that \( \frac{1}{4} = .25 \). If we try the same procedure to get a decimal equivalent for the fraction \( \frac{1}{3} \), we run into trouble. We arrange the work in the same way, as follows:

\[
\begin{array}{c|c c c c c}
3 & 1.0000 \\
\hline
9 & 3333 \\
9 & 10 \\
9 & 10 \\
9 & 10 \\
9 & 10 \\
\hline
1
\end{array}
\]

But, no matter how many steps we carry out, the division never comes to an end. After each subtraction there is a remainder of 1. So the fraction \( \frac{1}{3} \) cannot be represented as a decimal with a finite number of digits.

The persistent reappearance of the remainder 1 tempts us to keep dividing. If we do so, we get a decimal that never ends. If we want to represent the fraction \( \frac{1}{3} \) by a decimal at all, it will have to be an infinite decimal, that is, one that has an infinite number of digits after the decimal point. So, to decide whether every rational number can be represented as a decimal we have to investigate what meaning, if any, an infinite decimal can have.

To interpret the meaning of a finite decimal, we identify a numerator from the digits that we see, and a denominator by using the appropriate power of ten, indicated by the number of digits that appear after the decimal point. Then we put the two together in the form of a fraction. This method breaks down with an infinite decimal, so we have to try another approach. What we do is think of the infinite decimal as a sequence of finite decimals, made progressively longer by appending another digit at each step. In this view, the infinite decimal .333333 ... represents the infinite sequence of finite decimals .3, .33, .333, .3333, .33333, .... To see how this sequence is related to the fraction \( \frac{1}{3} \), let us compare each of the numbers in the sequence with the fraction.

Suppose, for example, we subtract .3 from \( \frac{1}{3} \). Writing the decimal as a common fraction, we say \( \frac{1}{3} - \frac{3}{10} = \frac{10}{30} - \frac{9}{30} = \frac{1}{30} \). This difference is rather small, and in many practical problems is small enough to be considered negligible. So we may use .3 as an approximation of the value of \( \frac{1}{3} \). If we subtract .33 from \( \frac{1}{3} \), we find the difference to be \( \frac{1}{300} \). This difference is smaller than \( \frac{1}{30} \), so .33 is a better approximation to the value of \( \frac{1}{3} \) than .3 is. If we try each of the decimals in the sequence in turn, we get better and better approximations to the number \( \frac{1}{3} \). The longer the decimal is, the better the approximation becomes, because the difference from \( \frac{1}{3} \) gets smaller and smaller. To approximate means