DOCUMENT RESUME

ED 143 558 SE 023 044

AUTHOR Syer, Henry W., Ed.
TITLE Supplementary and Enrichment Series: Algebraic Structures.
INSTITUTION Stanford Univ., Calif. School Mathematics Study Group.
SPONS AGENCY National Science Foundation, Washington, D.C.
REPORT NO SMSG-SP-16
PUB DATE 65
NOTE 37p.; Contains numerous light type

EDRS PRICE MF-$0.83 HC-$2.06 Plus Postage.
DESCRIPTORS *Algebra; *Instructional Materials; Mathematics; Number Concepts; Secondary Grades; *Secondary School Mathematics; *Textbooks
IDENTIFIERS *Group Theory; *School Mathematics Study Group

ABSTRACT

This is one of a series of publications written to supplement the secondary school School Mathematics Study Group program. This booklet will be most useful for enrichment at the eleventh and twelfth grade levels. It treats algebraic structures as abstract mathematical systems and introduces such important ideas as group, non-abelian group, field, and subfield. Proofs are rigorous, but not tedious. Answers to the problems are found in the back of the book. As background, the reader needs to be familiar with the following sets of numbers: integers, rationals, reals, and complex numbers. (Author/RH)

SCHOOL MATHEMATICS STUDY GROUP

SP-16

SUPPLEMENTARY and ENRICHMENT SERIES

ALGEBRAIC STRUCTURES

Edited by Henry W. Syer

Financial support for the School Mathematics Study Group has been provided by the National Science Foundation.

PREFACE

Mathematics is such a vast and rapidly expanding field of study that there are inevitably many important and fascinating aspects of the subject which, though within the grasp of secondary school students, do not find a place in the curriculum simply because of a lack of time.

Many classes and individual students, however, may find time to pursue mathematical topics of special interest to them. This series of pamphlets, whose production is sponsored by the School Mathematics Study Group, is designed to make material for such study readily accessible in classroom quantity.

Some of the pamphlets deal with material found in the regular curriculum but in a more extensive or intensive manner or from a novel point of view. Others deal with topics not usually found at all in the standard curriculum. It is hoped that these pamphlets will find use in classrooms in at least two ways. Some of the pamphlets produced could be used to extend the work done by a class with a regular textbook but others could be used profitably when teachers want to experiment with a treatment of a topic different from the treatment in the regular text of the class. In all cases, the pamphlets are designed to promote the enjoyment of studying mathematics.

Prepared under the supervision of the Panel on Supplementary Publications of the School Mathematics Study Group:

Professor R. D. Anderson, Department of Mathematics, Louisiana State University, Baton Rouge 3, Louisiana

Mr. Ronald J. Clark, Chairman, St. Paul's School, Concord, New Hampshire 03301

Dr. W. Eugene Ferguson, Newton High School, Newtonville, Massachusetts 02160

Mr. Thomas J. Hill, Montclair State College, Upper Montclair, New Jersey

Mr. Karl S. Kalman, Room 711D, Office of the Supt. of Schools, Parkway at 21st, Philadelphia 36, Pennsylvania 19103

Professor Augusta Schurrer, Department of Mathematics, State College of Iowa, Cedar Falls, Iowa

Dr. Henry W. Syer, Kent School, Kent, Connecticut

Professor Frank L. Wolf, Carleton College, Northfield, Minnesota 55057

Professor John E. Yarnelle, Department of Mathematics, Hanover College, Hanover, Indiana

FOREWORD

This booklet will be most useful for enrichment at the eleventh and twelfth grade levels. It treats algebraic structures as abstract mathematical systems and introduces such important ideas as group, non-abelian group, field and subfield. Proofs are rigorous, but not tedious. Answers to the problems will be found in the back of the booklet.

As background the reader needs familiarity with the following sets of numbers: integers, rationals, reals and complex numbers. No deep or strange theorems are presupposed, but the booklet requires mathematical maturity.

It was originally published as a chapter in the SMSG course called 'Intermediate Mathematics'.

CONTENTS

ALGEBRAIC STRUCTURES

1. Introduction.

During our study of mathematics, we use several number systems: the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers. In each of these systems our concern is with the following:

(1) Objects or elements: numbers;

(2) Two operations: addition and multiplication;

(3) Laws satisfied by these operations, such as the commutative and associative laws of addition and multiplication and the distributive law.

If we stop and reflect for a moment, we see that many of the algebraic computations which we carry out are independent of the nature of the numbers with which we are operating and depend solely on the fact that the operations in question are subject to laws respected in each system. Thus, for example, we consider the identity

$$a^2 - b^2 = (a + b)(a - b) \qquad 1a$$

and think of this assertion as applying to a and b taken as

(1) integers,

(2) rational numbers,

(3) real numbers,

(4) complex numbers.

We see that, if we established the Identity 1a at the earliest stage for integers and observed

(1) that the verification depended only on the distributive law, the associative laws and commutative laws and properties of the additive inverses, and

(2) that each of the laws and properties invoked were in force for the complex number system,

then it would be unnecessary to repeat the verification for the case where a and b are complex numbers.

