

ALGEBRA FOR ELEMENTARY TEACHERS
BASED ON CURRENT ELEMENTARY
MATHEMATICS TEXTBOOKS

By

DON PROCK

Bachelor of Science
Southwestern State College
Weatherford, Oklahoma
1951

Master of Education
University of Oklahoma
Norman, Oklahoma
1959

Master of Arts
University of Illinois
Urbana, Illinois
1962

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
May, 1969

Thesis
1948
P 163a
cop. 2

SEP 29 1969

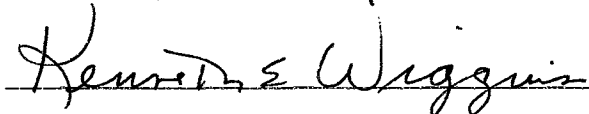
ALGEBRA FOR ELEMENTARY TEACHERS
BASED ON CURRENT ELEMENTARY
MATHEMATICS TEXTBOOKS

Thesis Approved:



Thesis Adviser







Dean of the Graduate College

725044

ACKNOWLEDGMENTS

I am deeply indebted to Dr. Gerald K. Goff for the guidance and assistance which he provided during the preparation of this dissertation. I also wish to express my deep appreciation to the other members of my dissertation committee, Dr. W. Ware Marsden and Dr. Kenneth E. Wiggins. A special thanks is extended to Dr. W. Ware Marsden, chairman, for his continued, sincere interest and encouragement.

The writer is grateful for the opportunities to participate in programs of the National Science Foundation. Special gratitude is expressed to Drs. Robert C. Fite, L. Wayne Johnson, and Milton E. Berg for extending these opportunities at Oklahoma State University.

Finally, to my wife, Peggy, and my children, Jim and Frances, I express my deepest appreciation for the sacrifices which they made while assisting in the completion of my program of study.

TABLE OF CONTENTS

Chapter	Page
I. THE PROBLEM	1
Need for the Study	2
Scope of the Study	4
Procedure	5
Summary and Preview	6
II. LANGUAGE, TERMINOLOGY, AND NOTATION	8
Basic Principles of Logic	8
Language and Operations on Sets	23
Constants, Variables, and Quantifiers	33
Relations	36
Function	40
Equivalence Relation	42
Order Relation	46
Summary	47
III. ALGEBRA OF REAL NUMBERS	49
Introduction	49
Binary Operations	51
Properties of the Real Numbers	55
Other Fields	79
The Real Number Line	88
Linear Equations and Solution Sets	89
Order	99
Absolute Value	109
Inequalities	114
Introduction to Quadratic Equations	124
Linear Equations and Inequalities in Two Variables	136
Systems of Linear Equations	151
IV. OTHER ALGEBRAIC SYSTEMS	161
Introduction	161
The Complex Number System	162
The Congruence Relation	175
Groups	191
Rings, Integral Domains, and Fields	207

Chapter	Page
V. SUMMARY AND CONCLUSIONS	222
Summary	222
Conclusions	224
A SELECTED BIBLIOGRAPHY	226
APPENDIX A	229
APPENDIX B	233
APPENDIX C	235

CHAPTER I

THE PROBLEM

During the past several years there have been significant changes in the elementary school mathematics curriculum due to the impact of modern mathematics on our society. It seems reasonable, therefore, that following this transitional period the mathematics curriculum will experience additional revision as elementary teachers become better oriented to the content and purposes of modern mathematics.

Several organizations of national prominence have made concerted efforts to aid in the mathematics training of secondary and junior high school teachers by making workshops, institutes, and conferences available. There has been no large scale effort on the national level, that is, no financial support from governmental agencies, to aid in improving the elementary school teacher's mathematics background. Teacher training institutions throughout the country have taken an intense interest in the mathematics training of elementary teachers and have afforded courses of study and workshops in an effort to aid the elementary teacher.

The content of many textbooks which have been written for elementary teachers is based on the modern approach to arithmetic. Most of these texts emphasize elementary logic, intuitive set theory, structure of the number system, geometry, and some algebraic

concepts. But even after completing such a course, many elementary teachers view mathematics as a collection of isolated topics, each of which belongs to the realm of arithmetic.

Mathematics educators generally agree that the elementary teacher should have an awareness of the algebraic concepts in mathematics that are an essential part of the elementary arithmetic program. Such an awareness could aid the teacher tremendously in foreseeing the kinds of experiences with which students will be faced in subsequent years. As a result, it is hoped that the teacher would not be satisfied to teach only those mathematical concepts and skills outlined for a particular grade level. As an example, the teacher may look upon $8 + 5 = \underline{\quad}$ and $13 - 5 = \underline{\quad}$ as two disconnected and unrelated problems in elementary arithmetic. The concept involved here is essentially that of solving a simple algebraic equation. An understanding of algebraic concepts by the teacher can aid tremendously in alleviating a student's difficulty when an equation of the type $24 + x = 9$ is encountered.

The purpose of this study is to identify the algebraic concepts experienced by elementary teachers in the teaching of modern mathematics in grades one through six. Further, a course of study in modern algebra for elementary teachers will be developed on the basis of the concepts thus identified.

Need for the Study

Elementary students can become aware of algebraic concepts at an early age through the skillful guidance of a capable teacher who has an understanding of mathematical concepts beyond the realm of

arithmetic. An awareness of such concepts can be achieved without giving a name to the concept.

There are numerous available texts and books which emphasize the structure of the number system, but the investigator is not aware of any that have been written primarily for the elementary teacher that present the algebraic concepts encountered in arithmetic. The major purpose of the majority of texts that have been published is to present a sequential development of the real number system and its subsystems. They have served their purpose well and will continue to make valuable contributions to the elementary teacher's repertoire. However, with the increased demands that are being made, it will be necessary for the elementary teacher to become thoroughly acquainted with algebraic concepts.

The Committee on the Undergraduate Program in Mathematics (hereafter referred to as CUPM) has prescribed a curriculum for training elementary teachers which includes a course devoted to the basic concepts of algebra. This curriculum has been approved by the Mathematical Association of America, has been endorsed by three conferences held by the National Association of State Directors of Teacher Education and Certification, and has been given a stamp of approval by the American Association for the Advancement of Science.

The great new demand on mathematics has had a revolutionary effect on the teaching of mathematics on both the college and the secondary school level during the past ten years. Most recently a number of modern primary curricula have been worked out, and the evidence indicates that these programs will spread rapidly. Therefore, there are two fundamental reasons why the mathematical training of elementary teachers must be changed: All elementary teachers in the future must be aware of the type of mathematics students will learn, starting in seventh grade; otherwise, they will not be able to give the students the right

kind of foundation in arithmetic. The second reason is that a great many teachers in the future will actually have to teach a more modern arithmetic program. [6]

Many elementary teachers have participated in workshops that were designed to aid in understanding and appreciating the modern approach to arithmetic. This investigator has had the pleasure of working with interested teachers, not only in workshops, but in extension classes and study groups sponsored by the Oklahoma Academy of Science. In such short contacts it is difficult to familiarize teachers with concepts and processes beyond the minimum essentials of arithmetic.

An article [27] that appeared in the American Mathematical Monthly in December, 1960, read in part,

. . . it is hoped that everyone recognizes good mathematics education to be a sequential experience. Thus, the teacher at any particular level should have an understanding of the mathematics which will confront the student in subsequent courses; and as a consequence, it is desirable that a teacher at a given level be prepared to teach at least some succeeding course.

A course of study in "Algebra for Elementary Teachers" would provide the teacher with insight into the content material a student would encounter in subsequent mathematics courses.

Scope of the Study

Since this paper is a study of the algebraic concepts contained in elementary textbooks, it is limited to the audience of elementary teachers. The reading and understanding of this paper presupposes a mathematical knowledge that is expected of one who completes the course in the structure of the number system as proposed by CUPM. It is the writer's feeling that a careful reading of this study will

increase the reader's knowledge and understanding of algebraic concepts and will create a greater appreciation of the role of algebraic concepts in elementary school mathematics. Therefore, the scope of this paper is limited to construction of a course guide which can serve as resource material as well as a guide on the language and applications of algebra in elementary arithmetic. Finally, it is hoped that this material will stimulate the elementary teacher's interest in mathematics.

Procedure

The investigator proposes to study four series of modern elementary mathematics textbooks for grades one through six. Those selected were the current publications available from the respective publishing companies as of January 1, 1968. The content will be analyzed in order to determine what algebraic concepts have been included in the texts. The results of this study will be utilized in preparing a systematic and coherent course guide designed especially for elementary teachers. Authors who have examined arithmetic textbooks in use in elementary schools include Carpenter [5], Mauro [22], Brown [4], Jones [19], and Sherman and Belding [29].

Due to the writer's contacts with elementary teachers, personal experiences will be relied upon as well as the opinions of others interested in the mathematical training of elementary teachers. In addition, material from other available sources (textbooks, periodicals, etc.) will be included whenever relevant.

Since there is disagreement among mathematicians as to the nature of mathematics itself, it is difficult to find universal agreement

on a definition of algebra. However, Kingston [21] relates that just recently have most mathematicians come to recognize in a practical way that arithmetic is specialized algebra or that algebra is generalized arithmetic.

This is indicated by the following definitions: One definition states that algebra is the branch of mathematics which deals in the most general way with the properties and relations of numbers, the generalization and extension of arithmetic [18]. Another states that the abstract symbolic study of arithmetic, with its many variations, generalizations, and associated studies, is called algebra [10]. Yet another definition states that algebra is a study of structure--the interrelations between symbols and operations performed on those symbols [28]. For the purposes of this study, algebra will be considered as the abstract symbolic study of the arithmetic of numbers. Although the primary concern will be the real number system, it will be appropriate to consider the system of complex numbers in Chapter IV. This exposition will certainly include not only the study of operations and relations in terms of real numbers, but also the general idea of operations and relations in more abstract structures. Therefore, in this study an algebraic concept will be an idea that is inherent in the abstract symbolic study of the arithmetic of real numbers.

Summary and Preview

In presenting some recommendations for improving mathematics programs, DeVault [8] says:

Elementary school teachers have the very important responsibility of assisting the elementary school child to develop an understanding of, and an interest in, mathematics. In order to perform this task more efficiently

they must have a better understanding of the basic concepts of mathematics than was typical of teachers of the past, or perhaps even the present.

Hence, one of the basic needs of teachers is adequate knowledge of mathematics as well as methods of teaching mathematics.

The writer's proposal to identify algebraic concepts and construct a course outline for elementary teachers is the result of several years' experience in consulting with teachers' groups and teaching mathematics classes for prospective teachers. There is an apparent need for a treatment of algebraic concepts in a language and style that will meet the needs of elementary teachers who already have an introduction to the structure of the number system. This can be accomplished in a manner that can be comprehended by the reading audience and yet be consistent with principles established in advanced mathematics courses.

CHAPTER II

LANGUAGE, TERMINOLOGY, AND NOTATION

Basic Principles of Logic

Possibly the reader has some familiarity with the basic properties of sets, the fundamental principles of elementary logic, the notation of a relation, and the concept of a function; however, this chapter will be devoted to definitions, terminology, and notation needed to establish meaningful communication between writer and reader. Such a basis for communication is essential if an exposition is to be understandable and purposeful.

No attempt will be made in this paper to present an extensive discourse in formal mathematical logic. A rigorous treatment of the subject is far too involved to be a part of the training of every elementary teacher. Consequently, this approach is informal and the results will be utilized freely in Chapters III and IV.

One of the basic concepts in logic is that of a statement. In a very formal treatment of mathematical logic the term "statement" would be left undefined; however, in this writing formality will be sacrificed in the interest of understanding whenever the writer deems it necessary to maintain clarity in exposition. An expression is a statement if and only if it has a truth value [20]. That is, the distinguishing feature of any statement is that it is either true or false, but it cannot be both. As interpreted in everyday life, the following are

examples of simple statements: "All triangles have three sides," which is true; "November 22, 1963, was a Tuesday," which is false; "The twenty-third digit in the decimal expansion of $3/7$ is 8." The latter example illustrates that one may not know whether the statement is true or false; but nevertheless, it is one or the other and certainly not both. That is to say, the required digit is either 8 or it is not 8.

A compound statement may be formed by combining two or more simple statements using the connectives "and" or "or." It is then natural to consider such derived statements and decide under what conditions they are true or false. In doing this it is convenient to employ the letters p, q, r, \dots , as a notational device for simple statements and the symbols " \wedge " and " \vee " to represent the connectives "and" and "or," respectively. As an illustration, let p and q represent the following simple statements:

p : The ball is black.

q : The weather is stormy.

It is now possible to write compound statements in symbolic form.

$p \wedge q$: The ball is black and the weather is stormy.

$p \vee q$: The ball is black or the weather is stormy.

The statement $p \wedge q$ is called the conjunction of p with q . It seems reasonable to say that the truth value of a conjunction depends upon the truth value of the simple statement components. Since each of the statements p and q may be either true or false, there are four distinct possibilities:

p is true; q is true.

p is true; q is false.

p is false; q is true.

p is false; q is false.

For each of these possibilities there is a corresponding truth value for the compound statement $p \wedge q$. It will be agreed that the conjunction is true if each of its components is true; and it is false if either, or both, of its components is false. This may be summarized very conveniently in a truth table (Figure 1) where T represents "true" and F represents "false."

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Figure 1

Although the table in Figure 1 was motivated by specific statements, it should be noted that p and q may represent any two statements, and the results of the table will still be valid according to the agreement about a conjunction.

In the ordinary English language the connective "or" has three different meanings as the following examples will illustrate: (1) "John Smith has a college degree or he has five years of college work." (2) "Jim Schmidt will eat lunch today in Oklahoma City, Oklahoma, or he will eat lunch today in Memphis, Tennessee." (3) "The price of Susan's dinner will include milk or hot tea." It is clear that in the first example the expression is considered true provided that either

one or both of the simple statements is true. Observe that in the second example it is impossible for Jim to fulfill the two lunch engagements simultaneously. Therefore, this expression is considered to be true if either one of the components is true, but not both of them are true. Finally, it should be noted that Susan is not compelled to accept one of the drinks that appears on the menu. The price she pays for the meal will be as advertised if she selects either the milk or the hot tea, but not both. Certainly the cost will not be reduced even if she does not order one of the drinks. Hence, in the third case, the statement is true only when she orders one and only one drink or neither of the drinks, but not both.

Although it is interesting and enlightening to point out the different and distinct uses of the connective "or" in the English language, only the first two will be pertinent in this context since they are the ones that are most useful in understanding mathematics. The first example above employs the connective "or" in the inclusive, or weak, sense. This use of the connective will be referred to as the inclusive disjunction and will be denoted by the symbol " \vee ." It is construed to mean "at least one" and will be read simply as "or." The second illustration above is a disjunction which means "exactly one." It is called the exclusive, or strong, disjunction and will be symbolized by " $\underline{\vee}$." The symbol is read as "exclusive or." To summarize, let p and q represent two statements and form the compound statements, $p \vee q$ and $p \underline{\vee} q$. The proposition $p \vee q$ is true if and only if one of the following is satisfied: (1) p is true; (2) q is true; (3) $p \wedge q$ is true. On the other hand, the statement $p \underline{\vee} q$ is true if and only if one of the following holds: (1) p is true and q is false,

(2) q is true and p is false. These results are displayed in Figure 2.

p	q	$p \vee q$	$p \underline{\vee} q$
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

Figure 2.

It should also be pointed out that the statement $p \vee q$ is false only when both p and q are false, while $p \underline{\vee} q$ is false if both p and q are true, or both p and q are false.

In addition to generating compound statements from other propositions, it is also possible to derive an expression from a simple statement such that the truth value of the result is solely dependent upon the truth value of the original proposition. For example, let p represent the statement, "It is raining." Then a derived proposition would be q --"It is not raining." Notice that if the given statement p is true, then the derived statement q is false; but, if p is false, then q is true. This illustrates the concept of "the negation of a proposition." The key word that is associated with the negation is "not," and the symbol that mathematicians commonly use is " \sim ". If p represents a simple statement, then $\sim p$ stands for the simple statement that is called "the negation of p ." In the example above the statement q is also the statement $\sim p$. The truth values of the proposition $\sim p$ are

given in Figure 3.

P	$\sim P$
T	F
F	T

Figure 3.

Again it should be noted that the truth value of $\sim p$ is only dependent upon the truth value of p , where p represents any simple statement.

Many of the statements that occur in mathematics, as well as in everyday experience, are in the form of a conditional statement. In other words, statements that are based upon a certain condition. A wife might say to a husband, "If you go to town, then you may bring home a gallon of milk." A statement such as "If Johnny would study more, then he would earn a better grade in arithmetic" is a conditional statement that might occur in a conversation between teacher and parent. In elementary school mathematics texts it is quite common for a statement similar to "If $4 + 6 = 10$, then $6 + 6 = 12$ " to appear. Notice that each of the above propositions is expressed in the form if p , then q . It is acceptable practice to utilize the symbol " \rightarrow " and write a conditional statement symbolically as $p \rightarrow q$.

It is reasonable to expect that it is possible to assign a truth value to a conditional just as was done for the conjunction, disjunction, and negation. However, an agreement must be reached as the different possibilities are considered. Consider again the following conditional proposition: "If Johnny would study more, then he would earn a better

grade in arithmetic." Suppose that Johnny does study more and that he does indeed earn a better grade, then it is clear that the conditional is true. On the other hand, suppose that Johnny does study more, but his report card does not indicate a better mark in arithmetic. In this case the conditional is false. Finally, Johnny might not be inclined to devote more time to studying mathematics; but nevertheless, the given conditional is true whether or not his grade improves, simply because the declared intention was on the condition that Johnny study more. More explicitly, the only stipulation for $p \rightarrow q$ to be true is that q be true whenever p is true. These assertions are formulated in Figure 4.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Figure 4.

There are numerous other forms in which a conditional statement may appear. Three of these related statements will be mentioned briefly. Consider the conditional proposition $p \rightarrow q$, then the following conditionals, $q \rightarrow p$, $\sim p \rightarrow \sim q$, and $\sim q \rightarrow \sim p$, are known as the converse, inverse, and contrapositive, respectively, of the given conditional. To illustrate, let p represent the statement "It is snowing;" and q , the statement, "The temperature is below freezing;" and consider the

conditional, "If it is snowing, then the temperature is below freezing."

The three related conditional statements are as follows:

Converse: $q \rightarrow p$ If the temperature is below freezing,
then it is snowing.

Inverse: $\sim p \rightarrow \sim q$ If it is not snowing, then the temper-
ature is not below freezing.

Contrapositive: $\sim q \rightarrow \sim p$ If the temperature is not below
freezing, then it is not snowing.

Notice that even though it is assumed that the statement $p \rightarrow q$ is true, there is no guarantee that the statement $q \rightarrow p$ is true. It could be true, but alternatively, it could be false. Similar observations may be made relative to the inverse statement $\sim p \rightarrow \sim q$. However, one readily sees that the truth of $p \rightarrow q$ will always assure the truth of the contrapositive $\sim q \rightarrow \sim p$. Figure 5 specifies the truth values for each of the above conditional statements.

p	q	$\sim p$	$\sim q$	State- ment $p \rightarrow q$	Converse $q \rightarrow p$	Inverse $\sim p \rightarrow \sim q$	Contrapositive $\sim q \rightarrow \sim p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Figure 5.

It is instructive to observe that the original implication and the contrapositive have the same truth values. Likewise, the same thing

can be said about the converse and the inverse. It can also be pointed out that the inverse is the contrapositive statement of the converse.

Two statement forms are said to be equivalent provided that they have the same truth values for corresponding truth values of the component statements.

Thus, $p \rightarrow q$ is equivalent to $\sim q \rightarrow \sim p$ and $q \rightarrow p$ is equivalent to $\sim p \rightarrow \sim q$.

The statements $\sim(p \vee q)$ and $\sim p \wedge \sim q$ are equivalent:

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim(p \vee q)$	$\sim p \wedge \sim q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

Figure 6.

Note that in Figure 6 the truth values of " $\sim(p \vee q)$ " and " $\sim p \wedge \sim q$ " are identical for the corresponding truth values of p and q. Therefore, the statement forms are equivalent. Similarly, a truth table could be constructed to show the equivalence of $\sim(p \wedge q)$ and $\sim p \vee \sim q$. As an actual illustration, the negation of the disjunction "3 + 4 = 6 or 3 + 4 = 7" is "3 + 4 \neq 6 and 3 + 4 \neq 7."

Although there are numerous examples of equivalent statement forms, it is not the intended purpose of this discourse to be exhaustive in this respect. Hence, as a final example, a truth table (Figure 7)

will be constructed to show the equivalence of the statements $\sim(p \rightarrow q)$ and $p \wedge \sim q$.

p	q	$\sim q$	$p \rightarrow q$	$\sim(p \rightarrow q)$	$p \wedge \sim q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

Figure 7.

Again observe that the truth values of " $\sim(p \rightarrow q)$ " and " $p \wedge \sim q$ " are identical for the corresponding truth values of p and q.

Consider a most interesting situation that occurs quite frequently in mathematics. It is possible to formulate a conjunction from an implication and its converse; namely, $(p \rightarrow q) \wedge (q \rightarrow p)$. Mathematicians refer to this conjunction as the biconditional; and since they are symbolminded people, one would expect an appropriate symbol to be utilized. This is certainly the situation, and the symbol that is agreed upon is " \leftrightarrow ." The conjunction may now be written as $p \leftrightarrow q$ which is read "p, if and only if q." Another convenient abbreviation for the biconditional is "iff." At this point perhaps a truth table (Figure 8) would be quite revealing.

Figure 8 points out that the biconditional "p iff q" is true only when both p and q are true, or both p and q are false. In other words,

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$ or $(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Figure 8.

$p \leftrightarrow q$ is true when both $p \rightarrow q$ and $q \rightarrow p$ have the truth value T. More specifically, it can be concluded that each of the following statements is true:

$$5 + 3 = 8 \text{ if and only if } 8 + 2 = 10.$$

$$5 + 3 = 9 \text{ if and only if } 8 + 2 = 11.$$

Observe that in the first biconditional both of the component parts are true while in the second both are false. Finally, each of the following biconditionals is false because exactly one component part of each of them is false:

$$5 + 3 = 8 \text{ if and only if } 8 + 2 = 11.$$

$$5 + 3 = 9 \text{ if and only if } 8 + 2 = 10.$$

The reader is cognizant of the fact that mathematics, whether it be in elementary school or graduate school, is founded upon logical reasoning. Therefore, it is imperative that correct methods of reasoning be established.

Some of the most useful and interesting statement forms employed in exhibiting proofs in mathematics are those which are true for all possible truth values assigned to the components. Such a

statement is called a tautology. Consider the disjunction $p \vee \sim p$ and the conjunction $p \wedge \sim p$. The truth values for these propositions are displayed in Figure 9.

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
T	F	T	F
F	T	T	F
F	T	T	F

Figure 9.

Notice that the compound statement $p \vee \sim p$ is indeed a tautology while the proposition $p \wedge \sim p$ is not a tautology because it is always false. In fact, a statement form which is always false for every truth value of the components is called a contradiction.

Many instances occur in mathematics in which a rule of reasoning is used that enables one to reach a conclusion from two premises, one of which is called a conditional statement. This rule is known as the law of detachment and is represented symbolically as $[p \wedge (p \rightarrow q)] \rightarrow q$ where p and $p \rightarrow q$ are the two premises. That the law of detachment is also a tautology is shown in Figure 10.

It should be emphasized that it is the statement $[p \wedge (p \rightarrow q)] \rightarrow q$ that is always true regardless of the truth values of the component parts. To illustrate, $2 = 2 \wedge (2 = 2 \rightarrow 2 + 3 = 2 + 3) \rightarrow 2 + 3 = 2 + 3$ has all the component statements true; while $2 = 3 \wedge (2 = 3 \rightarrow 2 + 5 = 3 + 5) \rightarrow$

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$[p \wedge (p \rightarrow q)] \rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Figure 10.

$2 + 5 = 3 + 5$ has all component statements false.

It should be intuitively clear to the reader that equivalent expressions may be substituted for one another. So, let there be common acceptance of the following law of replacement or substitution: "In a formula, any part may be replaced by an equivalent expression; and the resulting formula is equivalent to the original formula." [20] Now $8 = 6 + 2$ and $7 + 8 = 15$. Hence, by the rule of replacement the sentence $7 + (6 + 2) = 15$ is equivalent to $7 + 8 = 15$.

One of the most basic types of reasoning makes use of a chain of conditional statements. "Direct proofs" and "indirect proofs" are constructed according to this law.

A chain of conditional statements is called the law of the syllogism: $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$.

The technique of direct proof is not peculiar to the realm of mathematics. It is a procedure that lawyers use to present convincing arguments.

The main recognizable feature of every direct proof is that the argument starts by assuming the hypothesis to be true and then builds a chain of implication statements toward the final intended conclusion. [32]

This requires that the theorem to be proved be stated in the form $p \rightarrow q$. For example, to prove the theorem "If $8 + 2 = 10$, then $8 + 9 = 17$ " one would proceed as follows: If $8 + 2 = 10$, then $(8 + 2) + 7 = 10 + 7$. If $(8 + 2) + 7 = 10 + 7$, then $(8 + 2) + 7 = 17$. If $(8 + 2) + 7 = 17$, then $8 + (2 + 7) = 17$. If $8 + (2 + 7) = 17$, then $8 + 9 = 17$. Therefore, if $8 + 2 = 10$, then $8 + 9 = 17$.

To capture the significance of the law of detachment and the law of the syllogism in the preceding direct proof, let p , r , s , t , and q represent the statements $8 + 2 = 10$, $(8 + 2) + 7 = 10 + 7$, $(8 + 2) + 7 = 17$, $8 + (2 + 7) = 17$, and $8 + 9 = 17$ respectively. Now p is true, and each of the conditionals $p \rightarrow r$, $r \rightarrow s$, $s \rightarrow t$, and $t \rightarrow q$ is true. By the law of the syllogism $p \rightarrow q$ is also true. Since $[p \wedge (p \rightarrow q)] \rightarrow q$ is a tautology, it follows that q is true.

Perhaps, from past mathematical experiences, the reader is familiar with the so-called "column proof." The above theorem can also be proved by employing this method.

<u>Statement</u>	<u>Reason</u>
(1) $8 + 2 = 10$	[hypothesis]
(2) $7 = 7$	[identity]
(3) $(8 + 2) + 7 = 10 + 7$	[uniqueness property of addition]
(4) $10 + 7 = 17$	[renaming]
(5) $(8 + 2) + 7 = 10 + 7$	[(3), (4), and substitution]
(6) $8 + (2 + 7) = 10 + 7$	[associative property]
(7) $2 + 7 = 9$	[renaming]
(8) $8 + 9 = 17$	[(6), (7), and substitution]
(9) if $8 + 2 = 10$, then $8 + 9 = 17$	[(1) - (8)]

The method of indirect proof also applies to a theorem stated in the form $p \rightarrow q$. In order for the implication to be true whenever p is true, q must also be true. Now the distinguishing feature of an indirect proof is making the assumption $\sim q$, that is, that q is false. With this assumption the law of the syllogism is employed with the idea in mind of contradicting a known fact. If this is accomplished, then it can be concluded that the assumption $\sim q$ was false. Therefore, the only other alternative is to accept the truth of the proposition q . Quite often the assumption $\sim q$ will lead to the conclusion $\sim p$, i. e. $(\sim q \rightarrow \sim p)$, which the reader recognizes as the contrapositive of $p \rightarrow q$; and this of course, is equivalent to $p \rightarrow q$ since they have the same truth values.

A proof of the theorem "If x^2 is odd, then x is odd," where x represents a natural number, can be written very easily by using the indirect proof method. Now, either x is odd or x is even, but not both. If x is even, then there is a natural number k such that $x = 2k$. If there is a natural number k such that $x = 2k$, then $x^2 = 4k^2$. If $x^2 = 4k^2$, then $x^2 = 2(2k^2)$. If $x^2 = 2(2k^2)$, then x^2 is even. Therefore, the conditional "If x is even, then x^2 is even," is true. This is the contrapositive of the conditional stated at the beginning of this paragraph. Since the conditional and its contrapositive are equivalent, it can be concluded that the conditional is also true. So the theorem, "If x^2 is odd, then x is odd," has been proved.

At this point it will be instructive to consider an alternative indirect proof of the foregoing theorem. Let p represent the statement " x^2 is odd," and let q represent the statement " x is odd." Since a conditional is either true or false, but not both, it is possible to show

that $p \rightarrow q$ must hold by demonstrating that $\sim(p \rightarrow q)$ cannot be true. This is accomplished by showing that $\sim(p \rightarrow q)$ leads to some contradiction such as $r \wedge \sim r$. It was shown by means of a truth table on page 17 that $\sim(p \rightarrow q)$ and $p \wedge \sim q$ are equivalent. So to demonstrate that $\sim(p \rightarrow q) \rightarrow (r \wedge \sim r)$ it is sufficient to show that $(p \wedge \sim q) \rightarrow (r \wedge \sim r)$.

The argument proceeds as follows: Assume that x^2 is odd and x is not odd; that is, x is even. Now if x is even, then there exists a natural number k such that $x = 2k$. Hence, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$. So, x^2 is even. Therefore, x^2 is odd and x^2 is even ($r \wedge \sim r$). This is a contradiction, so the assumption, x^2 is odd and x is even, must be false. Since this is the negation of "If x^2 is odd, then x is odd," it follows that the conditional must be true.

A final technique to consider is a proof by counter-example. Actually, a better terminology would be a method of disproof. That is, show by example that a sentence is not true. This technique can be used to disprove the sentence, "All prime numbers are odd." All that is necessary is to exhibit at least one number that is prime but also even, which of course, is the number 2.

The writer has attempted in these few pages to provide the reader with the basic logical tools necessary for a comprehensive reading of the subsequent chapters.

Language and Operations on Sets

The occurrence of set terminology and set operations in elementary school mathematics textbooks has become somewhat standard in recent years.

It has been found that the set concept is so simple and helpful that it is being used in the elementary school—

as early as kindergarten level—as a foundation on which to build ideas in mathematics. [32]

Mathematicians generally agree that the notion of a set is a concept which unifies most of mathematics, and hence contributes to the lucidness and clarity of the subject.

In this writing the words set and element (or member) will be regarded as undefined terms, but past experience will be relied upon to give them meaning. Some appropriate synonyms for the term "set" are collection, aggregate, class, and assembly. All of these terms convey the same idea of a collection of objects regarded as a whole. The individual items in a set will be referred to as elements or members. For example, if A represents the set of all cities in the state of Oklahoma, then Stillwater is an element of set A. On the other hand, Charleston is not an element of set A. The Greek letter " ϵ " (Epsilon) is used to abbreviate the clause "is an element of," while the notation " \notin " is employed to say "is not an element of." That is, Stillwater ϵ A, but Charleston \notin A.

A set of elements is often described in what is referred to as set-builder notation. The devices used are the the symbols { } -- called braces -- which means "the set of;" a symbol (a, x, \square , Δ , etc.) to represent the element; a vertical bar to be interpreted as "such that;" and a sentence that characterizes the elements under consideration.

The latter is sometimes called the set selector. The set of all cities in Oklahoma may now be described in the following manner:

$A = \{x \mid x \text{ is a city in Oklahoma}\}$, which is read "A is the set of all x's such that x is a city in Oklahoma." Frequently it is more convenient to list the complete collection of objects within the braces, for example, {duck, airplane, space capsule}. This is commonly called the roster

notation for sets. There would definitely be no difficulty in obtaining agreement that it is far more convenient to write $\{1, 2, 3, 4\}$ than $\{\square \mid \square \text{ is one of the first four counting numbers}\}$.

It is obvious in the preceding example that a sentence such as "x is a city in Oklahoma" is not a statement as defined previously. However, it becomes a statement when x is replaced with a name of an object. More specifically, when x is replaced with the name "Stillwater" the resulting statement is true. If x is replaced with the name "Charleston" the consequence is a false statement. Correspondingly, the sentence $x \in A$ becomes a statement whenever x is replaced with a name of a city. Notice that whenever a replacement for x makes the sentence "x is a city in Oklahoma" a true statement (or false), the statement resulting from $x \in A$ is also true (or false), provided x is replaced with the same name as before; and, vice versa. Statements, like the one at the beginning of this paragraph, that cannot be identified as either true or false without additional information are called open sentences. An example of an open sentence from the realm of mathematics is " $n + 5 = 13$."

Many times properties inherent to the problem at hand force restrictions on the elements that are eligible for consideration. A convenient set which is chosen arbitrarily, but chosen in such a manner to include all the sets and all the elements in a discussion, is called a universal set or universe. A universal set is symbolized by "U." For example, if the topic of discussion is the set of all men who are over six feet tall and also have red hair, then an acceptable universal set might be the set of all men that are over six feet tall. The set of all men would also be a candidate for a universe, as would the set of all

red-haired men. Moreover, the set of all people would also suffice as a universal set. These examples do not exhaust all the possibilities for a universal set pertinent to the current discussion since there are many convenient sets that would be just as appropriate. Further, if a conversation is centered about the first ten counting numbers, then a universal set would be $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Let U be the set of all presidents of the United States and consider the set of all presidents who were born in Poland. According to the Constitution, there never has been, nor will there ever be, such a person. Obviously, the set mentioned above contains no members. A set containing no elements is referred to as an empty set, or null set, and is denoted by \emptyset . Therefore, if F is the set of all presidents who were born in Poland, then $F = \emptyset$.

The idea of an element being contained in a set, or being a member of a set, has already been mentioned. It is also worthwhile to be able to denote that a set is totally contained in some other set. The set $B = \{c, o, p, s\}$ is totally contained in the set $C = \{c, o, p, s, r, b, b, e, r\}$ since every element of set B is also an element of set C . Set B is called a subset of set C and is symbolized, $B \subset C$, where " \subset " means "is a subset of."

A is a subset of B ($A \subset B$) if and only if every element of set A is also an element of set B .

This definition allows a set B to be a subset of itself because every element of B is certainly an element of B . In this instance B is said to be an improper subset of B . If $U = \{1, 2, 3, 4, 5\}$ is a universal set, then $A = \{1, 3, 5\}$, $B = \{1, 3, 4, 5\}$, $C = \{2, 4\}$, $D = \{3, 4\}$, and $E = \{1, 2, 3, 4, 5\}$ are all subsets of U according to the definition. Notice

that set E is an improper subset of U while A, B, C, and D are not.

A is a proper subset of B if and only if A is a subset of B, and there is at least one element in B that is not contained in A.

Note in the example above that A is a proper subset of U because A is a subset of U, but U contains the elements 2 and 4 that are not in A.

Actually, only one of the members, 2 or 4, needed to be exhibited in order to classify A as a proper subset. The symbol " \subset " means "is a proper subset of," and thus, $A \subset U$. It should also be pointed out relative to the above example that $B \subset U$, $C \subset U$, $D \subset U$, $A \subset B$, and $D \subset B$.

The question naturally arises as to what consideration should be afforded the empty set. Is it a candidate for a subset of a given set? If so, will it then be considered as a proper subset or an improper subset? Since \emptyset satisfies the definition of subset, then it is considered to be a subset of every set. Also, since the empty set is somewhat of a special set, there is no universal agreement as to whether it should be classified as proper or improper. However, whenever the need arises in this paper, the empty set shall be referred to as a proper subset.

Let $A = \{4, 8, 9\}$, $B = \{9, 4, 8\}$, and $C = \{4, 9\}$, then $A \subset B$, $B \subset A$, $C \subset A$, and $C \subset B$. Observe that A is the same as B since they contain exactly the same elements, and the order in which the elements are named is irrelevant; but C is not the same as A nor is C the same as B.

Two sets are said to be equal ($A = B$) if and only if

$A \subset B$ and $B \subset A$; that is, they contain identically the

same elements.

The reader, being an arithmetic teacher, is already familiar with operations on sets and the contributions that sets have made to the continuity of content in elementary school mathematics textbooks. Namely, basic set theory principles have contributed to clarifying concepts, unifying and relating segmented topics, and simplifying complex situations. It is in keeping with this spirit of "modern mathematics" that the author wishes to utilize set properties and operations in an algebraic environment.

There are several ways in which new sets can be constructed from given sets. To illustrate, let $U = \{l, o, n, g, s, h, a, r, e, m, u, t\}$, $A = \{l, o, r, e\}$ and $B = \{m, e, n\}$. Construct the new set $D = \{l, o, r, m, e, n\}$. Now, think about any element of set D and consider what can be said about it. That is, consider the open sentence " $x \in D$." When will this sentence become a true statement? It is clear that whenever x is replaced with any one of the letters in D , the resulting statement will be true. But notice that the elements of D came from the given sets A and B . Therefore, it can be said that for each $x \in D$, either $x \in A$ or $x \in B$, or x is an element of both A and B . This operation is called "union" and will be symbolized with " \cup ." Thus, $A \cup B = D$. It should be noted that the element e is common to both sets A and B . Derived sets can be obtained by considering such common elements. This operation is named "intersection" and is symbolized by " \cap ." Hence, $A \cap B = \{e\}$. At this point it should be emphasized that both $A \cup B$ and $A \cap B$ are also subsets of U . By employing set builder notation and considering any two sets A and B , the following can now be formulated:

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

$$A \cup B = \{y \mid y \in A, \text{ or } y \in B, \text{ or } y \in A \cap B\}.$$

Even though either, or both, of the sets A and B may be the empty set or the sets may have no elements in common, it is still true that the results of the operations union and intersection will be a set. If $A = \emptyset$ and $B = \{o, m, e, n\}$, then $A \cup B = B$ and $A \cap B = \emptyset$. On the other hand, assume $A = \{l, o, n, g\}$ and $B = \{m, u, t\}$, then $A \cap B$ is a set, namely \emptyset , which is also a subset of U.

Two sets A and B are said to be disjoint if and only if $A \cap B = \emptyset$.

By appealing again to the foregoing illustration, the task of deriving other sets from the given ones can be undertaken. The sets $E = \{l, o, g, s, h, a, r, u, t\}$ and $F = \{l, o, r\}$ are called the "complement of B relative to U" and "the complement of B relative to A," respectively. Note that E contains all the elements in U that are not in A while F contains all the elements in A that are not in B. Another name for E is "B'" and, for F is "A - B." More formally, if U is a universal set, where A and B are subsets, then:

$$B' = \{a \mid a \in U \text{ and } a \notin B\}$$

$$A - B = \{b \mid b \in A \text{ and } b \notin B\}$$

The set selectors for these sets are characterized by "and" sentences which must become true statements whenever elements of the appropriate complementary sets are chosen.

Sets, under the operations of union and intersection, obey certain basic properties.

The commutative properties:

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

The associative properties:

$$(A \cup B) \cup C = A \cup (B \cup C)$$

$$(A \cap B) \cap C = A \cap (B \cap C)$$

The distributive properties:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

DeMorgan's laws:

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

Properties of the empty set and universal set:

$$A \cup \emptyset = A$$

$$A \cap U = A$$

$$A \cap \emptyset = \emptyset$$

$$A \cup U = U$$

It should be pointed out that each of the above consequences can be proved by basic laws of reasoning and the previously stated properties of sets. For example, here is a proof that $A \cup B = B \cup A$. If $x \in A \cup B$, then by definition of union $x \in A$ or $x \in B$. If $x \in A$ or $x \in B$, then $x \in B$ or $x \in A$. If $x \in B$ or $x \in A$, then $x \in B \cup A$. Hence, $A \cup B \subseteq B \cup A$. Similarly, $B \cup A \subseteq A \cup B$. Therefore, by definition of equality of sets, it follows that $A \cup B = B \cup A$.

Also, it is not difficult to convince one that DeMorgan's law, $(A \cup B)' = A' \cap B'$, is valid. For, if $x \in (A \cup B)'$, then by definition $x \notin A \cup B$. But this can only occur provided $x \notin A$ and $x \notin B$. So, if $x \notin A \cup B$, then $x \notin A$ and $x \notin B$. If $x \notin A$ and $x \notin B$, then $x \in A'$ and $x \in B'$. Therefore, $x \in A' \cap B'$. Hence, if $x \in (A \cup B)'$, then

$x \in A' \cap B'$, and it follows that $(A \cup B)' \subseteq A' \cap B'$. If the steps in the above proof are reversed, then the conclusion is reached that $A' \cap B' \subseteq (A \cup B)'$. It is therefore true that $(A \cup B)' = A' \cap B'$.

Finally, it is convenient to consider the "Cartesian product" or "cross product" of sets. But initially, it is essential to have an agreement on the meaning of "ordered pair." In elementary school mathematics texts, one is confronted with clauses such as: "3 pencils for 10 cents" or "5 of the 8 children are boys." Let there be common consent that in clauses like the first one the number of items will always precede the cost, while in those like the second, the number of boys will always precede the total number of children. It is then evident that each of these has something to do with a fixed sequence, or order. Since order is important, the first can be very profitably symbolized by $(3, 10)$ and the second, by $(5, 8)$. Thus, each of these is an example of an ordered pair. The set symbol $\{5, 8\}$ does not imply order, while the symbol $(5, 8)$ does. It is important to realize that $\{5, 8\} = \{8, 5\}$ but $(5, 8) \neq (8, 5)$. One could describe an ordered pair as a two-element set in which the two distinct roles of the elements are distinguishable verbally [15].

If (a, b) and (c, d) are ordered pairs, then $(a, b) = (c, d)$

if and only if $a = c$ and $b = d$.

Suppose that a high school baseball team has five boys who are equally able pitchers and four different boys who are equally capable of catching. It is clear that the team has twenty different batteries on which it can rely. If A is the set of pitchers and B is the set of catchers, then a battery can be considered as an ordered pair of elements where the first component is a member of A and the second component is a

member of B . It would then be appropriate to think about the set of all batteries, i. e., $\{(x, y) \mid x \in A \text{ and } y \in B\}$. The resulting set is called the Cartesian product, $A \times B$, of A and B . The symbol " $A \times B$ " is read "A cross B."

Let A and B be sets. The Cartesian product, $A \times B$, of A and B is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$. Thus, $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

As a culminating activity with sets, it would be appropriate to demonstrate how additional properties of sets can be derived by making use of the preceding definitions about sets together with logical principles. But first, perhaps an example would be informative. If $A = \{a, e, i, o, u\}$ and $B = \{d, u, e, l, s, c, o, i\}$, then $A \cap B = \{e, i, o, u\}$. The reader should be convinced that $A \cap B \subset A$. Here it is apparent that the symbol " \subset " is the proper one to use, but for arbitrary sets A and B the symbol " \subseteq " would be appropriate. A reasonable conjecture could be made at this point; i. e., regardless of the nature of the sets A and B , $(A \cap B) \subseteq A$ is always true. That this is indeed a correct generalization is demonstrated in the following: If A and B are any two sets, the desired conclusion is that $A \cap B \subseteq A$. Now, when will it be true that $A \cap B \subseteq A$? According to the definition of subset, every element of $A \cap B$ must also be an element of A . So, if $x \in A \cap B$, then it is true by definition of intersection that $x \in A$ and $x \in B$. But if $x \in A$ and $x \in B$ is true, then by definition of conjunction, $x \in A$ is certainly true. Therefore, it can be concluded that if $x \in A \cap B$, then $x \in A$. Since each of the conditionals applies to every element in $A \cap B$, the unavoidable conclusion is then reached that each of these elements is also in A . Consequently, it is true that $A \cap B \subseteq A$.

Constants, Variables, and Quantifiers

No doubt the reader has become acquainted with such terms as constant and variable in his prior experiences in mathematics. Earlier in this exposition the writer tacitly assumed, when statements such as $\text{Stillwater} \in A$ or $x \in A$ were made, that the reader had an awareness of the meanings of these terms.

- (i) A constant is a proper name. In other words, a constant is a name of a particular thing [15].
- (ii) A variable is a symbol that holds a place for constants [15].

"Henry Bellmon" is a constant since it is a name of a governor of the State of Oklahoma. Similarly, "5" is a constant because it is a name of a number. The expression " $4 + 2 = 5 + 1$ " means that " $4 + 2$ " and " $5 + 1$ " are different names for the same number.

The occurrence of variables in daily life is as commonplace as variables in mathematics. Perhaps an example from experience would clarify their use. A newspaper or magazine quiz might contain an expression such as " was a governor of Oklahoma who was impeached from office." The purpose of the " " is to hold the place of a name, or constant. The printed expression could just as well have been written as " x was a governor of Oklahoma who was impeached from office." The " x " is interpreted as holding a place in which a name may be inserted. The latter place holder is much more acceptable for mathematical purposes since it is not quite so clumsy.

A specified set of elements, such that the names of these elements are possible replacements for a variable, is called the replacement set.

Let the replacement set be P , the set of all presidents of the United States, and let x be a variable on the set P ; i. e., x is a placeholder for which the names of presidents are allowable replacements. Examine the following expression: "x was elected to more consecutive terms as president of the United States than any other person." By consensus, x can be replaced by the name of any president, but only when it is replaced with the constant, "Franklin D. Roosevelt," will a true statement ensue. The reader should observe that the above expression which employs the variable x is another instance of an open sentence.

Quite frequently variables are accompanied by other expressions which deal with "how many." Let x be a variable on the set P of the preceding paragraph and consider the following sentence: "For each x , x was born in the United States of America." The meaning conveyed here is that for each replacement of x by the name of a president, the expression is transformed into a true statement. This is synonymous with the truth of the conjunction: George Washington was born in the United States \wedge Thomas Jefferson was born in the United States \wedge Harry S. Truman was born in the United States \wedge . . . , etc., until a similar statement about each president has been included in the conjunction. The expression "for each," that introduced the statement under consideration, is called a universal quantifier since the intention was to say something concerning each element of the set P . Other expressions that are just as acceptable for universal quantifiers are "for all" and "for every."

Of significant concern in this paper will be universally quantified expressions that pertain to sets of numbers. A case in point

would be the statement "For each n in the set of counting numbers, $n + 2 = 2 + n$."

Again an appeal may be made to the set P of presidents to illustrate another very important concept in mathematics. If y is a variable on the set P , then the expression, "There exists a y such that y was assassinated while still in office," is certainly a valid one to scrutinize. The intended meaning in this sentence is that one can find at least one replacement of y by a name of a president such that the president that is named was assassinated while still occupying the office of President of the United States. If y is replaced with "John F. Kennedy," then the sentence under consideration becomes a true statement. Notice also that the sentence makes the claim that at least one of the individual statements in the following disjunction is true: Calvin Coolidge was assassinated while still in office \vee Abraham Lincoln was assassinated while still in office \vee Herbert Hoover was assassinated while still in office \vee . . . , etc., until the set P is exhausted. The expression "there exists" is called an existential quantifier. Other expressions that convey the same meaning are "there is" and "there is at least one." In mathematics the expression, "There exists an n in the set of whole numbers such that $n + 5 = 5$," relates very effectively the role of zero in addition of whole numbers.