Without such laws algebraic computation as we know it would cease to exist. The whole source of rules for algebraic computation is to be found in these laws.

We can, if we like, seek to abstract what is algebraically essential and common to several specific number systems and develop algebraic results which hold for each of these systems without having to repeat our work in each special case. This approach is of great importance in many parts of modern mathematics, especially in modern higher algebra which is sometimes called abstract algebra.

What is the nature of the fundamental algebraic operations that we have met? Let us take the addition of real numbers. We are given real numbers, say a and b, in order, or, if we like, the ordered pair (a,b). The operation of addition assigns to the ordered pair (a,b) a unique real number which we designate $a + b$. The words "assigns" and "unique" give the secret away. The operation of addition (of real numbers) is a function defined for each ordered pair of real numbers which assigns to each such ordered pair (a,b) of real numbers a real number, the sum, $a + b$.* It should be observed that while most of the functions which you have met assigned real numbers to real numbers, the function concept is an extremely general one and we may certainly consider a function f which assigns to each element a of a given class A a unique element (labelled $f(a)$) of a given class B. In the example of addition of real numbers, the class A is the set of ordered pairs of real numbers and the class B is the set of real numbers itself. There is a point concerning notation that should be made. Instead of writing the real number associated with the ordered pair (a,b) in function notation, say $S[(a,b)]$, where S (standing for "sum") is the function just described, we use the usual notation and write $a + b$.

2. Internal Operation.

Let us try to abstract what is algebraically essential in the example of addition of real numbers. Suppose that A is an arbitrary non-empty set of elements, the nature of which need not concern us. Suppose further that there is given a function which is defined for the ordered pairs (a,b), where $a \in A$ and $b \in A$, which assigns to each such ordered pair a member of A. Such a function is called an internal operation in A. (It is called "internal" because the components a and b of the input (a,b) are drawn from A and the output assigned by the function is also a member of A. Hence, the operation in question does not involve data taken outside of A.)

---

* See SMSG publication entitled FUNCTIONS.

There is also a notion of an external operation and, indeed, an example is to be found in the algebra of vectors when one considers real multiples of a given vector so that input is an ordered pair of the form (real number, vector) and output is a vector. Here we go outside the domain of vectors to specify the input --- hence "external."

In this chapter, however, we shall consider only internal operations and, for that reason we shall henceforth simply say "operation" rather than "internal operation." As it is customary, we shall usually denote an operation by a multiplication sign $\cdot$ and the element assigned to the ordered pair (a,b) by $a \cdot b$ when we are concerned with a single operation. We shall also write "ab" for "$a \cdot b$" when there is no doubt about the meaning. We shall have occasion later to deal with two operations and then we shall usually use $+$ and $\cdot$ to denote the two operations.

If we are concerned with a finite set A, we may specify with the aid of a multiplication table how a given operation acts in the same way that we listed the sum and product of certain important pairs of natural numbers with the aid of addition and multiplication tables in elementary arithmetic. The procedure is to use a square table marking rows by the elements of the set A and columns by the elements of the set A. The row markings are indicated at the left of the body of the table and the column markings are indicated above the body of the table. Given $a, b \in A$, in the space in the body of the table belonging to the row marked "a" and the column marked "b", we record the element associated with (a,b) by the operation.

Here is a simple example: Let $A = \{0,1\}$ and let $\cdot$ denote conventional multiplication in the real number system. Then the operation $\cdot$ may be tabulated as follows:

a \ b	0	1
0	0	0
1	0	1

Suppose that we consider a set A consisting of two distinct elements a and b and we ask in how many ways can we specify an operation in A. This amounts to constructing in all possible ways two-by-two square tables in each space of which is recorded an element of A. Here are some:

a \ b	a	b
a	a	a
b	a	a,

a \ b	a	b
a	b	b
b	b	b,

a \ b	a	b
a	a	a
b	a	b,

a \ b	a	b
a	a	b
b	b	a.

There are 16 such operations in A.

Exercises 2

1. List the remaining 12 operations in A .
2. Let A = {1, i, -1, -i} and let $\cdot$ denote conventional multiplication for complex numbers. Show that $\cdot$ is an operation in A and construct the table for $\cdot$.

It is of interest to note that, if A is a finite set containing n elements, then there are n^{n^2} distinct operations in A . (For n = 2 , we have $2^4 = 16$ distinct operations in A ; for n = 3 , we have $3^9 = 19{,}683$ distinct operations in A .)

We shall be interested in studying the composite object consisting of a non-empty set A and one or two operations in A . Precisely, the term "composite object" is to be taken here to mean either an ordered pair of the form $(A, \cdot)$ where $\cdot$ is an operation in A or an ordered triple of the form $(A, +, \cdot)$ where + and $\cdot$ are operations in A . Such a composite object is called an algebraic structure with one operation (or two operations respectively). An example of a structure with one operation is given by taking A as the set of integers and + as the customary addition. An example of a structure with two operations is given by taking A as the set of real numbers and + and $\cdot$ respectively as the customary addition and multiplication for the reals. Another example of a structure with two operations is given by taking A as the set of real numbers, + as the customary multiplication for the real numbers and $\cdot$ as the customary addition for the real numbers.