A universally quantified expression is a statement, and as such, it is either true or false. Therefore, a universally quantified statement is false if a counter-example can be found depicting that the expression is not a true statement. "For each n , $n + 8 = 8$ " is a universally quantified statement, where n is a variable on the set of counting numbers. If n is replaced with "3" the statement is false.

Therefore, the statement "there exists an n such that $n + 8 \neq 8$ " is the negation of the above universally quantified statement, and the negation is an existentially quantified statement.

Consider the expression: "There is an x in the set P of all presidents such that x was born in Texas." Notice that this existentially quantified expression is a true statement since Lyndon B. Johnson was indeed born in the Lone Star State. All that is required is to find one element for which the statement is true. On the other hand, an existentially quantified statement is false if it is not true for every element under consideration. For example, the statement, "There exists an n in the set of counting numbers such that $n + 3 = 3$," is false when n is replaced by a name for any counting number. Hence, for each n , $n + 3 \neq 3$. So, the negation of an existentially quantified statement is a universally quantified statement.

Relations

The concept of a relation is one of the most basic and useful ideas in mathematics. The notion occurs in everyday experiences when people think or speak of objects in the light of relations they bear to other objects. Even youngsters are aware of the effectiveness of comparing when they make statements such as "I am taller than you," or "Our car is newer than yours."

The realization of just how basic and fundamental this concept is in arithmetic and in mathematics is recognized and unchallenged. If anything is to be labeled "new math" in the elementary curriculum, the concept of relation must be included [26].

The Cartesian product of sets A and B was defined on page 31 as $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$. Now if A is the set of all United States

senators and B is the set of all fifty states, then $A \times B$ is the set of all ordered pairs where the first component is a senator and the second component is a state. This collection of ordered pairs is really not very revealing. However, by selecting all of those ordered pairs (a, b) such that a is a senator from state b , a worthwhile bit of information is obtained. Let R be the set of all such pairs, then the relation "is a senator from" has been used to define R as a subset of $A \times B$. On the other hand, a subset of the cross product $A \times B$ could be used to obtain a relation from the set A to set B . For example, the subset $T = \{(Monroney, Oklahoma), (Dirksen, Illinois), (Fullbright, Arkansas), \dots\}$ can be used to define the relation "is a senior senator from." There are also numerous other ways that a subset of $A \times B$ could be selected in order to define a relation from the set A to the set B .

A relation between sets A and B is a subset of $A \times B$ or $B \times A$. That is, if $R \subseteq (A \times B)$, then R is a relation from A to B .

To further demonstrate, let $A = \{1, 2, 3\}$, $B = \{3, 4\}$, and write the Cartesian product $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$. Choose R to be $\{(1, 3), (2, 4)\}$ and observe that for every ordered pair $(x, y) \in R$, it is true that x is 2 less than y . So, R defines the relation "is 2 less than."

If $T = \{(1, 4), (2, 3), (3, 3)\}$, then $T \subseteq (A \times B)$, and hence is a relation. But in this case it is difficult, if not impossible, to formulate a verbal statement that describes a relation which the first component of each ordered pair has to the corresponding second component. To reiterate, a relation is a subset of a cross product.

The set of first components in a relation is called the domain

of the relation, and the set of second components is called the range of the relation. Common usage is made of the symbols D_o and R_a to denote the domain and range, respectively. In the examples of the foregoing paragraph, the domain of the relation R is $\{1, 2\}$, and the range is $\{3, 4\}$, while the domain of T is $\{1, 2, 3\}$, and the range is $\{3, 4\}$. Obviously, the domain of any relation from the set A to the set B will be a subset of A , and the range will be a subset of B .

Let A and B be arbitrary sets and let R be any relation from A to B [$R \subseteq (A \times B)$], then the domain of R is the set $\{a \mid (a, b) \in R\}$ and the range of R is the set $\{b \mid (a, b) \in R\}$. That is to say, the only way an element a gains membership in the domain of R is for it to be the first component of an ordered pair $(a, b) \in R$. Similarly, the only elements b in the range of R are those elements that are second components of ordered pairs $(a, b) \in R$. Consider the following example where $A = \{1, 2, 3, 4, 5\}$ and $B = \{1, 2, 3, \dots, 10\}$. From the Cartesian product choose the subset S of all ordered pairs such that the second component is twice the first component. In set builder notation this can be written $\{(a, b) \mid b = 2a\}$, which is just the set $\{(1, 2), (2, 4), (3, 6), (4, 8), (5, 10)\}$. It follows that the domain of S is the set $\{a \mid (a, b) \in S\} = \{1, 2, 3, 4, 5\}$ and the range of S is the set $\{b \mid (a, b) \in S\} = \{2, 4, 6, 8, 10\}$.

Perhaps it would be convenient to employ a suitable symbol when discussing a relation S and referring to the elements $(a, b) \in S$. It is customary with mathematicians to use the symbol " $a S b$," which means " $(a, b) \in S$." The appropriate way to read " $a S b$ " is " a is in the relation S to b ." Hence, in the example above $1 S 2$, $2 S 4$, $3 S 6$, $4 S 8$, and $5 S 10$.

The definition of a relation on page 37 does not exclude the possibility that sets A and B may be the same; i. e., $A = B$. In this case, reference can be made to the Cartesian product of a set A with itself; namely, $A \times A$. Moreover, if $R \subseteq A \times A$, then R is called "a relation on A ." Such relations appear quite frequently in mathematics and provide a formidable basis for enriching experiences in all levels of mathematics from elementary school to graduate school.

Quite often it is more expedient to indicate the method of obtaining the ordered pairs in a relation rather than actually specifying them. For example, if S is the set of all freshman students enrolled at Oklahoma State University, then a relation R on the set S may be indicated as follows: $a R b [(a, b) \in R]$ if and only if a and b are in the same mathematics class. In other words, R is the relation "being in the same mathematics class as."

By returning momentarily to the example $A \times B$, where A is the set of all United States Senators and B is the set of all fifty states, a very important concept can be demonstrated. Recall that $T \subseteq (A \times B)$ is the relation of all ordered pairs $(x, y) \in (A \times B)$ such that x is the senior senator from state y . Notice that a set S of ordered pairs (y, x) , where $(y, x) \in B \times A$, may also be considered. The ordered pair $(y, x) \in S$ means that "y is the home state of the senior senator x." Therefore, S is a relation from set B to set A ; and in simple language, it can be said that the relation S is obtained from the relation T by interchanging the components of each ordered pair $(x, y) \in T$. Thus $(y, x) \in S$ whenever $(x, y) \in T$. S is called the "inverse relation" of T .

If R is a relation between sets A and B , then the inverse relation S is defined to be the set $S \subseteq (B \times A)$, where

$S = \{(y, x) \mid (x, y) \in R\}$. The inverse relation S of R is usually symbolized by " R^{-1} ."

If $A = \{2, 3, 4, 5, 6\}$ and $R = \{(2, 4), (2, 6), (3, 6)\}$, then R is the relation "is a proper factor of" on the set A . By the above definition, the inverse relation $R^{-1} = \{(4, 2), (6, 2), (6, 3)\}$, and is interpreted to be a subset of "is a multiple of."

Function

Probably it is not presumptuous to say that the concept of a "function" is one of the most frequently used ideas in mathematics. Apparently, writers of elementary school textbooks are convinced of the importance of this concept since some have elected to present the idea as early as the fourth grade. Moreover, some authors deemed it appropriate to employ the familiar "functional notation" of algebra in their arithmetic texts.

A function is a relation such that no two ordered pairs have the same first component. Equivalently, if two ordered pairs have the same first component, then the second components must also be the same.

The set $P = \{(1, 3), (2, 5), (7, 11), (6, 11)\}$ is an example of a function because it is a relation, and all the first components are different. Also, the set $G = \{(1, 1), (2, 4), (3, 9), (4, 16)\}$, where the second component is the square of the first component, is a function. However, note that the set $\{(1, 1), (1, 2), (2, 3), (3, 5)\}$ is a relation which is not a function since the ordered pairs $(1, 1)$ and $(1, 2)$ have the same first component but different second components. The example $T = \{(x, y) \mid x \text{ is the senior senator from state } y\}$, which was previously presented,

is also a function because a person can only be a senior senator from one and only one state. Furthermore, T^{-1} is a relation which is also a function, and so is G^{-1} of the relation G above.

Using set notation, let f be a relation from set A to set B [$f \subseteq (A \times B)$]. f is said to be a function provided that $y = z$ whenever $(x, y) \in f$ and $(x, z) \in f$.

Elementary teachers acquaint their pupils with the concept of a function when they are involved in teaching the fundamental operations of arithmetic. For instance, the addition facts about counting numbers, "1 + 3," "2 + 3," "3 + 3," etc., express the idea of "adding 3." This is simply the notion of a function where a relation g is defined on the set of counting numbers $N = \{1, 2, 3, 4, 5, \dots\}$. In this instance, if n is a variable ⁱⁿ on the set N , then $g = \{(n, n + 3) \mid n \in N\}$. It is easy to see that $g \subseteq N \times N$ since $n \in N$ and $n + 3 \in N$. Further, because of the uniqueness property of addition of counting numbers, the first components of ordered pairs $(n, n + 3) \in g$ are all distinct. Hence, by definition, g is a function. The domain of g is the set N while the range of g is the set $M = \{4, 5, 6, 7, 8, \dots\}$.

Since g is a relation on N , it is true that g^{-1} is also a relation on N . It is appropriate to raise the question, "Is g^{-1} a function?" Observe that since the second components of ordered pairs $(n, n + 3) \in g$ are unique, the first components of ordered pairs $(n + 3, n) \in g^{-1}$ will also be unique. Therefore, g^{-1} is a function whose domain is M and range is N . The function g^{-1} can also be characterized as $\{(m, m - 3) \mid m \in M\}$, which can be described as "subtracting 3."

The function g of the preceding paragraph can be used to

explain the phrase "functional notation" that was referred to earlier. For a ready reference, it is desirable to repeat that g is the set $\{(n, n + 3) \mid n \in \mathbb{N}\}$ and $g \subset \mathbb{N} \times \mathbb{N}$. Possibly some clarity can be achieved in using the language that mathematicians prefer when calling attention to the second components. In the example in question, it can be said that for each $n \in \mathbb{N}$, $n + 3$ is the image of n . In other words, the elements in the range of g are called the images of elements in the domain. Since the name of the function under discussion is g , it is appropriate to denote the image of n as " $g(n)$," which is read " g of n ." Thus, $g = \{(n, g(n)) \mid n \in \mathbb{N} \text{ and } g(n) = n + 3\}$.

A function can be defined by specifying the domain and a rule of correspondence or a scheme for associating elements in the domain with unique elements in the range. Obviously, the scheme or rule that is devised will determine the elements in the range. Alternatively, if the domain and range of a function are known, it may or may not be possible to discover a rule or scheme that associates elements in the domain with unique elements in the range. The alternate approach to a function is exemplified by the following. If $A = \{1, 2, 3, 4, 5, 6\}$ and for each $x \in A$, $f(x) = 2x + 1$, then these two ingredients specify the function $f = \{(x, f(x)) \mid x \in A \text{ and } f(x) = 2x + 1\}$. The domain of f is A while the range of f is the set $\{3, 5, 7, 9, 11, 13\}$.

Equivalence Relation

Although the general concept of a relation occupies a prominent niche in mathematics, some relations deserve more than just casual consideration. Relations can be quite different and distinct and yet possess certain common properties.

An equivalence relation on a set A is a relation $R \subseteq$

$A \times A$ which possesses the following three properties:

- (1) For all $a \in A$, $(a, a) \in R$ (reflexive).
- (2) If $(a, b) \in R$, then $(b, a) \in R$ (symmetric).
- (3) If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ (transitive).

Optionally, the above can be restated as follows:

- (1) For all $a \in A$, $a R a$.
- (2) If $a R b$, then $b R a$.
- (3) If $a R b$ and $b R c$, then $a R c$.

The reflexive property states that every element on which the relation is defined must bear the relationship to itself. The relation "has the same grade point average as," applied to a freshman class, possesses the reflexive property. That is, every freshman has the same grade point average as himself. Relative to the set of all people, the relation "is a brother of" does not enjoy the reflexive property.

A relation that is symmetric is one such that if a first element is related to a second element, then the second is related to the first in the same way. A specimen is the relation "is sitting next to." If Jan is sitting next to Sue, then Sue is sitting next to Jan. On the other hand, the relation "is a factor of," defined on the set of counting numbers, is not symmetric since 6 is a factor of 18, but 18 is not a factor of 6.

A transitive relation is one such that, if a first element has a relationship to a second, and the second has the same relationship to the third, then the first must bear the same relationship to the third. The relation "is sitting next to" does not possess the transitive property, if it is assumed that the seating arrangement is in a straight row. For

if Jan is sitting next to Sue, and Sue is sitting next to Faye, then it is not true that Jan is sitting next to Faye. "Is the father of" is not transitive. Jim may be the father of Dick, and Dick may be the father of Jerry, but this does not make Jim the father of Jerry. The relation "is faster than" is transitive. If Tom is faster than Harry and Harry is faster than Rufus, then certainly Tom is faster than Rufus.

If P is the set of all people residing in Oklahoma, then a relation can be defined on the set P in the following way: A resident x is related to a resident y if and only if x and y live in the same county. Let it be agreed that every resident lives in the same county as himself, and no person is considered to be a resident of more than one county.

This relation is reflexive because every resident is related to himself. If x lives in the same county as y , then unquestionably y lives in the same county as x . If x lives in the same county as y , and y lives in the same county as z , then it is true that x also lives in the same county as z . Therefore, the relation "lives in the same county as" is an equivalence relation.

Communication in mathematics depends very heavily upon the concept of "equals." In fact, without an agreement as to the usage of this term, the reader as well as the writer would be greatly handicapped.

The expression " $a = b$ " means that a and b are different symbols representing the same object. The symbol " $=$ " is called equals.

For instance, $5 + 3 = 8$ means that $5 + 3$ and 8 are different names for the same number. Also, $8 = 6 + 2$; thus $5 + 3$ and $6 + 2$ also name the same number.

Throughout this paper it will be agreed that the equals relation is an equivalence relation. That is,

- (1) For each a , $a = a$.
- (2) If $a = b$, then $b = a$.
- (3) If $a = b$ and $b = c$, then $a = c$.

As stated previously, equivalence relations play a central role in mathematics, but perhaps the major consequence is the effect that an equivalence relation has on the set on which it is defined. In the foregoing example, the equivalence relation "lives in the same county as" partitions the set of all people residing in Oklahoma into disjoint subsets, namely, the sets of people living in the individual counties.

Governor Bartlett is a resident of Oklahoma county; hence, every other person living in Oklahoma county is "related" to him. So, the set of all people living in Oklahoma county is just the set $\{x \mid x \text{ lives in the same county as Governor Bartlett}\}$. If c is a citizen of one of the seventy-seven counties, then the set $\{x \mid x \text{ lives in the same county as } c\}$ contains all the people residing in the same county as c . The seventy-seven pairwise (any two subsets are disjoint) disjoint subsets are called equivalence classes.

Let R be an equivalence relation on a set A . If a is any element of set A , then the equivalence class containing a is defined to be the set of all elements of A that are related to a . Thus, $[a] = \{x \mid x \in A \text{ and } x R a\}$, where "[a]" is read "the equivalence class containing a ."

An instructive illustration may be drawn from the set N of counting numbers. Define a relation R on N as follows: A counting number

x is related to a counting number y , ($x R y$), if and only if x and y are both even, or x and y are both odd. Even numbers have this relation to even numbers, and odd numbers have this relation to odd numbers. If x is even, then $x R x$; also, if x is odd, then $x R x$. Hence, the relation R is reflexive. Now suppose that both x and y are even, then $x R y$; and certainly it follows that $y R x$. Similarly, if x and y are both odd, then $x R y$ and $y R x$. Therefore, R enjoys the symmetric property. Finally, let $x R y$ and $y R z$. The only way for this to materialize is for both x and y to be even (or odd) and for both y and z to be even (or odd). So if x is even (or odd) then z has to be even (or odd). Thus, the conclusion can be reached that $x R z$; and therefore, R is transitive. It is then decisive that R is indeed an equivalence relation.

The relation R partitions the set N into equivalence classes. The class to which 1 belongs is $[1]$; the class to which 2 belongs is $[2]$; and the class to which 3 belongs is $[3]$. In general, for each $n \in N$, the class to which n belongs is $[n]$. The reader should ascertain by careful observation that 3 is also in the class $[1]$; and 4 is in the class $[2]$. In fact, all odd numbers are in the class $[1]$ while all even numbers are in the class $[2]$. So, there are really only two classes, the set $[1] = \{x \mid x R 1\}$ and the set $[2] = \{x \mid x R 2\}$.

Order Relation

Relations that specify the ordering of elements of a set hold a position of prominence in everyday life as well as in the discipline of mathematics, and they will be of particular interest in later developments.

A relation that is transitive, but not symmetric, is called an order relation.

Notice that according to this definition a relation can be reflexive and transitive, or only transitive, and still be termed an order relation. The relation "is taller than" is an example of an order relation since it is transitive but not reflexive nor symmetric. Recalling the definition of subset and proper subset, the reader will agree that the relation "is a subset of" (\subseteq) is reflexive and transitive but not symmetric; and the relation "is a proper subset of" (\subset) is neither reflexive nor symmetric, but it is transitive. So, these qualify to be order relations.

If the reader will appeal to his interpretation of the terms "is less than" and "is less than or equal to," the following examples of order relations are noteworthy of attention. If $S = \{1, 2, 3, 4\}$, then the relation "is less than" satisfies only the transitive property, while the relation "is less than or equal to" is reflexive and also transitive. The former is the set of ordered pairs $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$ while the latter is the set $\{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$.

Summary

It is a vital concern of elementary school teachers to teach a mathematics program that will meet the needs of today's youngsters. A creditable job has been done in the past, but there is a desire to do an even better job in the future. Yesterday's situation was rather simple and uncluttered. The primary concern was preparing children to do the kind of mathematics they would need in life situations. Certainly these needs still exist, but the concern is much more complex

today. More elementary students go to high school and college than ever before; therefore elementary teachers must be concerned with each student's understanding of mathematics as well as his computational skills. Elementary teachers will not be able to meet present demands unless they are prepared in a more meaningful way.

Mathematics is a rapidly growing body of knowledge. Careers that did not exist twenty years ago are available today for the mathematically trained person. Furthermore, many children are beginning their training now in elementary school for careers that are nonexistent at the present. Yesterday's mathematics will not prepare young people for tomorrow's demands. It is the sincere hope of the writer that this exposition will provide some assistance to the elementary teacher in the teaching of algebraic concepts with a greater degree of confidence.

The purpose of this Chapter II is to establish the framework for a development of algebraic concepts in subsequent chapters. For a convenient reference, and to further emphasize the role of mathematical language, the terms and symbols introduced in this chapter are listed together with the page location in Appendix A, page 229. This terminology and notation will be used freely in the development of Chapters III and IV.

CHAPTER III

ALGEBRA OF REAL NUMBERS

Introduction

The reader, being acquainted with a modern development of the real number system, will no doubt be familiar with some of the topics that are included in this exposition. However, one of the intended purposes of this writing is to capitalize on the reader's awareness of mathematical concepts so that a more mature understanding of these familiar topics can be realized and greater mathematical understanding can be achieved.

Beyond the development of the number system, the teacher of elementary mathematics should have some idea of the fascinating worlds of algebra and geometry that lie ahead for the students [17].

Even though some authors have a strong conviction that algebra can be taught effectively to elementary school children, this writer will not attempt to suggest what topics should be included in the elementary school mathematics texts. However, the algebraic concepts that were identified through research of four series of textbooks will be utilized in writing this course guide. The list of algebraic concepts that were identified appear in Appendix B.

Ordinarily, in a development of the real number system, one is initially introduced to the set N of natural numbers or counting numbers. A counting number is the abstract idea associated with the common

property possessed by equivalent sets (sets that can be placed in a one-to-one correspondence). The set W of whole numbers is then obtained by unioning the set N with the set containing the cardinal number of \emptyset , which is 0. Thus, $W = N \cup \{0\}$.

It is not the writer's aim to submit a detailed development of the real number system. However, it will be instructive to review briefly how the set Z of integers is formally developed from the set W . Initially, one forms the set of all ordered pairs of whole numbers, i.e., $W \times W = \{(a, b) \mid a, b \in W\}$. A relation is defined on $W \times W$, and then this relation is shown to be an equivalence relation. This equivalence relation partitions $W \times W$ into pairwise disjoint equivalence classes. The collection of all these classes is then called the set Z of integers. The operations of addition and multiplication are defined on the elements of Z , and it is verified that these operations possess the properties of integers that are familiar to the reader. There is a subset, say W' , of Z that is in a one-to-one correspondence with W . Furthermore, the addition and multiplication of elements in W' behave exactly like addition and multiplication in W . Because of this amazing fact, one can then think of W as a subset of Z in an intuitive and informal way.

Similarly, the set Q of rational numbers is derived by considering the cross product $Z \times Z$, defining a relation, and showing that this relation is an equivalence relation. The collection of equivalence classes is called the set Q of rational numbers. Properties of addition and multiplication are developed. Finally, it is shown that a subset Z' of Q is in a one-to-one correspondence with Z , and that there is no difference in the behavior of members of Z and Z' with respect to addition and multiplication. So, intuitively and informally, one thinks of Z

as a subset of Q .

To complete the development of the real number system, the set R of real numbers is developed from the set Q . There is a subset Q' of R that is equivalent to, and behaves exactly like, Q . So it is convenient to consider Q as a subset of R . Recall that the set R of real numbers contains the irrational numbers such as $\sqrt{2}$, $\sqrt{10}$, π ; etc.

With the agreements mentioned above, it will be convenient to consider the chain of subsets, $N \subset W \subset Z \subset Q \subset R$, as being pertinent and valid for the purposes of this paper. Thus, set R will be thought of as including the following sets of numbers:

- (1) The positive integers (counting or natural numbers);

$$N = \{1, 2, 3, \dots, n, \dots\} .$$

- (2) The whole numbers which consist of the positive integers and 0; $W = \{0, 1, 2, 3, \dots, n \dots\} .$

- (3) The integers which consist of the positive integers, 0, and the negative integers, $\dots, -3, -2, -1$;

$$Z = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \} .$$

- (4) the rational numbers; $Q = \{ a/b \mid a, b \in Z \text{ and } b \neq 0 \} .$

- (5) the irrational numbers such as $\sqrt{2}$, $-\sqrt{3}$, π , and $\sqrt{5}$.

Binary Operations

The concept of "operation" is one of the most important concepts in mathematics. It is also probably one of the least understood concepts among elementary teachers because there is much confusion

between the mathematical meaning of the term and the everyday usage. In mathematical language, an operation is an association of each ordered pair of a number system with a unique element of the system. The common usage of the term "operation" applies to what actually happens when one performs an arithmetic manipulation. A better name for these manipulations is "algorithm." For instance, the operation of addition in the set N would associate the ordered pair $(13, 21)$ with the number $13 + 21$, while the addition algorithm would permit one to say that "34" is a simpler name for the number represented by " $13 + 21$." Similarly, the operation of multiplication in N would associate the ordered pair $(8, 12)$ with the number 8×12 , and the multiplication algorithm would allow one to write " $8 \times 12 = 96$."

The operations of addition and multiplication in the set N can be considered as rules that associate with each ordered pair $(m, n) \in N \times N$ unique elements of N , denoted by $m + n$ and $m \times n$ (or $m \cdot n$), respectively. Often juxtaposition of letters is used to denote the operation of multiplication; i. e., mn is conveniently used to symbolize the image of (m, n) under the operation of multiplication.

The foregoing remarks suggest that a general definition of an operation on an arbitrary set S can be given. The important idea is that for each ordered pair $(a, b) \in S \times S$ there exists a unique element in S that is associated with (a, b) . Various symbols such as $a * b$, $a \odot b$, or $a ! b$ can be used to denote the element that is associated with (a, b) . It is convenient to refer to the operation as " $*$ ", " \odot ", or " $!$ ". Thus, it would be appropriate to write " $a * b = c$ ", " $a \odot b = d$ ", or " $a ! b = e$ ", where $c, d, e \in S$.

A binary operation $*$ on a set S is a function (or mapping) from $S \times S$ to S . That is, for each ordered pair $(a, b) \in S \times S$ there exists a unique element $a * b \in S$ that is associated with (a, b) .

Because of the importance of the set R of real numbers in mathematics, it is worthwhile to rephrase the above definition.

A binary operation $*$ on the set R is a function (or mapping) from $R \times R$ to R . That is, for each ordered pair $(a, b) \in R \times R$ there exists a unique element $a * b \in R$ that is associated with (a, b) .

In particular, addition and multiplication of elements of R are binary operations on R . That is, for any two real numbers there are uniquely determined real numbers called their sum and product, respectively. For example, the operation of addition associates $4\frac{1}{2}$ with $(\frac{1}{2}, 4)$ while multiplication associates 2 with $(\frac{1}{2}, 4)$. These properties are frequently called the closure properties of addition and multiplication of real numbers.

Let E be the subset of N consisting of the even natural numbers, i.e., $E = \{2, 4, 6, 8, \dots\}$. If $a \in E$ and $b \in E$, then so are $a + b$ and ab . Thus, E has the closure property under the operations of addition and multiplication. Another way of saying the same thing is that E is closed relative to the operations of addition and multiplication. On the other hand, let O be the subset of N consisting of the odd counting numbers. The set O is closed relative to the operation of multiplication because the product of two odd natural numbers is an odd natural number. However, O does not have the closure property for addition since a counter example can be exhibited; namely, $5, 7 \in O$, but $5 + 7 \notin O$.

That is, with ordinary addition it is impossible to find an element in E to associate with the pair $(5, 7)$. Consider the rule, $a * b = (a + b) \div 2$ where $a, b \in E$. Now $*$ is not a binary operation on the set E since $(8, 6) \in E \times E$, but $8 * 6 = (8 + 6) \div 2 = 7 \notin E$. Hence, E is not closed relative to $*$.

For a final example, consider the set S of four integers $\{0, 1, 2, 3\}$ and define an operation on S as follows. For any pair $(a, b) \in S \times S$, find the ordinary sum of a and b , divided this sum by 4, and select the remainder. Let the operation \oplus associate this remainder with the pair (a, b) . Thus, $3 \oplus 2 = 1$ because $3 + 2 = 5$ and 5 divided by 4 leaves a remainder of 1. Similarly, $1 \oplus 2 = 3$, $3 \oplus 1 = 0$, $2 \oplus 1 = 3$, $2 \oplus 2 = 0$, etc. This defines a binary operation on S , and the results of the operation \oplus are shown in Figure 11.

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 11

In Figure 11 the first component of each ordered pair is chosen from the left column while the second component is chosen from the top row. The result of the operation is found at the intersection of the corresponding row and column of the table. A table depicting a binary

operation such as Figure 11 is known as a Cayley square.

Properties of the Real Numbers

It has been seen that real numbers can be "combined" to obtain other real numbers. The binary operations of addition and multiplication on R are of particular interest in the study of algebra; perhaps not so much the operations as such, but the properties that these operations possess. There are fundamental properties of addition and multiplication which are true for all elements of R . These fundamental properties will be considered as axioms for the real number system. There are three categories of axioms for R : the properties of addition and multiplication, the properties of order, and the completeness property. The first two categories will be discussed in some detail in this discourse, but a discussion of the third one is beyond the scope of this exposition.

At this juncture it is convenient to list the axioms that govern the operations of addition and multiplication in the set R of real numbers.

- A. 1. Closure law for addition. For every pair $(a, b) \in R \times R$ (or equivalently, for every $a, b \in R$) there exists a unique element $a + b \in R$ that is associated with (a, b) and called the sum of a and b .
- A. 2. Commutative law for addition. For all $a, b \in R$, $a + b = b + a$.
- A. 3. Associative law for addition. For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$.
- A. 4. Identity elements for addition. There is an element in R ,

denoted by 0, such that for all $a \in R$, $a + 0 = 0 + a = a$.

- A. 5. Inverse elements for addition. For every $a \in R$ there exists an element in R , denoted by $-a$, such that $a + (-a) = (-a) + a = 0$.
- M. 1. Closure law for multiplication. For all $(a, b) \in R \times R$ there exists a unique element $ab \in R$ that is associated with (a, b) and is called the product of a and b .
- M. 2. Commutative law for multiplication. For all $a, b \in R$, $ab = ba$.
- M. 3. Associative law for multiplication. For all $a, b, c \in R$, $(ab)c = a(bc)$.
- M. 4. Identity element for multiplication. There exists an element in R , different from 0 and denoted by 1, such that for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$.
- M. 5. Inverse elements for multiplication. For every $a \in R$ such that $a \neq 0$, there is an element in R , denoted by a^{-1} , such that $aa^{-1} = a^{-1}a = 1$.
- MA Distributive laws. For all $a, b, c \in R$, $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$.

A set which satisfies the axioms stated above is called a field. Therefore, Axioms A.1 - A.5, M.1 - M.5, and MA are called the field properties of the real number system. More will be said about fields in general in subsequent pages.

The commutative properties for addition and multiplication of real numbers is one of the properties that is "retained" throughout the development of the number system from the natural numbers to the

real numbers. A similar statement can be made in regard to the associative and distributive axioms. Set N contains an identity element for multiplication, but not until the whole numbers are developed does one have access to an identity for addition. When the integers are developed from the whole numbers, it is seen that every integer has an additive inverse as stated in Axiom A.5. The additive inverse property was absent in the sets N and W . Finally, the multiplicative inverse property of Axiom M.5 is a property of rational numbers as well as real numbers, but it was not a property of any previous sets of numbers.

The development of algebraic concepts involves the study of the real numbers as a mathematical system.

A mathematical system has three basic parts:

- (1) A universal set.
- (2) Axioms which are statements assumed to be true with respect to this universal set.
- (3) Definitions yielding relations, operations, etc.

The study of a mathematical system is facilitated by proving statements called theorems. Theorems are statements about the structure of a mathematical system and are deduced from the axioms and definitions using the rules of logic [13].

In other words, a mathematical system consists of a set of elements, a list of axioms, definitions, and all the consequences obtained by rules of logic. A mathematical system might be thought of as a package deal since all of the above mentioned ingredients must be present.

It is clear from the commutativity axiom that the real number associated with the pair (a, b) is the same as that associated with the

pair (b, a) . Under the operation of addition, $8 + 7$ is associated with $(8, 7)$ while $7 + 8$ is associated with $(7, 8)$, but Axiom A.2 states that $8 + 7 = 7 + 8$; i.e., $8 + 7$ and $7 + 8$ are different names for the same number 15. Similarly, $7 \cdot 8 = 8 \cdot 7$ since these are different names for 56.

Consider the set $S = \{a, b\}$ and the binary operation \otimes defined by the Cayley square in Figure 12.

\otimes	a	b
a	a	b
b	a	b

Figure 12

This is a system in which \otimes does not enjoy the commutative property since $a \otimes b = b$, $b \otimes a = a$ and $a \neq b$.

Axioms A.3 and M.3, the associativity axioms, state that there is no difference between $(a + b) + c$ and $a + (b + c)$, nor between $(ab)c$ and $a(bc)$. For instance, consider $(5 + 9) + 6$ which indicates that the operation is applied first to 5 and 9 to obtain 14, then the operation is applied to 14 and 6 to yield the number 20. On the other hand, in $5 + (9 + 6)$ the binary operation is performed on 9 and 6 first to yield 15, and then applied to 5 and 15 to obtain 20. Hence, $(5 + 9) + 6 = 5 + (9 + 6)$. Since $(a + b) + c = a + (b + c)$, there is no ambiguity if the parentheses are omitted and $a + b + c$ is permitted to represent

either of the elements $(a + b) + c$ or $a + (b + c)$. According to this agreement, even though addition is a binary operation, it makes sense to consider expressions such as $8 + 4 + 7$, $9 + 3 + 6 + 2$, etc. Similar observations may be made relative to the operation of multiplication.

Lest one be led to believe that all mathematical systems possess the associative property, perhaps it would be instructive to examine the following structure. Let $T = a, b, c, d$ and let the operation $?$ be defined as in Figure 13:

$?$	a	b	c	d
a	b	c	a	a
b	c	c	b	b
c	a	b	a	c
d	a	b	c	d

Figure 13.

In this system $(b ? b) ? a = c ? a = a$, but $b ? (b ? a) = b ? c = b$. Therefore, $(b ? b) ? a \neq b ? (b ? a)$, and so $?$ is not an associative operation.

Examine the computation of $(8 + 9) + (12 + 11)$. One would probably compute $(8 + 12) + (9 + 11)$ to obtain 40. This is certainly valid, but one might ask why this is permissible. That $(8 + 9) + (12 + 11) = (8 + 12) + (9 + 11)$ is a consequence of the axioms of the real number system is demonstrated as follows:

$$\begin{aligned}
(8 + 9) + (12 + 11) &= 8 + 9 + (12 + 11) && \text{[associative law]} \\
&= 8 + (9 + 12) + 11 && \text{[associative law]} \\
&= 8 + (12 + 9) + 11 && \text{[commutative law]} \\
&= 8 + 12 + (9 + 11) && \text{[associative law]} \\
&= (8 + 12) + (9 + 11) && \text{[associative law]}
\end{aligned}$$

Therefore,

$$(8 + 9) + (12 + 11) = (8 + 12) + (9 + 11) \quad \text{[transitive property of equality]}$$

In Axiom MA it was convenient to state two distributive laws. The first one, $a(b + c) = ab + ac$, is often referred to as the left distributive property of multiplication over addition (ldpma), or just simply as the left distributive property. The second, $(b + c)a = ba + ca$, is appropriately called the right distributive property of multiplication over addition (rdpma), or just right distributive property. Actually, even though it was convenient to state both properties in Axiom MA, this was not necessary because by assuming one of them to be true, the other can be proved as a theorem. That is, $(b + c)a = ba + ca$ is a consequence of the field properties of the set R . This can be seen as follows:

$$\begin{aligned}
(b + c)a &= a(b + c) && \text{[commutative property]} \\
&= ab + ac && \text{[ldpma]} \\
&= ba + ca && \text{[commutative property]}
\end{aligned}$$

hence,

$$(b + c)a = ba + ca \quad \text{[transitive property of equality]}$$

Axioms A.4 and M.4 assert the existence of very special real numbers, namely 0 (zero) and 1 (one), respectively. These numbers are special, not because of the names "zero" and "one," but because

of the behavior of these particular numbers with respect to the operations of addition and multiplication. The element 0 is referred to as the additive identity element of R because for each $a \in R$, $a + 0 = 0 + a = a$. For example, $-6 + 0 = -6$, $(1/2 + 3/4) + 0 = (1/2 + 3/4)$, $0 + (-2) = -2$, etc. The element 1 is named the multiplicative identity of R because $a \cdot 1 = 1 \cdot a = a$ regardless of what real number a represents. Thus, $1 \cdot 0 = 0$, $(-3/4) \cdot 1 = -3/4$, $(\sqrt{2}) \cdot 3/3 = \sqrt{2}$, $(-7 + 1) \cdot 1 = (-7 + 1)$, etc.

Regardless of what real number a might represent, Axiom A.5 offers the assurance that there is another real number, represented by $-a$, such that $a + (-a) = -a + a = 0$. The real number represented by $-a$ is termed the additive inverse or the negative of a . Every real number has its own special additive inverse. Given the real number 11 there is a number, namely -11, such that $11 + (-11) = 0$. Since $-\sqrt{3}$ is a real number, it too has an additive inverse which is denoted by $-(-\sqrt{3})$. So, it is true that $-\sqrt{3} + [-(-\sqrt{3})] = 0$. The reader will certainly agree that it seems reasonable to expect " $-(-\sqrt{3})$ " and " $\sqrt{3}$ " to be different names for the same real number. In fact, for all $a \in R$, it is true that $-(-a) = a$. This will be proved as a theorem in due time.

The multiplicative inverse property of Axiom M.5 varies slightly from the additive inverse property. In order for $a \in R$ to have a multiplicative inverse, denoted by a^{-1} , it must be true that $a \neq 0$. The element a^{-1} is sometimes referred to as the reciprocal of a and symbolized by $1/a$. The multiplicative inverse of $2/3$ is $(2/3)^{-1}$ or $3/2$, the inverse of $-1/6$ is $(-1/6)^{-1}$ or -6 , and the inverse of 1 is 1.

It was pointed out previously that the set Q of rational numbers can be considered informally as a subset of R . Also, the operations

of addition and multiplication in Q can be thought of as the same as those in R since, as far as properties are concerned, they behave exactly the same way as addition and multiplication in Q' , which is a subset of R and equivalent to Q . It is only natural to ask what properties these two operations enjoy in the set Q . It just so happens that the same axioms that regulate addition and multiplication in R also govern these two operations in Q . So, it can be said that Q is a field. Because of this characteristic, Q is often termed the field of rational numbers.

With the axioms of the real number system, it is possible to derive some theorems about the real numbers. The theorems considered in this chapter will be statements about the structure of the real number system that can be deduced from the axioms and definitions by using rules of logic.

The first theorem to be considered is suggested by conditionals such as "if $10 = 8 + 2$, then $10 + 9 = (8 + 2) + 9$."

Theorem 3.1. If $a, b, c, d \in R$ such that $a = c$ and $b = d$, then $a + b = c + d$.

Proof. Suppose that $a = c$ and $b = d$, then $a + b = a + b$ by the reflexive property of equality. Therefore, by the law of substitution it follows that $a + b = c + b$. Hence, $a + b = c + d$ by using the law of substitution again.

This theorem does not depend on the set of axioms for R . In fact, if S is an arbitrary set on which a binary operation $*$ is defined, the statement "if $a, b, c, d \in S$ such that $a = c$ and $b = d$, then $a * b = c * d$ " is true. By a slight alteration in the proof of Theorem 3.1, the

proof of the following corollary is immediate.

Corollary. If $a, b \in \mathbb{R}$ such that $a = b$, then for all $k \in \mathbb{R}$, $a + k = b + k$.

The reader should also be convinced that a corresponding theorem and corollary can be proved about multiplication of real numbers. These are stated without proof.

Theorem 3.2. If $a, b, c, d \in \mathbb{R}$ such that $a = c$ and $b = d$, then $ab = cd$.

Corollary. If $a, b \in \mathbb{R}$ such that $a = b$, then for all $c \in \mathbb{R}$, $ac = bc$.

In the Corollary to Theorem 3.1 it was pointed out that the conditional "if $a, b \in \mathbb{R}$ such that $a = b$, then for all $k \in \mathbb{R}$, $a + k = b + k$ " is certainly true. Mathematical curiosity should certainly encourage one to wonder if the converse of this conditional is also true. That this is indeed the case is stated in the following theorem.

Theorem 3.3. If $a, b, c \in \mathbb{R}$ such that $a + c = b + c$, then $a = b$.

Proof. Suppose that $a + c = b + c$. Since Axiom A.5 assures the existence of a real number $-c$ such that $c + (-c) = 0$, it follows by Theorem 3.1 that $(a + c) + (-c) = (b + c) + (-c)$. Therefore, by the associative property, it can be concluded that $a + [c + (-c)] = b + [c + (-c)]$. But $c + (-c) = 0$, hence $a + 0 = b + 0$ by the logical rule of substitution. Since 0 is the additive identity element, it can be concluded that $a = b$.

This important consequence will be used frequently throughout

this exposition, so let it be agreed to identify this theorem as the cancellation law for addition of real numbers. To illustrate, consider the open sentence $a + 6 = 14$ where $a \in \mathbb{R}$. Observe that since $8 + 6 = 14$, the sentence can be written as $a + 6 = 8 + 6$. So, by the cancellation law, it is true that $a = 8$. In other words, the sentence is transformed into a true statement if the variable a is replaced by 8.

Of equal importance is the corresponding cancellation law for multiplication of real numbers. Since the axioms for multiplication are closely related to the axioms for addition, an analogous procedure can be used to derive this consequential result. However, it must be required that $c \neq 0$ in order to guarantee the existence of the multiplicative inverse c^{-1} .

Theorem 3.4. If $a, b, c \in \mathbb{R}$ such that $ac = bc$ and $c \neq 0$, then $a = b$.

Proof. Let $ac = bc$ and $c \neq 0$. By Axiom M. 5, c^{-1} exists and $cc^{-1} = 1$. By Theorem 3.2, $(ac)c^{-1} = (bc)c^{-1}$. So, $a(cc^{-1}) = b(cc^{-1})$ because of the associative law. Hence, $a \cdot 1 = b \cdot 1$ by substitution. Therefore, $a = b$ by virtue of Axiom M. 4.

The cancellation laws are advantageous when one considers an open sentence such as $3b + 5 = 26$ where $b \in \mathbb{R}$. This is equivalent to $3b + 5 = 21 + 5$. By the cancellation law for addition, it follows that $3b = 21$, and hence $3b = b \cdot 3 = 7 \cdot 3$. Therefore, it can be concluded that $b = 7$ due to the cancellation law for multiplication.

On page 61 it was suggested that for any $a \in \mathbb{R}$, it is true that $-(-a) = a$. This can be stated in the form of a theorem.

Theorem 3.5. For all $a \in \mathbb{R}$, $-(-a) = a$. That is, the additive inverse of $-a$ is a .

Proof. Since $a \in \mathbb{R}$ it is true that $-a \in \mathbb{R}$ and $a + (-a) = 0$ by Axiom A.5. Now, by the same reason, $-(-a) \in \mathbb{R}$ and $-(-a) + (-a) = 0$. So, by the transitive property of equals, $a + (-a) = -(-a) + (-a)$. But then $a = -(-a)$ because of the cancellation law for addition (Theorem 3.3).

As one might expect, there is an analogous theorem about multiplicative inverses. The proof of Theorem 3.6 is omitted since it is similar to the proof of Theorem 3.5.

Theorem 3.6. For all $a \in \mathbb{R}$ such that $a \neq 0$, $(a^{-1})^{-1} = a$. That is, the multiplicative inverse of a^{-1} is a .

Another useful and well known fact about real numbers is that $a \cdot 0 = 0$ for any $a \in \mathbb{R}$. In reality, this could have been included in the list of axioms, but it is desirable to have the least number of axioms possible. Consequently, this property will be deduced as a theorem. As a change of pace, a proof by the column method will be employed.

Theorem 3.7. For all $a \in \mathbb{R}$, $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Proof.

- | | |
|---|---------------|
| (1) $0 + 0 = 0$ | [Axiom A.4] |
| (2) $(0 + 0) a = 0 \cdot a$ | [Theorem 3.2] |
| (3) $a(0 + 0) = a \cdot 0$ | [Axiom M.2] |
| (4) $a \cdot 0 + a \cdot 0 = a \cdot 0$ | [ldpma] |
| (5) $a \cdot 0 + a \cdot 0 = 0 + a \cdot 0$ | [Axiom A.4] |
| (6) $a \cdot 0 = 0$ | [Theorem 3.3] |

$$(7) \quad a \cdot 0 = 0 \cdot a \quad [\text{Axiom M. 2}]$$

$$(8) \quad 0 \cdot a = 0 \quad [(6), (7), \text{ and substitution}]$$

For the purposes of this paper it is not expedient to attempt to formally present all the properties of the real number system. It is hoped that the reader, through prior mathematical experiences and reading this exposition, has gained some facility and proficiency for reading and writing mathematical proofs. However, one type of proof that is different from those previously considered needs to be presented.

In mathematics one is frequently confronted with the idea of "uniqueness" of certain elements in a set. For instance, the intuition leads one to believe that there is "one and only one" additive identity in \mathbb{R} ; that is, 0 is the only real number with the property that $a + 0 = 0 + a = a$ for every $a \in \mathbb{R}$. That 0 is the only real number with this important property is the statement of Theorem 3.8.

Theorem 3.8. The additive identity in \mathbb{R} is unique; that is, if there exists $\mu \in \mathbb{R}$ such that $a + \mu = \mu + a = a$ for all $a \in \mathbb{R}$, then $\mu = 0$.

Proof. Suppose there does exist $\mu \in \mathbb{R}$ such that $a + \mu = \mu + a = a$ for all $a \in \mathbb{R}$. Since 0 is an additive identity, it is known that $a + 0 = 0 + a = a$. Therefore, $\mu + a = 0 + a$ by the transitive property of equality. It then follows that $\mu = 0$ by Theorem 3.3. Thus, 0 is the only additive identity in \mathbb{R} .

Theorems such as Theorem 3.8 are called uniqueness theorems. Other uniqueness theorems about the multiplicative identity, additive inverses, and multiplicative inverses would be

proved similarly by using the cancellation laws. Consequently, one should be able to convince oneself of the truth of the following without any difficulty.

Theorem 3.9. The multiplicative identity element is unique.

Theorem 3.10. For all $a \in R$, the additive inverse of a is unique.

Theorem 3.11. For all $a \in R$ such that $a \neq 0$, the multiplicative inverse of a is unique.

Two very significant and indispensable results that are essential to the study of algebra need to be considered. These properties are the statements of the next two theorems.

Theorem 3.12. Let $a, b \in R$. If $a = 0$ or $b = 0$, then $ab = 0$.

Proof.

- | | |
|---|---------------|
| (1) $a = 0$ or $b = 0$ | [hypothesis] |
| (2) if $a = 0$, then $ab = 0$ | [Theorem 3.7] |
| (3) if $b = 0$, then $ab = 0$ | [Theorem 3.7] |
| (4) if $a = 0$ or $b = 0$, then $ab = 0$ | [(1) - (3)] |

Theorem 3.13. Let $a, b \in R$. If $ab = 0$, then $a = 0$ or $b = 0$.

Proof. The indirect method of proof will be used. Suppose $(ab = 0)$ and $\sim(a = 0 \text{ or } b = 0)$, then it follows that $(ab = 0)$ and $(a \neq 0 \text{ and } b \neq 0)$. Now the assumption that $a \neq 0$ and $b \neq 0$ ensures the existence of a^{-1} and b^{-1} . Hence, $a^{-1}(ab) = a^{-1} \cdot 0$ and $(ab)b^{-1} = 0 \cdot b^{-1}$, and it follows that $a = 0$ and $b = 0$. Both statements $(a \neq 0 \text{ and } b \neq 0)$

and $(a = 0 \text{ and } b = 0)$ cannot be true. Therefore, the supposition $(ab = 0)$ and $\sim(a = 0 \text{ or } b = 0)$, which is equivalent to $\sim(ab = 0 \rightarrow a = 0 \text{ or } b = 0)$, is false. So the only alternative is to accept the truth of the conditional; $ab = 0 \rightarrow a = 0 \text{ or } b = 0$.

Preferably, Theorems 3.12 and 3.13 are combined to formulate a single theorem. The reader will recognize the result to be a biconditional statement.

Theorem 3.14. For all $a, b \in \mathbb{R}$, $ab = 0$ if and only if $a = 0$ or $b = 0$.

When a sentence such as $(b + 3)(b + 5) = 0$ is encountered, it can be concluded immediately that $b + 3 = 0$ or $b + 5 = 0$. Consequently, $b = -3$ or $b = -5$.

Perhaps previous algebra courses provided experiences in which the reader became acquainted with expressions such as "the product of two negative numbers is a positive number" and "the product of a negative number and a positive number is a negative number." An appeal was made to the intuition by referring to physical situations such as the rising and falling of the thermometer, money earned and money disbursed, etc. There is nothing wrong with using one's intuition, but it is sound mathematics to use logical reasoning to verify that the intuition is indeed correct. Note that the above expressions are special instances of a more general result stated in Theorem 3.15.

Theorem 3.15. For all $a, b \in \mathbb{R}$, $a(-b) = -(ab)$ and $(-a)b = -(ab)$.

Proof. Since $b \in \mathbb{R}$ it follows that $-b \in \mathbb{R}$ and $b + (-b) = 0$. So $a[b + (-b)] = a \cdot 0 = 0$. Hence, $ab + a(-b) = 0$ because of the distribu-

tive law. However, it is already known that $ab + [-(ab)] = 0$ (Axiom A.5). Therefore, by Theorem 3.10, it is true that $a(-b) = -(ab)$.

To prove the second part of the theorem, just observe that $(-a)b = b(-a)$ and apply the result just proved to conclude that $(-a)b = b(-a) = -(ba)$. It then follows that $(-a)b = -(ab)$ by the transitive property of equality and the commutative law.

Corollary 1. For all $a \in R$, $a(-1) = -a$ and $(-1)a = -a$.

Proof. In Theorem 3.15 choose $b = 1$, then $a(-1) = -(a \cdot 1) = -a$. Similarly, $(-1)a = -a$.

Corollary 2. For all $a, b \in R$, $(-a)(-b) = ab$.

Proof.

$$\begin{aligned} (-a)(-b) &= -[a(-b)] && \text{[Theorem 3.15]} \\ &= -[-(ab)] && \text{[Theorem 3.15]} \\ &= ab && \text{[Theorem 3.5]} \end{aligned}$$

Hence,

$$(-a)(-b) = ab \quad \text{[transitive property of equality]}$$

Perhaps it would be helpful to rephrase Theorem 3.15 in the following manner: The product of a and the additive inverse of b is just the inverse of the product ab ; i. e., first determine the product ab and then find the additive inverse of this product. For example, immediate consequences of Theorem 3.15 are $5(-8) = -(5 \cdot 8) = -40$ and $(-5/6)(2/5) = -(5/6 \cdot 2/5) = -1/3$.

Corollary 1 can be rephrased as: The product of any real number a and -1 is the additive inverse of a . Corollary 2 says that

the product of any two real numbers is the same as the product of their additive inverses. For example, $(5/16)(-1) = -5/16$, $(-5)(-3) = 5 \cdot 3 = 15$, and $[-(-4)] \cdot (-7) = (-4) \cdot 7 = -28$.

The reader will agree that the proof of Corollary 2 to Theorem 3.15 was quite simple. However, an alternate proof is offered to further demonstrate the column method and to suggest that there may be alternate ways of attacking a proof to a theorem.

Theorem 3.16. For all $a, b \in \mathbb{R}$, $(-a)(-b) = ab$.

Proof.

- | | |
|---|------------------------------|
| (1) $a + (-a) = 0$ | [Axiom A.5] |
| (2) $[a + (-a)](-b) = 0 \cdot (-b)$ | [Theorem 3.2] |
| (3) $[a + (-a)](-b) = a(-b) + (-a)(-b)$ | [rdpma] |
| (4) $a(-b) + (-a)(-b) = 0 \cdot (-b)$ | [(2), (3), and substitution] |
| (5) $0 \cdot (-b) = 0$ | [Theorem 3.7] |
| (6) $a(-b) + (-a)(-b) = 0$ | [(4), (5), and substitution] |
| (7) $a(-b) = -(ab)$ | [Theorem 3.15] |
| (8) $-(ab) + (-a)(-b) = 0$ | [(6), (7), and substitution] |
| (9) $-(ab) + (ab) = 0$ | [Axiom A.5] |
| (10) $(-a)(-b) = ab$ | [(8), (9), and Theorem 3.10] |

To stress the fact that the field of real numbers is a mathematical structure with binary operations of addition and multiplication, the writer has consistently used the notation $a + (-b)$, $a + (-a)$, etc. However, the closure axiom and the additive inverse axiom provide the machinery to define the operation of subtraction in \mathbb{R} .

For all $a, b \in R$, the operation of subtraction in R , denoted by $a - b$, is defined as follows: $a - b = a + (-b)$.

Note that in this definition the symbol "-" has two different meanings, and they are not to be confused with one another. In the expression $a - b$ the symbol denotes an operation on the elements a and b , and in the expression $a + (-b)$ it denotes the additive inverse of b or the negative of b . Observe also that the closure and additive inverse postulates guarantee that subtraction is a binary operation in R . That is, for all $a, b \in R$, it is true that $a - b \in R$. Subtraction is also a binary operation on the sets Z and Q .

Subtraction is not a binary operation in N nor in W since these sets are not closed with respect to subtraction. This is because of the fact that the additive inverse axiom does not hold in these sets of numbers. It is true, nevertheless, that "subtraction" can be accomplished in a very limited sense in these two sets. One is convinced of this fact by observing that $8 - 5$ does indeed denote an element of N , but $7 - 11$ does not. What then is the restriction placed upon "subtraction" in sets N and W ? Formally, for all $a, b \in N$, $a - b \in N$ if and only if there exists $c \in N$ such that $a = b + c$. A similar statement may be made relative to elements of W . By properly choosing a subset S of $N \times N$ so that the pairs in S meet the above specification, it is possible to consider subtraction as a binary operation from S to N .

In the context of elementary school mathematics, one encounters the idea that "subtraction is the inverse operation of addition." However, a word of caution needs to be inserted.

Addition on N is a binary operation (function) that associates a unique element in N with each ordered pair in $N \times N$. For instance, the unique image of $(5, 3)$ is 8. But notice that the inverse relation does not associate a unique pair with 8. That is, the inverse relation associates all the pairs $(5, 3)$, $(2, 6)$, $(4, 4)$, and $(1, 7)$ with 8. So, the inverse relation is not a function.

It is convenient, however, to think of subtraction as "the inverse operation of addition" in the sense that subtraction undoes addition. Students learn that the expression " $(8 + 5) - 5$ " is just another way of naming the number 8. In general, $(a + b) - b = a$ where $a, b \in N$. Now addition is a binary operation in N ; therefore, there exists $c \in N$ that is associated with the pair (a, b) . Keeping in mind the restriction on "subtraction" in N , it can be said that a is the natural number associated with the pair (c, b) . In the above example, 13 is associated with the pair $(8, 5)$ while 8 is associated with the pair $(13, 5)$.

As concluding activities with subtraction in R , perhaps it would be informative to prove some familiar properties. The first theorem states that multiplication distributes over subtraction.

Theorem 3.17. For all $a, b, c \in R$, $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Proof.

$$\begin{array}{ll}
 (1) & a(b - c) = a[b + (-c)] \quad [\text{definition of subtraction}] \\
 (2) & = ab + a(-c) \quad [\text{ldpma}] \\
 (3) & = ab + [-(ac)] \quad [\text{Theorem 3.15}] \\
 (4) & = ab - ac \quad [\text{definition of subtraction}]
 \end{array}$$

$$(5) \quad a(b - c) = ab - ac \quad [\text{transitive property of equality}]$$

It may be shown similarly that $(b - c)a = ba - ca$

Theorem 3.18. For all $a, b \in \mathbb{R}$, $-(a + b) = (-a) + (-b) = -a - b$.

Proof.

$$(1) \quad -(a + b) = (-1)(a + b) \quad [\text{Corollary to Theorem 3.15}]$$

$$(2) \quad = (-1)a + (-1)b \quad [\text{ldpma}]$$

$$(3) \quad = (-a) + (-b) \quad [\text{Theorem 3.15}]$$

$$(4) \quad = -a - b \quad [\text{definition of subtraction}]$$

$$(5) \quad -(a + b) = -a - b \quad [\text{transitive property of equality}]$$

Theorem 3.18 states that the additive inverse of a sum of two real numbers is the same as the sum of their additive inverses, or the second number b subtracted from the additive inverse of a . This also applies to expressions such as $-(a - b)$. Notice that $-(a - b) = -a - (-b)$ by Theorem 3.18. But $-a - (-b) = -a + [-(-b)]$ by the definition of subtraction. Hence, by Theorem 3.5 and substitution, it follows that $-(a - b) = -a + b$. For example, $-(- + 7) = -(9 + 7) = -16$ and $-(3 - 8) = -3 + 8$.

The advantages of the property stated in Theorem 3.17 are synonymous with the advantages of the distributive property of multiplication over addition. If one is required to compute $42 \cdot 14 - 42 \cdot 4$, Theorem 3.17 makes provision for one to first calculate $14 - 4 = 10$ and then multiply 42 by 10 to obtain 420.

Subtraction of real numbers does not enjoy all the nice properties possessed by addition, for subtraction is not a commutative operation. To see this, observe that $5 - 2 \neq 2 - 5$. However, there

are some useful properties of subtraction that are noteworthy of attention. The content of each of the next three theorems has to do with subtraction of real numbers.

Theorem 3.19. For all $a, b \in \mathbb{R}$, $a - b = -b + a$.

Proof. By the definition of subtraction, $a - b = a + (-b)$.

Therefore, by Axiom A.2, it follows that $a - b = -b + a$.

Since Theorem 3.19 is true for all real numbers a and b , it is also true for the additive inverses $-a$ and $-b$. For example, $13 - 6 = -6 + 13$, $-11 - 4 = -4 - 11$, and $-12 - (-5) = -(-5) - 12$.

Theorem 3.20. For all $a, b, c, d \in \mathbb{R}$, $(a - b) + (d - c) = (a - c) + (d - b)$.

Proof.

$$\begin{aligned}
 (a - b) + (d - c) &= [a + (-b)] + [d + (-c)] && \text{[definition of subtraction]} \\
 &= a + \{(-b) + [d + (-c)]\} && \text{[Axiom A.3]} \\
 &= a + \{[(-b) + d] + (-c)\} && \text{[Axiom A.3]} \\
 &= a + \{(-c) + [(-b) + d]\} && \text{[Axiom A.2]} \\
 &= a + \{(-c) + [d + (-b)]\} && \text{[Axiom A.2]} \\
 &= [a + (-c)] + [d + (-b)] && \text{[Axiom A.3]} \\
 &= (a - c) + (d - b) && \text{[definition of subtraction]}
 \end{aligned}$$

Corollary. For all $a, b, c \in \mathbb{R}$, $(a - b) + (b - c) = a - c$.

Proof. By Theorem 3.20, $(a - b) + (b - c) = (a - c) + (b - b)$.

Since $b - b = 0$, it follows that $(a - b) + (b - c) = a - c$.

Theorem 3.20 has useful applications in computation. For instance, $(18 - 7) + (27 - 8) = (18 - 8) + (27 - 7) = 30$.

Theorem 3.21. For all $a, b, c, d \in \mathbb{R}$, $(a - b) + (c - d) = (a + c) - (b + d)$.

Proof.

$$\begin{aligned}
 (a - b) + (c - d) &= [a + (-b)] + [c + (-d)] && \text{[definition of subtraction]} \\
 &= \{a + [(-b) + c]\} + (-d) && \text{[Axiom A.3]} \\
 &= \{a + [c + (-b)]\} + (-d) && \text{[Axiom A.2]} \\
 &= [(a + c) + (-b)] + (-d) && \text{[Axiom A.3]} \\
 &= (a + c) + [(-b) + (-d)] && \text{[Axiom A.3]} \\
 &= (a + c) + [(-1)b + (-1)d] && \text{[Corollary to Theorem 3.15]} \\
 &= (a + c) + (-1)(b + d) && \text{[ldpma]} \\
 &= (a + c) + [-(b + d)] && \text{[Corollary to Theorem 3.15]} \\
 &= (a + c) - (b + d) && \text{[definition of subtraction]}
 \end{aligned}$$

Corollary. For all $a, b, c \in \mathbb{R}$, $(a + c) - (b + c) = a - b$.

Proof. By Theorem 3.21, $(a + c) - (b + c) = (a - b) + (c - c)$. Since $c - c = 0$, it follows that $(a + c) - (b + c) = a - b$.

The benefit derived from Theorem 3.21 is seen when one is doing computation involving both addition and subtraction. For example, either $(12 - 8) + (18 - 6)$ or $(12 + 18) - (8 + 6)$ will yield the same result, 16. In other words, one can subtract first and then add the results, or one can add and then subtract the results.

Analogously, the closure law and the multiplicative inverse laws afford the possibility of defining the operation of division in R . However, because of the restriction stated in the multiplicative inverse axiom, division in R is not always permissible.

For all $a, b \in R$ such that $b \neq 0$, the operation of division in R , denoted by $a \div b$, is defined as follows: $a \div b = a \cdot (1/b)$.

Division is not a binary operation in R , but by the above definition it is a binary operation in $R - \{0\}$ [complement of $\{0\}$ relative to R]. Another way to think about $a \div b$ is "a multiplied by the reciprocal of b," but by agreement this is just ab^{-1} . It is also acceptable to denote the element $a \div b$ by a/b , which is called the quotient of a by b. This lends to the usual observation that division by 0 is an undefined operation in R .

The sets N , W , and Z are not closed with respect to division because the multiplicative inverse axiom does not hold. Therefore, division is not a binary operation on N , W , and Z . For instance, in N , $4 \div 2$ names the number 2, but $2 \div 4$ does not name a natural number. Similarly, $-12 \div 3$ names the integer -4, but $3 \div (-12)$ does not represent an integer. It is then clear that for all $a, b \in N$ such that $b \neq 0$, $a \div b \in N$ if and only if there exists $c \in N$ such that $a = bc$. Here a is said to be a multiple of b , and b is said to be a factor or divisor of a . If the subset D of $N \times N$ is selected such that the first component of each ordered pair is a multiple of the corresponding second component, where no second components are 0, then it is certainly true that division is a binary operation from D to N . Similar deductions may be made about the sets W and Z .

Correspondingly, division is thought of as "the inverse operation of multiplication" in the proper context. That is, $(a \cdot b) \div b = a$ since there is a natural number c associated with (a, b) and a is the natural number associated with (c, b) . Notice that $c \div b$ is indeed a natural number because c is a multiple of b . A specific illustration would be $(42 \cdot 8) \div 8 = 42$.

The contrapositive of Theorem 3.12 is "if $\sim(a = 0 \text{ or } b = 0)$, then $\sim(ab = 0)$ " which is equivalent to "if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$." Since this contrapositive is equivalent to the original conditional, it too is an important characteristic of the system of real numbers.

For example, since $4 \neq 0$ and $3 \neq 0$ it can be concluded that 4^{-1} , or $1/4$, and 3^{-1} , or $1/3$, are not 0. Therefore, $(4^{-1})(3^{-1})$, or $(1/4)(1/3)$, is not 0. Notice that $(3 \cdot 4)(4^{-1} \cdot 3^{-1}) = 1$, and also $(3 \cdot 4)(3 \cdot 4)^{-1} = 1$. A definite conclusion is that $(4^{-1} \cdot 3^{-1}) = (3 \cdot 4)^{-1}$ because of the uniqueness of the multiplicative inverse of $3 \cdot 4$, or 12. Reasonable conjectures would be that for all $a, b \in \mathbb{R}$ such that $a \neq 0$ and $b \neq 0$, it is true that $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

Theorem 3.22. For all $a, b \in \mathbb{R}$ such that $a \neq 0$ and $b \neq 0$, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

Proof. Since $a \neq 0$ and $b \neq 0$, it follows that a^{-1} , b^{-1} , and $(ab)^{-1}$ exist and are different from 0. By the contrapositive of Theorem 3.12, $ab \neq 0$ and $b^{-1}a^{-1} \neq 0$. It is known that $(ab)(ab)^{-1} = 1$. Also, $(ab)(b^{-1}a^{-1}) = 1$ since $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$. Therefore, by the uniqueness of multiplicative inverse, it follows that $(ab)^{-1} = b^{-1}a^{-1}$. By Axiom M.2, $b^{-1}a^{-1} = a^{-1}b^{-1}$, and it is clear that $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

In a mathematical system where inverses exist and the binary operation is not commutative, the latter statement in Theorem 3.17 would not necessarily be true. That is, it is always the case that $(ab)^{-1} = b^{-1}a^{-1}$, but in a noncommutative system it may not be true that $a^{-1}b^{-1} = b^{-1}a^{-1}$.

As culminating activities in this section on properties of the real numbers, consider other familiar properties that merit attention.

Theorem 3.23. For all $a, b, c, d \in \mathbb{R}$ such that $b \neq 0$ and $d \neq 0$, $(a/b)(c/d) = ac/bd$.

Proof. If $b \neq 0$ and $d \neq 0$, then b^{-1} and d^{-1} exist by the multiplicative inverse axiom. By agreement $a/b = ab^{-1}$ and $c/d = cd^{-1}$, and therefore $(a/b)(c/d) = (ab^{-1})(cd^{-1})$. By the commutative and associative laws $(ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1})$. But $b^{-1}d^{-1} = (db)^{-1} = (bd)^{-1}$ by Theorem 3.22 and the commutative law. Hence, $(a/b)(c/d) = (ac)(bd)^{-1} = ac/bd$.

Theorem 3.24. For all $a, b, c, d \in \mathbb{R}$ such that $b \neq 0$ and $d \neq 0$,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Proof.

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= ab^{-1} + cd^{-1} && \text{[definition]} \\ &= (ab^{-1}) \cdot 1 + (cd^{-1}) \cdot 1 && \text{[Axiom M.4]} \\ &= (ab^{-1})(dd^{-1}) + (cd^{-1})(bb^{-1}) && \text{[Axiom M.5]} \\ &= (ad)(b^{-1}d^{-1}) + (bc)(b^{-1}d^{-1}) && \text{[Axioms M.2 and M.3]} \\ &= (ad)(bd)^{-1} + (bc)(bd)^{-1} && \text{[Theorem 3.22]} \end{aligned}$$

$$= (ad + bc)(bd)^{-1} \quad [\text{rdpma}]$$

$$= \frac{ad + bc}{bd} \quad [\text{definition}]$$

Corollary. For all $a, b, c \in \mathbb{R}$ such that $c \neq 0$, $\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}$.

Proof.

$$\frac{a}{c} + \frac{b}{c} = \frac{ac + cb}{cc} \quad [\text{Theorem 3.24}]$$

$$= \frac{ac + bc}{cc} \quad [\text{Axiom M. 2}]$$

$$= \frac{(a + b)c}{cc} \quad [\text{rdpma}]$$

$$= \frac{a + b}{c} \cdot \frac{c}{c} \quad [\text{Theorem 3.23}]$$

$$= \frac{a + b}{c} \cdot 1 \quad [\text{Axiom M. 5}]$$

$$= \frac{a + b}{c} \quad [\text{Axiom M. 4}]$$

To reiterate, an important realization in regard to the system of real numbers is that all of the familiar and useful properties can be deduced from the field axioms. Even though this cannot be done in the limited confine of this paper, perhaps the reader has attained a feel for the logical proofs submitted here and has been convinced that other properties could be developed just as systematically and efficiently as the foregoing.

Other Fields

The axioms on pages 55 and 56 were identified as the field properties of the real number system. If the system of real numbers were the only system that satisfied each of those named properties,

then it would be superfluous to use the term "field" for identification. It was seen that the operations of addition and multiplication in the set R of rational numbers are also governed by the same axioms. Examples of systems that are fields as well as examples of systems that are not fields will be forthcoming. But first, a restatement of the assumptions that are made about a set that is called a field is in order.

A field is a set F , containing at least two elements and having the following properties.

A. 1. There is a binary operation on F that is called addition and denoted by "+".

A. 2. For all $a, b \in F$, $a + b = b + a$.

A. 3. For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$.

A. 4. There exists $z \in F$ such that for all $a \in F$,
 $a + z = z + a = a$.

A. 5. For every $a \in F$ there exists $a' \in F$ such that
 $a + a' = a' + a = z$.

M. 1. There is a binary operation on F called multiplication and denoted by " \times ", " \cdot ", or juxtaposition.

M. 2. For all $a, b \in F$, $ab = ba$.

M. 3. For all $a, b, c \in F$, $(ab)c = a(bc)$.

M. 4. There exists $u \in F$ such that for all $a \in F$,
 $au = ua = a$.

M. 5. For all $a \in F$ such that $a \neq z$, there exists $a'' \in F$ such that $aa'' = a''a = u$.

As previously pointed out, these assumptions are called "axioms," and in particular they are called "field axioms." Even though the terms "addition" and "multiplication" are used to name the binary operations on F , these are not to be confused with the ordinary operations on numbers. It is possible to exhibit fields whose binary operations are governed by these axioms, but the operations themselves are quite different from ordinary addition and multiplication. Correspondingly, the notations for addition and multiplication are employed to denote the field operations although there may not be any resemblance whatsoever to these familiar operations.

The field elements z and u , whose existence is asserted in Axioms A.4 and M.4 will be denoted by 0 and 1 , respectively, when it is apparent that no confusion will arise. The previously established symbols for inverse elements will suffice in this discussion of fields. The symbol " $-a$ " will mean the "additive inverse of a ," and " a^{-1} " will represent the "multiplicative inverse" of an element a which is distinct from z .

A significant and noteworthy observation may now be made. Each one of the properties of real numbers that was deduced from the field properties of the real numbers and logical reasoning has a corresponding theorem that is true about the elements of an arbitrary field F . For example, Theorem 3.15 on page 68 stated that for all $a, b \in \mathbb{R}$, $a(-b) = -(ab)$ and $(-a)b = -(ab)$. The analog of Theorem 3.15 for an arbitrary field F would be stated in precisely the same way with one minor alteration. \mathbb{R} would be replaced with F . Furthermore, the proof of this analog would correspond accordingly to the proof of Theorem 3.15. Similar parallels could be drawn relevant to the other

theorems about real numbers.

Occasionally in computations the main concern is with the evenness and oddness of integers rather than with any other properties they may possess. It is known from elementary arithmetic that a sum of two even integers is even; a sum of an even and an odd integer is odd; a sum of any two odd integers is even; a product of any two even integers is even; a product of an even integer and an odd integer is even; and a product of two odd integers is odd. If the even integers are symbolized by "e" and the odd integers by "o," then in tabular form this arithmetic may be described as in Figure 14.

	+	e	o
e	e	e	o
o	o	o	e

	·	e	o
e	e	e	e
o	o	e	o

Figure 14.

It is time consuming, but not difficult, to verify that the set $F = \{e, o\}$ is indeed a field. The tables in Figure 14 define two binary operations on F . That the commutative laws hold may be verified by substantiating from the tables that $e + o = o + e = o$ and $e \cdot o = o \cdot e = e$. The physical appearance of the tables also provides a device for checking the validity of the commutative laws in this system. That is, if one would imagine a line being drawn from the

upper left corner of each table to the lower right corner, then the entries in each table are "symmetric" with respect to this line.

The task of showing that the field operations are associative becomes a little more involved. It may be done for the operation of "addition" by checking the truth of the following eight statements.

$$(e + e) + e = e + (e + e) \qquad (o + e) + e = o + (e + e)$$

$$(e + e) + o = e + (e + o) \qquad (o + e) + o = o + (e + o)$$

$$(e + o) + e = e + (o + e) \qquad (o + o) + e = o + (o + e)$$

$$(e + o) + o = e + (o + o) \qquad (o + o) + o = o + (o + o)$$

Similar statements about the field operation "multiplication" are also true.

Another glance at the "addition" and "multiplication" tables in Figure 14 will reveal that $e + o = o$ and $e + e = e$. Thus, e satisfies the requirements to be the additive identity. Similarly, $e \cdot o = e$ and $o \cdot o = o$, which is sufficient for o to qualify for the multiplicative identity.

The reader should also observe that $e + e = e$ and $o + o = e$, and thus e serves as the additive inverse of e , and o serves the additive inverse of o . In other words, e is the same as $-e$ and o is the same as $-o$.

Since e is the additive identity and $o \neq e$, Axiom M.4 will be satisfied provided that o has a multiplicative inverse. By the multiplication table it is true that $o \cdot o = o$, where o is also the identity element for multiplication. Thus, o is its own multiplicative inverse; i. e., $o^{-1} = o$.

The distributive law (Axiom MA) may be verified by using Figure 14 to check the truth of the statements listed below.

$$\begin{array}{ll}
 e \cdot (e + e) = e \cdot e + e \cdot e & o \cdot (e + e) = o \cdot e + o \cdot e \\
 e \cdot (e + o) = e \cdot e + e \cdot o & o \cdot (e + o) = o \cdot e + o \cdot o \\
 e \cdot (o + e) = e \cdot o + e \cdot e & o \cdot (o + e) = o \cdot o + o \cdot e \\
 e \cdot (o + o) = e \cdot o + e \cdot o & o \cdot (o + o) = o \cdot o + o \cdot o
 \end{array}$$

Since the set $F = \{o, e\}$ satisfies all of the field axioms, it can be concluded that F is indeed a field. Again the reader should be cognizant of the fact that for each of the theorems that was proved about the field of real numbers, there would be a corresponding theorem stating an analogous property relative to F .

The field F of the preceding example may be constructed in another way. Since division of an even integer by 2 leaves a remainder of 0 and division of an odd integer by 2 leaves a remainder of 1, let 0 represent e of the field F and let 1 represent o . Let Z_2 be the set $\{0, 1\}$. Construct an "addition" table by the method employed in the example on page 54. That is, for any pair $(a, b) \in Z_2 \times Z_2$, find the ordinary sum of a and b , divide the sum by 2, and select the remainder. Similarly, construct a "multiplication" table, but this time find the product of a and b and choose the remainder upon dividing the product by 2. The resulting tables are arranged in Figure 15.

It is not difficult to see that Z_2 is also a field. In fact, every statement that was made about the field F can also be made about the field Z_2 by replacing e with 0 and o with 1.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Figure 15.

Again an appeal is made to the example on page 54. In this example the set S contained the four integers 0, 1, 2, and 3; i.e., $S = \{0, 1, 2, 3\}$. It is convenient to rename the set S with the symbol " Z_4 ". The operation of "addition" was symbolized by " \oplus ". Now define the operation of "multiplication" on set Z_4 as follows. For any pair $(a, b) \in Z_4 \times Z_4$, find the ordinary product of a and b , divide this product by 4, and select the remainder. Let the operation of "multiplication", denoted by " \otimes ", associate this remainder with the pair (a, b) . The table in Figure 11 on page 54 is reproduced in Figure 16 for convenient reference along with the newly constructed "multiplication" table.

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\otimes	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figure 16.

A natural question arises relative to this mathematical system. Is Z_4 a field? Certainly the two Cayley squares in Figure 16 reveal that \oplus and \odot are binary operations on Z_4 . The symmetric quality of each table also convinces one that the operations satisfy the commutative laws.

The associative laws and the distributive law are somewhat laborious to verify, but one can be persuaded that these properties do hold by checking the truth of several representative examples such as $(2 \oplus 3) \oplus 1 = 2 \oplus (3 \oplus 1)$, $(3 \odot 1) \odot 0 = 3 \odot (1 \odot 0)$, and $2 \odot (1 \oplus 3) = (2 \odot 1) \oplus (2 \odot 3)$. Actually, a complete verification would require checking 64 statements to establish the associative law together with the same number for the distributive law. So let there be agreement that Z_4 does indeed enjoy these properties.

It is easy to see that 0 is the additive identity, 1 is the multiplicative identity, and that every element has an additive inverse. But what about multiplicative inverses? The element 1 is its own multiplicative inverse, and 3 is its own inverse; but 2 does not have a multiplicative inverse. There is no element $a \in Z_4$ such that $2 \odot a = 1$ or $a \odot 2 = 1$. Therefore, all of the field axioms are not satisfied. Thus, Z_4 is not a field.

It was stated earlier that the cancellation laws are valid in an arbitrary field. To further substantiate that the system Z_4 is not a field, notice that $2 \odot 2 = 0$ and $2 \odot 0 = 0$, and thus $2 \odot 2 = 2 \odot 0$. However, $2 \neq 0$, so the cancellation law does not hold in this system Z_4 .

As a concluding illustration, examine the system Z of integers. The field axioms satisfied by this mathematical system are A.1, A.2, A.3, A.4, A.5, M.1, M.2, M.3, M.4, and MA. More specifically,

addition and multiplication are binary operations on Z ; addition and multiplication are commutative and associative; and multiplication distributes over addition. Furthermore, every integer has an additive inverse, and 0 is the additive identity. The multiplicative identity is 1, but every non-zero integer does not have a multiplicative inverse. For example, 5 has no multiplicative inverse since there is no element $a \in Z$ such that $5 \cdot a = 1$. It is true that the only integers that have multiplicative inverses are 1 and -1, and they are their own inverses. The integers, therefore, do not satisfy all of the field axioms, and thus they do not constitute a field. However, certain theorems that have already been proved are also valid if the elements are restricted to Z . This is true because only the axioms that hold in Z as well as in R were used in the proofs. These theorems are 3.1 - 3.3, 3.5, 3.7 - 3.12, and 3.15 - 3.21.

If an additional assumption is made about the elements of Z , then there is a cancellation law for multiplication of integers even though the multiplicative inverse axiom does not hold in Z . Recall that the proof of the multiplication cancellation law for elements of R depended on the existence of multiplicative inverses for non-zero real numbers. The additional assumption needed about elements of Z is "for all $a, b \in Z$, if $ab = 0$, then $a = 0$ or $b = 0$."

Notice that in this assumption a and b are restricted to Z . It is true that $ab = 0$ implies $a = 0$ or $b = 0$, where $a, b \in R$ (Theorem 3.13). However, the proof of this property relied on the multiplicative inverse property, which does not hold in Z .

Theorem 3.25. For all $a, b, c \in Z$, if $ac = bc$ and $c \neq 0$, then $a = b$.

Proof. Suppose $ac = bc$ and $c \neq 0$. Now $-(bc)$ exists and $[bc + -(bc)] = 0$ by Axiom A.5. So by Theorem 3.1 it follows that $ac + [-(bc)] = bc + [-(bc)]$. Hence, $ac + [-(bc)] = ac + [(-b)c] = 0$ by Theorem 3.15, and it follows that $[a + (-b)]c = 0$ because of Axiom MA. By the additional agreement that was made relative to Z , $[a + (-b)]c = 0$ implies $a + (-b) = 0$ or $c = 0$. By assumption $c \neq 0$. So $a + (-b) = 0$, which implies $[a + (-b)] + b = 0 + b$. By A.3, A.4, and A.5 it then follows that $a = b$.

The Real Number Line

The concept of a "line," even though it is categorized as a geometric concept, makes its appearance so frequently in elementary school mathematics texts to help explain and support number concepts that its being mentioned in this context is paramount. The importance and usefulness of this concept in algebra will become manifest as the remainder of this chapter unfolds.

Every line is considered to be a set of points. It is possible to show that there is a one-to-one correspondence between the set of points on a line and the elements of the set of real numbers. The line is then referred to as the real number line or just simply the number line. In the established correspondence mentioned above, the number corresponding to a unique point is called the coordinate of the point. Figure 17 shows a "model" or a "picture" of the real number line with some of the points appropriately labeled.

That the set of real numbers can be partitioned into three mutually disjoint sets, namely, the set of positive real numbers, $\{0\}$, and the set of negative real numbers, is more evident when the number

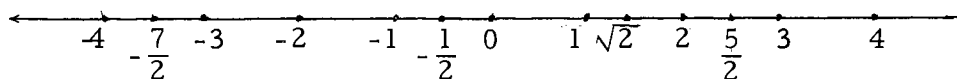


Figure 17.

line is considered. It is by agreement only that an arbitrary point is chosen and assigned the coordinate 0 while the points to the left of this point are assigned negative numbers, and the points to the right are assigned positive numbers. It is also an arbitrary agreement how a unit segment is chosen. For the sake of convenience in speaking and writing, it is customary to refer to the points in terms of their coordinates. For example, to refer to the point with coordinate 3, let it be agreed that "the point 3" will convey the same meaning. "The point $1/2$ " and "the point -2" indicate the points with coordinates $1/2$ and -2, respectively.

Linear Equations and Solution Sets

Conventionally, it is thought that an equation is a statement that two numbers (or quantities) are equal. Does it really make sense to say that two numbers are equal when the only thing a number is equal to is itself? As one considers the sentence $5 + 4 = 7 + 2$ the assertion is being made that the same number results when 4 is added to 5 as when 2 is added to 7.

An equation is a sentence obtained by connecting expressions by the equality symbol.

According to this definition, some examples of equations are:

$$(1) 5 \cdot 4 = 8 + 12$$

$$(3) x + 7 = 9$$

$$(2) 8 + 5 = 36 \div 4$$

$$(4) x + 3 = x - 2$$

An equation can be a statement such as (1) and (2), or an open sentence such as (3) and (4). It is important for the reader to understand that here the word "equation" refers to the form of a sentence and not to its "content."

Recall that an open sentence is neither true nor false without the introduction of additional information. In examples (3) and (4) above, let R be the replacement set and let x be a variable on the set R . There are numerous replacements for the variable x that will transform the sentence $x + 7 = 9$ into a false statement. If x is replaced by 4, the resulting statement is $4 + 7 = 9$, which is certainly false. However, if x is replaced by 2, the statement $2 + 7 = 9$ is true. On the other hand, the equation $x + 3 = x - 2$ is false for all replacements of the variable x .

The set of replacements of a variable which make a mathematical sentence true is called its truth set or solution set. The elements of the solution set of an equation are the solutions or the roots of the equation.

Equations such as $x + 7 = 9$, which are not true for all elements in the replacement set, are called conditional equations. On the other hand, an equation whose solution set is the same as the replacement set for the variable is called an identity. If $x \in R$, then the equation $x + 3 = 3 + x$ is an identity because of the commutative law for addition. Unless otherwise specified, the replacement set for the variable

appearing in an equation will be the set R of real numbers.

For the time being interest will be focused upon linear or first-degree equations in one variable. The equations of the foregoing discussion are linear equations and so are $1/2 x - 9 = 17 1/2 - 7x + 2 = 72$, and $5(x + 2) = 5x + 10$. Generally, linear equations can be written in the form $ax + b = 0$ where $a, b \in R$ and $a \neq 0$. For convenience, the expression appearing to the left of the equals symbol will be called the "left member of the equation," and the expression appearing to the right will be called the "right member of the equation."

Seeking a solution of a linear equation, or any equation, without specifying the replacement set for the variable really does not make sense. If one is asked to find a solution of the equation $x + 2 = -6$ without any additional information, then he would be justified in ignoring this request because it would not be known what principles to apply in seeking a solution. Suppose the replacement set for x is either N or W , then the solution set is \emptyset . On the other hand, if Z , Q , or R is the specified replacement set, then the solution set is -8 . Similarly, $2x = 7$ has no solutions in N , W , or Z , but does have a solution in Q and R .

In fact, any linear equation $ax + b = 0$, where a, b and x are elements of a field F and $a \neq 0$, always has a solution in F . Furthermore, there is one and only one solution for the equation.

Theorem 3.26. For all $a, b, x \in F$ such that $a \neq 0$, $ax + b = 0$ has a unique solution in F .

Proof. First of all, a solution will be exhibited. Since $a, b \in F$ and $a \neq 0$, it is true that $-b$ and a^{-1} exist and $a^{-1}(-b) \in F$. Now,

$$\begin{aligned}
 a [a^{-1}(-b)] + b &= aa^{-1}(-b) + b \\
 &= 1(-b) + b \\
 &= -b + b \\
 &= 0.
 \end{aligned}$$

Therefore, $a^{-1}(-b) = (-b)a^{-1} = -ba^{-1}$ is a solution of $ax + b = 0$.

Suppose y is also a solution of $ax + b = 0$, then $ay + b = 0$. Hence,

$$\begin{aligned}
 (ay + b) + (-b) &= 0 + (-b) \\
 ay + [b + (-b)] &= -b \\
 ay + 0 &= -b \\
 a^{-1}(ay) &= a^{-1}(-b) \\
 (a^{-1}a)y &= a^{-1}(-b) \\
 1 \cdot y &= a^{-1}(-b) \\
 y &= a^{-1}(-b).
 \end{aligned}$$

So if y is a solution, then $y = a^{-1}(-b)$ and it follows that $a^{-1}(-b)$, or $-ba^{-1}$ is the unique solution of $ax + b = 0$.

In the foregoing examples, the solution set of the equation $x + 7 = 9$ is the set $\{2\}$ and the solution set of $x + 3 = x - 2$ is the set \emptyset . Using set builder notation, these solution sets may also be denoted by $\{x \in \mathbb{R} \mid x + 7 = 9\}$, the solution set of $x + 7 = 9$, and $\{x \in \mathbb{R} \mid x + 3 = x - 2\}$, the solution set of $x + 3 = x - 2$. That is, $\{x \in \mathbb{R} \mid x + 7 = 9\} = \{2\}$ and $\{x \in \mathbb{R} \mid x + 3 = x - 2\} = \emptyset$.

The number line may be used to picture the solution set of the equation $x + 7 = 9$. Since the solution set contains the single element

2, it may be indicated on the number line by an enlarged dot at the point 2 as in Figure 18. This picturing of the set $\{2\}$ is called the graph of the solution set of $x + 7 = 9$.

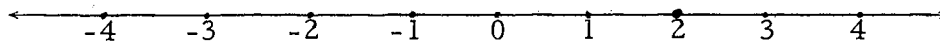


Figure 18.

The graph of the solution set of $x + 3 = x - 2$ will not consist of any points whatsoever since the equation has no solutions. Hence, in Figure 19 there are no enlarged dots representing points on the number line.

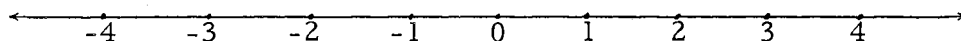


Figure 19.

The associative property of multiplication is sufficient justification to say that the equation $-5(3x) = [(-5) \cdot 3]x$ is an identity. Its graph in Figure 20 is the entire number line and is indicated by picturing the number line somewhat "heavier" than usual.

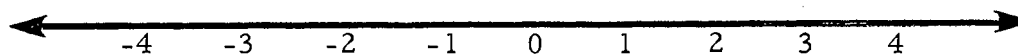


Figure 20.

So far no mention has been made as to how the properties of the real number system can aid in finding the solutions of equations. Consider again the equation $x + 7 = 9$. By renaming 9 as $2 + 7$, the equation $x + 7 = 2 + 7$ is obtained. Since x is a variable on the set \mathbb{R} and 7 and 2 are real numbers, the cancellation law for addition may be used to arrive at the conclusion that $x = 2$. In other words, it has been shown that if $x + 7 = 9$, then $x = 2$. On the other hand, if $x = 2$, then $x + 7 = 9$. Thus, the equation has been solved. To solve an equation is to find all of its roots or to find its solution set. An equation whose solution set is \emptyset has no roots.

Consider the open sentence $x + 3 = x - 2$. Because of the cancellation law for addition it can be concluded that $3 = -2$. But this is a false statement; therefore, the assumption $x + 3 = x - 2$ must be false. This follows from the agreement about conditions that only a false statement can imply a false statement. In other words, $x + 3 = x - 2$ is false for all replacements of the variable x . Thus, the conclusion that the solution set is \emptyset follows at once.

Not all equations have solutions that are evident by inspection or that are as easily obtained as in the examples above. The properties of the real numbers provide the mathematical tools for solving more complicated equations. For example, finding the solution set

of $-6 + x = 5 + 6(x - 1)$ requires a little more labor and the concept of equivalent equations.

Equations which have the same solution set are said to be equivalent equations.

Consider the equations $3x + 5 = 17$, $3x = 12$, and $x = 4$, each of which has the set $\{4\}$ as solution set. That 4 is a solution of each of the equations may be verified by replacing x with 4 in each of the open sentences to obtain the true statements $17 = 17$, $12 = 12$, and $4 = 4$, respectively. So by the above definition these statements are equivalent.

The major objective is to find the solution set of an equation by obtaining an equivalent equation that is "simpler" to solve. Here no attempt will be made to define the terms "simpler" or "simplify." However, an appeal will be made to the reader's intuition to give interpretation to the terms.

One would readily agree that "15" is a simpler name for the number fifteen than " $16 - 5 + 12 - 8$." If $x \in R$, then $5x + 4x = (5 + 4)x$ because of the distributive law. Now, $(5 + 4)x = 9x$ is obtained by replacing $5 + 4$ with 9. Therefore, it can be said that " $9x$ " is a simpler expression than " $5x + 4x$," or that the expression " $5x + 4x$ " has been simplified.

Perhaps the solution set of the equation $8x - 7x = 21$ is not evident to the reader. Since $8x - 7x = x$ by virtue of the distributive property of multiplication over subtraction, the fact that $8 - 7 = 1$, and the multiplicative identity property, $8x - 7x$ can be replaced by x to obtain the equation $x = 21$. The solution set of this equation is obviously $\{21\}$. Therefore, the solution set of $8x - 7x = 21$ is $\{21\}$.

because of the properties of R mentioned above. This example points out that one way to derive an equivalent equation is to simplify one or both members of the equation by using properties of R .

Other methods of transforming an equation into an equivalent equation are the following:

E. 1. For all $a, b, c \in R$, if $a = b$, then $a + c = b + c$.

E. 2. For all $a, b, c \in R$, if $a + c = b + c$, then $a = b$.

E. 3. For all $a, b, c \in R$ such that $c \neq 0$, if $a = b$, then $ac = bc$.

E. 4. For all $a, b, c \in R$ such that $c \neq 0$, if $ac = bc$, then $a = b$.

These will be known as the transformation principles for equations.

Applying any one of the above principles to an equation will always result in an equivalent equation because they are established properties of R . The reader will undoubtedly recognize the principles stated in E. 1, E. 2, and E. 4 as the uniqueness property of addition, the cancellation law for addition, and the cancellation law for multiplication, respectively.

Principle E. 3 is almost a restatement of the uniqueness property of multiplication. The only difference is that c is required to be different from 0. This is necessary because the principle will be used to generate equivalent equations. The uniqueness property guarantees that every root of $x - 7 = 10$ will also be a root of $(x - 7)0 = (10)0$, but the two equations are not equivalent since 17 is the only root of the first one while any real number is a root of the second.

To illustrate how the transformation principles for equations are used, together with other real number properties, the reasoning involved in a general procedure will be demonstrated by seeking all solutions of the equation $4x - 3 + 2x = 5 - 10x$. Again it is understood

that the replacement set is R .

The intention is to seek real numbers that make the equation $4x - 3 + 2x = 5 - 10x$ true. The assumption, there exists a real number replacement for x such that $4x - 3 + 2x = 5 - 10x$ is true, will be made. The objective is to begin with this assumption and use the law of the syllogism together with the law of detachment to arrive at a conclusion about x .

Since $x \in R$, each member of the equation $4x - 3 + 2x = 5 - 10x$ represents a real number. The left member $4x - 3 + 2x$ may be re-written by using the field properties of R . In other words, simplify this left member. The associative, commutative, and distributive laws, together with the definition of subtraction, justify the statement

$$4x - 3 + 2x = 6x + (-3)$$

because

$$\begin{aligned} 4x - 3 + 2x &= 4x + (-3) + 2x \\ &= 4x + 2x + (-3) \\ &= 6x + (-3). \end{aligned}$$

So if

$$4x - 3 + 2x = 5 - 10x$$

is true, then

$$6x + (-3) = 5 - 10x,$$

and

$$6x + (-3) = 5 + (-10x)$$

are also true. Now, from the statement

$$6x + (-3) = 5 + (-10x),$$

it follows that

$$6x + (-3) + 10x = 5 + (-10x) + 10x$$

by Principle E. 1. Thus,

$$6x + 10x + (-3) = 5 + (-10x + 10x)$$

because of Axioms A. 2 and A. 3. That is,

$$16x + (-3) = 5$$

by Axioms MA and A. 5. Therefore, by E. 1, it follows that

$$16x + (-3) + 3 = 5 + 3$$

or

$$16x = 8.$$

Hence, if $4x - 3 + 2x = 5 - 10x$ is true, then $16x = 8$ is likewise true.

Since $1/16$ is the multiplicative inverse of 16 and $1/16 \neq 0$, it follows that

$$1/16 \cdot (16x) = 1/16 \cdot (8)$$

because of Principle E. 3. Therefore, $x = 1/2$.

By the law of the syllogism, it has been shown that if there exists a real number such that

$$4x - 3 + 2x = 5 - 10x$$

then that real number must be $1/2$ because of Theorem 3. 26. That $1/2$ is indeed a solution of the equation can be substantiated by replacing x in the equation $4x - 3 + 2x = 5 - 10x$ by $1/2$. That is, if $x = 1/2$, then $4x - 3 + 2x = 5 - 10x$. Hence, $\{x \in \mathbb{R} \mid 4x - 3 + 2x = 5 - 10x\} = \{1/2\}$.

Order

It was stated on page 55 that in addition to the field axioms for the real number system there is an additional list of axioms that pertains to an order relation defined on \mathbb{R} . The field axioms were properties that governed the binary operations of addition and multiplication in \mathbb{R} , and the order axioms will govern an order relation that is yet to be defined on \mathbb{R} .

Before stating the order axioms, perhaps it is wise to re-emphasize an earlier observation that was made. In the discussion of the real number line it was pointed out that the set \mathbb{R} is naturally partitioned into three pairwise disjoint subsets; namely, the set of positive real numbers, $\{0\}$, and the set of negative real numbers. Let \mathbb{R}^+ denote the set of positive real numbers and \mathbb{R}^- denote the set of negative real numbers.

The additional assumptions that are made about elements of \mathbb{R} are called order axioms and are listed below.

- O. 1. For each $a \in \mathbb{R}$, one and only one of the following statements is true: (i) $a = 0$, (ii) $a \in \mathbb{R}^+$,
 (iii) $-a \in \mathbb{R}^+$.
- O. 2. For all $a, b \in \mathbb{R}^+$, $a + b \in \mathbb{R}^+$
- O. 3. For all $a, b \in \mathbb{R}^+$, $ab \in \mathbb{R}^+$

Axiom O. 1 is called the trichotomy law of the real numbers. That this is a reasonable assumption to make follows from the fact that \mathbb{R}^+ , \mathbb{R}^- , and $\{0\}$ are mutually disjoint subsets of \mathbb{R} . Axioms O. 2 and O. 3 simply state that addition and multiplication are binary operations on \mathbb{R}^+ .

It will be seen that, with this seemingly small number of axioms, many useful properties of real numbers can be deduced. For instance, it is obvious that 3 is positive and its additive inverse -3 is negative, or that -4 is negative and its additive inverse $-(-4)$ is positive. This obvious property is a consequence of Axiom O. 1.

Theorem 3.27. For all $a \in \mathbb{R}^+$, $-a \in \mathbb{R}^-$ and for all $a \in \mathbb{R}^-$, $-a \in \mathbb{R}^+$.

Proof. By Axiom O. 1 either $-a = 0$, $-a \in \mathbb{R}^+$, or $-a \in \mathbb{R}^-$. If $-a = 0$, then $a = 0$ because 0 is its own additive inverse. But $a \neq 0$ since the assumption is that $a \in \mathbb{R}^+$. Therefore $-a \neq 0$. If $-a \in \mathbb{R}^+$, then both a and $-a$ are positive. This contradicts Axiom O. 1, hence $-a \notin \mathbb{R}^+$. Since every real number has to be in either \mathbb{R}^+ , \mathbb{R}^- , or $\{0\}$, the only alternative is to conclude that $-a \in \mathbb{R}^-$. Similarly, it can be proved that $-a \in \mathbb{R}^+$ whenever $a \in \mathbb{R}^-$.

A proof, such as the one above, in which all the different possibilities are considered is sometimes called a proof by exhaustion. Of course, one needs to know that at least one of the different possibilities has to be true before such a procedure is beneficial.

It is important to notice again that if $a \in \mathbb{R}$, then $-a$ denotes the real number called the additive inverse of a . The number represented by a may be positive, negative, or 0. If $a = 3/4$, then $-a = -3/4$. On the other hand, if $a = -6$, then its additive inverse $-a$ is $-(-6) = 6$, which is positive. In other words, if $a \in \mathbb{R}^+$, then $-a \in \mathbb{R}^-$ or if $a \in \mathbb{R}^-$, then $-a \in \mathbb{R}^+$. That is, the symbol $-a$ does not always represent a negative number.

Axiom O. 3 states that the product of two positive real numbers is also a positive real number. That this can also be said about the product of two negative numbers is the statement of the following theorem.

Theorem 3.28. For all $a, b \in \mathbb{R}^-$, $ab \in \mathbb{R}^+$, i. e., the product of two negative real numbers is a positive real number.

Proof.

- | | |
|---|------------------------------|
| (1) $a, b \in \mathbb{R}^-$ | [hypothesis] |
| (2) $-a \in \mathbb{R}^+$ and $-b \in \mathbb{R}^+$ | [Theorem 3.27] |
| (3) $(-a)(-b) \in \mathbb{R}^+$ | [(2) and Axiom O. 3] |
| (4) $(-a)(-b) = ab$ | [Theorem 3.16] |
| (5) $ab \in \mathbb{R}^+$ | [(3), (4), and substitution] |

Many examples can be given illustrating that the product of a positive real number and a negative real number is a negative real number. Specifically, $(-2)(3) = -(2 \cdot 3) = -6$, which is negative since 6 is positive; and $(1/4)(-4) = -(1/4) \cdot 4 = -1$, a negative number. It is natural to ask if this property is always true.

Theorem 3.29. If $a \in \mathbb{R}^+$ and $b \in \mathbb{R}^-$, then $ab \in \mathbb{R}^-$.

Proof.

- | | |
|--|----------------------|
| (1) $a \in \mathbb{R}^+$ and $b \in \mathbb{R}^-$ | [hypothesis] |
| (2) $-b \in \mathbb{R}^+$ | [(1) and Axiom O. 1] |
| (3) $a \in \mathbb{R}^+$ and $-b \in \mathbb{R}^+$ | [(1) and (2)] |
| (4) $a(-b) \in \mathbb{R}^+$ | [Axiom O. 3] |
| (5) $a(-b) = -(ab)$ | [Theorem 3.15] |

- | | |
|---------------------------------|------------------------------|
| (6) $-(ab) \in \mathbb{R}^+$ | [(4), (5), and substitution] |
| (7) $-[-(ab)] \in \mathbb{R}^-$ | [(6) and Theorem 3.27] |
| (8) $-[-(ab)] = ab$ | [Theorem 3.5] |
| (9) $ab \in \mathbb{R}^-$ | [(7), (8), and substitution] |

Surely the reader is beginning to wonder about the sum of two negative real numbers. In physical situations relating to thermometer readings, one's intuition would lead to the conjecture that the sum of two negative numbers is a negative number. But any doubt or misbelief can be dispelled once and for all by proving the following theorem.

Theorem 3.30. For all $a, b \in \mathbb{R}^-$, $a + b \in \mathbb{R}^-$.

Proof.

- | | |
|------------------------------------|---|
| (1) $a, b \in \mathbb{R}^-$ | [hypothesis] |
| (2) $-a, -b \in \mathbb{R}^+$ | [Theorem 3.27] |
| (3) $(-a) + (-b) \in \mathbb{R}^+$ | [Axiom O.2] |
| (4) $(-a) + (-b) = (-1)a + (-1)b$ | [Corollary 1 to Theorem 3.15] |
| (5) $(-1)a + (-1)b = (-1)(a + b)$ | [Idpma] |
| (6) $(-1)(a + b) = -(a + b)$ | [Corollary 1 to Theorem 3.15] |
| (7) $(-a) + (-b) = -(a + b)$ | [(4) - (6) and transitive property of equality] |
| (8) $-(a + b) \in \mathbb{R}^+$ | [(3), (7), and substitution] |
| (9) $-[-(a + b)] \in \mathbb{R}^-$ | [Theorem 3.27] |
| (10) $-[-(a + b)] = a + b$ | [Theorem 3.5] |
| (11) $a + b \in \mathbb{R}^-$ | [(11), (12), and substitution] |

On page 47 an order relation was defined to be a relation that is transitive but not symmetric. So if an order relation on the set R is to

be defined, then it must meet the specifications as set forth in the foregoing definition.

Consider the cross product of R with itself, i. e., $R \times R$. Now any subset of $R \times R$ is a relation on R . Choose a subset S so that the second component of each ordered pair subtracted from the corresponding first component is a positive real number. In set builder notation $S = \{(a, b) \mid (a, b) \in R \times R \text{ and } a - b \in R^+\}$. This set of ordered pairs defines an order relation on the set R and is denoted by the symbol " $>$ ", which is read "is greater than." Therefore, $(a, b) \in S$ if and only if $a > b$; i. e., a is greater than b . Also, $(a, b) \in S$ if and only if $a - b \in R^+$. Thus, the following definition can be given.

For all $a, b \in R$, $a > b$ if and only if $a - b \in R^+$.

For example, $8 > 3$ because $8 - 3 = 5$, a positive number, and $-3 > -6$ because $-3 - (-6) = 3$, which is a positive number. However, it is false that $-5 > -2$ since $-5 - (-2) = -3$.

Although the relation "greater than" has been defined and the symbol " $>$ " employed, many times it is more convenient to use the companion relation denoted by " $<$."

For all $a, b \in R$, $b < a$ if and only if $a > b$. The symbol " $<$ " means is less than and " $b < a$ " is read " b is less than a ." Thus, b is less than a if and only if a is greater than b . Since $a > b$ if and only if $a - b \in R^+$, it can also be stated that $b < a$ if and only if $b - a \in R^-$.

To illustrate this definition, consider the sentence $-2 < 3$. This is equivalent to saying $3 > -2$, which is true because $3 - (-2) = 5$. Therefore, $-2 < 3$ is also true. It could also be pointed out that $-2 < 3$ is true because $-2 - 3 = -5 \in R^-$.

It is somewhat awkward to write sentences such as "it is false that $-5 > 2$ " and "it is false that $5 < -1$." For convenience the symbol " $\not>$ " will be employed to mean "is not greater than," and " $\not<$ " will be used to mean "is not less than." So the sentences above can be rewritten as " $-5 \not> -2$ " and " $5 \not< -1$."

It still remains to be shown that the relation $>$ is indeed an order relation. To reiterate, it must be true that the relation is transitive but not symmetric.

Theorem 3.31. For all $a, b, c \in \mathbb{R}$, if $a > b$ and $b > c$, then $a > c$.

Proof. By hypothesis $a > b$ and $b > c$; hence, by definition $a - b \in \mathbb{R}^+$ and $b - c \in \mathbb{R}^+$. It follows by Axiom O.2 that $(a - b) + (b - c) \in \mathbb{R}^+$. But $(a - b) + (b - c) = (a - c) + (b - b) = a - c$ by the corollary to Theorem 3.20. Therefore, $a - c \in \mathbb{R}^+$ and it can be concluded that $a > c$.

If the relation $>$ were to be symmetric it would have to be true that $b > a$ whenever $a < b$. That this cannot happen is shown by means of a counter example. Now $5 > 3$ because $5 - 3 = 2$ is a positive number. For $3 > 5$ to be true also would mean that $3 - 5 = -2$ is a positive number. But both 2 and -2 cannot be positive. Therefore, it is false that $3 - 5 = -2 \in \mathbb{R}^+$. Consequently, $3 \not> 5$.

It is now conclusive that the relation $>$ is an order relation on \mathbb{R} . Similar arguments could be given to show that the relation $<$ is also an order relation on \mathbb{R} .

Another appropriate symbol to introduce is " \geq ", which is read "is greater than or equal to." The "or" that is used here is the

"inclusive or." The statement $8 \geq 2$ then is interpreted as $8 > 2 \vee 8 = 2$. Since $8 > 2$ is true and $8 = 2$ is false, the statement $8 \geq 2$ is true by agreement on the usage of the inclusive disjunction. In general, if $a, b \in \mathbb{R}$, then " $a \geq b$ " is written to mean " $a > b \vee a = b$." Similarly, " $a \leq b$ " is used to denote that " $a < b \vee a = b$."

For all $a, b \in \mathbb{R}$, one and only one of the following is true by Axiom O.1: $a - b = 0$, $a - b \in \mathbb{R}^+$, or $-(a - b) \in \mathbb{R}^+$ [equivalently, $a - b \in \mathbb{R}^-$]. So one and only one of the following is true: $a = b$, $a > b$, or $a < b$. This is an equivalent way of stating the trichotomy law, which many authors choose in preference to the form that is stated in this writing. Because of this alternate form of the trichotomy law, $a \not> b$ means that $(a = b) \vee (a < b)$ which is written as $a \leq b$. Correspondingly, $a \not< b$ is equivalent to $a \geq b$.

Just as useful properties of the binary operations of addition and multiplication on \mathbb{R} were developed, helpful properties of the relation $>$ can also be deduced. The first theorem to consider is stated below and will be proved without elaborating on field properties that are used.

Theorem 3.32. For all $a, b, c \in \mathbb{R}$, if $a > b$, then $a + c > b + c$.

Proof. By definition $a > b$ iff $a - b \in \mathbb{R}^+$. But $a - b = (a - b) + 0$, and since 0 may be replaced with $c - c$, it follows that $a - b = (a - b) + (c - c)$. Hence, $a - b = (a + c) - (b + c)$ by the corollary to Theorem 3.21. Therefore, $(a + c) - (b + c)$ represents a positive number; so $a + c > b + c$.

If the argument in the above proof is reversed, another impor-

tant consequence results. This result is a theorem stated thus:

Theorem 3.33. For all $a, b, c \in \mathbb{R}$, if $a + c > b + c$, then $a > b$.

Similar theorems for the relation $<$ could also be stated. The arguments would parallel those above, so the proofs will not be presented here.

Preliminary to contemplating some characteristics of order that involve the operation of multiplication, some introductory examples will be enlightening. Consider the statement $-5 > -9$. Choose the positive number 6 and find the products $(-5)6$ and $(-9)6$, which are -30 and -54 . Obviously, $-30 > -54$, so $(-5)6 > (-9)6$. Alternatively, choose the negative number -6 and compute the products $(-5)(-6)$ and $(-9)(-6)$. The reader will agree that $30 < 54$. It is clear that the nature of the number that -5 and -9 were multiplied by has some effect on the order of the resulting two products.

Theorem 3.34. For all $a, b \in \mathbb{R}$ and for all $c \in \mathbb{R}^+$, if $a > b$, then $ac > bc$.

Proof. By definition $a > b$ iff $a - b \in \mathbb{R}^+$. Since $c \in \mathbb{R}^+$, it follows that $(a - b)c \in \mathbb{R}^+$ by Axiom O.3. Now, $(a - b)c = ac - bc$ by Theorem 3.17. Hence, $ac - bc \in \mathbb{R}^+$, and so $ac > bc$.

Theorem 3.35. For all $a, b \in \mathbb{R}$ and for all $c \in \mathbb{R}^-$, if $a > b$, then $ac < bc$.

Proof.

$$(1) \quad a > b$$

[hypothesis]

$$(2) \quad a - b \in \mathbb{R}^+$$

[(1) and definition of $>$]

- | | |
|------------------------------------|--|
| (3) $c \in \mathbb{R}^-$ | [hypothesis] |
| (4) $(a - b)c \in \mathbb{R}^-$ | [Theorem 3.29] |
| (5) $-[(a - b)c] \in \mathbb{R}^+$ | [Theorem 3.27] |
| (6) $-[(a - b)c] = [-(a - b)]c$ | [Theorem 3.15] |
| (7) $-(a - b) = -[a + (-b)]$ | [definition of subtraction] |
| (8) $-[a + (-b)] = -a - (-b)$ | [Theorem 3.18] |
| (9) $-a - (-b) = -a + [-(-b)]$ | [definition of subtraction] |
| (10) $-a + [-(-b)] = -a + b$ | [Theorem 3.5] |
| (11) $-a + b = b - a$ | [Theorem 3.19] |
| (12) $-(a - b) = b - a$ | [(7) - (11) and transitive property of equality] |
| (13) $-[(a - b)c] = (b - a)c$ | [(6), (12), and substitution] |
| (14) $(b - a)c = bc - ac$ | [Theorem 3.17] |
| (15) $-[(a - b)c] = bc - ac$ | [(13), (14), and substitution] |
| (16) $bc - ac \in \mathbb{R}^+$ | [(5), (15), and substitution] |
| (17) $bc > ac$ | [definition of $>$] |
| (18) $ac < bc$ | [definition of $<$] |

Possibly it would be a challenge to the reader to state and prove the analogs of Theorems 3.34 and 3.35 relative to the relation $<$. The proofs would follow the same lines of reasoning that were used in the two previous theorems.

Suppose that $a \in \mathbb{R}^+$, then also $a - 0 \in \mathbb{R}^+$. By definition of $>$ it is true that $a > 0$. Conversely, if $a > 0$, then $a \in \mathbb{R}^+$. Consequently, $a \in \mathbb{R}^+$ if and only if $a > 0$. So $a > 0$ is just an equivalent and more convenient way to say that a is a positive real number. On the other hand, suppose that $a \in \mathbb{R}^-$, then $-a \in \mathbb{R}^+$, and consequently $-a - 0 \in \mathbb{R}^+$. Thus, $-a > 0$. By Theorem 3.35 it follows that $(-a)(-1) < 0 \cdot (-1)$.

Therefore, $a < 0$. So if $a \in \mathbb{R}^-$, then $a < 0$, and conversely. That is, $a \in \mathbb{R}^-$ if and only if $a < 0$.

The sentence $a \geq 0$ means that $a > 0 \vee a = 0$. The set of all such real numbers is called the set of non-negative real numbers and in set builder notation can be denoted by $\{x \in \mathbb{R} \mid x \geq 0\}$. Similarly, the set of non-positive real numbers is the set $\{x \in \mathbb{R} \mid x \leq 0\}$. In particular $-7/8$ is non-positive while $3/4$ is non-negative. The additive identity 0 is both non-negative and non-positive.

The above discussion of order was centered around the field of real numbers, but any field in which the order axioms O.1, O.2, and O.3 are true is called an ordered field. In particular, the field of real numbers is an ordered field and so is the field of rational numbers.

It was shown previously that the system \mathbb{Z} of integers is not a field. Nevertheless, an order relation can be defined on \mathbb{Z} similar to the way an order relation was defined on \mathbb{R} . If \mathbb{Z}^- and \mathbb{Z}^+ represent the sets of negative integers and positive integers, respectively, then for all $a, b \in \mathbb{Z}$, $a > b$ iff $a - b \in \mathbb{Z}^+$. Order axioms for \mathbb{Z} can be formulated similar to the order axioms for \mathbb{R} . In fact, with the order axioms for \mathbb{Z} and the order relation $>$ it can be shown that Theorems 3.27 - 3.35, inclusive, are valid for elements of \mathbb{Z} .

Perchance the reader's curiosity has motivated him to ask if the three order axioms are valid in every field. To satisfy this curiosity examine the field \mathbb{Z}_2 .

If \mathbb{Z}_2 is to be an ordered field, then the order axioms O.1, O.2, and O.3 must hold. In \mathbb{Z}_2 , 0 is the additive identity, 1 is the multiplicative identity, and $0 \neq 1$. Now in order for \mathbb{Z}_2 to be an ordered field it must be true that 1 is positive or the additive inverse of 1 is positive.

	+	0	1
0	0	0	1
1	1	1	0

	·	0	1
0	0	0	0
1	0	0	1

Figure 20.

The element 1 is its own additive inverse; i. e., $-1 = 1$. Suppose 1 is positive, then $-1 = 1$ is negative. In other words, 1 is positive and 1 is negative, which is a contradiction. Hence, 1 is not positive. A similar predicament results if one makes the assumption that 1 is negative. Consequently, $1 \neq 0$, 1 is not positive, and 1 is not negative. Thus, Axiom O. 1 cannot be valid in Z_2 . Z_2 is, therefore, not an ordered field.

Absolute Value

Thus far only binary operations have been considered formally. Recall that a binary operation on the set R is a rule that associates a unique real number with each pair $(a, b) \in R \times R$. Addition and multiplication were seen to be binary operations on R . A binary operation requires that an operation be performed on a pair of elements.

Recall that for each $a \in R$, $-a$ is not necessarily a negative number. The symbol " $-a$ " is often interpreted as "the opposite of a ." For example $-15/2$ is the opposite of $15/2$; -7 is the opposite of 7 ; and 0 is the opposite of 0 . The reader should be willing to agree to this language without anticipating any difficulty in communication.

It seems feasible that there are operations on R that depend

entirely upon a real number and not upon a pair of real numbers. Examine the set of ordered pairs $\{(0, 0), (1, -1), (-1/2, 1/2), (2, -2), (-5, 5), \dots\}$. Careful observation will reveal the relation that each second component has to the corresponding first component. The second component is the additive inverse of the first component in each case. This may be stated in set builder notation as $\{(x, y) \in R \times R \mid y \text{ is the additive inverse of } x\}$ or as $\{(x, y) \in R \times R \mid y = -x\}$. Another way of describing this relation is that the second component of each ordered pair is the opposite of the corresponding first component. Notice that in this relation there is no duplication of first components. In other words, for each $x \in R$ the opposite of x is the unique real number $-x$. Therefore, this relation is a function from R to R and it is referred to as the "operation of oppositing." In this case $D_o = R$ and $R_a = R$.

The number line was utilized earlier to picture solution sets of equations. Perhaps a visual interpretation would aid in considering the operation of oppositing. But in this case "two number lines" will be necessary. To further emphasize that the choice of points to the left of 0 to represent negative numbers and the choice of points to the right of 0 to represent positive numbers was arbitrary, in Figure 21 one of the number lines pictures the negative numbers to the right of 0 and the positive numbers to the left of 0.

It is impossible to picture completely the association of every real number with its opposite. The utilization of two number lines, however, helps one to see how the association is made. In Figure 21 rays are used to establish the correspondence. For instance, the ray extending from the point 2 on line M to the point -2 on line N indicates

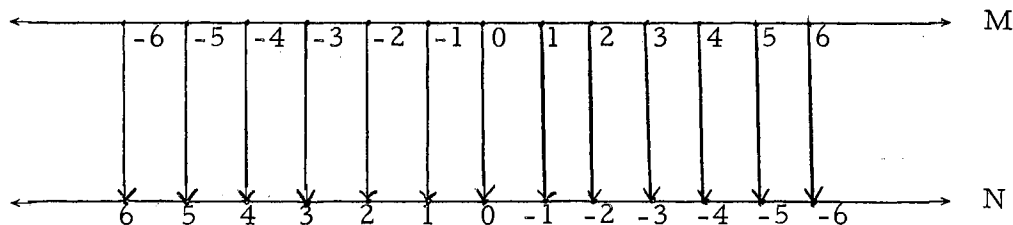


Figure 21.

that -2 is the opposite of 2 . Since it is inappropriate to attempt to illustrate how each real number is associated with its opposite, Figure 21 might be referred to as an "incomplete" representation of the correspondence.

In a like manner, consider the relation defined by the set of ordered pairs $\{(0, 0), (1, 1), (-1, 1), (2/3, 2/3), (-23, 2/3), \dots\}$. In this set of ordered pairs each second component is either 0 or a positive real number, i. e., non-negative. This relation is also a function from \mathbb{R} to \mathbb{R} since the first components are all unique.

One gets the impulse at this point to attempt to express the above relation in set builder notation. But first, it is appropriate to introduce a new term. The second component of each ordered pair is called the absolute value of the corresponding first component. Thus, $3/4$ is the absolute value of $3/4$; $3/4$ is the absolute value of $-3/4$; and 0 is the absolute value of 0 . This function is sometimes called the "operation of absolute valueing." Now the relation can be expressed as $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \text{ is the absolute value of } x\}$. This is still lengthy and cumbersome, so it is desirable to be a little more formal and introduce the symbol " $|$ " to mean "absolute value." Now the relation

is stated thus $\{(x, y) \mid y = |x|\}$. Here $D_o = \mathbb{R}$ and $R_a =$ the set of non-negative real numbers. The following is a formal definition of absolute value.

For each $x \in \mathbb{R}$ if $x \geq 0$, then $|x| = x$; if $x < 0$, then

$$|x| = -x.$$

The absolute value of a non-negative number is that non-negative number, while the absolute value of a negative number is the opposite of that negative number, which is a positive number. For example, $|12| = 12$, $|-16| = -(-16) = 16$, $|5 - 9| = |-4| = -(-4) = 4$, and $|10 - 10| = |0| = 0$.

Two number lines may also be used to represent an incomplete picture of the association of real numbers resulting from absolute valueing. The rays in Figure 22 convey the usual meaning.

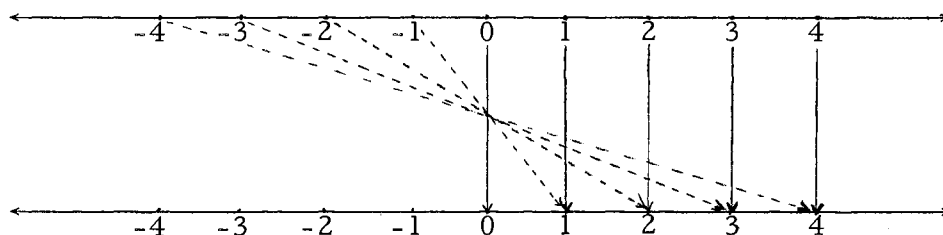


Figure 22.

Now it is possible to consider equations that involve absolute value. The equation $|x| = 3$ may be solved by inspection or by making an appeal to the definition of absolute value. Since the solutions of some equations are not as obvious as in this one, the definition will be

used to illustrate a general procedure. If $x \geq 0$, then $|x| = x$; but since $|x| = 3$, it follows that $x = 3$ by the transitive property of equality. If $x < 0$, then $|x| = -x$. Therefore, $-x = 3$. Thus, $x = -3$. The solution set of $|x| = 3$ is $\{x \in \mathbb{R} \mid |x| = 3\} = \{3, -3\}$. This set is pictured on the real number line in Figure 23.

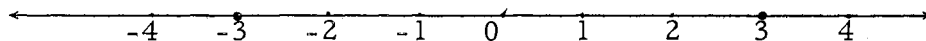


Figure 23.

As a concluding activity with absolute value, the equation $|x - 2| = 5$ will be solved. Again inspection would be a dependable tool, but the definition will be relied on. If $x - 2 \geq 0$, then $|x - 2| = x - 2$. So $x - 2 = 5$ and it follows that $x = 7$. On the other hand, if $x - 2 < 0$, then $|x - 2| = -(x - 2)$. But $-(x - 2) = -x + 2$, so $-x + 2 = 5$. Therefore, $x = -3$. The solution set $\{7, -3\}$ is graphed in Figure 24.

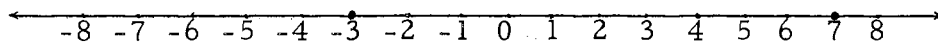


Figure 24.

Inequalities

In the discussion about the ordering of the real numbers, the relation symbols $>$, \geq , $<$, and \leq were introduced. These symbols are also called inequality symbols or inequality signs. The sentence $-3 < 2$ is true while the sentence $9 < 5$ is false; but the sentence $x > 4$ is an open sentence. It is understood that since the discussion of order relations was in the context of the field of real numbers, the concept of inequality will be discussed in the same environment.

An inequality is a sentence obtained by connecting real number expressions by one of the inequality symbols.

An inequality that involves either $>$ or $<$ is called a strict inequality, while one that employs either \geq or \leq is termed a weak inequality. Thus, $7 < 15/2$ and $x - 3 > 4$ are strict inequalities, but $5 \leq 8$ and $x + 2 \geq 0$ are weak inequalities.

The language used in studying inequalities is similar to that used in working with equalities. A linear inequality is an inequality that can be expressed in the form $ax + b < 0$, where $a, b \in \mathbb{R}$, $a \neq 0$, and \mathbb{R} is the replacement set for x . Similar forms using the other inequality symbols are also called linear inequalities. The expression written to the left of the inequality symbol will be called the left member and the expression to the right, the right member. An open sentence that is an inequality — open inequality — is said to be an absolute inequality if its solution set is equal to the replacement set for the variable. A conditional inequality results when the solution set is a proper subset of the replacement set. For example, $x + 4 > x$ is an absolute inequality since it is true for all real number replace-

ments of x . However, $x \leq 1$ is a conditional inequality because any number greater than 1 is not in its solution set. Consequently, its solution set is a proper subset of R .

To solve an inequality, or to find its solution set, means to find the set of replacements that make the inequality true. Similar to what was done in solving equations, finding the solution set of an inequality will involve finding an equivalent inequality that is "simpler" to solve than the given one. The basic properties for transforming an inequality into an equivalent one were proved in Theorems 3.32, 3.33, 3.34, and 3.35. These results are restated as follows:

I. 1. For all $a, b, c \in R$, $a > b$ iff $a + c > b + c$

I. 2. For all $a, b, c \in R$ such that $c > 0$, if $a > b$, then $ac > bc$.

I. 3. For all $a, b, c \in R$ such that $c < 0$, if $a > b$, then $ac < bc$.

These properties are called the transformation principles for inequalities. It is also clear that corresponding statements may be made about $<$, \leq , and \geq .

The reader will recall that to solve an equation such as $x + 2 = 5$ the assumption was made that there exists $x \in R$ such that $x + 2 = 5$ is true. With this assumption an argument was formulated to reach the conclusion $x = 3$, which also must be true. That is, if there exists $x \in R$ such that $x + 2 = 5$, then $x = 3$. This does not say that 3 is a solution of the equation. It must be verified that replacing x with 3 does indeed result in a true statement. Hence, the converse — if $x = 3$, then $x + 2 = 5$ — is also true. Therefore, the solution set of $x + 2 = 5$ is $\{3\}$.

In seeking the solution set of an inequality, a pattern similar to that for solving an equation will guide the reasoning. The assumption

will be made that there exists a real number for which the inequality is true. With this assumption an argument will be built with the hope of finding out more about the number or numbers.

Suppose that there exists $x \in \mathbb{R}$ such that $x + 4 < 10$. By Principle I.1 it is true that $(x + 4) + (-4) < 10 + (-4)$. But this says that $x + 0 < 6$, or $x < 6$. Now life is too short to replace x with every real number less than 6 to find out that each of these belongs to the solution set. So if $x < 6$, then by I.1 it follows that $x + 4 < 6 + 4$, or $x + 4 < 10$. The solution set of the inequality $x + 4 < 10$ is $\{x \in \mathbb{R} \mid x < 6\}$.

The number line is used in Figure 25 to graph the set $\{x \in \mathbb{R} \mid x < 6\}$.

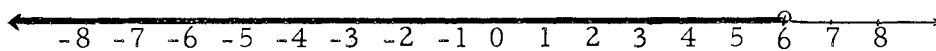


Figure 25.

In Figure 25, the symbol "o" at the point 6 denotes that 6 is not in the solution set. That every point to the left of the point 6 is in the solution set is indicated by making that portion of the picture of the number line somewhat heavier. Of course it is impossible to represent every point in the graph of the solution set, so Figure 25 would be termed an "incomplete" graph.

For the next example illustrating the utilization of the transformation principles, examine the inequality $3x - 10 > x - 2$. If there exists $x \in \mathbb{R}$ such that

$$3x - 10 > x - 2$$

is true, then by I. 1, 10 may be added to each number to arrive at the true sentence

$$(3x - 10) + 10 > (x - 2) + 10,$$

or

$$3x > x + 8.$$

Using I. 1 again it follows that

$$3x + (-x) > (x + 8) + (-x),$$

and hence

$$3x + (-x) > 8 + x + (-x).$$

Therefore,

$$2x > 8.$$

By I. 2 each member may be multiplied by $1/2$ to obtain

$$1/2(2x) > 1/2(8),$$

from which it is concluded that

$$x > 4.$$

Thus, if there exists $x \in \mathbb{R}$ such that $3x - 10 > x - 2$, then the real number must be greater than 4. To see that the converse is true, assume that

$$x > 4.$$

By I. 2 it follows that

$$2 \cdot x > 2 \cdot 4$$

or

$$2x > 8.$$

Therefore, by I. 1

$$2x + (-10) > 8 + (-10).$$

So

$$2x + (-10) > -2.$$

By applying I. 1 again, the sentence

$$2x + (-10) + x > -2 + x$$

is obtained. But this means that

$$2x + x + (-10) > x + (-2).$$

Hence,

$$3x + (-10) > x + (-2),$$

or

$$3x - 10 > x - 2.$$

Therefore, every number greater than 4 is indeed in the solution set of the inequality $3x - 10 > x - 2$. In set builder notation the solution set is $\{x \in \mathbb{R} \mid x > 4\}$, and its graph is shown in Figure 26.

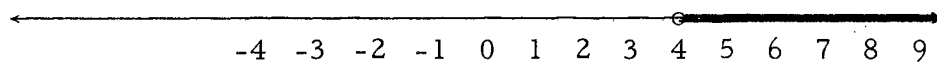


Figure 26.

As a final example of solving a linear inequality, the solution set of $7 - 4x < -13$ will be sought. In this example the writer will not elaborate on the justifying properties used.

Assume there exists $x \in \mathbb{R}$ such that the inequality is true, then

$$7 - 4x \leq -13$$

$$(7 - 4x) + (-7) \leq -13 + (-7)$$

$$-4x \leq -20$$

$$-1/4 (-4x) \geq -1/4 (-20)$$

$$x \geq 5$$

Notice that Principle I.3 was used to transform the inequality in the third line of the proof to the one in the fourth line.

In other words, if there exist $x \in \mathbb{R}$ such that

$$7 - 4x \leq -13$$

is true, then $x > 5$ or $x = 5$. Conversely, suppose that $x > 5$ or $x = 5$,

$$x \geq 5$$

$$(-4)x \leq (-4)5$$

$$-4x \leq -20$$

$$-4x + 7 \leq -20 + 7$$

$$7 + (-4x) \leq -20 + 7$$

$$7 - 4x \leq -13$$

Therefore, the solution set of $7 - 4x \leq -13$ is $\{x \in \mathbb{R} \mid x \geq 5\}$, and its graph is shown in Figure 27.

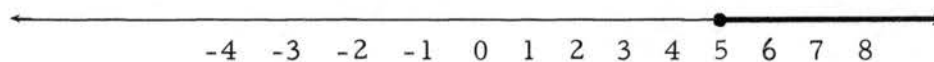


Figure 27.

The enlarged dot at the point 5 in Figure 27 means that 5 is an element of the solution set. The "heavy line" extending to the right of the point 5 indicates that every real number greater than 5 is also in the solution set.

Because of the agreement about the absolute value operation, or function, the image of a real number x is denoted by $|x|$, which represents a non-negative real number. The alternate statement of the trichotomy law would then say that one and only one of the following is true: $|x| = 3$, $|x| < 3$, or $|x| > 3$. In a previous example it was seen that if $|x| = 3$ is true, then the solution set is $\{3, -3\}$.

A careful examination of the graph in Figure 28 will reveal that apparently the points 3 and -3 determine three mutually disjoint sets of points; namely, the set of points to the left of the point -3, the set of points "between" the points -3 and 3 unioned with the set containing the points -3 and 3, and the set of points to the right of the point 3. It seems reasonable, in light of the trichotomy stated in the preceding paragraph, that the solution sets of $|x| \leq 3$ and $|x| > 3$ might possibly be associated with the three mutually disjoint sets of points on the number line.

If $|x| \leq 3$ is true, then the definition of absolute value may be used to learn something about x . Suppose $x > 0$, then $|x| = x$, and by substitution it follows that $x \leq 3$. Alternatively, if $x < 0$, then $|x| = -x$. Therefore, $-x \leq 3$, which implies that $x \geq -3$ by I. 3.

Are there any real number replacements for x that will transform both $x \leq 3$ and $x \geq -3$ into true statements? In other words, do real numbers exist such that the conjunction $(x \leq 3) \wedge (x \geq -3)$ is true? Since $x \geq -3$ iff $-3 \leq x$, $(-3 \leq x) \wedge (x \leq 3)$ is equivalent to the foregoing

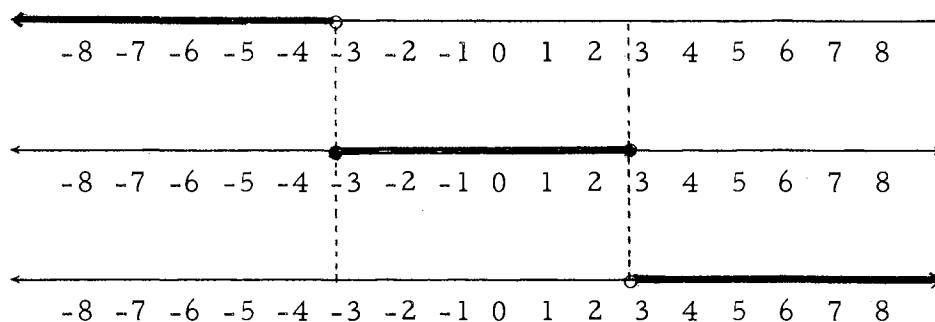


Figure 28.

conjunction. Another way of writing this conjunction is $-3 \leq x \leq 3$. Any real number that makes this compound sentence true will have to be both greater than or equal to -3 and less than or equal to 3 . In particular, the numbers 0 , $2 \frac{1}{2}$, 2.99 , -1 , -1.6 , -3 , 3 , and -2.75 make the sentence true while 3.1 , 4 , -3.5 , -5 make the sentence false. The reader undoubtedly is convinced that the real numbers -3 and 3 together with all real numbers associated with points between the points -3 and 3 are in the solution set of $|x| \leq 3$.

The solution sets of $x \leq 3$, $x \geq -3$, and $|x| \leq 3$ are $\{x \in \mathbb{R} \mid x \leq 3\}$, $\{x \in \mathbb{R} \mid x \geq -3\}$, and $\{x \in \mathbb{R} \mid -3 \leq x \leq 3\}$, respectively. Notice that $\{x \in \mathbb{R} \mid -3 \leq x \leq 3\} = \{x \in \mathbb{R} \mid x \leq 3\} \cap \{x \in \mathbb{R} \mid x \geq -3\}$. Figure 29 gives one a visual interpretation of this fact.

On the other hand, suppose that $|x| > 3$ is true. If $x \geq 0$, then $|x| = x$ and $x > 3$. If $x < 0$, then $|x| = -x$ and $-x > 3$, or $x < -3$. Consider the conjunction $(x > 3) \wedge (x < -3)$. If $x < -3$, then the transitive property of order says that $x < 3$ since $-3 < 3$. Therefore, the conjunction is always false because of the trichotomy law. Another way of stating this is $\{x \in \mathbb{R} \mid x > 3\} \cap \{x \in \mathbb{R} \mid x < -3\} = \emptyset$. So, the

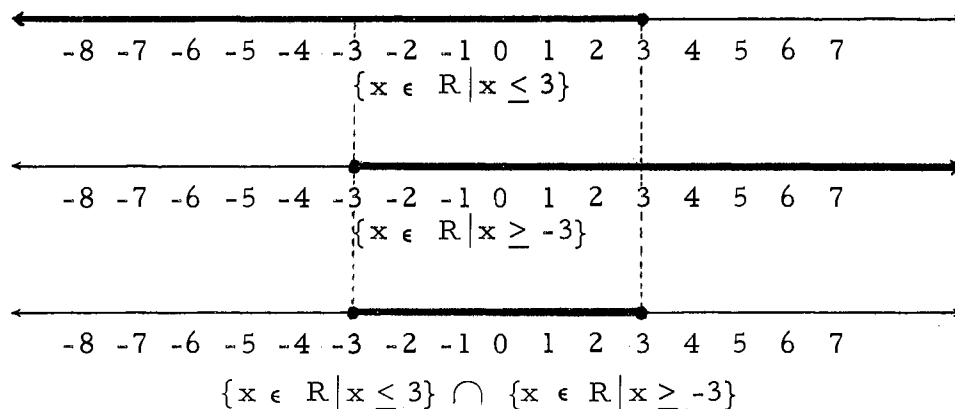


Figure 29.

conjunction $(x > 3) \wedge (x < -3)$ yields no real number solutions.

On the other hand, the disjunction $(x > 3) \vee (x < -3)$ reveals a great deal about the solution set of $|x| > 3$. That is, any real number greater than 3 or any real number less than -3 is in the solution set. Using set builder notation this may be written as $\{x \in \mathbb{R} \mid |x| > 3\} = \{x \in \mathbb{R} \mid (x > 3) \vee (x < -3)\} = \{x \in \mathbb{R} \mid x > 3\} \cup \{x \in \mathbb{R} \mid x < -3\}$. An appeal may be made to the sequence of three graphs in Figure 30 to obtain the desired graph of the solution set of $|x| > 3$.

Arguments closely paralleling the ones employed in finding the solution sets of $|x| = 3$, $|x| < 3$, and $|x| > 3$ may be used in solving $|x - 2| = 5$, $|x - 2| < 5$, and $|x - 2| > 5$. It is already known that the solution set for $|x - 2| = 5$ is $\{x \in \mathbb{R} \mid |x - 2| = 5\} = \{7, -3\}$. The graph of this set together with the graphs of the solution sets of $|x - 2| > 5$ and $|x - 2| < 5$ are shown in Figure 31.

Perchance the experience that the reader has already gained would be all that is necessary to decide immediately what the solution

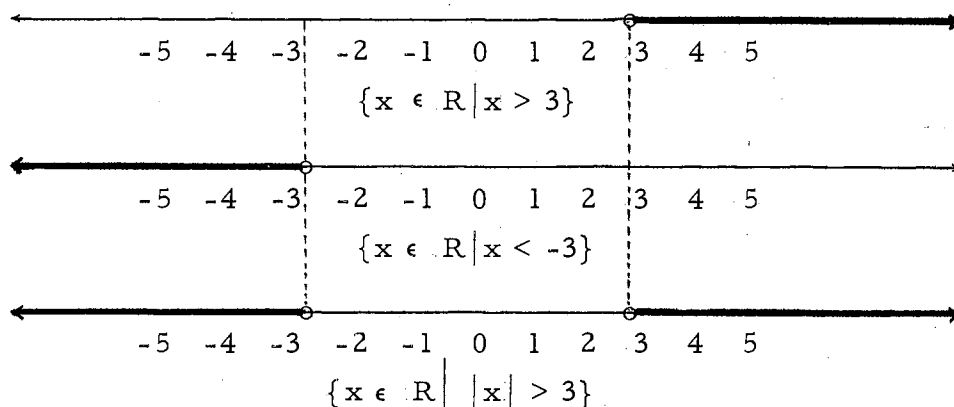


Figure 30.

sets of $|x - 2| < 5$ and $|x - 2| > 5$ are. Certainly one should be able to do this, but it is essential to have the proficiency to justify a conjecture if called on to do so.

So if $x - 2 \geq 0$, then $|x - 2| = x - 2$; and it follows immediately that $x - 2 > 5$ whenever $|x - 2| > 5$. Principle I.1 then guarantees that $x > 7$. Suppose $x - 2 < 0$, then $|x - 2| = -(x - 2) = -x + 2$. Therefore, $|x + 2| > 5$ implies $-x + 2 > 5$, from which it can be concluded that $x < -3$. Again the "inclusive or" is appropriate in expressing the solution set for $|x - 2| > 5$ as $\{x \in \mathbb{R} \mid (x > 7) \vee (x < -3)\}$, which is just the set union of the disjoint sets $\{x \in \mathbb{R} \mid x > 7\}$ and $\{x \in \mathbb{R} \mid x < -3\}$.

Finally, consider the remaining alternative, $|x - 2| < 5$. Now $x - 2 \geq 0$ and $|x - 2| < 5$ imply that $x < 7$ while $x - 2 < 0$ and $|x - 2| < 5$ imply that $x > -3$. Therefore, $|x - 2| < 5$ is equivalent to the conjunction $-3 < x < 7$. The solution set for $|x - 2| < 5$ is $\{x \in \mathbb{R} \mid -3 < x < 7\} = \{x \in \mathbb{R} \mid x > -3\} \cap \{x \in \mathbb{R} \mid x < 7\}$.

The sets $\{x \in \mathbb{R} \mid |x - 2| = 5\}$, $\{x \in \mathbb{R} \mid |x - 2| > 5\}$, and $\{x \in \mathbb{R} \mid |x - 2| < 5\}$ are mutually disjoint. That is, there is no

real number that is contained in any two of the sets. Figure 31 is a pictorial representation of this fact.

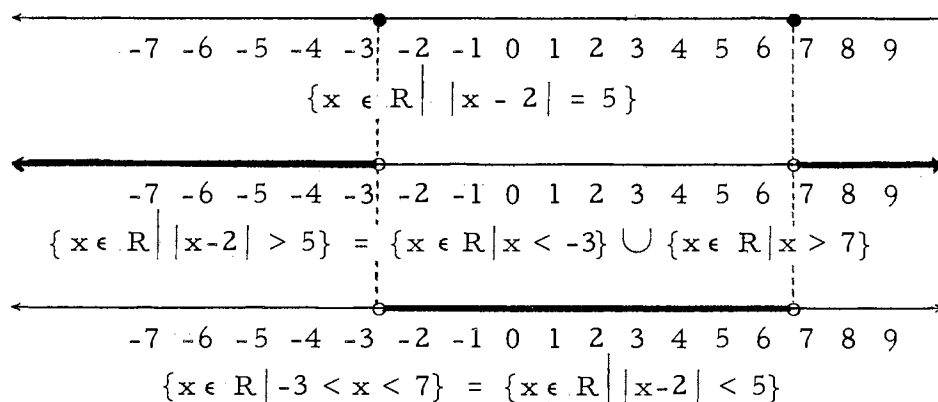


Figure 31.

Introduction to Quadratic Equations

The underlying theory of quadratic equations is a rather involved subject. It is the intent in this section to provide the elementary teacher with an intuitive introduction to the "idea" of quadratic equations since this concept does appear in some of the elementary arithmetic texts.

Even an intuitive discussion of quadratic equations involves a basic understanding of exponents. No elaboration will be made in regard to exponents since it is assumed that the reader has command of this topic through previous experiences in the development of the number system. However, if it is necessary, the reader may consult Fehr [11] or Drooyan [9] for excellent discussions of properties of exponents.

A sizeable portion of Chapter III has been devoted to the consideration of linear equations and inequalities in one variable, i. e., expressions of the form $ax + b = 0$, $ax + b < 0$, and $ax + b > 0$. These were called linear expressions because the exponent associated with the variable is one. In other words, the first power of a variable is all that appears. Each of the above is identified with the word "linear" because of the nature of the expressions in the left members of the equation or inequality.

An expression of the form $ax + b$ is said to be a linear or first-degree polynomial over R whenever it is assumed that $a, b \in R$, $a \neq 0$, and x is a variable on R . The real numbers a and b are called coefficients of the polynomial. Specifically, a is known as the coefficient of the variable x .

Examples of first degree polynomials over R are $1/2 x - 3$, $-4y + 7$, and $(\sqrt{2})z$. In the first of these x is the variable while $1/2$ and -3 are the coefficients of the polynomial — $1/2$ being the coefficient of x . In the second example y is the variable, -4 is the coefficient of y , and 7 is also a coefficient. Notice in the third instance that z is the variable while $\sqrt{2}$ and 0 are the coefficients.

Let $ax + b$ and $cx + d$ be any two linear polynomials over R . For any real number replacement for x , each of these polynomials will represent a real number. Since multiplication is a binary operation on R , it then follows that $(ax + b)(cx + d)$ also represents a real number. This product of two linear polynomials will be examined in some detail.

$$\begin{aligned}
(ax + b)(cx + d) &= (ax + b)(cx) + (ax + b)d && [\text{ldpma}] \\
&= (ax)cx + b(cx) + (ax)d + bd && [\text{rdpma}] \\
&= (ac)x \cdot x + bc(x) + (ad)x + bc && [\text{Axioms M. 2 and M. 3}] \\
&= (ac) x \cdot x + (bc + ad)x + bd && [\text{rdpma}] \\
&= (ac)x \cdot x + (ad + bc)x + bd && [\text{Axiom A. 2}] \\
&= acx^2 + (ad + bc)x + bd && [x \cdot x = x^2]
\end{aligned}$$

Therefore,

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd \quad [\text{transitive property of equality}]$$

It is seen that the product of two linear polynomials over R will not be a linear polynomial over R . The resulting expression will involve the variable x to the second power. It would seem that the product in this instance might also be called a polynomial.

An expression of the form $px^2 + qx + r$ is said to be a quadratic or second-degree polynomial over R whenever it is assumed that $p, q, r \in R$, $p \neq 0$, and x is a variable on R . The real numbers p, q , and r are the coefficients of the polynomial, where p and q are the coefficients of x^2 and x , respectively.

Recall that one property of real numbers is that $ac \neq 0$ whenever $a \neq 0 \wedge c \neq 0$. Thus, the product of $ax + b$ and $cx + d$ is a quadratic polynomial $px^2 + qx + r$ where $p = ac \neq 0$, $q = ad + bc$, and $r = bd$. The linear polynomials $ax + b$ and $cx + d$ are said to be factors of the quadratic polynomial $px^2 + qx + r$. In particular, the product of $3x - 1$ and $2x + 5/2$ is $(3 \cdot 2)x^2 + [3(5/2) + (-1)2]x + (-1)(5/2) = 6x^2 + 11/2x - 5/2$. Thus, 6 is the coefficient of x^2 ; $11/2$ is the coefficient of x ; and $-5/2$ is also a coefficient. Observe that $3x - 1$ and $2x + 5/2$ are factors of

$$6x^2 - 11/2 x - 5/2.$$

At this point it is necessary to emphasize that the "theory of polynomials" is too involved to be an integral part of this discourse. Certainly the underlying theory of the study of polynomials in general would be a valuable asset and would contribute greatly to one's mathematical knowledge, but the writer must be constantly aware of the background of the reading audience and the intended purpose of this paper. Therefore, some of the ideas associated with polynomials will be introduced by examples.

In the foregoing definitions of linear and quadratic polynomials, specifying the set R from which the coefficients are selected does not discount the possibility that the coefficients may be chosen from other sets. However, it will be understood that the coefficients of polynomials over R will be chosen from Z , Q , or R . Although it would not be pertinent here, a thorough study of the subject would include forms such as $ax^3 + bx^2 + cx + d$, $ax^4 + bx^3 + cx^2 + dx + e$, etc., where the coefficients could be chosen from any mathematical system with a structure comparable to the system of integers. Let it suffice for the present to say that such a system is called a ring and will be defined and discussed in Chapter IV.

For example $-3x + 4$ and $x^2 + 2$ are polynomials whose coefficients are integers while $2x - 3/4$ and $x^2 - 1/4$ are polynomials whose coefficients are rational numbers. The polynomials $3x + \sqrt{2}$ and $5x^2 + \pi$ have real number coefficients. Similarly, $1 \cdot x^2 + 1 \cdot x + 1$ could be thought of as a quadratic polynomial over Z_2 .

Given two linear polynomials over R , the product will always be a quadratic polynomial over R because of previously developed proper-

ties of the field R . However, it is not always possible to find two linear factors over R of a quadratic polynomial whose coefficients are real numbers. The quadratic $x^2 + 1$ has the real number coefficients 1 and 1. The fact that this polynomial cannot be decomposed into a product of two linear polynomials whose coefficients are in R will be the basis for further developments in Chapter IV.

Although the elementary school teacher may not have been aware of it at the time, some of his experiences in arithmetic have been directly associated with the concept of polynomials. In developing an algorithm for multiplication of two whole numbers, say 24 and 15, the expanded notations $2 \cdot 10 + 4$ and $1 \cdot 10 + 5$ were utilized. Now the product of $2x + 4$ and $x + 5$ is $2x^2 + 14x + 20$. Hence, the product of $2 \cdot 10 + 4$ and $1 \cdot 10 + 5$ is $2 \cdot 10^2 + 14 \cdot 10 + 20$, which is basically the product of two linear polynomials. One would then rename to obtain $3 \cdot 10^2 + 6 \cdot 10 + 0$, the expanded notation for the product of 24 and 15.

Together with considering the problem of factoring either first or second degree polynomials, it will be instructive and revealing to examine some other products that have linear polynomials as factors. Actually, most of the following products could be generated from the sentence $(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$, but selected ones will be discussed separately.

It is undoubtedly clear that the product of a linear polynomial and a non-zero real number will be a linear polynomial. If $t \neq 0$, then $t(ax + b) = tax + tb$ is a consequence of the distributive property. The real number t is called a constant factor of $tax + tb$ and $ax + b$ is a linear factor. Certainly if $t = 1$, then $1 \cdot (ax + b) = ax + b$.

To approach the problem of factoring a polynomial intelligently, one must know from which subset of \mathbb{R} the coefficients are selected. For instance, consider the polynomial $-6x + 15$ where -6 and 15 are thought of as elements of the system of integers. The polynomial can then be factored as $-3(2x - 5)$ or $3(-2x + 5)$. If -6 and 15 are considered to be elements of the field of rationals, then $3/2(-4x + 10)$ and $-6(x + 5/2)$ would be valid factorizations. If -6 and 15 are considered to be elements of the field of reals, then $3/\sqrt{2}(-2\sqrt{2}x + 5\sqrt{2})$ and $\sqrt{6}(-\sqrt{6}x + 15/\sqrt{6})$ would be valid. The foregoing factorizations do not contribute essentially to the simplification of the polynomial $-6x + 15$. In other words, for linear polynomials with rational or real coefficients, there is no unique way of writing the polynomial as a product of a linear polynomial and a constant. The polynomial $3x + 5/4$ is not factorable over \mathbb{Z} , but it is factorable over the rationals and the reals.

Next consider the product of the two linear polynomials $ax + b$ and $ax - b$. The reader should be able to supply the reasons for the following abbreviated procedure.

$$\begin{aligned}
 (ax + b)(ax - b) &= (ax + b) [ax + (-b)] \\
 &= (ax + b)(ax) + (ax + b)(-b) \\
 &= (ax)(ax) + b(ax) + (ax)(-b) + b(-b) \\
 &= a^2x^2 + (ab)x + -(ab)x - b^2 \\
 &= a^2x^2 - b^2
 \end{aligned}$$

Therefore,

$$(ax + b)(ax - b) = a^2x^2 - b^2.$$

Since $(ax + b)(ax - b) = ax^2 - b^2$, each of the linear polynomials is a factor of the quadratic polynomial. Specifically, $x + 3$ and $x - 3$ are factors of $x^2 - 9$ since it is true that $(x + 3)(x - 3) = x^2 - 9$. In this case the coefficients of the polynomial are integers, and the coefficients in each factor are also integers, so the quadratic polynomial is factorable over the set of integers. The polynomial $x^2 - 1/4$ is not factorable over Z , but it can be factored over Q or R because $x^2 - 1/4 = (x + 1/2)(x - 1/2)$. The polynomial $x^2 - 2$ may be considered as a polynomial over Z , over Q , or over R . Regarded as a polynomial over R it may be factored as $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$, but it is not factorable over Q nor over Z .

The reader should have no difficulty verifying that:

$$(ax + b)^2 = (ax + b)(ax + b) = a^2x^2 + 2abx + b^2$$

and

$$(ax - b)^2 = (ax - b)(ax - b) = a^2x^2 - 2ab + b^2.$$

Examples of these are

$$(3x + 5)^2 = (3x + 5)(3x + 5) = 9x^2 + 30x + 25$$

and

$$(2x - 7)^2 = (2x - 7)(2x - 7) = 4x^2 - 28x + 49.$$

Consider a special case of a product of two linear polynomials; namely, $cx(ax + b) = (ax + b)cx = acx^2 + bcx$. Notice again the dependence upon the properties of real numbers, especially the distributive property.

The major objective in this context for centering attention on quadratic polynomials is to see how equations other than linear equa-

tions can be solved. Many such equations can be solved by applying what is already known about solving linear equations.

Initially one becomes acquainted with the concept of "square root" in the context of non-negative integers. The set of all divisors or factors of a non-negative integer n is examined to see if any factor can be paired with itself to obtain the number n . In terms of the binary operation of multiplication, this is the same as asking if there is an ordered pair (a, a) , $a \geq 0$, such that n is associated with that pair. That is, $a \cdot a = a^2 = n$. If there exists such an integer a , then it is called the square root of n . This idea of square root is then extended to the non-negative rational numbers and then to the non-negative real numbers according to the following definition.

For all $a \in \mathbb{R}$ such that $a \geq 0$, there exists $b \in \mathbb{R}$ such that $b \geq 0$ and $b^2 = a$. The number b is called the square root of a and is denoted by \sqrt{a} . Thus, $b = \sqrt{a}$.

The square root of the integer 49 is 7, and the square root of $9/16$ is $3/4$ since $7^2 = 49$ and $(3/4)^2 = 9/16$. Notice also that $(-7)^2 = 49$, but -7 is the additive inverse of 7. This additive inverse could also be rewritten as $-\sqrt{49}$, but the square root of 49 is $\sqrt{49} = 7$. Similarly, $-\sqrt{9/16} = -3/4$ because $(-3/4)^2 = 9/16$. However, as the reader well knows, the square root of 2 is an irrational number symbolized by $\sqrt{2}$ where $(\sqrt{2})^2 = 2$. Many times in actual computation it is necessary to find a rational approximation for irrational numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt{24}$, etc.

To introduce a very interesting theorem that is beneficial in approximating square roots, consider the following situation. Suppose the dimensions of a rectangle are known, then the area may be

computed. Let a and b represent the measures of the sides of the rectangle and let c represent the area measure, then $c = a \cdot b$. The problem is to find the measure of a side of the square with the same area $c = a \cdot b$. If x represents the length of a side of the square, then the area is $x \cdot x = x^2$; i. e., $x^2 = c = a \cdot b$. It is required to solve the equation $x^2 = c$, or equivalently $x^2 - c = 0$. Notice that the left member of this equation is a quadratic polynomial.

A quadratic equation is an equation that can be expressed in the form $px^2 + qx + r = 0$ where $px^2 + qx + r$ is a quadratic polynomial over R .

In the problem submitted above, the number x is just the square root of c . In other words, $x = \sqrt{c}$. If the dimensions of the rectangle were 4 and 9, then $c = 36$ and $\sqrt{c} = 6$: and so $x = 6$. Alternatively, the dimensions might be 4 and 8, and this would say that $x = \sqrt{32}$, which is an irrational number.

Theorem 3.36. For all $a, b, c \in \mathbb{R}^+$ if $c = ab$ and $a \leq b$, then $a \leq \sqrt{c} \leq b$.

Proof. By the trichotomy law, either $a \leq \sqrt{c}$ or $\sqrt{c} < a$. Suppose $\sqrt{c} < a$, then since $a \leq b$ it follows that $\sqrt{c} < b$. This implies that $a\sqrt{c} < ab = c$. Since $c > 0$, the definition of square root guarantees that $\sqrt{c} > 0$. Hence, $(\sqrt{c})^{-1}$ exists and $(\sqrt{c})^{-1} > 0$. Therefore, it follows that $a\sqrt{c}(\sqrt{c})^{-1} < c(\sqrt{c})^{-1}$, but this is equivalent to $a\sqrt{c}(\sqrt{c})^{-1} < \sqrt{c}\sqrt{c}(\sqrt{c})^{-1}$ since $c = (\sqrt{c})(\sqrt{c})$. By the multiplicative inverse axiom the conclusion that $a < \sqrt{c}$ is reached. Now both the assumption that $\sqrt{c} < a$ and the conclusion that $a < \sqrt{c}$ cannot be true. Therefore, the assumption must be false, and it follows that

the alternative, $a \leq \sqrt{c}$, is true. Similarly, one could conclude that $\sqrt{c} \leq b$, so the conjunction $a \leq \sqrt{c} \leq b$ is true.

Perchance this theorem has stirred the reader's interest to the point that he would like to see how it is applied in approximating square roots. Goff and Berg [13] offer some excellent examples in their programmed text.

Finally, consider the problem of seeking solutions for a quadratic equation over R . A special instance of a more general result found in Barnes [2], states that a quadratic equation over R can have at most two roots in R . This does not offer assurance that there will be any roots at all in R ; but if there are any roots, there cannot be more than two. Therefore, in seeking solutions for quadratic equations over R , one will know that there will either be no solutions, one solution, or two distinct solutions.

To solve a quadratic equation such as $x^2 + 3x = 0$, one can factor the polynomial $x^2 + 3x$ as $(x + 3)x$ and rewrite the equation as $(x + 3)x = 0$. Since $x \in R$ and $x + 3 \in R$, it follows by Theorem 3.13 that either $x + 3 = 0$ or $x = 0$. Each of these linear equations has a unique solution in R because of Theorem 3.26. Therefore, $x = -3$ or $x = 0$. Thus, if there is a real number replacement for x such that $x^2 + 3x = 0$, then $x = -3$ or $x = 0$. Conversely, if $x = -3$ or $x = 0$, it is seen that $x^2 + 3x$ is indeed 0. The result stated in the preceding paragraph then guarantees that the solution set of the quadratic equation $x^2 + 3x = 0$ is $\{-3, 0\}$. That is, $\{x \in R \mid x^2 + 3x = 0\} = \{-3, 0\}$.

Similarly, solutions for the quadratic equation $x^2 - 6x + 8 = 0$ can be sought. Linear factors of $x^2 - 6x + 8$ are $(x - 4)$ and $(x - 2)$

because $(x - 4)(x - 2) = x^2 - 6x + 8$. If there exists a real number replacement for x such that $x^2 - 6x + 8 = 0$ is true, then $(x - 4)(x - 2) = 0$ is also true. Now, $(x - 4)(x - 2) = 0$ implies that $x - 4 = 0$ or $x - 2 = 0$. The unique solutions of these two linear equations are 4 and 2, respectively. Substitution in $x^2 - 6x + 8 = 0$ reveals that both 4 and 2 are solutions. Therefore, since $x^2 - 6x + 8 = 0$ has at most two real number solutions, it follows that 4 and 2 are the only solutions of the quadratic equation.

Analogously, one could seek solutions for the equation $3x^2 + 11x - 4 = 0$ by first factoring $3x^2 + 11x - 4$ as $(3x - 1)(x + 4)$. The search for solutions is then reduced to the problem of finding solutions of the linear equations $3x - 1 = 0$ and $x + 4 = 0$. Thus, it follows that $x = 1/3$ or $x = -4$, and the solution set of $3x^2 + 11x - 4 = 0$ is $\{1/3, -4\}$.

The three preceding examples involved quadratic equations that had two distinct roots. The equation $x^2 + 1 = 0$ has coefficients in \mathbb{R} but no solutions in \mathbb{R} . This equation will be discussed in detail in Chapter IV. For an example of a quadratic equation over \mathbb{R} that has only one solution in \mathbb{R} , consider $x^2 - 6x + 9 = 0$. The reader should be able to see that this is equivalent to $(x - 3)(x - 3) = 0$. It is then clear that $x = 3$ or $x = 3$. That is, if there exists $x \in \mathbb{R}$ such that $x^2 - 6x + 9 = 0$, then $x = 3$. Conversely, if $x = 3$, then $x^2 - 6x + 9 = 0$. Hence, the solution set of $x^2 - 6x + 9 = 0$ is $\{3\}$.

It is not very laborious to decide that the solutions of $x^2 - 4 = 0$ are 2 and -2 by using the factorization method. As an alternative, examine the equivalent form $x^2 = 4$. Obviously, the solution can be found by observing that 2 is the square root of 4 and -2 is the additive inverse of 2. This raises the question as to the possibility of solving

such an equation by "taking the square root of each member." Remember that square root is defined for non-negative real numbers so it is possible to talk about the square root of 4. Now how about x^2 ? Is it permissible to write $\sqrt{x^2} = x$? Suppose $x = -2$. Is it true that $\sqrt{(-2)^2} = -2$? Obviously not, since $\sqrt{(-2)^2} = \sqrt{4} = 2$. To alleviate the situation one can involve the concept of absolute value and require that $\sqrt{x^2} = |x|$. It is then true that $|x| = 2$ is equivalent to $x^2 = 4$ because its solution set is also $\{2, -2\}$.

An equation such as $(x - 5)^2 = 16$ could be solved by writing the equivalent form $x^2 - 10x + 9 = 0$ and then using the factorization method. However, in the original form it is clear that to solve the equation is to find a real number x such that the square of $x - 5$ is 16. By the agreement in the preceding paragraph it then follows that

$\sqrt{(x - 5)^2} = |x - 5|$ and $|x - 5| = 4$. Therefore, $x - 5 = 4$ or $-(x - 5) = 4$. Hence, $x = 9$ or $x = 1$. These are the only solutions of $|x - 5| = 4$ and also of $(x - 5)^2 = 16$, so the two equations are equivalent.

The discussion here by no means exhausts the methods and techniques of solving quadratic equations. The stated objective was to introduce the reader to the concept of quadratic equations so that he would have confidence to cope with situations arising when the concept is encountered in elementary texts. The reader that is interested in pursuing the topic further could benefit tremendously from other sources [9].

Linear Equations and Inequalities in Two Variables

The reader has already seen that linear equations and inequalities in one variable can be solved by using properties of the field of real numbers. An extension of the ideas of linear equations and inequalities in one variable can be made to include linear equations and inequalities in two variables.

A linear equation in two variables is an equation that can be expressed in the form $ax + by + c = 0$ where $a, b, c \in R$, $a \neq 0 \vee b \neq 0$, and R is the replacement set for the variables x and y .

A linearⁱⁿ inequality in two variables is an inequality that can be expressed in the form $ax + by + c < 0$, or similar forms obtained by using $>$, \geq , and \leq , where $a, b, c \in R$, $a \neq 0 \vee b \neq 0$, and R is the replacement set for the variables x and y .

Open sentences such as $x + y = 5$ and $x + y < 5$ are called a linear equation in two variables and a linear inequality in two variables, respectively. In each of these open sentences if x is replaced by 2, then the open sentences, $2 + y = 5$ and $2 + y < 5$, in one variable are obtained. Thus, it is seen that a pair of replacements from R is needed in order for an open sentence in two variables to be transformed into a statement.

Actually, in order to solve the equation $x + y = 5$, or the inequality $x + y < 5$, the problem is to find ordered pairs of real numbers so that if x is replaced by the first component and y is replaced by the second component, the resulting statement is true.

For $x + y = 5$, $(2, 3)$ is such a pair. If x is replaced by 2 and y is replaced by 3, then $2 + 3 = 5$ is true. Other pairs that may be used are $(4, 1)$, $(-1, 6)$, $(0, 5)$, $(1/2, 4 1/2)$, and $(6 3/4, -1 3/4)$, just to mention a few. Some ordered pairs whose components would transform $x + y < 5$ into a true statement are $(1, 1)$, $(2, 2)$, $(-1/2, 5)$, $(-3, -1)$, and $(0, 4)$. Of course it is impossible in either case to use the roster notation to list all such ordered pairs.

Because of the agreement above, any pair of real numbers (x, y) that makes the equation $x + y = 5$ true will be called a solution of the equation. Likewise, any pair (x, y) that transforms $x + y < 5$ into a true statement will be called a solution of the inequality $x + y < 5$. The following can now be formulated.

The solution set of the equation $ax + by + c = 0$ is

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid ax + by + c = 0 \text{ is true}\}.$$

The solution set of the inequality $ax + by + c < 0$

$$\text{is } \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid ax + by + c < 0 \text{ is true}\}.$$

In the definitions above the phrase "is true" was included in the set selector in each case for emphasis. It will not always be necessary to do this for specific instances, for it will be understood that only those ordered pairs that create true statements will be included in the respective solution set. For instance, the solution set of $x + y = 5$ is $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y = 5\}$ and that for $x + y < 5$ is $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y < 5\}$.

Now the set $\mathbb{R} \times \mathbb{R} = \{(a, b) \mid a \in \mathbb{R} \text{ and } b \in \mathbb{R}\}$ is the Cartesian product of \mathbb{R} with itself. The solution sets of $x + y = 5$ and $x + y < 5$ are subsets of $\mathbb{R} \times \mathbb{R}$, and hence these sets are relations on the set \mathbb{R} .

Therefore, the equation $x + y = 5$ and the inequality $x + y < 5$ are sentences that define relations on the set of real numbers.

Just as numbers and sets of numbers were graphed on a number line, it is also possible to graph ordered pairs of numbers and sets of ordered pairs of numbers. But in this case "two number lines" will be necessary, and it will be understood that they are mutually perpendicular in such a way that the point 0 of one line corresponds to the point 0 of the other. The two lines are then called coordinate axes. The horizontal axis is known as the x-axis, and the vertical axis is called the y-axis (Figure 32).

One learns in geometry that two intersecting straight lines determine a "plane." The coordinate axes will then be thought of as being in the plane determined by them. The coordinate axes partition the set of all points in the plane into four mutually disjoint subsets of points. These four regions of the plane are called quadrants as shown in Figure 32.

Since there is a one-to-one correspondence between points on a line and the set R , and a plane is determined by two mutually perpendicular number lines, it is reasonable to expect that there is a one-to-one correspondence between points in the plane and the set $R \times R$. This is indeed the case, and the resulting system is known as a rectangular coordinate system or Cartesian coordinate system.

The components of an ordered pair (x, y) associated with a point p in the plane are called the rectangular coordinates of the point p . The first component is referred to as the x-coordinate or abscissa, while the second component is called the y-coordinate or ordinate. The point of intersection of the two axes is called the origin of the coordinate system.

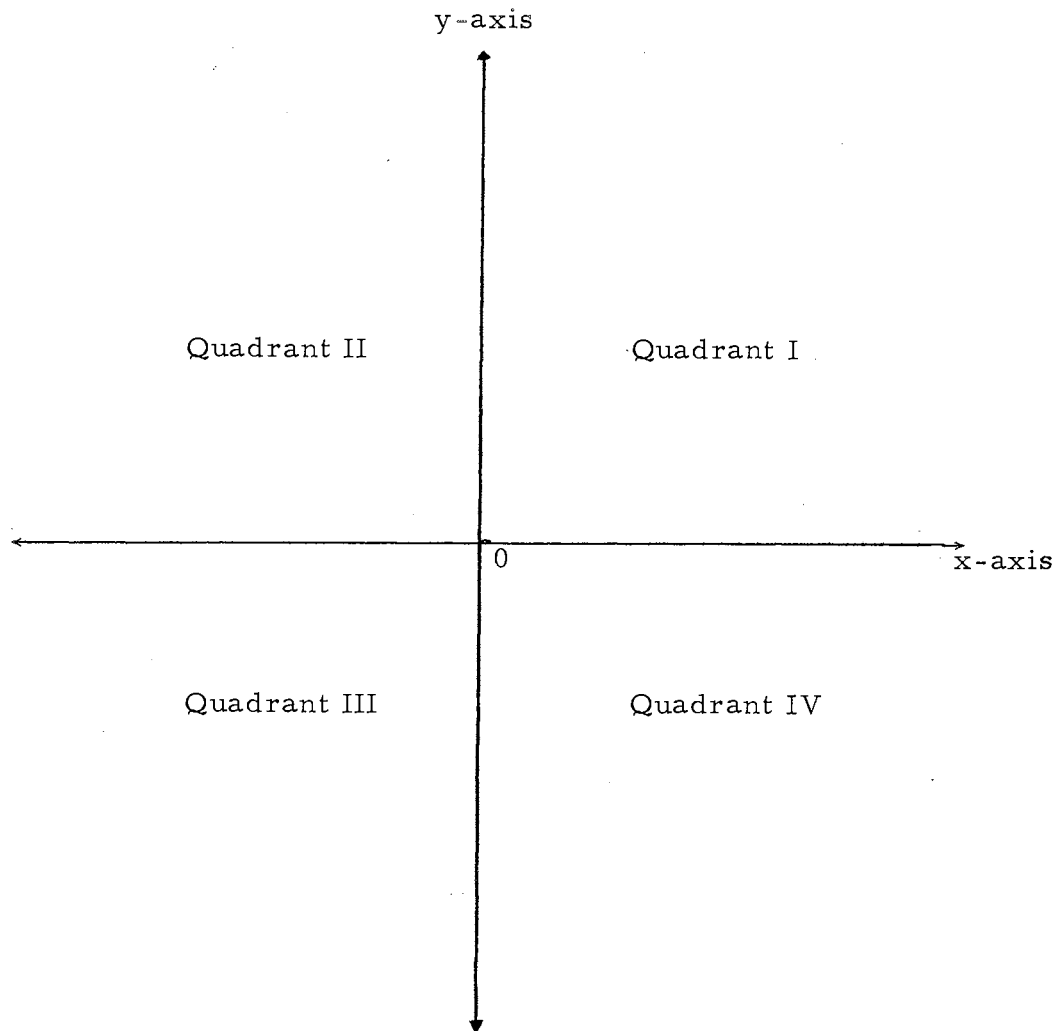


Figure 32.

Even though points on each of the axes are also points in the plane, it is not customary to identify them by an ordered pair when constructing a rectangular coordinate system. In other words, if $b \in \mathbb{R}$, then b corresponds to a point on the real line. On the x-axis of the coordinate system the point will be identified by the real number b , but it will be understood that in the plane the pair associated with this point is $(b, 0)$. Similarly, when a point on the y-axis is identified by a real number c ,

it is agreed that in the reference frame of the coordinate system this means the point corresponds to the pair $(0, c)$. For example, the points $(-3, 0)$ and $(0, 2)$ are identified on the x and y -axes as -3 and 2 , respectively. Since the origin is on both axes, the pair corresponding to it is $(0, 0)$.

To represent a number pair, say $(3, 4)$, as a point in the plane, find the point which is on the vertical line constructed through the point 3 on the x -axis and also on the horizontal line constructed through the point 4 on the y -axis. In general, for any $(a, b) \in \mathbb{R} \times \mathbb{R}$, the point corresponding to (a, b) may be pictured as follows: Find the point which is on the same vertical line as the point a on the x -axis and also on the same horizontal line as the point b on the y -axis. Likewise, given a point p in the plane, consider a vertical and a horizontal line through p . The first component of the ordered pair corresponding to p will be the coordinate of the point on the x -axis where the vertical line intersects the x -axis. The second component will be determined by the intersection of the horizontal line with the y -axis. Figure 33 illustrates the foregoing ideas.

In Figure 33 it is clear that the pairs corresponding to the points m, n , and t are $(3, 4)$, $(-5, 3)$, and $(1, -5)$, respectively. The rectangular coordinates of point p are 5 and 0 ; of point q , 0 and -5 ; and of point s , -4 and -2 .

Consider again the equation $x + y = 5$. Five elements of the solution set of this equation are $(2, 3)$, $(5, 0)$, $(-1, 6)$, $(4, 1)$, and $(0, 5)$. After locating the points corresponding to these pairs (called plotting the points), one observes that these points appear to lie in a line (Figure 34).

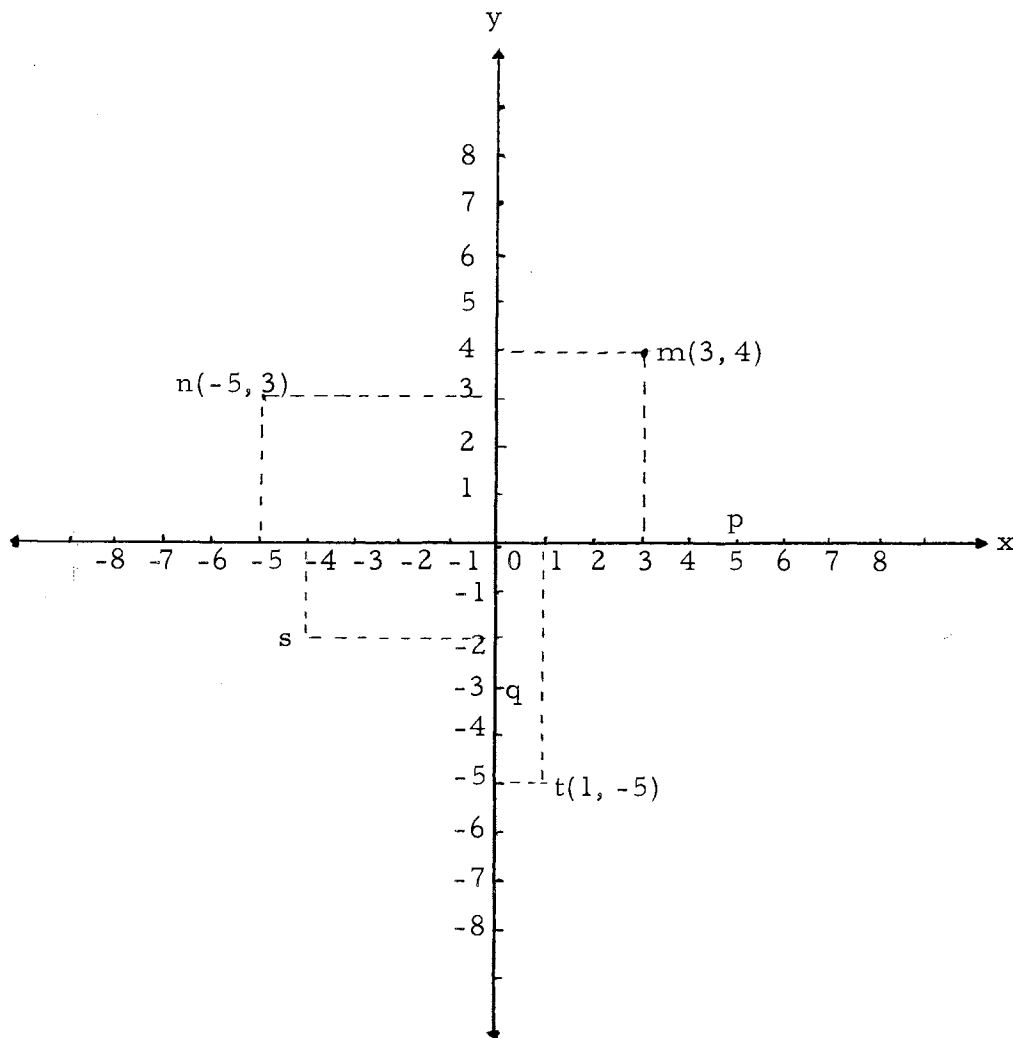


Figure 33.

It is true that the graph of the solution set of $x + y = 5$ is indeed a line. In fact, it can be shown in general that the graph of $ax + by + c = 0$ is a line. That is, every pair in the solution set corresponds to a point on the line, and every point on the line corresponds to a pair that is in the solution set. So it will be agreed that the graphs of all linear equations in two variables are lines.

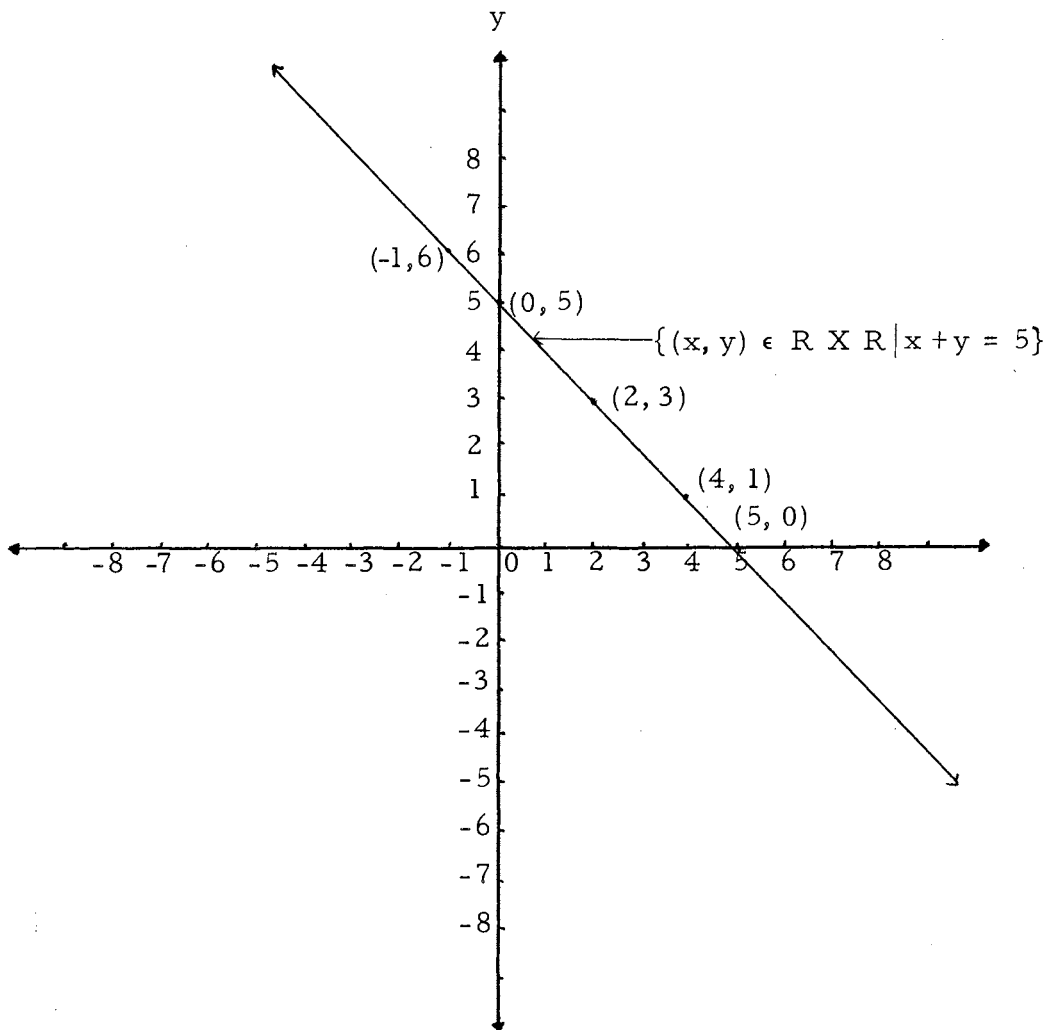


Figure 34.

It was pointed out previously that the equation $x + y = 5$ or $y = 5 - x$ defines the relation $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y = 5\}$ on the set \mathbb{R} . Since $(2, 3)$ is a solution of $x + y = 5$, it is true that $(2, 3) \in f$. Is it possible for some other ordered pair with first component 2, but with a second component different from 3, to be an element of f ? Suppose there is a pair, say $(2, y) \in f$, such that $y \neq 3$. Now $(2, 3) \in f$ means that $2 + 3 = 5$, or $3 = 5 - 2$. Notice that $(2, y) \in f$ says that $y = 5 - 2$.

By the transitive property of equality it follows that $y = 3$. The contradiction $y \neq 3$ and $y = 3$ results. So the supposition that $(2, y) \in f$ where $y \neq 3$ is false. Therefore, it is true that $y = 3$. In other words, there is only one ordered pair in f with first component 2. In general, if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$. By the definition on page 41 it is then true that f is a function. Since the function f is determined by the linear equation $x + y = 5$ it would make sense to call f a linear function.

A linear function is a function defined by a linear equation in two variables $ax + by + c = 0$, where $b \neq 0$.

The graph of the equation $x + y = 5$ (Figure 34), which is a line, is also called the graph of the function f . In Chapter II it was emphasized that if f is a function and $(x, y) \in f$, then y may be considered as the image of x . This was expressed as $y = f(x)$. The set of ordered pairs $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 5 - x\}$ may then be expressed as $\{(x, f(x)) \in \mathbb{R} \times \mathbb{R} \mid f(x) = 5 - x\}$. Denote the domain of f by $D_o(f)$ and the range by $R_a(f)$, then $D_o(f) = \mathbb{R}$ and $R_a(f) = \mathbb{R}$.

The reader may be wondering why, in the definition of linear function, the restriction on b was made. Consider the equation $x = 3$, or equivalently $x - 3 = 0$. This certainly can be written as $1 \cdot x + 0 \cdot y - 3 = 0$. Every ordered pair in this set has the same first component 3, but different second components. A few of the solutions are $(3, 0)$, $(3, 2)$, $(3, -2)$, $(3, 3)$, $(3, -3)$, and $(3, 5)$. The equation $x - 3 = 0$ does not define a linear function; but its graph, shown in Figure 35, is a line that is parallel to the y -axis.

Just as a point partitions a line into three pairwise disjoint sets of points, a line partitions the plane into three pairwise disjoint sets. In Figure 35 the sets of points are $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < 3\}$,

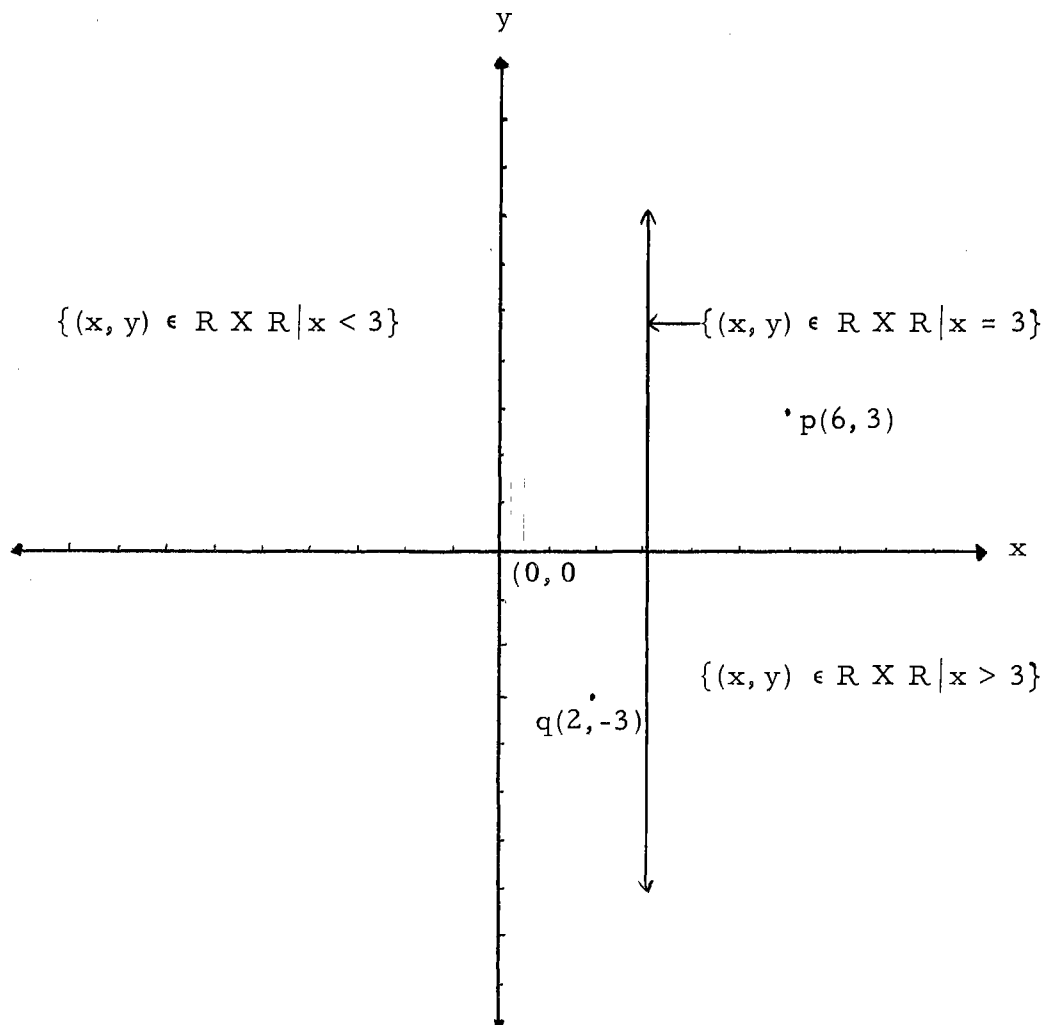


Figure 35.

$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = 3\}$, and $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > 3\}$. Notice that $(0, 0)$ is in the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < 3\}$. Therefore, the origin of the coordinate system is not on the line $x = 3$, but it is in one of the half planes determined by the line. The point $(2, -3)$, denoted by q in Figure 35, is in the same half plane as the origin since $(2, -3) \in \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < 3\}$. Thus, the origin and q are on the same side of the line $x = 3$ as the origin. On the other hand, the point $(6, 3)$,

denoted by p , is in the opposite half plane from the origin because $(6, 3) \in \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > 3\}$. So the origin and the point $(6, 3)$ are on opposite sides of the line $x = 3$. Also, the points p and q are on opposite sides. Furthermore, all points with first coordinate greater than 3 and all points with first coordinate less than 3 are on opposite sides of the line $x = 3$.

The equation $y + 2 = 0$ can be expressed in the general form of a linear equation in two variables where $a = 0$, $b = 1$, and $c = 2$; i. e., $0 \cdot x + 1 \cdot y + 2 = 0$. Its solution set is $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = -2\}$, which is a function since all first components are unique. If g denotes this function, then $g = \{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) = -2\}$. Observe that $D_0(g) = \mathbb{R}$ and $R_a(g) = \{-2\}$. Due to the fact that every second component is -2 , g is called a constant function, and the defining equation can be written as $g(x) = -2$. The function g is graphed in Figure 36.

Also, it should be pointed out here that the line $g(x) = -2$ partitions the plane into the classes $\{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) > -2\}$, $\{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) = -2\}$, and $\{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) < -2\}$. Observe that $(0, 0) \in \{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) > -2\}$, and hence the origin is not on the line $g(x) = -2$. All points on the same side of the line as the origin correspond to ordered pairs in the set $\{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) > -2\}$ while all points on the opposite side correspond to ordered pairs in the set $\{(x, g(x)) \in \mathbb{R} \times \mathbb{R} \mid g(x) < -2\}$.

As a final example, consider an equation of the form $ax + by = c$ where $a, b, c \in \mathbb{Z}_2$ and \mathbb{Z}_2 is the replacement set for the variables x and y . Instances of such equations are $1 \cdot x + 1 \cdot y = 0$ and $1 \cdot x + 1 \cdot y = 1$. To solve these equations it might be necessary to refer to the tables for \mathbb{Z}_2 in Figure 15. Since \mathbb{Z}_2 contains only two

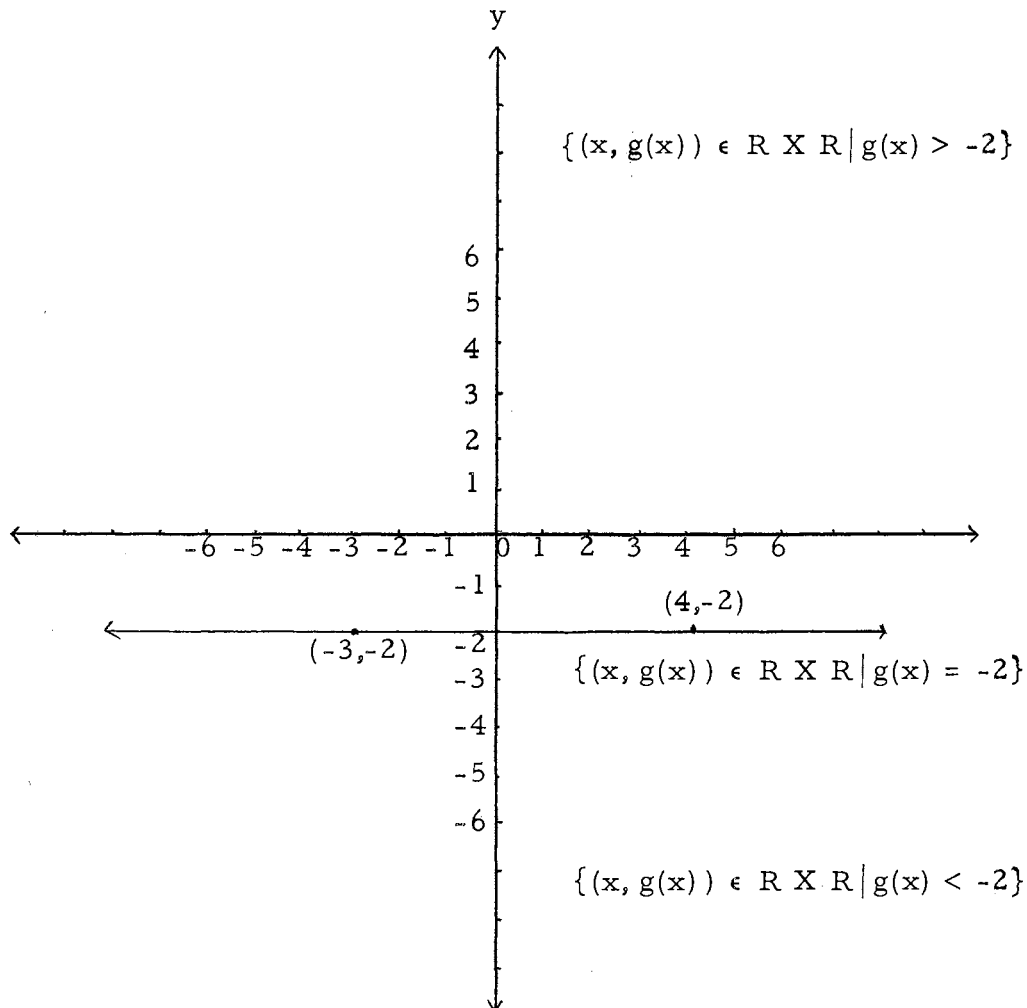


Figure 36.

elements, and hence $Z_2 \times Z_2$ contains only four pairs, there are only four possible candidates for solutions. The four distinct possibilities are $(0, 0)$, $(0, 1)$, $(1, 0)$, and $(1, 1)$. In regard to the first equation the resulting statements are $1 \cdot 0 + 1 \cdot 0 = 0$, $1 \cdot 0 + 1 \cdot 1 = 0$, $1 \cdot 1 + 1 \cdot 0 = 0$, and $1 \cdot 1 + 1 \cdot 1 = 0$, respectively. Only the first and last of these are true, therefore $\{(0, 0), (1, 1)\}$ is the solution set for $1 \cdot x + 1 \cdot y = 0$. Similarly, it can be concluded that the solution

set for $1 \cdot x + 1 \cdot y = 1$ is $\{(0, 1), (1, 0)\}$.

Linear inequalities in two variables such as $x - y < -2$, $2x > y + 1/2$, $3x - 2 \leq y$, and $y \geq x - 1$ also have ordered pairs of real numbers as solutions. The pair $(3, 6)$ is a member of the solution set of $x - y < -2$. If x is replaced by 3 and y is replaced by 6, then the resulting statement, $3 - 6 < -2$, is true. Also $(3, 8)$ is a member of the solution set since $3 - 8 < -2$ is likewise a true statement. Thus, both $(3, 6)$ and $(3, 8)$ are in the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y < -2\}$. In fact, if $x = 3$, then the inequality $3 - y < -2$ is equivalent to $5 < y$ because of the transformation principles for inequalities. There are numerous replacements for y such that $5 < y$ is true. Therefore, there are many ordered pairs in $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y < -2\}$ that have 3 as first component. Hence $x - y < -2$ does not define a function. Furthermore, all of the examples at the beginning of this paragraph also illustrate the fact that inequalities define relations that are not functions.

The graph of the solution set of $ax + by + c = 0$ is a line. The line partitions the plane into three pairwise disjoint sets of points, namely the line itself, the set of points in one of the half planes determined by the line, and the set of points in the opposite half plane. It is natural to ask if these three portions of the plane can be described in terms of equations and inequalities.

Consider the relation $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y < 5\}$. The defining inequality can be rewritten equivalently in the form $y < 5 - x$. For each real number replacement for x , the real number replacement for y must be less than $5 - x$.

Recall that the graph of $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 5 - x\}$ is a line (Figure 37). Every point on the line has coordinates that transform

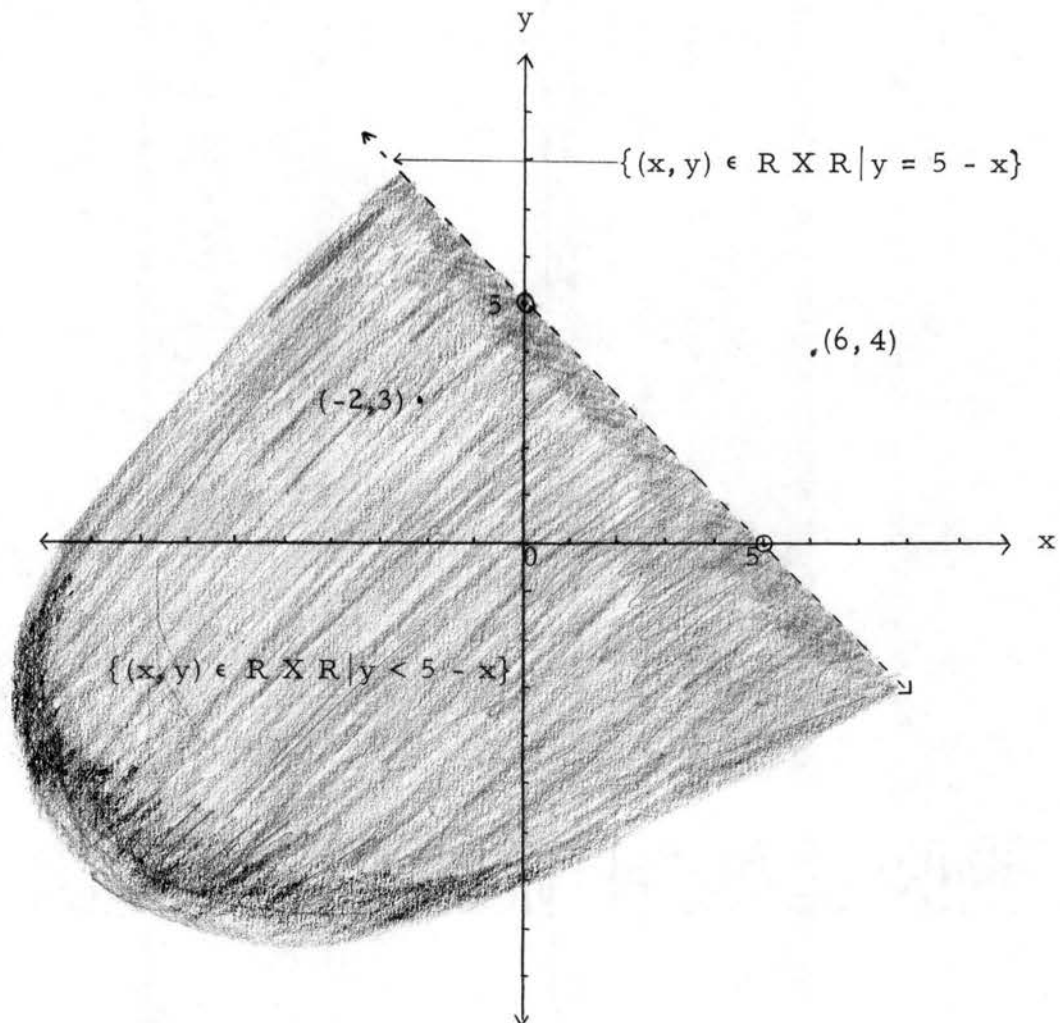


Figure 37.

$y = 5 - x$ into a true statement, and every pair that transforms the equation into a true statement corresponds to a point on the line. Observe that the pair $(0, 0)$ transforms $y = 5 - x$ into a false statement; hence, the origin is not on the line. So the origin is in one of the half planes determined by the line $y = 5 - x$. Note that the pair $(-2, 3)$ also transforms $y = 5 - x$ into a false statement.

Furthermore, both $(0, 0)$ and $(-2, 3)$ transform $y < 5 - x$ into a

true statement. Thus, one can conclude that the points $(0, 0)$ and $(-2, 3)$ are on the same side of the line. However, the pair $(6, 4)$ transforms both $y = 5 - x$ and $y < 5 - x$ into false statements. So, the point $(6, 4)$ is not on the line nor on the same side of the line as the origin. Hence, the point $(6, 4)$ must be on the side opposite the one containing the origin.

To summarize, all points in the plane that are on the same side of the line $y = 5 - x$ as the point $(0, 0)$ correspond to pairs in the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y < 5 - x\}$ while all points on the opposite side correspond to pairs in the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y > 5 - x\}$.

To graph the solution set of $y < 5 - x$, the graph of $y = 5 - x$ is first drawn by using a "broken line." This indicates that the line is not a part of the graph of the inequality. The shaded portion in Figure 37 shows the graph of $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y < 5 - x\}$. Similarly the inequality $y > 5 - x$ could be graphed.

Sometimes it is convenient to consider the graph of inequalities such as $x - y - 2 \leq 0$, or equivalently $y \geq x - 2$. The solutions of both $y = x - 2$ and $y > x - 2$ are included in the solution set. Thus,

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x - 2\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x - 2\} \cup \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y > x - 2\}.$$

Again it is convenient to consider the point $(0, 0)$. The inequality $y > x - 2$ becomes a true statement and the equation $y = x - 2$ becomes a false statement when both x and y are replaced by 0. The origin then is not on the line $y = x - 2$, but it is on one side of the line. Thus, all points on the same side of the line as the point $(0, 0)$ are included in the graph of $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x - 2\}$. On the other hand, the points on the side opposite the point $(0, 0)$ correspond to pairs in the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y < x - 2\}$.

To give a pictorial representation of the solution set of $y \geq x - 2$, first draw the graph of $y = x - 2$. This is shown in Figure 38 as a "solid line" to indicate that the line is a part of the graph. The portion representing the graph of $y > x - 2$ is then shaded.

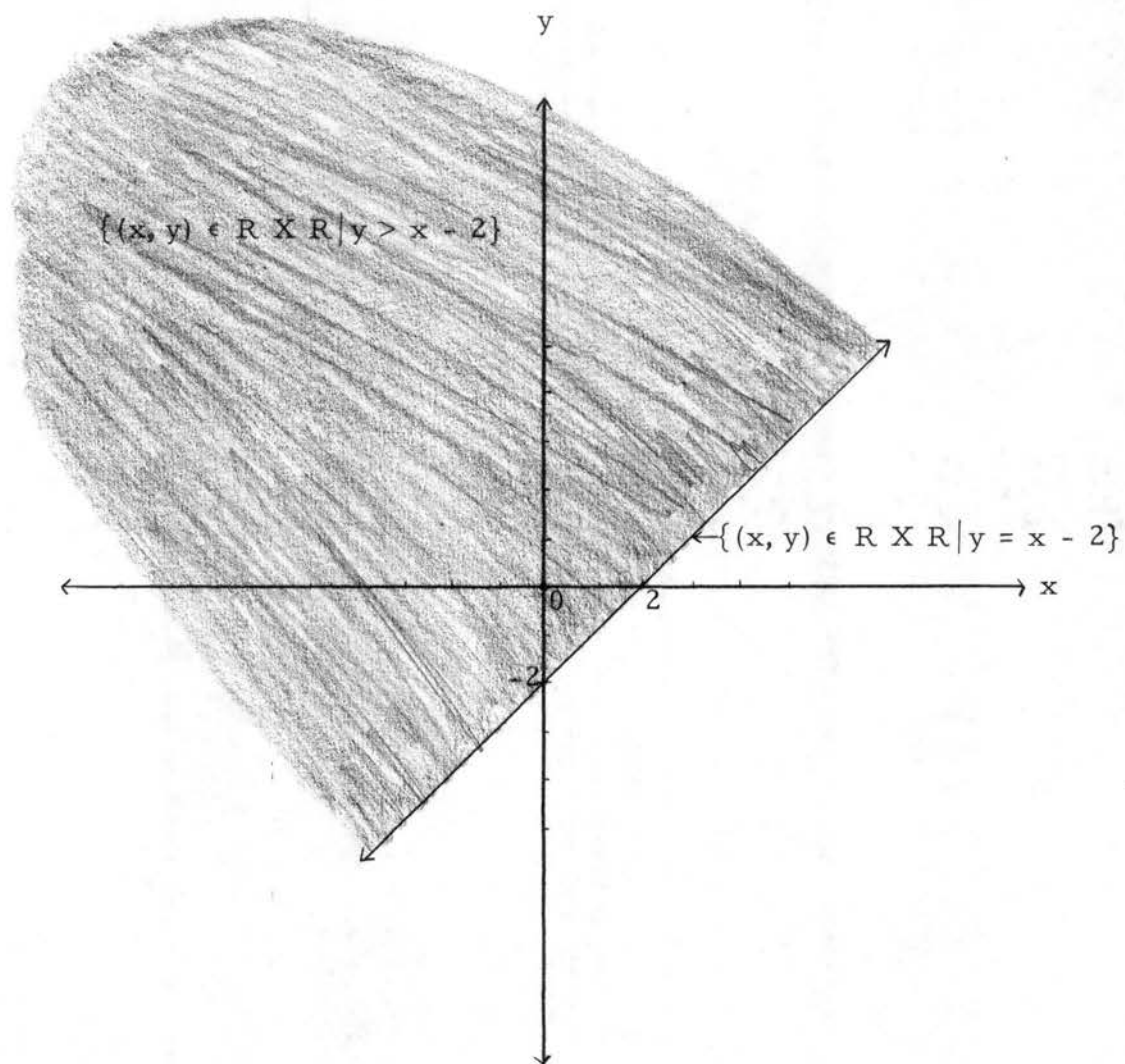


Figure 38.

Systems of Linear Equations

A pair of linear equations in two variables x and y is called a system of two linear equations in two variables x and y . To solve a system of two equations is to find all ordered pairs (x, y) which are solutions of both equations in the system. Therefore, to solve the system of linear equations

$$\begin{cases} ax + by + c = 0 \\ dx + ey + f = 0 \end{cases}$$

is to find the members of

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid ax + by + c = 0\} \cap \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid dx + ey + f = 0\}.$$

This is the same as finding the members of

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid ax + by + c = 0 \wedge dx + ey + f = 0\}.$$

The latter is the solution set of the system, and each of its members is called a solution of the system.

For example, consider the following system:

$$\begin{cases} 2x + y - 8 = 0 \\ 4x - y - 10 = 0 \end{cases}$$

By the transformation principles for equations, the equivalent equations

$$\begin{cases} y = 8 - 2x \\ y = 4x - 10 \end{cases}$$

are obtained. By the logical principle of substitution $8 - 2x$ may be substituted for y in $y = 4x - 10$ to conclude that

$$8 - 2x = 4x - 10$$

or $x = 3$. So if there is a pair (x, y) that is a solution of the system, then the first component must be 3. By substituting 3 for x in one of the equations of the system it is found that $y = 2$. Thus, the solution of the system is $(3, 2)$, or the solution set is $\{(3, 2)\}$. Note that the pair $(3, 2)$ converts both equations of the system into true statements.

The graph of the solution set $\{(3, 2)\}$ is the point of intersection of the graphs of $2x + y - 8 = 0$ and $4x - y - 10 = 0$. If these two equations are expressed in the equivalent forms $y = 8 - 2x$ and $y = 4x - 10$, then the graphs can be drawn easily by utilizing the result of Theorem 3.7.

If $x = 0$, then $y = 8 - 2x$ becomes $y = 8$ and $y = 4x - 10$ becomes $y = -10$. Thus, the point $(0, 8)$ is the point of intersection of the line $y = 8 - 2x$ with the y -axis while the point $(0, -10)$ is the point of intersection of the line $y = 4x - 10$ with the y -axis. On the other hand, if $y = 0$, then $y = 8 - 2x$ becomes $0 = 8 - 2x$, or $x = 4$. Similarly, $y = 4x - 10$ is transformed into $0 = 4x - 10$, or $x = 5/2$, whenever $y = 0$. So the points $(4, 0)$ and $(5/2, 0)$ are the points of intersection of $y = 8 - 2x$ and $y = 4x - 10$ with the x -axis, respectively. The points $(0, 8)$ and $(4, 0)$ determine the line $y = 8 - 2x$ and the points $(0, -10)$ and $(5/2, 0)$ determine the line $y = 4x - 10$. These lines are graphed in Figure 39.

In the preceding example it was easy to "solve each equation for y ." Solving each of the equations of some systems for y is somewhat more complicated. A better way for solving each system will be demonstrated. Consider the following system:

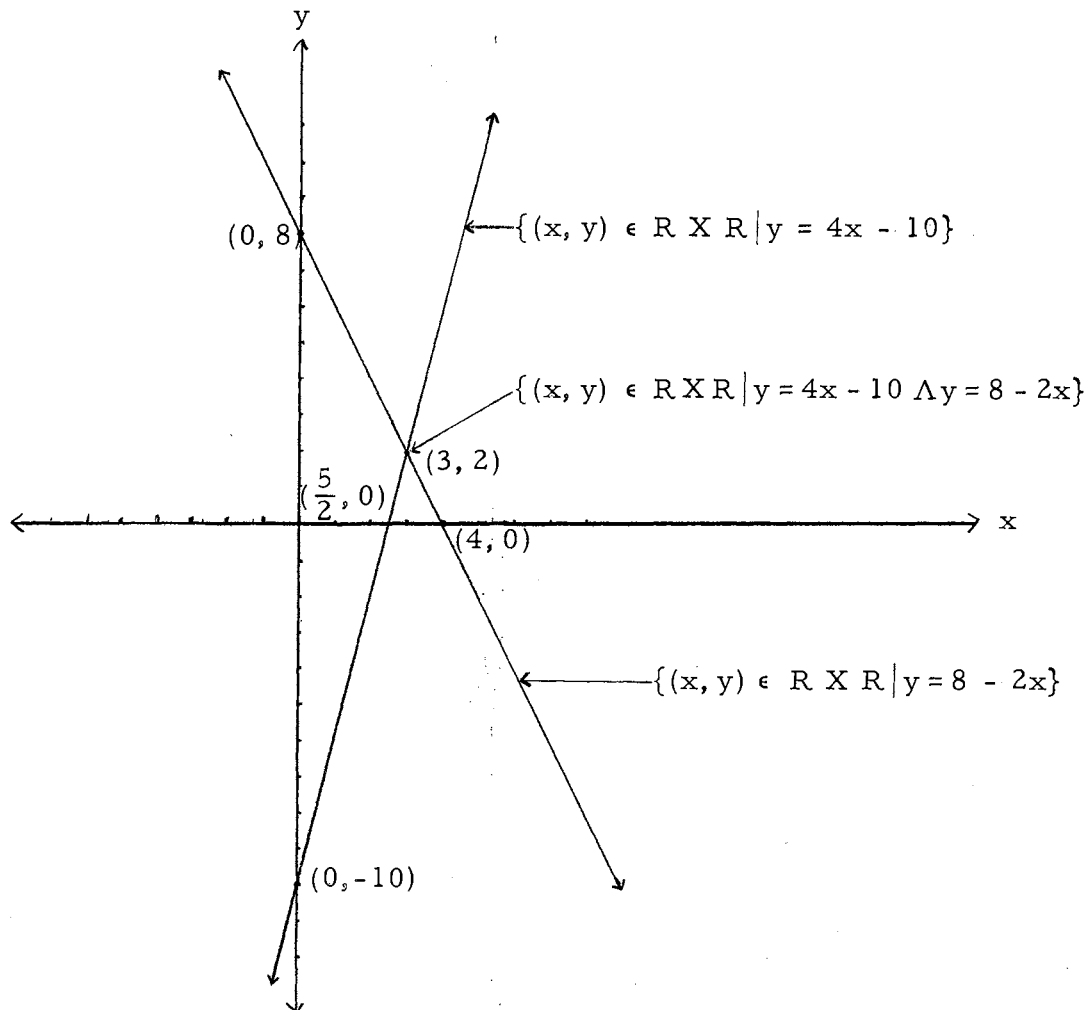


Figure 39.

$$\begin{cases} 2x - 3y - 7 = 0 \\ 5x + 4y - 6 = 0 \end{cases}$$

If there is an ordered pair (x, y) that is a solution of the system, then since $2x - 3y - 7 = 0$ and $5x + 4y - 6 = 0$, it follows that for all $p, q \in \mathbb{R}$, $p(2x - 3y - 7) = 0$ and $q(5x + 4y - 6) = 0$. Now if $p(2x - 3y - 7) = 0$ and $q(5x + 4y - 6) = 0$, then by Theorem 3.1 it is concluded that

$$p(2x - 3y - 7) + q(5x + 4y - 6) = 0.$$

The properties of the real number system may be used to simplify the left member of this equation to obtain

$$(2p + 5q)x + (-3p + 4q)y + (-7p - 6q) = 0.$$

At this point the reader will probably agree that this equation appears more unfavorable than the original system. Now this equation is true for all real number replacements for p and q ; therefore, it can be transformed into a simpler equation by carefully choosing replacements for p and q . Appropriate choices would be those that make either $2p + 5q = 0$ or $-3p + 4q = 0$ a true statement. For instance, if $p = 5$ and $q = -2$, then $2p + 5q = 0$, and it follows that

$$(2p + 5q)x + (-3p + 4q)y + (-7p - 6q) = 0$$

is transformed into

$$(10 - 10)x + (-15 - 8)y + (-35 + 12) = 0.$$

But this equation is equivalent to $-23y - 23 = 0$ or $y = -1$. Thus, if there is a pair (x, y) that is a solution of the system, then the second component y must be -1 . Substitution of -1 for y in either of the equations of the system reveals that $x = 2$. Substituting the components of the pair $(2, -1)$ for x and y in the equations of the system result in true statements. So the solution set of the system is $\{(2, -1)\}$.

Notice that a similar method could have been employed to solve the system if choices for p and q had been 4 and 3 , respectively. The consequence would have been

$$(8 + 15)x + (-12 + 12)y + (-28 - 18) = 0,$$

which is equivalent to $23x - 46 = 0$; and thus equivalent to $x = 2$.

In reality, the above procedure may be summarized as follows:

$$\begin{cases} 2x - 3y - 7 = 0 & (1) \\ 5x + 4y - 6 = 0 & (2) \end{cases}$$

$$10x - 15y - 35 = 0 \quad [\text{multiply (1) by 5}]$$

$$\underline{-10x - 8y + 12 = 0} \quad [\text{multiply (2) by -2}]$$

$$-23y - 23 = 0 \quad [\text{Theorem 3.1}]$$

$$y = -1$$

$$2x - 3(-1) - 7 = 0 \quad [\text{substitution in (1)}]$$

$$2x - 4 = 0$$

$$x = 2$$

Check $5(2) + 4(-1) - 6 = ? \quad [\text{substitution in (2)}]$

$$10 - 4 - 6 = 0$$

Therefore, the solution set is $\{(2, -1)\}$.

It would be instructive for the reader to graph the solution sets of the equations $2x - 3y - 7 = 0$ and $5x + 4y - 6 = 0$ and observe that the graph of the solution set of the above system is the point of intersection. That is,

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 2x - 3y - 7 = 0\} \cap \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 5x + 4y - 6 = 0\} = \{(2, -1)\}.$$

A system of two linear equations in two variables may not always have a solution. If there is no ordered pair (x, y) which satisfies each equation of the system, then the solution set is \emptyset . This is illustrated in the following example:

$$\begin{cases} x + 2y - 5 = 0 \\ -2x - 4y + 18 = 0. \end{cases}$$

For convenience, the abbreviated procedure will be followed.

$$\begin{cases} x + 2y - 5 = 0 & (1) \\ -2x - 4y + 18 = 0 & (2) \end{cases}$$

$$2x + 4y - 10 = 0 \quad [\text{multiply (1) by 2}]$$

$$\underline{-2x - 4y + 18 = 0} \quad [\text{multiply (2) by 1}]$$

$$8 = 0 \quad [\text{Theorem 3.1}]$$

Therefore, if there is a pair (x, y) such that both (1) and (2) are true, it must also be true that $8 = 0$. But this is absurd. Thus, the assumption is false, so it must follow that for all ordered pairs $(x, y) \in \mathbb{R} \times \mathbb{R}$, (x, y) is not a solution of the system. In other words,

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + 2y - 5 = 0\} \cap \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid -2x - 4y + 18 = 0\} = \emptyset.$$

A graphic interpretation (Figure 40) can be made by first graphing the equations $x + 2y - 5 = 0$ and $-2x - 4y + 18 = 0$. The result-
ing ^{two} parallel lines depict very vividly that the solution set of the system is \emptyset .

If $ax + by + c = 0$ is a linear equation in the two variables x and y , then for all $k \in \mathbb{R}$ such that $k \neq 0$, $k(ax + by + c) = k \cdot 0 = 0$ is an equivalent equation. In particular, $3(x - 2y - 6) = 0$ is equivalent to $x - 2y - 6 = 0$. The solution set of the system

$$\begin{cases} -3x - 2y - 16 = 0 & (1) \\ 3x - 6y - 18 = 0 & (2) \end{cases}$$

will be sought.

Suppose there is an ordered pair (x, y) that is a solution of the system, then

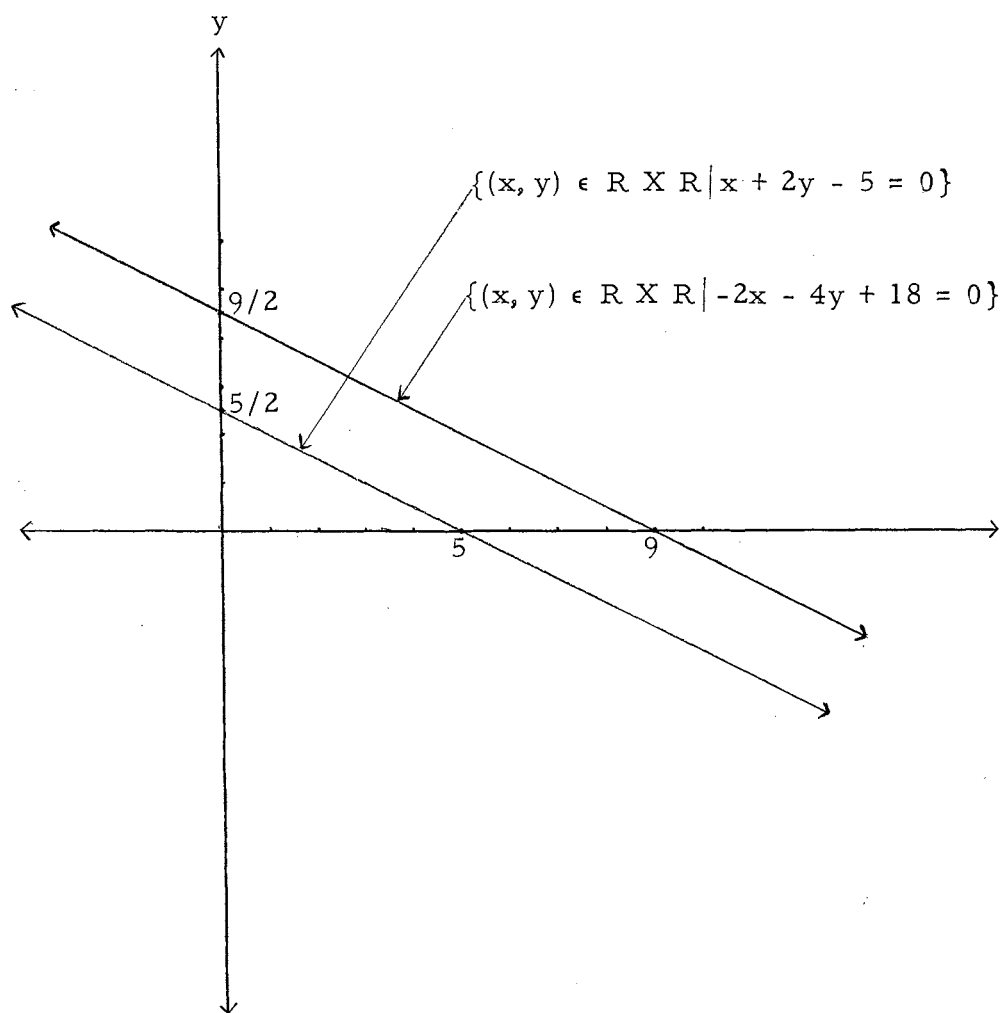


Figure 40.

$$\begin{array}{ll}
 -3x + 6y + 18 = 0 & \text{[multiply (1) by -3]} \\
 \underline{3x - 6y - 18 = 0} & \text{[multiply (2) by 1]} \\
 0 = 0 & \text{[Theorem 3.1]}
 \end{array}$$

The conclusion that $0 = 0$ is always true, so the supposition must always be true. That is, every ordered pair that is a solution of (1) is also a solution of (2), and vice versa. A graphic interpretation would be that the graph of $x - 2y - 6 = 0$ is the "same line as" the

graph of $x - 2y - 6 = 0$.

In the preceding examples of systems of linear equations in two variables relative to the field of real numbers, only the axioms and theorems pertaining to the binary operations of addition and multiplication of real numbers were used to find solutions. Each of these properties used has its analog in any other field. The question as to the feasibility of considering solutions of "systems of linear equations" relative to some other field is worthy of attention. Take for example the system:

$$\begin{cases} 1 \cdot x + 1 \cdot y = 1 \\ 1 \cdot x + 0 \cdot y = 1 \end{cases}$$

relative to the field Z_2 . To seek solutions of this system, one proceeds as follows.

$$\begin{aligned} \begin{cases} 1 \cdot x + 1 \cdot y = 1 \\ 1 \cdot x + 0 \cdot y = 1 \end{cases} & \begin{matrix} (1) \\ (2) \end{matrix} \\ (1+1) \cdot x + (1+0) \cdot y = 1+1 & \text{[Theorem 3.1]} \\ 0 \cdot x + 1 \cdot y = 0 & \text{[1+1=0 and 1+0=1]} \\ 0+1 \cdot y = 0 & \text{[0} \cdot x = 0\text{]} \\ y = 0 & \text{[1} \cdot y = y\text{]} \\ 1 \cdot x + 1 \cdot 0 = 1 & \text{[substitution in (1)]} \\ x = 1 & \\ \text{Check. } 1 \cdot 1 + 0 \cdot 0 = 1 & \text{[substitution in (2)]} \end{aligned}$$

Hence, the solution set is $\{(1, 0)\} \subset Z_2 \times Z_2$.

To conclude Chapter III attention will be focused again on equations of the form $ax + by = c$, where $a, b, c, x, y \in Z_2$. Since there

are only two possible replacements for each of a, b, and c, there will only be eight such equations to consider. These equations together with their solution sets are as follows:

(1) $1 \cdot x + 1 \cdot y = 1$	$\{(1, 0), (0, 1)\}$
(2) $1 \cdot x + 1 \cdot y = 0$	$\{(1, 1), (0, 0)\}$
(3) $1 \cdot x + 0 \cdot y = 1$	$\{(1, 0), (1, 1)\}$
(4) $1 \cdot x + 0 \cdot y = 0$	$\{(0, 0), (0, 1)\}$
(5) $0 \cdot x + 1 \cdot y = 1$	$\{(1, 1), (0, 1)\}$
(6) $0 \cdot x + 1 \cdot y = 0$	$\{(0, 0), (1, 0)\}$
(7) $0 \cdot x + 0 \cdot y = 0$	$Z_2 \times Z_2$
(8) $0 \cdot x + 0 \cdot y = 1$	\emptyset

The solution sets of equations (1) - (6) are all proper subsets of $Z_2 \times Z_2$. Equation (7) has $Z_2 \times Z_2$ for its solution set while equation (8) has no solutions. So let it be agreed that only equations (1) - (7) will be considered in the following discussion.

Let each of the pairs in $Z_2 \times Z_2$ represent a "bead." These beads may be pictured by large dots as in Figure 41. Also, consider the "lines" in Figure 41 as "wires." To illustrate, the pairs (1, 0) and (0, 1) are solutions of the equation $1 \cdot x + 1 \cdot y = 1$; therefore, the "beads" (1, 0) and (0, 1) are on the wire $1 \cdot x + 1 \cdot y = 1$. In other words, $1 \cdot x + 1 \cdot y = 1$ is the equation of the wire that is on the beads (1, 0) and (0, 1). Similarly, $1 \cdot x + 1 \cdot y = 0$ is the equation of the wire on beads (1, 1) and (0, 0), $1 \cdot x + 0 \cdot y = 1$ is the equation of the wire on beads (1, 0) and (1, 1), etc. Each wire in Figure 41 is identified with its corresponding equation by using the method used for identifying the equations at the beginning of this discussion.

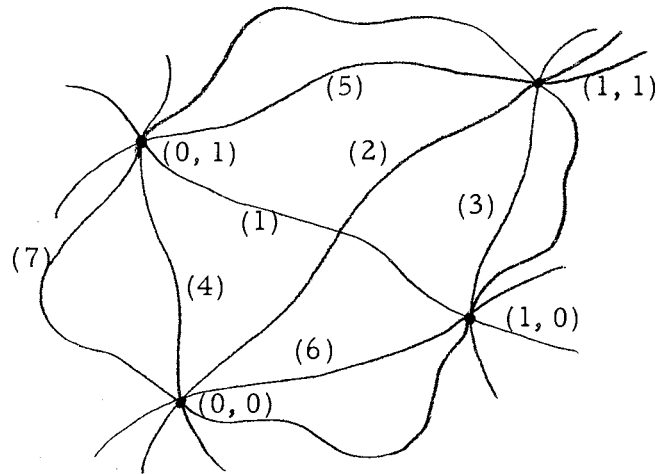


Figure 41.

In the example preceding this one, it was shown that equations (1) and (3) had the pair $(1, 0)$ as a common solution. Thus, in Figure 41 wires (1) and (3) have the bead $(1, 0)$ in common. Observe that wires (6) and (7) are also on the bead $(1, 0)$. Similarly, wires (2), (3), (5), and (7) have bead $(1, 1)$ in common; wires (1), (4), (5), and (7) have bead $(0, 1)$ in common; and wires (2), (4), (6), and (7) have bead $(0, 0)$ in common. But notice that there are no beads on both wires (1) and (2). Thus, the solution set of the system of equations consisting of (1) and (2) is \emptyset . Correspondingly, there are no beads on both wires (3) and (4) nor on wires (5) and (6). Finally, all four beads are on wire (7); but this was to be expected since the solution set of $0 \cdot x + 0 \cdot y = 0$ was $Z_2 \times Z_2$.

CHAPTER IV

OTHER ALGEBRAIC SYSTEMS

Introduction

The real number system as it is known today has evolved from a very humble beginning. Numbers were invented by civilized man to meet the needs of man's civilization. The successive extensions from counting numbers to real numbers was no doubt motivated, at least partially, by man's need to solve equations.

In order to have a number system extensive enough to provide solutions for linear equations such as $x + 5 = 2$, it is necessary to introduce the set Z of integers. Furthermore, there are linear equations with integers as coefficients that do not have solutions in the set Z . For example, $2x - 3 = 0$ is such an equation.

Any linear equation with coefficients in the set Q of rational numbers will always have a solution in Q because Q is a field. In fact, any linear equation over a field F has a unique solution in F according to Theorem 3.26 on page 91.

In other words, equations such as $x - 3/4 = 2/3$, $2x - 3 = 0$, and $5x + 2 = 6$ will always have solutions in Q . Observe, however, that $3x + \sqrt{2} = 0$ has no solution in Q since $\sqrt{2} \notin Q$, but it does have a unique solution in R .

What can be said about a quadratic equation such as $x^2 - 2 = 0$ with coefficients in Q ? If $x^2 - 2 = 0$ has a solution in Q , then it must

be true that $x^2 = 2$. The only numbers that satisfy $x^2 = 2$ are the irrational numbers $\sqrt{2}$ and $-\sqrt{2}$. Therefore, $x^2 - 2 = 0$ has no solution in \mathbb{Q} . In other words, to provide for solutions to equations such as $x^2 - 2 = 0$, the system of rational numbers is not sufficient. Hence, the motivation for an extension to the system of real numbers is provided.

The Complex Number System

Consider the quadratic equation $x^2 + 1 = 0$ over the set \mathbb{R} . Now this equation appears simple enough and one may be led to believe that it has a solution in \mathbb{R} . If there is a solution in \mathbb{R} , then x^2 must represent the additive inverse, -1 , of 1 . Can 0 , 1 , or -1 be a solution of $x^2 + 1 = 0$? The answer is no because $0^2 + 1 = 1 \neq 0$, $1^2 + 1 = 2 \neq 0$, and $(-1)^2 + 1 = 1 + 1 = 2 \neq 0$. Is there any real number that is a solution? If $a > 0$, then $a \cdot a = a^2 > 0$ and $a^2 + 1 > 0$. Therefore, no positive real number can be a solution. How about a negative real number? If $a < 0$, then $a \cdot a = a^2 > 0$ and $a^2 + 1 > 0$. So no negative real number is a solution. It is therefore conclusive that $x^2 + 1 = 0$ has no solution in \mathbb{R} .

The inadequacy of \mathbb{R} to afford solutions for equations such as $x^2 + 1 = 0$ plagued mathematicians even as late as the beginning of the nineteenth century. Regarding the search for a number system in which solutions could be found, Haag [14] states:

In the 1840's Hamilton defined the complex number system as follows. He associated each point of the plane with a complex number denoted by an ordered pair of real numbers (a, b) , just as each point of the number line is associated with a real number. His initial problem was to define equality, addition, and multiplication of these "points" in such a way that the

resulting system of complex numbers is a field which includes the real number system as a proper subsystem. He was motivated in his definitions by the desire to have the solutions of the equation $x^2 = -1$ in this system.

In previous experiences in the development of the real number system, the reader has seen that the properties of operations in the extension of a number system depend upon the properties of the operations in the system from which the extension is made. In particular, properties of addition and multiplication of integers depend upon properties of addition and multiplication of whole numbers. This principle should be kept in mind as the system of "complex numbers" is developed from the system of reals.

Consider the set $C = \{(x, y) \mid x \in R \text{ and } y \in R\}$, which is just the set of all ordered pairs of real numbers. The elements of C are called complex numbers. Now if C is to be a field, an equals relation and two binary operations must be defined to satisfy the field axioms. In keeping with the agreement made in Chapter III about binary operations in a field, use of the terms "addition," "multiplication," and "equals," together with the symbols "+," " \cdot ," and "=" will be continued in this context. Definitions of these terms are as follows:

Equals: For all $(x, y), (z, w) \in C$, $(x, y) = (z, w)$ iff $x = z$ and $y = w$.

Addition: For all $(x, y), (z, w) \in C$, $(x, y) + (z, w) = (x + z, y + w)$.

Multiplication: For all $(x, y), (z, w) \in C$, $(x, y) \cdot (z, w) = (xz - yw, xw + yz)$.

It will be shown first of all that the equals relation thus defined on C is indeed an equivalence relation. To do this it must be shown that the relation is reflexive, symmetric, and transitive.

The Reflexive Property. For all $(x, y) \in C$, $(x, y) = (x, y)$. This is true because $x, y \in R$ and $x = x$ and $y = y$.

The Symmetric Property. If $(x, y) = (z, w)$, then $(z, w) = (x, y)$. To prove this note that if $(x, y) = (z, w)$, then by definition $x = z$ and $y = w$. Now $x = z$ and $y = w$ implies that $z = x$ and $w = y$ because of the symmetric property of equality of real numbers. Therefore, $(z, w) = (x, y)$. Hence, if $(x, y) = (z, w)$, then $(z, w) = (x, y)$.

The Transitive Property. If $(x, y) = (z, w)$ and $(z, w) = (u, v)$, then $(x, y) = (u, v)$. To prove this observe that if $(x, y) = (z, w)$ and $(z, w) = (u, v)$, then $x = z$ and $y = w$; $z = u$ and $w = v$. Therefore, $x = u$ and $y = v$ by the transitive property of equality of real numbers. So $(x, y) = (u, v)$. Hence, if $(x, y) = (z, w)$ and $(z, w) = (u, v)$, then $(x, y) = (u, v)$.

To show that addition and multiplication of elements in C are binary operations, it will be essential to show that when two members of C are added or multiplied the "answers" will be unique. This can be accomplished in the following way.

Addition. Since addition of real numbers is a binary operation on R , it follows that $x + z$ and $y + w$ are unique real numbers. Therefore, the ordered pair $(x + z, y + w)$ is a unique element in C . Hence, addition of complex numbers is a binary operation.

Multiplication. Since addition, multiplication, and subtraction are binary operations on R , it follows that $xz - yw$ and $xw + yz$ are unique real numbers and the ordered pair $(xz - yw, xw + yz)$ is a unique

element in C . Therefore, multiplication of complex numbers is a binary operation.

Thus, the set C is closed with respect to addition and multiplication, and Axioms A. 1 and M. 1 of the field axioms on page 80 are satisfied. If C is to be a field, then the remaining field axioms must hold for members of C . In the following verifications of these field axioms for C , the axioms for R , the definition of subtraction in R , and other derived properties of operations in R will be utilized.

Commutative law for addition. For all $(x, y), (z, w) \in C$, $(x, y) + (z, w) = (z, w) + (x, y)$.

Proof:

$$\begin{aligned} (x, y) + (z, w) &= (x + z, y + w) && \text{[definition of addition]} \\ &= (z + x, w + y) && \text{[Axiom A. 2]} \\ &= (z, w) + (x, y) && \text{[definition of addition]} \end{aligned}$$

Commutative law for multiplication. For all $(x, y), (z, w) \in C$, $(x, y) \cdot (z, w) = (z, w) \cdot (x, y)$.

Proof:

$$\begin{aligned} (x, y) \cdot (z, w) &= (xz - yw, xw + yz) && \text{[definition of multiplication]} \\ &= (zx - wy, wx + zy) && \text{[Axiom M. 2]} \\ &= (zx - wy, zy + wx) && \text{[Axiom A. 2]} \\ &= (z, w) \cdot (x, y) && \text{[definition of multiplication]} \end{aligned}$$

Associative law for addition. For all $(x, y), (z, w), (u, v) \in C$, $[(x, y) + (z, w)] + (u, v) = (x, y) + [(z, w) + (u, v)]$.

Proof:

$$\begin{aligned}
 [(x, y) + (z, w)] + (u, v) &= (x + z, y + w) + (u, v) && \text{[definition of addition]} \\
 &= ((x + z) + u, (y + w) + v) && \text{[definition of addition]} \\
 &= (x + (z + u), y + (w + v)) && \text{[Axiom A. 3]} \\
 &= (x, y) + (z + u, w + v) && \text{[definition of addition]} \\
 &= (x, y) + [(z, w) + (u, v)] && \text{[definition of addition]}
 \end{aligned}$$

Associative law for multiplication. For all $(x, y), (z, w), (u, v) \in C$, $[(x, y) \cdot (z, w)] \cdot (u, v) = (x, y) \cdot [(z, w) \cdot (u, v)]$.

Proof:

$$\begin{aligned}
 [(x, y) \cdot (z, w)] \cdot (u, v) &= (xz - yw, xw + yz) \cdot (u, v) && \text{[definition of multiplication]} \\
 &= ((xz - yw)u - (xw + yz)v, (xz - yw)v + (xw + yz)u) && \text{[definition of multiplication]} \\
 &= ((xz - yw)u + [-(xw + yz)v], (xz - yw)v + (xw + yz)u) && \text{[definition of subtraction]} \\
 &= ((xz - yw)u + [-(xw) - (yz)]v, (xz - yw)v + (xw + yz)u) && \text{[Theorems 3.15 and 3.18]} \\
 &= ([((xz)u - (yw)u) + [-(xw)v - (yz)v], [(xz)v - (yw)v] + [(xw)u + (yz)u]) && \text{[Axiom MA and Theorem 3.17]} \\
 &= ((xz)u + [-(yw)u] + [-(xw)v] + [-(yz)v], (xz)v + [-(yw)v] + (xw)u + (yz)u) && \text{[definition of subtraction and Axiom A.3]} \\
 &= ((xz)u + [-(xw)v] + [-(yz)v] + [-(yw)u], (xz)v + (xw)u + (yz)u + [-(yw)v]) && \text{[Axioms A.2 and A.3]} \\
 &= (x(zu) + [x(-wv)] + [-y(zv)] + [-y(wu)], x(zv) + x(wu) + y(zu) + [y(-wv)]) && \text{[Axiom M.3 and Theorem 3.15]} \\
 &= (x[zu + (-wv)] + (-y)(zv + wu), x(zv + wu) + y[zu + (-wv)]) && \text{[Axiom MA]} \\
 &= (x(zu - wv) - y(zv + wu), x(zv + wu) + y(zu - wv)) && \text{[definition of subtraction and Theorem 3.15]}
 \end{aligned}$$

$$= (x, y) \cdot (zu - wv, zv + wu) \quad [\text{definition of multiplication}]$$

$$= (x, y) \cdot [(z, w) \cdot (u, v)] \quad [\text{definition of multiplication}]$$

Distributive law. For all $(x, y), (z, w), (u, v) \in C$, $(x, y) \cdot$

$$[(z, w) + (u, v)] = (x, y) \cdot (z, w) + (x, y) \cdot (u, v).$$

Proof:

$$(x, y) \cdot [(z, w) + (u, v)]$$

$$= (x, y) \cdot (z + u, w + v) \quad [\text{definition of addition}]$$

$$= (x(z + u) - y(w + v), x(w + v) + y(z + u)) \quad [\text{definition of multiplication}]$$

$$= (x(z + u) + (-y)(w + v), x(w + v) + y(z + u)) \quad [\text{definition of subtraction and Theorem 3.15}]$$

$$= (xz + xu + (-y)w + (-y)v, xw + xv + yz + yu) \quad [\text{Axiom MA}]$$

$$= ([xz + (-y)w] + [xu + (-y)v], (xw + yz) + (xv + yu)) \quad [\text{Axioms A.2 and A.3}]$$

$$= ((xz - yw) + (xu - yv), (xw + yz) + (xv + yu)) \quad [\text{Theorem 3.15 and definition of subtraction}]$$

$$= (xz - yw, xw + yz) + (xu - yv, xv + yu) \quad [\text{definition of addition}]$$

$$= (x, y) \cdot (z, w) + (x, y) \cdot (u, v) \quad [\text{definition of multiplication}]$$

Identity element for addition. There exists $(a, b) \in C$ such that for all $(x, y) \in C$, $(x, y) + (a, b) = (x, y)$. To prove this note that

$$(x, y) + (0, 0) = (x + 0, y + 0) \quad [\text{definition of addition}]$$

$$= (x, y) \quad [\text{Axiom A.4}]$$

Identity element for multiplication. There exists $(c, d) \in C$ such that for all $(x, y) \in C$, $(x, y) \cdot (c, d) = (x, y)$. To verify this observe that

$$\begin{aligned}
(x, y) \cdot (1, 0) &= (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) && \text{[definition of multiplication]} \\
&= (x \cdot 1 + (-y) \cdot 0, x \cdot 0 + y \cdot 1) && \text{[definition of subtraction and Theorem 3.15]} \\
&= (x + 0, 0 + y) && \text{[Axiom M.4 and Theorem 3.7]} \\
&= (x, y) && \text{[Axiom A.4]}
\end{aligned}$$

Inverse elements for addition. For all $(x, y) \in C$ there exists $(a, b) \in C$ such that $(x, y) + (a, b) = (0, 0)$. To prove this notice that $-x$ and $-y$ exist since $x, y \in R$, and

$$\begin{aligned}
(x, y) + (-x, -y) &= (x + (-x), y + (-y)) && \text{[definition of addition]} \\
&= (0, 0) && \text{[Axiom A.5]}
\end{aligned}$$

The element $(-x, -y)$ may be written as $-(x, y)$.

The final field property to be verified is Axiom M.5, which asserts that every element different from the additive identity must have a multiplicative inverse. If C is to be a field, then every $(x, y) \in C$ such that $(x, y) \neq (0, 0)$ must have a multiplicative inverse. That is, there must exist $(c, d) \in C$ such that $(x, y) \cdot (c, d) = (1, 0)$ whenever $x \neq 0 \vee y \neq 0$. Suppose there does exist such an element in C and observe that $(x, y) \cdot (c, d) = (1, 0)$ implies $(xc - yd, xd + yc) = (1, 0)$ by the definition of multiplication in C . However, by the definition of equality of complex numbers it then follows that $xc - yd = 1$ and $xd + yc = 0$. But $xc - yd = xc + (-y)d = (-y)d + xc$ by the definition of subtraction of real numbers, Theorem 3.15, and Axiom A.2. Therefore, $(-y)d + xc = 1$ and $xd + yc = 0$.

Consider the following system of two linear equations in two variables over R , where c and d are considered as variables.

$$\begin{aligned} &\begin{cases} (-y)d + xc = 1 & (1) \\ xd + yc = 0 & (2) \end{cases} \\ &\begin{cases} x(-y)d + x^2c = x & [\text{multiply (1) by } x] \\ xyd + y^2c = 0 & [\text{multiply (2) by } y] \end{cases} \\ &\begin{aligned} &-(xy)d + x^2c = x & [\text{Theorem 3.15}] \\ &\underline{(xy)d + y^2c = 0} \\ &(x^2 + y^2)c = x & [\text{Theorem 3.1}] \end{aligned} \end{aligned}$$

Since $x \neq 0 \vee y \neq 0$, it follows that $x^2 + y^2 \neq 0$ and $(x^2 + y^2)^{-1}$ exists.

Hence,

$$c = x(x^2 + y^2)^{-1} = \frac{x}{x^2 + y^2}.$$

In a similar manner it can be shown that

$$d = \frac{-y}{x^2 + y^2}$$

provided that $x \neq 0 \vee y \neq 0$. Therefore, if there exists $(c, d) \in C$ such that $(x, y) \cdot (c, d) = (1, 0)$, then

$$c = \frac{x}{x^2 + y^2} \quad \text{and} \quad d = \frac{-y}{x^2 + y^2}.$$

It still remains to show that the complex number (c, d) is indeed the multiplicative inverse of (x, y) .

Inverse elements for multiplication. For all $(x, y) \in C$ such that $(x, y) \neq (0, 0)$, there exists $(c, d) \in C$ such that $(x, y) \cdot (c, d) = (1, 0)$.

To prove this notice again that

$$\frac{x}{x^2 + y^2} \quad \text{and} \quad \frac{-y}{x^2 + y^2}$$

do indeed represent real numbers provided that $x \neq 0 \vee y \neq 0$.

Furthermore,

$$\begin{aligned}
 (x, y) & \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) \\
 & = \left(x \cdot \frac{x}{x^2 + y^2} - y \cdot \frac{-y}{x^2 + y^2}, x \cdot \frac{-y}{x^2 + y^2} + y \cdot \frac{x}{x^2 + y^2} \right) \\
 & \qquad \qquad \qquad \text{[definition of multiplication]} \\
 & = \left(x \cdot \frac{x}{x^2 + y^2} + (-y) \cdot \frac{-y}{x^2 + y^2}, x \cdot \frac{-y}{x^2 + y^2} + y \cdot \frac{x}{x^2 + y^2} \right) \\
 & \qquad \qquad \qquad \text{[definition of subtraction and Theorem 3.15]} \\
 & = \left(\frac{x^2}{x^2 + y^2} + \frac{y^2}{x^2 + y^2}, \frac{-(xy)}{x^2 + y^2} + \frac{xy}{x^2 + y^2} \right) \\
 & \qquad \qquad \qquad \text{[Theorem 3.23, Theorem 3.15, and Axiom M.2]} \\
 & = \left(\frac{x^2 + y^2}{x^2 + y^2}, \frac{-(xy) + xy}{x^2 + y^2} \right) \qquad \text{[Corollary to Theorem 3.24]} \\
 & = \left(\frac{x^2 + y^2}{x^2 + y^2}, \frac{0}{x^2 + y^2} \right) \qquad \text{[Axiom A.5]} \\
 & = ((x^2 + y^2)(x^2 + y^2)^{-1}, 0 \cdot (x^2 + y^2)^{-1}) \qquad \text{[definition]} \\
 & = (1, 0) \qquad \qquad \qquad \text{[Axiom M.5 and Theorem 3.7]}
 \end{aligned}$$

Since it has been shown that the field axioms govern the binary operations of addition and multiplication in \mathbb{C} , it can be concluded that

C is a field. Therefore, all the theorems that are true for fields are also true for C .

Select the subset R' of C containing all complex numbers of the form $(a, 0)$; i. e., $R' = \{(a, 0) \mid (a, 0) \in C\}$. For every $a \in R$ there exists $(a, 0) \in R'$ that can be matched with a , and for every $(a, 0) \in R'$ there exists $a \in R$ that can be matched with $(a, 0)$. That is, there is a one-to-one correspondence between R' and R . Let this correspondence of unique elements in R' with unique elements in R be denoted by " $(a, 0) \leftrightarrow a$," which is read "the pair $(a, 0)$ corresponds to a ." In particular, $(0, 0) \leftrightarrow 0$ and $(1, 0) \leftrightarrow 1$.

It is natural to ask how addition and multiplication behave when applied to elements of R' . For all $(a, 0), (b, 0) \in R'$, $(a, 0) + (b, 0) = (a + b, 0)$ and $(a, 0) \cdot (b, 0) = (ab, 0)$. Therefore, addition and multiplication are binary operations on R' since $a + b$ and ab represent real numbers. Furthermore, $(a, 0) + (-a, 0) = (0, 0)$ and $(a, 0)(a^{-1}, 0) = (1, 0)$ provided that $a \neq 0$. So every element $(a, 0)$ in R' has an additive inverse and every element $(a, 0)$, where $a \neq 0$, has a multiplicative inverse. By definition of R' it is obvious that both $(0, 0)$ and $(1, 0)$ are in R' . By what was shown previously about the operations in C , one can conclude that the commutative, associative, and distributive laws hold. Thus, R' is a field in its own right and is called a subfield of C .

In making a further observation the pictorial arrangements in Figure 42 are particularly helpful.

The correspondences in Figure 42 can be interpreted to mean that a "sum" of any two elements in R' corresponds to the "sum" of the corresponding elements in R , and a "product" of two elements in R' corresponds to the "product" of the corresponding elements in R . In

$$\begin{array}{ccc}
 \underline{R'} & & \underline{R} \\
 (a, 0) \longleftrightarrow & a & \\
 (b, 0) \longleftrightarrow & b & \\
 (a + b, 0) \longleftrightarrow & a + b & \\
 \end{array}
 \qquad
 \begin{array}{ccc}
 \underline{R'} & & \underline{R} \\
 (a, 0) \longleftrightarrow & a & \\
 (b, 0) \longleftrightarrow & b & \\
 (ab, 0) \longleftrightarrow & ab & \\
 \end{array}$$

Figure 42.

other words, "addition" and "multiplication" in R' behave exactly like "addition" and "multiplication" in R . Therefore, from a mathematical viewpoint, there is no difference in the structure of the field R' and the field R .

At the beginning of this section the motivating factor for extending the real number system was the inability to solve the equation $x^2 + 1 = 0$ in R . Since $(0, 0) \leftrightarrow 0$ and $(1, 0) \leftrightarrow 1$, consider the equation $x^2 + (1, 0) = (0, 0)$ where $x \in C$. Hopefully there is a complex number that will satisfy this equation. Since

$$\begin{aligned}
 (0, 1)^2 &= (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) \\
 &= (-1, 0)
 \end{aligned}$$

and

$$(-1, 0) + (1, 0) = (-1 + 1, 0 + 0) = (0, 0),$$

it follows that the complex number $(0, 1)$ is indeed a solution of $x^2 + (1, 0) = (0, 0)$.

The complex number $(0, 1)$ is called the imaginary unit and is denoted by "i"; i. e., $(0, 1) = i$. Also, since the operations in R' and R are essentially the same, and there is a one-to-one correspondence between R' and R , one might as well write $a + b$ instead of $(a, 0) + (b, 0)$

and ab instead of $(a, 0) \cdot (b, 0)$. With this agreement in mind it is more convenient to write $i^2 = i \cdot i = -1$ rather than $(0, 1)^2 = (0, 1) \cdot (0, 1) = (-1, 0)$. It is then seen that i is a solution of $x^2 + 1 = 0$ since $i^2 + 1 = -1 + 1 = 0$.

With the above notation a more convenient representation of a complex number (x, y) can be found. Observe that

$$(x, y) = (x, 0) + (0, y)$$

and

$$\begin{aligned} (0, 1) \cdot (y, 0) &= (0 \cdot y - 1 \cdot 0, 0 \cdot 0 + 1 \cdot y) \\ &= (0, y). \end{aligned}$$

Therefore,

$$\begin{aligned} (x, y) &= (x, 0) + (0, 1) \cdot (y, 0) \\ &= x + iy. \end{aligned}$$

The set C can now be thought of as $\{x + iy \mid x, y \in \mathbb{R} \text{ and } i^2 = -1\}$. In other words, C is the set composed of all real numbers [complex numbers of the form $(x, 0)$] together with all complex numbers of the form (x, y) where $y \neq 0$. A worthwhile activity for the reader would be to restate all the properties of addition and multiplication of complex numbers by employing the new notation. For example, $(x + iy) \cdot (z + iw) = (xz - yw) + i(xw + yz)$ and $(x + iy) + [-(x + iy)] = (x + iy) + (-x) + i(-y) = 0 + i \cdot 0$.

It was shown previously that the equation $x^2 + 1 = 0$ with real coefficients has i as a solution in C . Now $x^2 + 1 = 0$ has no solution in \mathbb{R} . Therefore, it follows that $i \notin \mathbb{R}$. Furthermore, since there is no difference in the structure of the fields \mathbb{R}^1 and \mathbb{R} , no confusion arises

if one considers R as a proper subset of C in an informal and intuitive way. It is also convenient to think of R as a subfield of C .

The field R is also an ordered field. It is natural to ask if C is an ordered field. If C is to be an ordered field, then all elements of C will have to satisfy the order axioms stated on page 99. In particular, consider the element i . Now $i \neq 0$ since $(0, 1) \neq (0, 0)$. So either i is positive or $-i$ is positive. Suppose i is positive, then by O.3 $i \cdot i = -1$ is positive, which is a contradiction. Therefore, i is not positive. Suppose, on the other hand, that $-i$ is positive, then $(-i)(-i) = -1$ is positive, which is also a contradiction. Thus, the imaginary unit fails to satisfy the trichotomy law, and it follows that C cannot be an ordered field.

One of the most significant theorems in algebra, called the Fundamental Theorem of Algebra, was proved by the great mathematician Karl Friedrich Gauss in 1799. For the purposes of this paper it is sufficient to say the theorem states that every quadratic equation, $px^2 + qx + r = 0$, over R has a solution in C .

Perhaps some examples at this point would be illuminating. For instance, the equation $x^2 + 4 = 0$ has a solution in C . Observe that $(2i)(-2i) = 2(-2) \cdot i \cdot i = (-4)(-1) = 4$ since 2 and i are elements of the field C and $i \cdot i = -1$. Therefore, $x^2 + 4 = (x + 2i)(x - 2i) = 0$. In the field C $(x + 2i)(x - 2i) = 0$ implies $x + 2i = 0$ or $x - 2i = 0$. Thus, $x = -2i$ or $x = 2i$. To reiterate, observe how field properties were used to find the solution set $\{2i, -2i\}$.

As a final activity with complex numbers, notice again the utilization of field properties in solving $x^2 + 4x + 13 = 0$. Now $x^2 + 4x + 13 = (x^2 + 4x + 4) + 9$ and $x^2 + 4x + 4 = (x + 2)^2$. Therefore,

$(x + 2)^2 + 9 = 0$. But this is equivalent to $[(x + 2) + 3i][(x + 2) - 3i] = 0$, or $(x + 2 + 3i)(x + 2 - 3i) = 0$. It then follows that $x = -2 - 3i$ or $x = -2 + 3i$. It would be of sufficient value to repay the reader's efforts if one were to complete the problem by proving the converse. That is, if $x = -2 - 3i$ or $x = -2 + 3i$, then $x^2 + 4x + 13 = 0$.

The Congruence Relation

Up to this point the discussion of mathematical systems has centered about structures that are called fields. The field of rational numbers, the field of real numbers, and the field of complex numbers are all infinite systems because the set of elements in each of these fields is an infinite set. On the other hand, the field Z_2 is a finite system since the number of elements in the system is finite. Although they are not fields, the system of natural numbers, the system of whole numbers, and the system of integers are also infinite systems; while the system Z_4 , also not a field, is a finite system. More will be said about finite systems subsequently.

The systems Z_2 and Z_4 are called modular systems. Z_2 is often referred to as the system of integers modulo 2, where 2 is called the modulus. The addition in this system is called "addition modulo 2" while multiplication in this system is called "multiplication modulo 2." It is convenient to write "mod 2" instead of "modulo 2." The system Z_4 is the system of integers mod 4, where 4 is the modulus, and the operations are "addition mod 4" and "multiplication mod 4."

Actually, for any integer m such that $m > 1$, one could construct the system of integers mod m , denoted by Z_m . The procedure would be similar to that for constructing Z_2 and Z_4 . Notice that the elements

in Z_2 are 0 and 1, which are the only possible remainders when an integer is divided by 2. Similarly, the elements in Z_4 [0, 1, 2, and 3] are the only candidates for remainders when an integer is divided by 4. The set of remainders obtained when dividing integers by m is $Z_m = \{0, 1, 2, \dots, m-1\}$ according to the Division Algorithm, which is stated here for reference.

For all $a, b \in Z$ such that $b > 0$, there exist unique

integers q and r such that $a = bq + r$, where $0 \leq r < b$.

The foregoing comments provide a basis for the study of congruence relations on the set Z of integers.

For all $a, b, m \in Z$ such that $m > 0$, a is congruent to b modulo m iff $a - b$ is a multiple of m . This congruence relation is symbolized as " $a \equiv b(\text{mod } m)$." Thus, $a \equiv b(\text{mod } m)$ iff there exists $k \in Z$ such that $a - b = km$.

On the other hand, $a - b$ is not a multiple of m iff a is not congruent to b modulo m . This is written as

" $a \not\equiv b(\text{mod } m)$."

To illustrate, one can say that $42 \equiv 10(\text{mod } 8)$, $-4 \equiv 17(\text{mod } 7)$, and $41 \equiv -39(\text{mod } 2)$ because $42 - 10 = 32$, a multiple of 8; $-4 - 17 = -21$, a multiple of 7; and $41 - (-39) = 80$, a multiple of 2. Observe that $15 \not\equiv 3(\text{mod } 8)$, $-11 \not\equiv -3(\text{mod } 7)$, and $17 \not\equiv 4(\text{mod } 2)$ since $15 - 3 = 12$, $-11 - (-3) = -8$, and $17 - 4 = 13$ are not multiples of 8, 7, and 2, respectively. Note that 42 and 10 have the same remainder when divided by 8; -6 and 15 have the same remainder when divided by 7; while 41 and -39 have the same remainder when divided by 2. This is easily seen by using the division algorithm.

$$42 = 8 \cdot 5 + \underline{2} \quad \text{and} \quad 10 = 8 \cdot 1 + \underline{2}; \quad \text{thus, } 42 \equiv 10 \pmod{8}.$$

$$-4 = 7 \cdot (-1) + \underline{3} \quad \text{and} \quad -17 = 7 \cdot 2 + \underline{3}; \quad \text{thus, } -4 \equiv -17 \pmod{7}.$$

$$41 = 2 \cdot 20 + \underline{1} \quad \text{and} \quad -39 = 2 \cdot (-20) + \underline{1}; \quad \text{thus, } 41 \equiv -39 \pmod{2}.$$

Probably the reader has already surmised that there is some connection between two integers being congruent and these same two integers having the same remainder when divided by a positive integer m . That these two statements are equivalent is the content of the following theorem.

Theorem 4.1. For all $a, b, m \in \mathbb{Z}$ such that $m > 0$, $a \equiv b \pmod{m}$ iff a and b have the same remainder when divided by m .

Proof: Suppose $a \equiv b \pmod{m}$, then by definition there exists $k \in \mathbb{Z}$ such that $a - b = km$. By the division algorithm there exist unique integers q, p, r , and s such that $a = qm + r$ and $b = pm + s$, where $0 \leq r < m$ and $0 \leq s < m$. Therefore, $a - b = km = (q - p)m + (r - s)$, and it must be true that m divides $r - s$ since m divides km and m divides $(q - p)m$. If m divides $r - s$, then m must also divide $-(r - s) = s - r$.

If $s < r$, then $0 < r - s$ and $r - s < m - s < m$. Hence, $0 < r - s < m$. Now m must divide $r - s$. Since there is no positive integer less than m that is a multiple of m , the assumption that $s < r$ must be false. On the other hand, assume that $s > r$, then $s - r > 0$. Now $m > m - r > s - r$, and it follows that $m > s - r > 0$. But m cannot divide $s - r$ if $s - r > 0$. So the assumption that $s > r$ is false. Thus $s \neq r$. By the trichotomy law it must be true that $r = s$. So a and b have the same remainder when divided by m .

Conversely, suppose that a and b have the same remainder r when divided by m ; i. e., $a = qm + r$ and $b = pm + r$. It is then true that $a - b = (q - p)m + (r - r)$, or equivalently $a - b = (q - p)m$. Since $q - p \in \mathbb{Z}$, it follows that $a - b$ is a multiple of m . So $a \equiv b \pmod{m}$.

The mathematical systems that result from congruence relations on \mathbb{Z} are significant in connection with many different and varied topics in mathematics. The importance stems from the fact that the congruence relation on \mathbb{Z} is an equivalence relation for all moduli greater than one.

The Reflexive Property. For all $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$. This is proved very easily by observing that for all $a \in \mathbb{Z}$, $a - a = 0$ and 0 is a multiple of m .

The Symmetric Property. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$. To prove this note that $a \equiv b \pmod{m}$ means that there exists $k \in \mathbb{Z}$ such that $a - b = km$. Now $-(a - b) = -(km)$, and it follows that $b - a = (-k)m$. Therefore, $b \equiv a \pmod{m}$. Hence, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

The Transitive Property. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. Observe that $a \equiv b \pmod{m}$ implies there exists $k \in \mathbb{Z}$ such that $a - b = km$, and $b \equiv c \pmod{m}$ implies that there exists $l \in \mathbb{Z}$ such that $b - c = lm$. Hence, $(a - b) + (b - c) = km + lm$, and it is seen that $a - c = (k + l)m$. Since $k + l \in \mathbb{Z}$, it is then true that $a \equiv c \pmod{m}$. Thus, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

The congruence relation, being an equivalence relation on Z , will partition Z into equivalence classes, i. e., pairwise disjoint subsets of Z whose union is equal to Z . For all $a \in Z$, $[a] = \{x \in Z \mid x \equiv a \pmod{m}\}$ is the equivalence class containing the integer a , or the equivalence class determined by a . Of more than passing interest is the problem of deciding just how many equivalence classes there will be. This question can be settled by using the result of the following theorem.

Theorem 4.2. For all $a, b \in Z$, let $[a]$ and $[b]$ be the equivalence classes determined by the congruence relation mod m . If $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Proof: If $[a] \cap [b] \neq \emptyset$, then there exists $x \in [a] \cap [b]$. So $x \in [a]$ and $x \in [b]$, and it follows that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{m}$. Now the congruence relation is symmetric, hence $a \equiv x \pmod{m}$. Since $a \equiv x \pmod{m}$ and $x \equiv b \pmod{m}$, it follows by the transitive property that $a \equiv b \pmod{m}$.

To prove that $[a] = [b]$ it will be shown that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. For all $y \in [a]$, $y \equiv a \pmod{m}$. Since $a \equiv b \pmod{m}$, it follows that $y \equiv b \pmod{m}$ by the transitive property. Now $y \equiv b \pmod{m}$ means that $y \in [b]$. Therefore, $[a] \subseteq [b]$.

On the other hand, for all $y \in [b]$, $y \equiv b \pmod{m}$. Now $a \equiv b \pmod{m}$ implies that $b \equiv a \pmod{m}$ by the symmetric property. So $y \equiv b \pmod{m}$ and $b \equiv a \pmod{m}$ implies that $y \equiv a \pmod{m}$ because of the transitive property. Hence, $y \in [a]$ and $[b] \subseteq [a]$. Thus, it is true that $[a] = [b]$.

Corollary: For all $a, b \in \mathbb{Z}$, $a \equiv b \pmod{m}$ iff $[a] = [b]$.

Proof: It was shown in the proof of Theorem 4.2 that $a \equiv b \pmod{m}$ implies $[a] = [b]$. The converse is proved by observing that $[a] = [b]$ implies $a \in [b]$. Hence, it follows that $a \equiv b \pmod{m}$.

Notice that the contrapositive of Theorem 4.2 is also true. That is, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$. The theorem together with the contrapositive guarantee that the disjunction, $[a] \cap [b] = \emptyset \vee [a] = [b]$, is true.

By the division algorithm there is a unique remainder whenever an integer is divided by m , and this is one of the m possible remainders $0, 1, 2, \dots, m - 1$. Suppose that r and s are any two of these possible remainders such that $[r] \cap [s] \neq \emptyset$, then by Theorem 4.2 it follows that $[r] = [s]$. Therefore, $r \equiv s \pmod{m}$, or $r - s$ is a multiple of m .

Now r and s satisfy the inequalities $0 \leq r < m$ and $0 \leq s < m$. It then follows by Theorem 3.35 that $-m < -s \leq 0$. But then, by Theorem 3.32, $-m + r < -s + r \leq r$, or equivalently $-m + r < r - s \leq r$. Now $0 \leq r$ implies that $-m \leq -m + r$ also by Theorem 3.32. The fact that $r < m$ together with the preceding inequalities imply that $-m \leq -m + r < r - s \leq r < m$. Hence, $-m < r - s < m$ by the transitive property of inequalities. Now $r - s$ is a multiple of the positive integer m and satisfies the inequality $-m < r - s < m$. But every positive multiple of m is greater than m and every negative multiple of m is less than m . Hence, it must be true that $r - s = 0$. Therefore, $r = s$.

So if $[r] \cap [s] \neq \emptyset$, then $r = s$. Thus, the contrapositive — if $r \neq s$, then $[r] \cap [s] = \emptyset$ — reveals that the equivalence classes $[0], [1], \dots$, and $[m - 1]$ are all unique.

Since every integer has one and only one of the distinct remainders when divided by m and every integer is congruent to its remainder, it follows that every integer is in one and only one of the m distinct equivalence classes $[0], [1], \dots, [m - 1]$. Because of this fact the union of all the m equivalence classes is just the set Z .

The five distinct equivalence classes mod 5 are as follows:

$$[0] = \{x \in Z \mid x \equiv 0(\text{mod } 5)\} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$[1] = \{x \in Z \mid x \equiv 1(\text{mod } 5)\} = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$[2] = \{x \in Z \mid x \equiv 2(\text{mod } 5)\} = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$[3] = \{x \in Z \mid x \equiv 3(\text{mod } 5)\} = \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$[4] = \{x \in Z \mid x \equiv 4(\text{mod } 5)\} = \{\dots, -6, -1, 4, 9, 14, \dots\}$$

The congruence relation and the equals relation are both equivalence relations. Some of the other important properties of the equals relation on R and also on Z are the following:

(1) If $a = b$ and $c = d$, then $a + c = b + d$.

(2) If $a + c = b + c$, then $a = b$.

(3) If $a = b$ and $c = d$, then $ac = bd$.

The above properties are also true when the relation is the congruence relation mod m . They are stated and proved in the next three theorems.

Theorem 4.3. For all $a, b, c, d \in Z$, if $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then $a + c \equiv b + d(\text{mod } m)$.

Proof: If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then there exist $k, \ell \in Z$ such that $a - b = km$ and $c - d = \ell m$. Hence, $(a - b) + (c - d) =$

$km + \ell m$, which is equivalent to $(a + c) - (b + d) = (k + \ell)m$ by Theorem 3.21 and Axiom MA. Thus, $a + c \equiv b + d \pmod{m}$.

A particular instance of Theorem 4.3 occurs when $c = d$. One would then have the useful result that $a + c \equiv b + c \pmod{m}$. For example, $42 \equiv 7 \pmod{5}$; therefore, $42 + 129 \equiv 7 + 129 \pmod{5}$.

Theorem 4.4. For all $a, b, c \in \mathbb{Z}$, if $a + c \equiv b + c \pmod{m}$, then $a \equiv b \pmod{m}$.

Proof: Suppose $a + c \equiv b + c \pmod{m}$, then there exists $k \in \mathbb{Z}$ such that $(a + c) - (b + c) = km$. But this implies that $(a - b) = km$ by The Corollary to Theorem 3.21. Therefore, $a \equiv b \pmod{m}$.

The reader will surely recognize Theorem 4.4 as being a cancellation law corresponding to the cancellation law for addition of integers. The above property of congruences is called the cancellation law for addition mod m. For an illustration of this law consider $97 \equiv 41 \pmod{8}$. This congruence is the same as $57 + 40 \equiv 1 + 40 \pmod{8}$. Thus, $57 \equiv 1 \pmod{8}$ by Theorem 4.4.

Theorem 4.5. For all $a, b, c, d \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then there exist $k, \ell \in \mathbb{Z}$ such that $a - b = km$ and $c - d = \ell m$. So $(a - b)c = (km)c$ and $b(c - d) = b(\ell m)$, or $ac - bc = (kc)m$ and $bc - bd = (b\ell)m$. Therefore, $(ac - bc) + (bc - bd) = (kc + b\ell)m$. But $(ac - bc) + (bc - bd) = ac - bd$ by the Corollary to Theorem 3.21, so it follows that $ac - bd = (kc + b\ell)m$. Thus, $ac \equiv bd \pmod{m}$.

An immediate consequence of Theorem 4.5 results if $c = d$. The conclusion would then be that $ac \equiv bc \pmod{m}$. It is true that $32 \equiv 8 \pmod{12}$, so by Theorem 4.5 it follows that $32(-2) \equiv 8(-2) \pmod{12}$, or $-64 \equiv -16 \pmod{12}$.

To see that the cancellation law for multiplication mod m does not hold in general, examine the congruence $16 \equiv 24 \pmod{4}$. Now this is equivalent to $4 \cdot 4 \equiv 6 \cdot 4 \pmod{4}$, but this does not imply that $4 \equiv 6 \pmod{4}$. That is, $4 \not\equiv 6 \pmod{4}$. However, under certain conditions there is a cancellation law for multiplication mod m . This modified cancellation law is stated in the following theorem. For proofs of the divisibility theorems used in the proof of the theorem see Peterson and Hashisaki [26].

Theorem 4.6. For all $a, b, c \in \mathbb{Z}$, if $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Proof. Since d is the greatest common divisor of c and m , there exist $c', m' \in \mathbb{Z}$ such that $c = c'd$ and $m = m'd$, where $(c', m') = 1$. If $ac \equiv bc \pmod{m}$, then there exists $k \in \mathbb{Z}$ such that $ac - bc = km$. Therefore, $(a - b)c = km$. By substitution it follows that $(a - b)(c'd) = k(m'd)$, or $(a - b)c'd = (km')d$. Therefore $(a - b)c' = km'$ by the cancellation law for multiplication of integers (Theorem 3.25).

Since m' divides km' , it must be true that m' divides $a - b$ or m' divides c' . But m' cannot divide c' since $(c', m') = 1$. Therefore, m' divides $a - b$, or equivalently there exists $\ell \in \mathbb{Z}$ such that $a - b = \ell m'$. This is equivalent to $a - b = \ell(m/d)$ since $m' = m/d$. Hence, $a \equiv b \pmod{m/d}$.

Consider the congruence $128 \equiv 32 \pmod{12}$, or $16 \cdot 8 \equiv 4 \cdot 8 \pmod{12}$. The greatest common divisor of 8 and 12 is 4. So by Theorem 4.6, $16 \equiv 4 \pmod{3}$. Another illustration is $117 \equiv 45 \pmod{12}$. In this case $13 \cdot 9 \equiv 5 \cdot 9 \pmod{12}$ and $(9, 12) = 3$. Hence, $13 \equiv 5 \pmod{4}$.

In Theorem 4.6 if the greatest common divisor of c and m is 1; i. e., $(c, m) = 1$, then it follows immediately that $a \equiv b \pmod{m}$. From the congruence $12 \cdot 5 \equiv 4 \cdot 5 \pmod{8}$ one can conclude that $12 \equiv 4 \pmod{8}$ since $(5, 8) = 1$.

Before the subject of congruences is abandoned, perhaps it would be beneficial to meditate momentarily on the equivalence classes determined by the congruence mod m . Perchance the reader has already conjectured that there is some connection between these m equivalence classes and the system of integers mod m . Is it possible to define binary operations on the set of equivalence classes, $\{[0], [1], \dots, [m-1]\}$? The answer is yes, and two operations are defined as follows.

Denote the set of equivalence classes by $\overline{\mathbb{Z}}_m$, and let "+" and "." symbolize the operations of "addition" and "multiplication" on $\overline{\mathbb{Z}}_m$. The operations are defined in the following manner.

$$\text{For all } [a], [b] \in \overline{\mathbb{Z}}_m, [a] + [b] = [a + b].$$

$$\text{For all } [a], [b] \in \overline{\mathbb{Z}}_m, [a] \cdot [b] = [ab].$$

Notice that the symbol "+" is being used to represent two operations, "addition" of equivalence classes and addition of integers. The symbol "." means "multiplication" of equivalence classes while juxtaposition is used to denote multiplication of integers. Furthermore, the definition of addition of elements in $\overline{\mathbb{Z}}_m$ states that the result of the

operation being performed on $[a]$ and $[b]$ is the class containing $a + b$, i. e., $[a + b]$. On the other hand, the definition of multiplication of elements in \bar{Z}_4 says that the equivalence class containing ab is the result of multiplying the classes $[a]$ and $[b]$.

Since every integer is contained in one and only one of the m classes in \bar{Z}_4 , it follows that both $[a + b]$ and $[ab]$ will be elements of \bar{Z}_4 . That is, $a + b \equiv r \pmod{m}$ and $ab \equiv s \pmod{m}$ for some $r, s \in Z_4$. It still remains to decide whether these equivalence classes are unique. In other words, would it be possible to choose other representatives of the classes $[a]$ and $[b]$ such that the results of the operations would be classes different from $[a + b]$ and $[ab]$?

Suppose $c \in [a]$ and $d \in [b]$, then by Theorem 4.2 it follows that $[c] = [a]$ and $[d] = [b]$. Now $[c] + [d] = [c + d]$ by the definition of addition. But $c \in [a]$ implies that $c \equiv a \pmod{m}$ and $d \in [b]$ implies that $d \equiv b \pmod{m}$. By Theorem 4.3 this means that $c + d \equiv a + b \pmod{m}$. Hence, $c + d \in [a + b]$. Therefore, $[c + d] = [a + b]$ by Theorem 4.2. Thus, the "answer" is unique whenever two classes are added regardless of the representatives of those classes that are chosen, and so addition is a binary operation on \bar{Z}_4 .

Similarly, it can be concluded that $[cd] = [ab]$ whenever $[c] = [a]$ and $[d] = [b]$. The proof here would parallel the one above with the exception that Theorem 4.5 would be used instead of Theorem 4.3; therefore, the proof that multiplication of equivalence classes is a binary operation on \bar{Z}_m will be omitted.

The reader should be "conditioned" to the point that the next logical consideration would be to examine the two binary operations on \bar{Z}_m to determine what properties they enjoy. The fact that the opera-

tions of addition and multiplication are binary operations on \overline{Z}_m permits one to say that the closure laws are satisfied.

Commutative laws. For all $[a], [b] \in \overline{Z}_m$, $[a] + [b] = [b] + [a]$ and $[a] \cdot [b] = [b] \cdot [a]$.

Proof:

$$\begin{aligned} [a] + [b] &= [a + b] && \text{[definition of addition]} \\ &= [b + a] && \text{[Axiom A. 2]} \\ &= [b] + [a] && \text{[definition of addition]} \end{aligned}$$

The proof that multiplication is commutative is similar and will be omitted.

Associative laws. For all $[a], [b], [c] \in \overline{Z}_m$, $([a] + [b]) + [c] = [a] + ([b] + [c])$ and $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$.

Proof:

$$\begin{aligned} ([a] \cdot [b]) \cdot [c] &= [ab] \cdot [c] && \text{[definition of multiplication]} \\ &= [(ab)c] && \text{[definition of multiplication]} \\ &= [a(bc)] && \text{[Axiom M. 3]} \\ &= [a] \cdot [bc] && \text{[definition of multiplication]} \\ &= [a] \cdot ([b] \cdot [c]) && \text{[definition of multiplication]} \end{aligned}$$

Similarly, one could verify the associative law for addition.

Distributive law. For all $[a], [b], [c] \in \overline{Z}_m$, $([a] + [b]) \cdot [c] = [a] \cdot [c] + [b] \cdot [c]$.

Proof:

$$\begin{aligned}
 ([a] + [b]) \cdot [c] &= [a + b] \cdot [c] && \text{[definition of addition]} \\
 &= [(a + b)c] && \text{[definition of multiplication]} \\
 &= [ac + bc] && \text{[rdpma]} \\
 &= [ac] + [bc] && \text{[definition of addition]} \\
 &= [a] \cdot [c] + [b] \cdot [c] && \text{[definition of multiplication]}
 \end{aligned}$$

Because of the commutative law for addition and multiplication of equivalence classes, it can be shown very easily that $[c] \cdot ([a] + [b]) = [c] \cdot [a] + [c] \cdot [b]$.

Since 0 is the additive identity in Z , one would suspect that $[0]$ is the identity element for addition of equivalence classes in \bar{Z}_m . Also, $[1]$ is the identity element for multiplication in \bar{Z}_m .

Identity elements. For all $[a] \in \bar{Z}_m$, $[a] + [0] = [0] + [a] = [a]$ and $[a] \cdot [1] = [1] \cdot [a] = [a]$.

Proof:

$$\begin{aligned}
 [a] + [0] &= [0] + [a] && \text{[commutative law]} \\
 &= [0 + a] && \text{[definition of addition]} \\
 &= [a] && \text{[Axiom A. 4]}
 \end{aligned}$$

Similarly, it follows that $[1]$ is the identity element for multiplication.

Inverse elements for addition. For all $[a] \in \bar{Z}_m$, there exists $[d] \in \bar{Z}_m$ such that $[a] + [d] = [d] + [a] = 0$.

Proof: Note first of all that $[0] + [0] = [0]$. So $[0]$ is its own inverse. Observe also that for each $[a] \in \bar{\mathbb{Z}}_m$, where $0 < a < m$, $[m - a] \in \bar{\mathbb{Z}}_m$ since $0 < m - a < m$. Furthermore, $[m] = [0]$ because $m \equiv 0 \pmod{m}$. Therefore,

$$\begin{aligned}
 [a] + [m - a] &= [a + (m - a)] && \text{[definition of addition]} \\
 &= [a + (-a + m)] && \text{[Theorem 3.19]} \\
 &= [(a + (-a)) + m] && \text{[Axiom A. 3]} \\
 &= [0 + m] && \text{[Axiom A. 5]} \\
 &= [m] && \text{[Axiom A. 4]} \\
 &= [0] && \text{[[m] = [0]]}
 \end{aligned}$$

In particular, inspect the elements in $\bar{\mathbb{Z}}_6$. Since $[1] + [5] = [0]$, $[2] + [4] = 0$, and $[3] + [3] = 0$, it follows that $[1]$ and $[5]$ are inverses of each other, $[2]$ and $[4]$ are inverses of each other, while $[3]$ is its own inverse.

Unfortunately the momentum that was accumulated in verifying the above laws has been lost at this juncture. Hopefully $\bar{\mathbb{Z}}_m$ together with the binary operations of addition and multiplication would constitute a field, but this is not always the case. The only thing lacking for $\bar{\mathbb{Z}}_m$ to be a field is for every $a \neq 0$ to have a multiplicative inverse. In other words, for any $m > 0$, $\bar{\mathbb{Z}}_m$ satisfies all field properties except possibly Axiom M. 5.

Perhaps by constructing addition and multiplication tables for several different moduli, information can be obtained regarding the multiplicative inverse property.

The first two examples submitted here will no doubt resemble

other Cayley squares with which the reader is already acquainted.

These are \bar{Z}_2 and \bar{Z}_4 . The addition and multiplication tables for \bar{Z}_2 appear in Figure 43, while those for \bar{Z}_4 appear in Figure 44.

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Figure 43.

Note that there is a one-to-one correspondence between $\bar{Z}_2 = \{[0], [1]\}$ and $Z_2 = \{0, 1\}$. Now $[1] \neq [0]$ and $[1] \cdot [1] = [1]$. Hence, $[1]$ is the multiplicative inverse of $[1]$. Since operations in \bar{Z}_2 satisfy all the other field properties, it follows that \bar{Z}_2 is a field. A further observation reveals that the operations "+" and "·" behave in \bar{Z}_2 just like the corresponding operations in Z_2 . Structurally there is no difference in the two systems.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Figure 44.

It is already known that the system \bar{Z}_4 , i. e., the set \bar{Z}_4 together with the properties of addition and multiplication, satisfies at least every field axiom except possibly the multiplicative inverse property. An examination of the tables for the binary operations in \bar{Z}_4 might be revealing.

A close look at the multiplication table in Figure 44 discloses that there is no $[a] \in \bar{Z}_4$ such that $[2] \cdot [a] = 1$. Since the one element $[2]$ fails to have a multiplicative inverse, \bar{Z}_4 cannot be a field. It can be remarked further that the cancellation law does not hold since $[2] \cdot [2] = [0] \cdot [2]$, but $[2] \neq [0]$. Note that this is consistent with the statement $2 \cdot 2 \equiv 0 \cdot 2 \pmod{4}$, but $2 \not\equiv 0 \pmod{4}$.

Also, the reader should be convinced that the structure of \bar{Z}_4 is the same as that for Z_4 even though the elements in the sets are quite different. The elements in \bar{Z}_4 are equivalence classes while the elements in Z_4 are integers.

Before making a generalization about the conditions under which \bar{Z}_m , together with "+" and "." will be a field, two final examples should provide the motivation. To repeat, for all $m > 0$, \bar{Z}_m satisfies at least every field property except possibly the multiplicative inverse axiom. Therefore, attention will be given to these concluding examples without the aid of Cayley squares.

Consider \bar{Z}_5 and \bar{Z}_6 . In \bar{Z}_5 $[1] \cdot [1] = [1]$, $[2] \cdot [3] = [1]$, and $[4] \cdot [4] = 1$. Hence, for every $[a] \in \bar{Z}_5$ such that $[a] \neq [0]$, it is true that $[a]$ has a multiplicative inverse. Thus, \bar{Z}_5 is a field. On the other hand, in \bar{Z}_6 $[2]$ has no multiplicative inverse because $[2] \cdot [0] = [0]$, $[2] \cdot [1] = [2]$, $[2] \cdot [2] = [4]$, $[2] \cdot [3] = [0]$, $[2] \cdot [4] = [2]$, and $[2] \cdot [5] = [4]$. It is also true that $[3]$ and $[4]$ have no multiplicative

inverses. Therefore, \overline{Z}_6 is not a field.

In the above examples a prime modulus resulted in a field while a composite modulus yielded a system that is not a field. More will be said about systems that are not fields later in this chapter, but for the present one might wonder if a prime modulus always produces a system that is a field. The answer is in the affirmative.

Theorem 4.7. Let p be a positive prime. For all $[a] \in \overline{Z}_p$ such that $[a] \neq [0]$, there exists $[x] \in \overline{Z}_p$ such that $[a] \cdot [x] = [1]$.

Proof: Since $[a] \neq [0]$, it follows that $a \not\equiv 0 \pmod{p}$. In other words, a is not a multiple of p . Hence, a and p are relatively prime; i. e., $(a, p) = 1$. Therefore, there exist $x, y \in Z$ such that $ax + py = 1$. This implies that $ax - 1 = p(-y)$. So $ax - 1$ is a multiple of p , hence $ax \equiv 1 \pmod{p}$. Therefore, $[ax] = [1]$, or $[a] \cdot [x] = 1$.

For a proof of the statement that there exist $x, y \in Z$ such that $ax + py = 1$ whenever $(a, p) = 1$, the reader may refer to Hamilton and Landin [15] or McCoy [23]. The essential point to emphasize in this discourse is that \overline{Z}_p , where p is a positive prime, is a field.

Groups

The previous pages of this paper have been concerned with a systematic study of fields, especially the field of real numbers. An attempt has been made to emphasize the idea of structure that a field possesses in a way that will be meaningful to elementary teachers.

No particular significance would be associated with the binary operations of addition and multiplication on a set if they did not possess some interesting properties. Just the idea of a binary operation by

itself would certainly lead to a fruitless study of the set on which the operation is defined.

In the preceding chapter some examples were given of mathematical systems, or algebraic structures, that did not qualify to be called fields. It is interesting to study systems in which the binary operations only satisfy some of the field properties. Such systems are less restricted in the sense that fewer restrictions are imposed on the elements. It is the purpose of this section to consider systems which involve only one binary operation. Several examples of such systems will arise quite naturally from mathematical systems that have already been given careful attention.

It was convenient to refer to the binary operations in a field as addition and multiplication. The names are really not important so long as it is known how the operation is defined. Again the main concern is the properties of a binary operation. By closely examining again the field axioms on page 80, one recognizes that the pairs of Axioms A. 1 and M. 1, A. 2 and M. 2, A. 3 and M. 3, A. 4 and M. 4, A. 5 and M. 5 are statements about the same algebraic concepts; namely, closure, commutativity, associativity, identity element, and inverse elements, respectively. However, it should be pointed out hastily that the statement in M. 5 is only about all elements distinct from the additive identity. Conceivably there are systems with only one binary operation defined which enjoys the common properties possessed by addition and multiplication in a field.

The abstract mathematical system that will be defined henceforth is less familiar than a field. Notice the weaker restrictions imposed on the elements in the following definition.

A group is a structure consisting of a binary operation, denoted here by " $*$ ", defined on a non-empty set G that satisfies the following:

- G. 1. Closure. For all $a, b \in G$, $a * b$ is a unique element in G .
- G. 2. Associative law. For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- G. 3. Identity element. There exists $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
- G. 4. Inverse elements. For each $a \in G$ there exists an inverse element $a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a = e$.

In addition to the above stated axioms for a group, if the following axiom holds, then the group is said to be a commutative group or Abelian group.

- G. 5. Commutative law. For all $a, b \in G$, $a * b = b * a$.

Let $G = \mathbb{Z}$, the set of integers, and let the binary operation be multiplication. Axiom M. 3 states that multiplication is associative and Axiom M. 4 states that 1 is the identity element. However, G. 4 does not hold since every integer does not have a multiplicative inverse in \mathbb{Z} . Therefore, \mathbb{Z} is not a multiplicative group; that is, the system consisting of \mathbb{Z} and the operation of multiplication is not a group.

If $G = \mathbb{Q} - \{0\}$ and the binary operation is multiplication of rational numbers, then G is a group. The associative law certainly holds because of M. 3. The identity element is 1, and every element in G has a multiplicative inverse by M. 5. So G is indeed a group. Furthermore, G is a commutative group since M. 2 holds.

Recall that $\overline{\mathbb{Z}}_4$ is not a field. However, $\overline{\mathbb{Z}}_4$ under addition satisfies all the group axioms including G. 5. Therefore, it can be

said that \bar{Z}_4 is an additive, commutative group.

Consider the set Z under ordinary addition. Here also, axioms G. 1 - G. 5 are satisfied. So Z is an additive, commutative group.

Any field F under addition is an additive, Abelian group; but care must be exercised when the operation of multiplication is considered because of the additive identity 0. The set $F - \{0\}$ under multiplication qualifies to be a multiplicative, Abelian group.

The discussion of the finite system $F = \{e, o\}$, where e represents the even integers and o represents the odd integers, disclosed that computation can become quite tedious when checking to see if a binary operation enjoys the associative property. In this example the writer pointed out that eight different statements needed to be verified in order to be positive that the associative property does indeed hold. On the other hand, the Cayley table for the operation "+" revealed quite readily that the closure law is satisfied, e is the identity element, the operation is commutative, and every element has an inverse.

The example of Figure 13 on page 59 involved the system consisting of $T = \{a, b, c, d\}$ and the binary operation "?" defined on T . It was shown by finding a counter example, namely, $(b ? b) ? a \neq b ? (b ? a)$, that the operation does not satisfy the associative law. Thus, T is not a group.

If one did not have a particular counter example in mind relative to associativity in the above mentioned system T , then an exhaustive examination of 64 different statements might have been necessary before a counter example was found. Furthermore, checking for associativity in a system containing five elements would necessitate verifying 125 different statements. One would certainly be discouraged

before this exhaustive activity had terminated.

Fortunately there are methods by which associativity can be checked without having to test all possibilities. Zassenhaus [35] developed a technique that reduces the number of computations substantially. This method is called the "rectangle rule," and it requires that the entries in the Cayley table be rearranged so that the identity element appears in every entry along the main diagonal of the table, that is, from the upper left corner to the lower right corner.

Before discussing Zassenhaus' method it should be pointed out that a loop is a system, or structure, in which the group axioms G.1, G.3, and G.4 hold. A loop is then a group if Axiom G.2, the associative law, holds.

Consider the set $S = \{a, b, c, d\}$ with binary operation $*$ defined on S by the Cayley square in Figure 45.

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

Figure 45.

It is not difficult to conclude that S is closed with respect to $*$ and that a is the identity element for $*$. Furthermore, the table reveals that

a, d, c, and b are the inverses for a, b, c, and d, respectively. However, it is not known at this point that S under the operation * is a group since the associative law has not been verified.

To employ the method of Zassenhaus, it is necessary to rearrange the entries of the table so that the identity element appears in every position along the main diagonal. In doing this it is convenient to disregard the elements of S that are listed in the extreme left column and the extreme top row of the Cayley square. This result is depicted by Figure 46.

a	d	c	b
b	a	d	c
c	b	a	d
d	c	b	a

Figure 46.

Observe that every element in the table of Figure 46 can be identified according to the row and column in which it appears. Since each of the elements a, b, c, and d appears several times in the table, it is essential to be able to specify which entry is being considered. Let it be agreed to denote the position of an element in the table by employing an ordered pair. The first component will designate the row in which the element appears, and the second component will designate the column. For instance, the notations $d_{(1, 2)}$, $b_{(3, 2)}$, $c_{(2, 4)}$,

and $a_{(2, 2)}$ refer to d in the first row and second column, b in the third row and second column, c in the second row and fourth column, and a in the second row and second column, respectively. A word of caution is in order. The symbols $b_{(1, 4)}$, $b_{(3, 2)}$, and $b_{(4, 3)}$ all represent the same element b of the set S. The ordered pair notation simply specifies position in the table of Figure 46. Similar observations can be made about the elements a, c, and d. By using this new notation the array in Figure 47 is obtained.

$a_{(1, 1)}$	$d_{(1, 2)}$	$c_{(1, 3)}$	$b_{(1, 4)}$
$b_{(2, 1)}$	$a_{(2, 2)}$	$d_{(2, 3)}$	$c_{(2, 4)}$
$c_{(3, 1)}$	$b_{(3, 2)}$	$a_{(3, 3)}$	$d_{(3, 4)}$
$d_{(4, 1)}$	$c_{(4, 2)}$	$b_{(4, 3)}$	$a_{(4, 4)}$

Figure 47.

Everything is now in order to begin the computations necessary to find out if the operation $*$ is associative. Choose the element $d_{(1, 2)}$ from row 1 and column 2 of Figure 47. Now "operate" on every element in row 2 of Figure 47 by $d_{(1, 2)}$ "on the left." Observe that every element in the second row has the row component 2. By using the table of Figure 45 to perform these computations the results are:

$$d * b = d_{(1,2)} * b_{(2,1)} = a = a_{(1,1)}$$

$$d * a = d_{(1,2)} * a_{(2,2)} = d = d_{(1,2)}$$

$$d * d = d_{(1,2)} * d_{(2,3)} = c = c_{(1,3)}$$

$$d * c = d_{(1,2)} * c_{(2,4)} = b = b_{(1,4)}$$

Notice that each of the results of the foregoing computations have the same row component as $d_{(1,2)}$. Furthermore, the column components of $a_{(1,1)}$, $d_{(1,2)}$, $c_{(1,3)}$, and $b_{(1,4)}$ are the same as those of $b_{(2,1)}$, $a_{(2,2)}$, $d_{(2,3)}$, and $c_{(2,4)}$, respectively. Actually, since it is known that a is the identity element for $*$, the second of the foregoing computations could be omitted. So there are only three computations involving $d_{(1,2)}$.

Now choose the element $c_{(1,3)}$ and "operate" on every element having row component 3 by $c_{(1,3)}$ "on the left." By omitting the computation involving $a_{(3,3)}$ there are three such computations as follows:

$$c_{(1,3)} * c_{(3,1)} = a_{(1,1)}$$

$$c_{(1,3)} * b_{(3,2)} = d_{(1,2)}$$

$$c_{(1,3)} * d_{(3,4)} = b_{(1,4)}$$

Similarly, there are three computations involving the element $b_{(1,4)}$.

The remaining necessary computations follow the previously established pattern. Each of the remaining three rows in Figure 47 contains three entries that are different from the identity element. There are three necessary computations involving each of these nine entries for a total of twenty-seven computations.

To summarize, let x , y , and z represent elements of S and let

i , j , and k represent elements of the set $\{1, 2, 3, 4\}$. With this agreement $x_{(i,j)}$, $y_{(j,k)}$, and $z_{(i,k)}$ represent entries of Figure 47 that are in row \underline{i} and column \underline{j} , row \underline{j} and column \underline{k} , and row \underline{i} and column \underline{k} , respectively. The method of Zassenhaus states that if $x_{(i,j)} * y_{(j,k)} = z_{(i,k)}$ for all possible computations mentioned previously, then the operation $*$ is associative and hence S is a group.

Using Zassenhaus' method to check the system S for associativity requires a maximum of 64 computations. However, the actual number required in the preceding example was 36 since all computations involving the identity (28 of them) can be disregarded. On the other hand, if one were to check for associativity in the usual manner, then it would be required to check 64 different statements of the form $(x * y) * z = x * (y * z)$, where $x, y, z \in S$. So it is seen that the method of Zassenhaus requires substantially less labor than the usual method for checking associativity.

Watson [31] gave a generalization which improved the rule of Zassenhaus in two ways: the binary operation table does not have to be in any special form; no computations are necessary because identification is made from the pattern of the table.

In explaining this rule Watson states:

The improved rule is this. In the multiplication table of the loop choose any four places forming the vertices of a rectangle. Suppose that the entries in these places are:

q	r
p	s

If this loop is a group then all other rectangles having p, q, r as entries at successive vertices, with p and q sharing a column, will have s as the entry at the fourth vertex. The converse is also true.

To illustrate this method consider again the table of Figure 45. The writer will not attempt to point out all possible rectangles that need to be considered but will select several to illustrate the procedure (Figures 48 and 49).

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

Figure 48.

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

Figure 49.

In Figure 48 the rectangle indicated in the upper left of the table has a, b, and c at successive vertices, a and b in the same column, and b at the fourth vertex. Notice that the rectangle indicated in the lower right of the table also has a, b, and c at successive vertices, a and b in the same column, and b at the fourth vertex. Observe further that these are the only two rectangles in which a and b share a column. Similar observations may be made relative to the rectangles indicated in the upper right and lower left portions of the table.

The three rectangles indicated in the table of Figure 49 have d, b, and c as successive vertices with a at the fourth vertex. Notice that d and b also share the same column in the respective rectangles.

Also note that there are three other rectangles in which d and b share a column, but in these b, d, and c are at successive vertices with a at the fourth vertex. Furthermore, there are three rectangles with a, c, and d at successive vertices with b at the fourth vertex and three with c, a, and d at successive vertices with b at the fourth vertex. In each of these sets of three rectangles a and c share a column in the respective rectangles (see Figure 50).

*	a	b	c	d
a	a-----b	c-----d		
b	b	c-----d	a	
c	c-----d	a-----b		
d	d	a-----b	c	

Figure 50.

The procedure would continue until all possibilities satisfying the conditions of Watson's rule have been exhausted. The reader can see that this method would certainly eliminate any errors resulting from computation. Finally, with a little practice, facility and proficiency could be accomplished in checking finite systems for associativity.

So that the reader is not misled to believe that all groups are commutative, an example of a group that is not commutative will be

given. The basis for this concluding example is taken from a familiar context; namely, that of one-to-one correspondences between sets.

The example will depend on the set $S = \{1, 2, 3\}$ and the one-to-one correspondences that can be established between S and itself. There are three ways that any one of the elements of S can be matched with an element of S ; for instance, 1 can be matched with 1, 2, or 3. After an element has been paired with an element, there are two ways that any one of the two remaining members can be matched with a member. Suppose 1 is matched with 1, then 2 can be matched with either 2 or 3. Finally, after this pairing is made, there is only one way to match the remaining element. Thus, there are $\underline{3} \cdot \underline{2} \cdot \underline{1} = 6$ one-to-one correspondences between S and itself.

A convenient notation will be employed to denote the one-to-one correspondences. One particular correspondence is used to illustrate the procedure:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

In using this notation it is advantageous to have the integers 1, 2, and 3 arranged in order in the top row. It is then understood that the correspondence illustrated above matched 1 with 2, 2 with 3, and 3 with 1.

Using this scheme it is not difficult to list all the one-to-one correspondences between set S and itself. However, to facilitate the construction of a Cayley square using these correspondences, a shorter name for each correspondence is essential. The one-to-one correspondences together with their shorthand names are as follows:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad E = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

It is now convenient to let G be the set of all one-to-one correspondences between S and itself; i. e., $G = \{I, A, B, C, D, E\}$.

The objective is to define a binary operation $*$ on G so that, hopefully, G will be a group. To introduce the procedure suppose there is a one-to-one correspondence between twelve pupils and twelve chairs. If there is also a one-to-one correspondence between the twelve chairs and twelve pencils, then it follows that a similar correspondence exists between pupils and pencils. In other words, a one-to-one correspondence followed by another one will result in a one-to-one correspondence. In considering the members in G for instance, $A * B$ means "the correspondence A followed by the correspondence B ." $A * B$ is also a one-to-one correspondence between S and itself.

$$A * B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = C$$

Since A , i. e., the one-to-one correspondence A , matches 1 with 1 and B matches 1 with 2, it follows that $A * B$ matches 1 with 2. Also, A pairs 2 with 3 and B pairs 3 with 3; therefore, $A * B$ pairs 2 with 3. Finally, A matches 3 with 2, B matches 2 with 1, and $A * B$ matches 3 with 1. So $A * B = C$.

The correspondence I matches every element of set S with itself.

It is interesting to note the effect I has on some other correspondence whenever the operation $*$ is performed.

$$I * D = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = D$$

The computation here is easy and the details are omitted. Similarly, it can be seen that D followed by I is also D. Thus $I * D = D * I = D$. Hence, it appears as though I is the identity element for $*$.

Before exhibiting the Cayley table for the binary operation $*$ on G, perhaps a detailed computation involving an element of G and its inverse will be beneficial. Consider $C * D$.

$$C * D = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

The correspondence C matches 1 with 2, 2 with 3, and 3 with 2; while D matches 2 with 1, 3 with 2, and 1 with 3. Putting these together and using the fact that $C * D$ means C followed by D, one sees that $C * D = I$. Similarly, $D * C = I$. Therefore, C and D are inverses of each other.

Since G contains 6 elements, a total of 36 computations need to be performed in order to exhibit the complete Cayley table. However the remaining computations will not be performed here. The table is displayed as Figure 51 without further details.

If one were not convinced before that $*$ is a binary operation, there should be no doubt that it is indeed after studying Figure 51. Other nice things revealed by the table are: I is the identity element for $*$, and every element has an inverse. The inverses of I, A, B, C, D,

*	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	C	B	E	D
B	B	D	I	E	A	C
C	C	E	A	D	I	B
D	D	B	E	I	C	A
E	E	C	D	A	B	I

Figure 51.

and E are I, A, B, D, C, and E, respectively.

If G under the operation $*$ is to be a group, then the associative law must hold. There are three alternatives to consider in reaching a decision; do all the necessary computation involving elements of G , use the method of Zassenhaus [35] or Watson [31], or find a more general approach that is less demanding. For this example the latter is preferred.

Suppose a correspondence associates an element x with y , another associates y with z , and a third associates z with w . By using the notation that was agreed on and only indicating the above mentioned associations, observe the following:

$$\left[\left(\begin{array}{ccccccc} \cdot & \cdot & \cdot & x & \cdot & \cdot & \cdot \\ & & & \downarrow & & & \\ \cdot & \cdot & \cdot & y & \cdot & \cdot & \cdot \end{array} \right) * \left(\begin{array}{ccccccc} \cdot & \cdot & \cdot & y & \cdot & \cdot & \cdot \\ & & & \downarrow & & & \\ \cdot & \cdot & \cdot & z & \cdot & \cdot & \cdot \end{array} \right) \right] * \left(\begin{array}{ccccccc} \cdot & \cdot & \cdot & z & \cdot & \cdot & \cdot \\ & & & \downarrow & & & \\ \cdot & \cdot & \cdot & w & \cdot & \cdot & \cdot \end{array} \right) = \left(\begin{array}{ccccccc} \cdot & \cdot & \cdot & x & \cdot & \cdot & \cdot \\ & & & \downarrow & & & \\ \cdot & \cdot & \cdot & w & \cdot & \cdot & \cdot \end{array} \right)$$

On the other hand, by reassociating one obtains

$$\left(\begin{array}{cccc} \dots & x & \dots & \dots \\ & \downarrow & & \\ \dots & y & \dots & \dots \end{array} \right) * \left[\left(\begin{array}{cccc} \dots & y & \dots & \dots \\ & \downarrow & & \\ \dots & z & \dots & \dots \end{array} \right) * \left(\begin{array}{cccc} \dots & z & \dots & \dots \\ & \downarrow & & \\ \dots & w & \dots & \dots \end{array} \right) \right] = \left(\begin{array}{cccc} \dots & x & \dots & \dots \\ & \downarrow & & \\ \dots & w & \dots & \dots \end{array} \right)$$

Therefore, regardless of how the correspondences are associated, the end result is x being matched with w . Since this happens when arbitrary elements x , y , z , and w from S are considered, it is reasonable to expect that the operation $*$ is associative.

All of the group axioms are satisfied. However, it still remains to see if $*$ is a commutative operation. The fact that Figure 51 is not symmetric leads one to suspect that $*$ is not commutative. Hence, a counter example is sought to verify this suspicion. Note that $C * A = E$ and $A * C = B$, and hence $C * A \neq A * C$. Therefore, G with binary operation $*$ is a noncommutative group.

To terminate the discussion of groups three general observations will be made. In a field it is true that identity elements and inverses are unique and that a linear equation $ax = b$ over the field always has a solution in the field. The analogs of these properties for groups are stated as theorems.

Theorem 4.7. If G is a group with binary operation $*$, then the identity element e is unique.

Proof: Suppose there exists $e' \in G$ such that for all $a \in G$, $a * e' = e' * a = a$. In particular, this statement must be true for e ; that is, $e * e' = e' * e = e$. But e is known to be an identity element, so $e' * e = e * e' = e'$. Now, by the transitive property of equality, it follows that $e' = e$. Therefore, the identity e is unique.

Theorem 4.8. Let G be a group with binary operation $*$. For all $a \in G$, a^{-1} is unique.

Proof: Suppose there exists $b \in G$ such that $a * b = b * a = e$. Now it is known that $a * a^{-1} = a^{-1} * a = e$. Therefore, $b * a = a^{-1} * a$ by the transitive property of equality. Hence, it follows that $(b * a) * a^{-1} = (a^{-1} * a) * a^{-1}$. By using the associative law and the inverse property it is seen that $b^{-1} = a$. Thus, the inverse of a is unique.

Theorem 4.9. Let G be a group with binary operation $*$. For all $a, b \in G$, $a * x = b$ has a unique solution in G .

Proof: Notice that $a^{-1} * b$ is a solution since $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$. Now suppose there exists $y \in G$ such that $a * y = b$, then $a^{-1} * (a * y) = a^{-1} * b$. But $a^{-1} * (a * y) = (a^{-1} * a) * y = e * y = y$. Therefore, $y = a^{-1} * b$. Thus, $a^{-1} * b$ is the only solution of $a * x = b$.

Rings, Integral Domains, and Fields

The definition of a group was motivated by the fact that addition and multiplication in a field had certain common properties. The bases for the algebraic structure to be introduced here are the properties shared by each of the familiar systems Z , Q , R , and C , integers, rational numbers, real numbers, and complex numbers.

It was agreed in Chapter III that one may regard the inclusions, $Z \subset Q \subset R \subset C$, in an intuitive and informal way. However, as the reader well knows, the system Q is formally constructed from the system Z , and there is a one-to-one correspondence between Z and a

proper subset Z' of Q . Furthermore, the binary operations in Z behave exactly like the binary operations in Z' . The system Q is then used to construct R formally, and R is used to construct C .

Each of the above structures possesses some common properties.

These are listed as follows:

1. Addition and multiplication are binary operations in each system; i. e. , each system is closed with respect to addition and multiplication.
2. Addition is commutative.
3. Addition is associative.
4. Each system has an additive identity.
5. Each element in each system has an additive inverse.
6. Multiplication is commutative.
7. Multiplication is associative.
8. Multiplication is distributive over addition.

Observe further that each of the systems with the binary operation of addition constitutes an additive, Abelian group by virtue of properties 2 - 5. If T represents any one of the systems Z , Q , R , or C , then properties 1 - 8 may be summarized in the following way.

T is a system with two binary operations, addition and multiplication, symbolized by "+" and "." such that:

- 1'. T is an additive, Abelian group;
- 2'. Multiplication is commutative;
- 3'. Multiplication is associative;
- 4'. Multiplication distributes over addition.

The reader will agree that the above observations about the particular properties the systems Z , Q , R , and C have in common are

noteworthy of attention. However, there are many other systems with two binary operations that enjoy the properties 1' - 4'. Before some examples are given such structures will be classified according to the following definition.

A ring is a set R_1 on which two binary operations, called "addition" and "multiplication" and denoted by "+" and "." are defined such that:

1. R_1 is an Abelian group with respect to addition;
2. Multiplication is associative;
3. Multiplication distributes over addition; i. e., for all $a, b, c \in R_1$, $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

If, in addition to the foregoing axioms, a ring satisfies the following axiom, then the ring is said to be a commutative ring.

4. Multiplication is commutative.

Furthermore, the ring might contain a multiplicative identity.

If the following axiom also holds, then the ring is called a ring with unity element.

5. R_1 contains a multiplicative identity.

An abundance of examples of rings can be found in the modular arithmetic systems. For any positive integer m , it is already known that addition in \bar{Z}_m is a binary operation, $[0]$ is the identity element for addition, every $[a] \in \bar{Z}_m$ has an additive inverse, and addition is commutative and associative. Therefore, \bar{Z}_m is an additive, Abelian group. Furthermore, it was shown on page 186 that multiplication is associative and multiplication distributes over addition. Hence, for any positive integer m , \bar{Z}_m is a ring.

Further properties enjoyed by \bar{Z}_m are Axioms 4 and 5. \bar{Z}_m is then a commutative ring with unity element [1].

That multiplication be commutative is not a requirement in the definition of a ring. There are rings of considerable value and significance which are noncommutative, and an example of one will now be given.

The set $Z \times Z$ is the set of all ordered pairs of integers. The idea of the cross product of the set Z with itself can be extended to the cross products $Z \times Z \times Z$ and $Z \times Z \times Z \times Z$. $Z \times Z \times Z$ is the set of all ordered triples of integers, while $Z \times Z \times Z \times Z$ is the set of all ordered quadruples of integers. For instance, $(2, -3, 0) \in Z \times Z \times Z$ and $(-4, 5, 1, -1) \in Z \times Z \times Z \times Z$. As a notational device it is convenient to let $M = Z \times Z \times Z \times Z$, then $M = \{(a, b, c, d) | a, b, c, d \in Z\}$. To further facilitate the notation the ordered quadruples (a, b, c, d) are written

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

This symbol denoting the ordered quadruple (a, b, c, d) can be thought of as having two rows and two columns. The first row is composed of the elements a and b while the second row is composed of the elements c and d . The first column contains the elements a and c ; the second column contains the elements b and d .

Set M is called the set of 2 X 2 matrices over Z . Any particular member of M is called a 2 X 2 matrix. The symbol "2 X 2" is read "two by two."

Some criterion is needed for distinguishing the members of set M . The following defines what is meant by "equality" of 2×2 matrices.

The matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

are said to be equal, which is symbolized by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix},$$

iff

$$a = e, b = f, c = g, \text{ and } d = h.$$

It is not difficult to verify that this equals relation on M is an equivalence relation.

If a structure is to be imposed on M , then careful attention will have to be given to the problem of how to operate on the elements of M . Define addition and multiplication on M by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a + e & b + f \\ c + g & d + h \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix},$$

respectively. It remains to be shown that addition and multiplication are indeed binary operations on M . Notice that $a + e$, $b + f$, $c + g$, and $d + h$ all represent integers since addition of integers is a binary operation on \mathbb{Z} . Therefore, the "sum" of two matrices in M is again a

matrix in M . Furthermore, multiplication of integers is a binary operation on Z ; therefore, $ae + bg$, $af + bh$, $ce + dg$, and $cf + dh$ also represent integers. Thus, the "product" of two members of M is a member of M . It follows that addition and multiplication of 2×2 matrices are binary operations on M .

For particular instances, let

$$M_1 = \begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} -1 & 4 \\ 2 & 1 \end{bmatrix},$$

then

$$\begin{aligned} M_1 + M_2 &= \begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} -1 & 4 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 3 + (-1) & (-2) + 4 \\ 1 + 2 & 0 + 1 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} M_1 M_2 &= \begin{bmatrix} 3 & -2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 4 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 3(-1) + (-2)(2) & 3 \cdot 4 + (-2) \cdot 1 \\ 1(-1) + 0 \cdot 2 & 1 \cdot 4 + 1 \cdot 1 \end{bmatrix} \\ &= \begin{bmatrix} -7 & 10 \\ -1 & 5 \end{bmatrix}. \end{aligned}$$

The next objective is to show that M under addition and multiplication is a ring. To accomplish this objective the ring axioms must be satisfied. In the following verifications of the ring axioms for M , the writer will not elaborate on use of the properties of the system Z , nor on the use of the definitions of addition and multiplication of 2×2 matrices.

Commutative law for addition. For any two matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

in M ,

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} &= \begin{bmatrix} a + e & b + f \\ c + g & d + h \end{bmatrix} \\ &= \begin{bmatrix} e + a & f + b \\ g + c & b + d \end{bmatrix} \\ &= \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \end{aligned}$$

Identity element for addition. The matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

is the identity element for addition because for any matrix in M ,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a + 0 & b + 0 \\ c + 0 & d + 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Inverse elements. For any matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

in M , the matrix

$$\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

is also in M , and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} a + (-a) & b + (-b) \\ c + (-c) & d + (-d) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Associative law for addition. For all matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

in M ,

$$\begin{aligned} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix} &= \begin{bmatrix} a + e & b + f \\ c + g & d + h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\ &= \begin{bmatrix} (a + e) + i & (b + f) + j \\ (c + g) + k & (d + h) + l \end{bmatrix} \\ &= \begin{bmatrix} a + (e + i) & b + (f + j) \\ c + (g + h) & d + (h + l) \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e + i & f + j \\ g + h & h + l \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right) \end{aligned}$$

Associative law for multiplication. For all

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

in M ,

$$\begin{aligned}
\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} i & j \\ k & l \end{bmatrix} &= \begin{bmatrix} ae+bg & af+bh \\ ce+dh & cf+dh \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(cf+dh)k & (ce+dg)j+(cf+dh)l \end{bmatrix} \\
&= \begin{bmatrix} (ae)i+(bg)i+(af)k+(bh)k & (ae)j+(bg)j+(af)l+(bh)l \\ (ce)i+(dg)i+(cf)k+(dh)k & (ce)j+(dg)j+(cf)l+(dh)l \end{bmatrix} \\
&= \begin{bmatrix} a(ei)+a(fk)+b(gi)+b(hk) & a(ej)+a(fl)+b(gj)+b(hl) \\ c(ei)+c(fk)+d(gi)+d(hk) & c(ej)+c(fl)+d(gj)+d(hl) \end{bmatrix} \\
&= \begin{bmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right).
\end{aligned}$$

Distributive law. For all

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

in M ,

$$\begin{aligned}
\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} i & j \\ k & l \end{bmatrix} &= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} (a+e)i + (b+f)k & (a+e)j + (b+f)l \\ (c+g)i + (d+h)k & (c+g)j + (d+h)l \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
&= \begin{bmatrix} (ai+ei) + (bk+fk) & (aj+ej) + (bl+fl) \\ (ci+gi) + (dk+hk) & (cj+gj) + (dl+hl) \end{bmatrix} \\
&= \begin{bmatrix} (ai+bk) + (ei+fk) & (aj+bl) + (ej+fl) \\ (ci+dk) + (gi+hk) & (cj+dl) + (gj+hl) \end{bmatrix} \\
&= \begin{bmatrix} ai + bk & aj + bl & ei + fk & ej + fl \\ ci + dk & cj + dl & gi + hk & gj + hl \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}.
\end{aligned}$$

Similarly, the other distributive can be verified.

According to the definition, all the requirements have been met for M , with binary operations addition and multiplication, to be a ring.

However, the product

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and the product

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

are not the same since

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus, M is a noncommutative ring.

Finally, the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the identity element for multiplication in M because

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

M is therefore a noncommutative ring with unity element.

The systems Z , Q , R , and C , mentioned at the beginning of this section, are examples of rings. However, Z is the only one of these structures that is not also a field. Because of this fact the system Z is often referred to as the ring of integers.

Consider the set C of complex numbers and let $G = \{a + ib \mid a, b \in Z \text{ and } i^2 = -1\}$, then $G \subset C$. The elements in G are called Gaussian integers, and it will be verified that G is a ring with respect to addition and multiplication of complex numbers.

First, note that according to the definitions of addition and multiplication of complex numbers,

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

and

$$(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

It is easy to see that $(a + c) + i(b + d)$ and $(ac - bd) + i(ad + bc)$ are elements in G because addition, subtraction, and multiplication are binary operations on Z . One does not have to stretch the imagination to realize that addition in G is commutative; $0 + i \cdot 0$ is the additive identity, $-a + i(-b)$ is the additive inverse of $a + ib$; and addition is

associative. Therefore, G is an Abelian group.

Further, one should be convinced that multiplication in G is associative, and multiplication distributes over addition. G also has a multiplicative identity, namely $1 + i \cdot 0$; and multiplication is commutative. So G is an example of a commutative ring with unity element.

If an algebraic structure is a field, then it is true that $ab = 0$ implies $a = 0$ or $b = 0$. This property is not required to hold in a ring. In regard to the ring \bar{Z}_4 it was remarked previously that $[2] \cdot [2] = 0$, where $[2] \neq 0$. Also in the ring M of 2×2 matrices, notice that

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

but

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Let R_i be a ring. If there exist $a, b \in R_i$ such that $a \neq 0$, $b \neq 0$, and $ab = 0$, then a is called a left divisor of zero, and b is called a right divisor of zero.

In the examples above, $[2]$ is both a left and a right divisor of zero in \bar{Z}_4 , while

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

is a left divisor of zero in M and

$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

is a right divisor of zero in M . In the ring \bar{Z}_6 , $[2] \cdot [3] = [3] \cdot [2] = [0]$.

Here both [3] and [2] are left divisors of zero as well as right. So it is seen that in a commutative ring a left divisor of zero is also a right divisor of zero, and vice versa. In this case it is convenient to speak of "a divisor of zero."

Perhaps there should be some distinction made between rings that have no divisors of zero and rings that do have divisors of zero. In a ring R_1 having no divisors of zero it is true that for all $a, b \in R_1$, $ab = 0$ implies $a = 0$ or $b = 0$. Notice that the negation of this statement is there exists $a, b \in R_1$ such that $ab = 0$ and $a \neq 0$ and $b \neq 0$. This latter statement is just the condition that was specified in the definition of divisors of zero.

A commutative ring which contains no divisors of zero is called an integral domain.

According to this definition it can be ascertained that the systems Z , Q , R , and C are integral domains. Furthermore, all modular systems with prime moduli are integral domains. A modular system with composite modulus is not an integral domain, neither is the system M of 2×2 matrices over Z .

In every field the cancellation law for multiplication is valid; i. e., $ab = ac$ and $a \neq 0$ implies $b = c$. An interesting result involving the cancellation law for multiplication in rings is the statement of the following theorem.

Theorem 4.10. Let R_1 be a commutative ring. R_1 is an integral domain iff the cancellation law for multiplication holds.

Proof: Suppose R_1 is an integral domain, then by definition R_1 has no divisors of zero. That is, for all $x, y \in R_1$, if $xy = 0$ then $x = 0$

or $y = 0$. If $ab = ac$ and $a \neq 0$, then $ab + [-(ac)] = ac + [-(ac)] = 0$. But, $ab + [-(ac)] = ab + a(-c)$. (Refer to the proof of Theorem 3.14 in which only properties of an integral domain were used.). Now $ab + a(-c) = a[b + (-c)]$, and hence $a[b + (-c)] = 0$. Since $a \neq 0$, it must be true that $b + (-c) = 0$ because R_i has no divisors of zero. Thus, it follows that $b = c$ whenever $ab = ac$ and $a \neq 0$. Therefore, the cancellation law for multiplication holds in R_i .

Conversely, suppose that the cancellation law for multiplication holds in R_i . Suppose $ab = 0$ and $a \neq 0$. Now $ab = 0 = a \cdot 0$, and $ab = a \cdot 0$. Since $a \neq 0$, it follows by the cancellation law that $b = 0$. Hence, a is not a divisor of zero. That is, for any $a \in R_i$ such that $a \neq 0$, a is not a divisor of zero. Therefore, R_i is an integral domain.

Probably the most prominent example of an integral domain that is not a field is the system Z . On the other hand, the systems Q , R , and C are integral domains which are also fields. The essential difference is that not all non-zero integers have multiplicative inverses while all non-zero elements in Q , R , and C have multiplicative inverses. An important class of structures are those integral domains in which each non-zero element has a multiplicative inverse.

A field F is an integral domain with unity element $e \neq 0$ such that for each $a \in F$, where $a \neq 0$, there exists a multiplicative inverse $a^{-1} \in F$ possessing the property that $aa^{-1} = a^{-1}a = e$.

Finally, an alternate definition of a field is the following.

A field is a set F with at least two elements and two binary operations called addition and multiplication such that:

1. F is an additive, Abelian group;
2. $F - \{0\}$ is a multiplicative, commutative group;
3. Multiplication distributes over addition; i. e., for all $a, b, c \in F$, $a(b + c) = ab + ac$.

CHAPTER V

SUMMARY AND CONCLUSIONS

Summary

The problem of this study was to design a suggested course of study for elementary teachers based on the algebraic concepts that were identified through research of four contemporary series of elementary school mathematics textbooks. The four series, which were representative of those available at the time the research was initiated, were recommended by Dr. Vernon Troxel, Associate Professor of Education at Oklahoma State University. Analysis of all four sets of textbooks was conducted on an independent page-by-page basis with the sole purpose in mind of determining whether or not, in the judgment of this writer, certain algebraic concepts were presented. No attempt was made to analyze the quality or the quantity of material presented in the texts.

In this paper a systematic and logical discussion of material relating to the algebraic concepts thus identified is presented. Although previous experience with mathematical reasoning and the employment of mathematical symbolism on the part of the reader would be desirable, it is not essential since Chapter II provides the basis for the language, terminology, and notation that are used in subsequent chapters. The content of Chapter III presupposes that the reader has a knowledge of the basic properties of the natural numbers, the whole

numbers, the integers, the rational numbers, and the real numbers. Experiences gained through studying Chapter III are utilized to relate certain concepts to more general mathematical structures such as groups, rings, and integral domains in Chapter IV. The structure of subsystems of the real number system are emphasized in Chapter IV as well as in Chapter III.

Encountering algebraic concepts in elementary arithmetic is unavoidable. Whether the specific term "algebra" is used or not, the idea is inherent whenever operations with numbers, number sentences, less than, greater than, clock arithmetic, etc., are referred to. The study of algebra cannot be divorced from arithmetic, nor can arithmetic be divorced from algebra. But rather, a study of algebra leads to a deeper and more mature understanding of arithmetic. Algebra serves to answer many of the questions about arithmetic that confront the elementary teacher. A knowledge of algebra provides the tools with which an elementary teacher can gain valuable insight into the pattern and structure of mathematics. This need for better understanding of the structure of mathematics is essential for a satisfactory and permanent grasp of the subject matter.

The elementary teacher who is cognizant of the power of considering sets of abstract objects and the properties under a given binary operation is in an advantageous position to alleviate fears and anxieties of youngsters when different degrees of abstraction are needed to comprehend the idea of "number." Two very important aspects in mathematics are generalization and abstraction. The teacher, possessed with these processes, can guide young minds to interpret other mathematical systems on the basis of already familiar systems.

Hence, it appears as though algebraic concepts have appropriate uses at every level of mathematics in the elementary school. The final decisions concerning the extent and degree to which these ideas are emphasized must be made by the teachers at the particular grade level.

Conclusions

This study and the authoritative opinions of others lend support to this writer's premise that the study of algebraic concepts has value in the mathematical training of elementary school teachers as more abstraction is being reflected in the arithmetic textbooks.

Evidence is accumulating from experimental centers to indicate that the mathematics program for children of grades 1 - 6 may be greatly enriched and broadened by including some simple algebraic ideas [7].

Furthermore, in making a study of the compatibility of content in textbooks for teachers and textbooks for elementary children, Hicks [16] reported that "There was less consensus in either category on algebraic topics, with the disagreement being greater in the texts for teachers." It is therefore reasonable that the material which authors of elementary arithmetic texts include in their books would provide a formidable and legitimate basis for a course guide for elementary teachers.

A study such as this one, in addition to presenting a systematic and logical arrangement of algebraic concepts, provides the elementary teacher with the background for anticipating the kind of mathematics youngsters will encounter in subsequent years. It is also of significance that the reader may find motivation for material in the classroom.

The result of this study is not intended to suggest any restriction in the mathematical training of elementary teachers; however, this

writer strongly suggests that a course in algebra be an integral part of the teacher's experience. This writer is convinced that a study in algebraic topics would contribute substantially to the elementary teacher's understanding of mathematics. However, certain questions have been raised while preparing this paper. Research to evaluate the effect that a study of algebraic concepts has on the teacher's attitude toward mathematics in general is suggested. It is also a strong conviction of the writer that experienced teachers as well as prospective teachers could profit substantially through a knowledge of basic algebraic concepts. But research is needed to determine if such a course would be more effective at the preservice level or the in-service level.

Finally, this material might possibly be used in the training of elementary teachers to satisfy the recommendation of CUPM for a course in basic concepts in algebra.

A SELECTED BIBLIOGRAPHY

- (1) Banks, J. Houston. Elementary-School Mathematics, A Modern Approach for Teachers. Boston: Allyn and Bacon, Inc., 1966.
- (2) Barnes, Wilfred E. Introduction to Abstract Algebra. Boston: D. C. Heath and Company, 1963.
- (3) A Brief Course in Mathematics for Elementary School Teachers. School Mathematics Study Group, IX.
- (4) Brown, Kenneth E. "What are the Changes?" Audiovisual Instruction, VII (March, 1962), 138-40.
- (5) Carpenter, Raymond. "Identifying Concepts and Processes in Mathematics Needed for the Adequate Preparation of Elementary Teachers." (Doctoral dissertation, Oklahoma State University, 1959).
- (6) "Course Guides for the Training of Teachers of Elementary School Mathematics." Committee on Undergraduate Program in Mathematics. July, 1964.
- (7) Deans, Edwina. Elementary School Mathematics: New Directions. Washington: U. S. Department of Health, Education, and Welfare, 1963, pp. 6-7.
- (8) DeVault, M. Vere, editor. Improving Mathematics Programs. Columbus, Ohio: Charles E. Merrill Books, Inc., 1961.
- (9) Drooyan, Irving, Walter Hadel, and Frank Fleming. Elementary Algebra, Structure and Skills. New York: John Wiley and Sons, Inc., 1966.
- (10) Eves, Howard and Carroll V. Newson. An Introduction to the Foundations and Fundamental Concepts of Mathematics. New York: Holt, Rinehart, and Winston, 1964.
- (11) Fehr, Howard F. and Thomas J. Hill. Contemporary Mathematics for Elementary Teachers. Boston: D. C. Heath and Company, 1966.
- (12) Goals for School Mathematics. "The Report of the Cambridge Conference on School Mathematics." Boston: Educational Services Incorporated, 1963.

- (13) Goff, Gerald K. and Milton E. Berg. Basic Mathematics - A Programmed Introduction. New York: Appleton, Century, Crofts, 1968.
- (14) Haag, Vincent H. Structure of Algebra. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1964.
- (15) Hamilton, Norman T, and Joseph Landin. Set Theory, the Structure of Arithmetic. Boston: Allyn and Bacon, Inc., 1961.
- (16) Hicks, Randall. "Elementary Series and Texts for Teachers - How Well do they Agree?" The Arithmetic Teacher, XV (March, 1968), 266-70.
- (17) Hlavaty, Julius H. "A Message to Teachers of Elementary Mathematics." The Arithmetic Teacher, XV (May, 1968), 399.
- (18) James, Glen and Robert C. James, editors. Mathematics Dictionary. Princeton: D. Van Nostrand Company, Inc., 1959.
- (19) Jones, George Lucas. "A Study to Determine which Basic Mathematical Concepts Commonly Presented in Grades IV Through VIII are Least Understood by Certain Elementary Education Majors." (Doctoral dissertation, Colorado State College, 1962).
- (20) Kenelly, John W. Informal Logic. Boston: Allyn and Bacon, Inc., 1967.
- (21) Kingston, J. Maurice. Mathematics for Teachers of the Middle Grades. New York: John Wiley and Sons, Inc., 1966.
- (22) Mauro, Carl. "A Survey of the Presentation of Certain Topics in Ten Series of Arithmetic Textbooks." (Doctoral dissertation, University of Maryland, 1957).
- (23) McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.
- (24) Number Systems. School Mathematics Study Group, VI.
- (25) Parker, F. D. "When is a Loop a Group." The American Mathematical Monthly, LXXII, No. 7, 765-66.
- (26) Peterson, John A. and Joseph Hashisaki. Theory of Arithmetic. New York: John Wiley and Sons, Inc., 1967.
- (27) "Recommendations of the Mathematical Association for the Training of Teachers of Mathematics." American Mathematical Monthly, LXVII (December, 1960), 72.
- (28) Schaaf, William L. Basic Concepts of Elementary Mathematics. New York: John Wiley and Sons, Inc., 1960.

- (29) Sherman, Homer C. and Robert E. Belding. "Are Soviet Arithmetic Books Better than Ours?" The Arithmetic Teacher, XII (December, 1965), 633-37.
- (30) Topics in Mathematics for Elementary School Teachers. Washington, D. C.: National Council of Teachers of Mathematics, 1964.
- (31) Watson, Donald. "Condition for a Loop to be a Group." The American Mathematical Monthly. LXXIV, No. 7, 843-44.
- (32) Weaver, Jay D. and Charles T. Wolf. Modern Mathematics for Elementary Teachers. Scranton, Pennsylvania: International Textbook Company, 1965.
- (33) Willerding, Margaret F. and Ruth A. Hayward. Mathematics — The Alphabet of Science. New York: John Wiley and Sons, Inc., 1968.
- (34) Van Engen, Henry, Maurice L. Hartung, and James E. Stochl. Foundations of Elementary School Arithmetic. Chicago: Scott, Foresman and Company, 1965.
- (35) Zassenhaus, H. The Theory of Groups. New York: Chelsea, 1949.
- (36) Zassenhaus, H. "What Makes a Loop a Group?" The American Mathematical Monthly. LXXV, No. 2, 139-42.

APPENDIX A

SYMBOLS AND NOTATION

Symbol	Meaning	Page
\wedge	Conjunction— <i>and</i>	9
\vee	Disjunction— <i>inclusive or</i>	9
p, q, r, \dots	Symbols for statements	9
$\underline{\vee}$	Disjunction — <i>exclusive or</i>	11
\sim	Negation	12
\rightarrow	Conditional — <i>if, then</i>	13
\leftrightarrow	Biconditional	17
<i>iff</i>	Biconditional	17
$p \wedge (\sim p)$	Contradiction	19
$[p \wedge (p \rightarrow q)] \rightarrow q$	Law of detachment	19
$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Law of the syllogism	20
$\{ \}$	Brace notation for sets	24
ϵ	Is an element of	24
\notin	Is not an element of	24
$\{x x \text{ is } \dots\}$	Set builder notation	24
$\{a, b, c, \dots\}$	Roster notation	24
U	Universal set	25
\emptyset	Empty set	26
\subseteq	Is a subset of	26
\subset	Is a proper subset of	27

Symbol	Meaning	Page
\cup	Union	28
\cap	Intersection	28
A'	Complement of A, relative to U	29
$B - A$	Complement of A, relative to B	29
(a, b)	Ordered pair	31
$A \times B$	Cartesian product, or cross product, of A and B	32
$2, \pi, \sqrt{2}, \dots$	Constant	33
x, y, z, \dots	Variable	33
For each or for all	Universal quantifier	34
There exists	Existential quantifier	35
$R \subseteq (A \times B)$	Relation	37
D_o	Domain	37
R_a	Range	38
R^{-1}	Inverse Relation	39
f, g, \dots	Function	40
f^{-1}, g^{-1}, \dots	Inverse function	41
$g(n)$	Functional notation	42
$=$	Equals relation	44
$[a]$	Equivalence class	45
N	Set of all counting numbers	49
W	Set of all whole numbers	49
Z	Set of all integers	49
Q	Set of all rational numbers	50
R	Set of all real numbers	50
$*, ?, !, \text{etc.}$	Binary operations	51

Symbol	Meaning	Page
ldpma	Left distributive property of multiplication over addition	60
rdpma	Right distributive property of multiplication over addition	60
$-a$	Additive inverse of a	61
a^{-1}	Multiplicative inverse of a	61
F	A field	80
$\{x \mid x \text{ makes } P \text{ a true statement}\}$	Truth set or solution set	90
$3x + 2 = 0$, etc.	Conditional equation	90
$x + 4 = 4 + x$, etc.	Identity	90
$ax + b = 0$, $a \neq 0$	Linear equation in one variable	91
R^+	Set of all positive real numbers	99
R^-	Set of all negative real numbers	99
$>$	Is greater than	103
$<$	Is less than	103
\nlessgtr	Is not greater than	104
\nlessgtr	Is not less than	104
\geq	Is greater than or equal to	104
\leq	Is less than or equal to	105
$ x $	Absolute value of x	111
$ax + b < 0$	Linear inequality	114
$x + 4 > x$, etc.	Absolute inequality	114
$x < -2$, etc.	Conditional inequality	114
$ax + b$	Linear polynomial	125
$px^2 + qx + r$	Quadratic polynomial	126
\sqrt{a} , $a \geq 0$	Square root of a	131

Symbol	Meaning	Page
$px^2 + qx + r = 0$	Quadratic equation in one variable	132
$ax + by + c = 0$	Linear equation in two variables	136
$ax + by + c < 0$	Linear inequality in two variables	136
$f = \{(x, f(x)) \mid f(x) = ax + b\}$	Linear function	143
C	Set of all complex numbers	163
i	Imaginary unit	172
Z_m	Modular system	175
\equiv	Congruence relation	176
\bar{Z}_m	Set of equivalence classes mod m	184
G	A group	193
$x_{(i,j)}$	Entry in row i and column j of a rectangular array	196
R_i	A ring	209
$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	2 X 2 Matrix	210
$a + ib; a, b \in Z$	Gaussian integer	217

APPENDIX B

ALGEBRAIC CONCEPTS AND THE ASCRIBED ELEMENTARY MATHEMATICS TEXTBOOKS

Algebraic Concepts

Absolute value	Group
Additive inverses	Identity elements
Associative property	Inequality
Binary operations	Integral domain
Closure	Inverse operations
Commutative property	Mathematical structure
Complex numbers	Open sentences
Constants	Ordered pairs – Cartesian product
Distributive property	Partition
Equation	Real numbers
Equivalent equations	Relations
Existential quantifier	Replacement set
Exponents	Ring
Field properties or axioms	Solution set
Finite mathematical systems	Universal quantifier
Function	Variables
Graphing functions, equations, and relations	

Ascribed Elementary Mathematics Textbooks

- School Mathematics Study Group. Mathematics for the Elementary School - Grades 1 - 6. New Haven: Yale University Press, 1965
- Deans, Edwina, et al. ABC Mathematics - Grades 1-6. Dallas: American Book Company, 1963.
- Eicholz, Robert E., et al. Elementary School Mathematics - Grades 1-2. Reading: Addison-Wesley Publishing Company, 1967.
- Eicholz, Robert E., et al. Elementary School Mathematics - Grades 3-6. Reading: Addison-Wesley Publishing Company, 1963.
- Hartung, Maurice L., et al. Seeing Through Arithmetic - Grade 1. Dallas: Scott, Foresman and Company, 1964.
- Hartung, Maurice L., et al. Seeing Through Arithmetic - Grade 2. Dallas: Scott, Foresman and Company, 1965.
- Hartung, Maurice L., et al. Seeing Through Arithmetic - Grade 3. Dallas: Scott, Foresman and Company, 1966.
- Hartung, Maurice L., et al. Seeing Through Arithmetic - Grade 4. Dallas: Scott, Foresman and Company, 1967.
- Hartung, Maurice L., et al. Seeing Through Arithmetic - Grades 5 and 6. Dallas: Scott, Foresman and Company, 1963.

APPENDIX C

SELECTED DEFINITIONS

1. An expression is a statement if and only if it has a truth value. Page 8.
2. A constant is a proper name. In other words, a constant is a name of a particular thing. Page 33.
3. A variable is a symbol that holds a place for constants. Page 33.
4. A specified set of elements, such that the names of these elements are possible replacements for a variable, is called the replacement set. Page 33.
5. A relation between sets A and B is a subset of $A \times B$ or $B \times A$. That is, if $R \subseteq (A \times B)$, then R is a relation from A to B. Page 37.
6. A function is a relation such that no two ordered pairs have the same first component. Equivalently, if two ordered pairs have the same first component, then the second components must also be the same. Page 40.
7. A relation that is transitive, but not symmetric, is called an order relation. Page 47.
8. A binary operation * on a set S is a function (or mapping) from $S \times S$ to S. That is, for each ordered pair $(a, b) \in S \times S$ there exists a unique element $a * b \in S$ that is associated with (a, b) . Page 53.
9. For all $a, b \in R$, the operation of subtraction in R, denoted by $a - b$, is defined as follows: $a - b = a + (-b)$. Page 71.
10. For all $a, b \in R$ such that $b \neq 0$, the operation of division in R, denoted by $a \div b$, is defined as follows: $a \div b = a \cdot (1/b)$. Page 76.

11. An equation is a sentence obtained by connecting expressions by the equality symbol. Page 89.
12. Equations which have the same solution set are said to be equivalent equations. Page 95.
13. An inequality is a sentence obtained by connecting real number expressions by one of the inequality symbols. Page 114.
14. An expression of the form $ax + b$ is said to be a linear or first-degree polynomial over R whenever it is assumed that $a, b \in R$, $a \neq 0$, and x is a variable on R . The real numbers a and b are called coefficients of the polynomial. Specifically, a is known as the coefficient of the variable x . Page 125.
15. An expression of the form $px^2 + qx + r$ is said to be a quadratic or second-degree polynomial over R whenever it is assumed that $p, q, r \in R$, $p \neq 0$, and x is a variable on R . The real numbers p, q , and r are the coefficients of the polynomial, where p and q are the coefficients of x^2 and x , respectively. Page 126.
16. A linear equation in two variables is an equation that can be expressed in the form $ax + by + c = 0$ where $a, b, c \in R$, $a \neq 0 \vee b \neq 0$, and R is the replacement set for the variables x and y . Page 136.
17. A linear function is a function defined by a linear equation in two variables $ax + by + c = 0$ where $b \neq 0$. Page 143.
18. For all $a, b, m \in Z$ such that $m > 0$, a is congruent to b modulo m iff $a - b$ is a multiple of m . This congruence relation is symbolized as " $a \equiv b(\text{mod } m)$." Thus, $a \equiv b(\text{mod } m)$ iff there exists $k \in Z$ such that $a - b = km$. On the other hand, $a - b$ is not a multiple of m iff a is not congruent to b modulo m . This is written as " $a \not\equiv b(\text{mod } m)$," Page 176.
19. Set $M = \{(a, b, c, d) \mid a, b, c, d \in Z\}$ is called the set of 2×2 matrices over Z . Any particular member of M is called a 2×2 matrix. The symbol " 2×2 " is read "two by two," Page 211.
20. A commutative ring which contains no divisors of zero is called an integral domain. Page 219.

21. A field F is an integral domain with unity element $e \neq 0$ such that for each $a \in F$, where $a \neq 0$, there exists a multiplicative inverse $a^{-1} \in F$ possessing the property that $aa^{-1} = a^{-1}a = e$. Page 220.
22. A field is a set F with at least two elements and two binary operations called addition and multiplication such that:
 1. F is an additive, Abelian group;
 2. $F - \{0\}$ is a multiplicative, commutative group;
 3. Multiplication distributes over addition; i. e., for all $a, b, c \in F$, $a(b + c) = ab + ac$. Page 220.

VITA
2
Don Prock

Candidate for the Degree of
Doctor of Education

Thesis: ALGEBRA FOR ELEMENTARY TEACHERS BASED ON
CURRENT ELEMENTARY TEXTBOOKS

Major Field: Higher Education

Minor Field: Mathematics

Biographical:

Personal Data: Born in Hollis, Oklahoma, February 19, 1927,
the son of Mr. and Mrs. Otto Prock.

Education: Graduated from Hollis High School, Hollis, Oklahoma,
in May, 1945; received the Bachelor of Science degree
from Southwestern State College, Weatherford, Oklahoma,
in May, 1951, with a major in education (mathematics);
received the Master of Education degree from the Univer-
sity of Oklahoma, Norman, Oklahoma, in August, 1959,
with a major in secondary administration; attended the
University of South Carolina, Columbia, South Carolina,
during the summer of 1960; received the Master of Arts
degree from the University of Illinois in August, 1962, with
a major in mathematics; completed requirements for the
Doctor of Education degree at Oklahoma State University,
Stillwater, Oklahoma, in May, 1969.

Professional Experience: Entered the teaching profession in 1950;
taught business at Lone Wolf High School, Lone Wolf,
Oklahoma, from September, 1950 to May, 1952; mathe-
matics teacher at Erick High School, Erick, Oklahoma,
from September, 1952 to May, 1956; taught mathematics
at Hollis High School, Hollis, Oklahoma, from September,
1956 to May, 1958; employed as mathematics teacher at
Southwestern State College, Weatherford, Oklahoma, since
September, 1958; served as staff assistant in mathematics
at Oklahoma State University during the summer and fall
of 1965.

Organizations: Member of Mathematics Association of America,
National Council of Teachers of Mathematics, Oklahoma
Council of Teachers of Mathematics, and Oklahoma Educa-
tion Association.