Now it turns out that the interesting structures are those which are subject to various laws. We saw that the number systems which we studied earlier were structures with two operations which respected such laws as the commutative laws, the associative laws, and the distributive law. If we wished to take into account structures which are not subject to any restrictions or laws, we would be faced with many different kinds of structures having very few properties in common. We could not hope to find interesting results which would be valid for all structures with a given set A and with a given number of operations.

On occasion, instead of referring to the structure "$(A, \cdot)$" or "$(A, +, \cdot)$" we shall use the less formal "A together with the operation $\cdot$ " or "A together with the operations + and $\cdot$ " respectively, as well as "A and the operation $\cdot$ ", etc.

We shall concentrate on two important structures which permeate elementary algebra -- the group and the field. Our interest will center principally on the notion of a field which embraces three of the important number systems which we have met so far -- the systems of the rational numbers, the real numbers, and the complex numbers.

3. Group.

Suppose that we consider a structure with one operation $(A, \cdot)$. One example which we cited above, where A is the set of integers and $\cdot$ is the customary addition, has the following two properties:

(1) The associative law for addition is satisfied.

(2) Given integers a and b, there exists a unique integer x satisfying $a + x = b$ and there exists a unique integer y satisfying $y + a = b$.

(We ignore deliberately the question of the equality of x and y for a reason which will become clear presently.) If we ask for structures with one operation which have these listed properties and this special structure, we are led to the very important structures with one operation called groups. They appear throughout mathematics in many different guises. The study of groups as such is an instance of algebra at its most abstract.

Specifically $(A, \cdot)$ is said to be a group provided that the following two conditions are satisfied:

G 1. The operation $\cdot$ is associative. That is, given elements a, b, c in A, we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) .$$

G 2. Given elements a, b in A, each of the equations

$$a \cdot x = b$$

and

$$y \cdot a = b$$

has a unique solution in A:

It is to be observed that we have not required that the operation $\cdot$ be commutative. In fact, we shall meet examples where $\cdot$ does not satisfy the commutative law which asserts that $a \cdot b = b \cdot a$ for all $a, b \in A$. This is why it was important in defining the notion of operation to have as our input an ordered pair of elements of A. The order in which the components are assigned may very well be essential. If the operation $\cdot$ satisfies the

commutative law, the group is called commutative or, as is more usual, abelian, in honor of the great Norwegian mathematician N. H. Abel (1802-1829) who did pioneer work in the theory of groups.

Let us consider some examples of groups drawn from our earlier experience. In these examples the operations are the standard ones of the number systems so that the groups in question are necessarily abelian. We shall consider an example of a non-abelian group later (Section 5).

Example 1. A = set of integers; the operation $\cdot$ is the conventional addition $+$. The second postulate states that the equation $a + x = b$, where a and b are integers, has a unique integral solution.

Example 2. A = set of real numbers different from zero; $\cdot$ is the conventional multiplication.

Example 3. A = set of vectors in 3-space; $\cdot$ is the usual addition of vectors.

Exercises 3

1. Verify that each of the cited examples satisfies the group postulates G 1 and G 2. Show that the following are also examples of groups:

   Example 4. A is the set of n^{th} roots of 1, where n is a positive integer, and $\cdot$ is the conventional multiplication for complex numbers. Here it is to be observed that A has just n elements.

   Example 5. A is the set of positive rational numbers; $\cdot$ is the conventional multiplication.

2. In what way does the following fail to yield an example of a group: A = set of all complex numbers and $\cdot$ is the conventional multiplication?
3. Let A denote the set of real numbers of the form $a + b\sqrt{2}$ where a and b are integers and let $\cdot$ be the conventional addition. Verify that $\cdot$ is an operation in A and that the group postulates are satisfied.
4. Let A denote the set of real numbers different from zero of the form $a + b\sqrt{2}$ where a and b are rational and let $\cdot$ be the conventional multiplication. Verify that $\cdot$ is an operation in A and that the group postulates are satisfied.

4. Some General Properties of Groups.

Earlier work with number systems may have convinced you that an important role was played by the notions of additive identity, additive inverse, multiplicative identity, multiplicative inverse. The counterparts of these notions appear in general group theory as we shall now see. Bear in mind that the commutative law need not be in effect for an arbitrary group!

Identity element. Here we ask whether there is an element e in A which has the property that $a \cdot e = e \cdot a = a$ for all elements $a \in A$. In each of the cited examples of Section 3 there is precisely one element with this property. Thus in Example 1, the integer 0 is the unique element having the stated property; in Example 2, it is 1; in Example 3, it is the zero vector $(0,0,0)$; in Example 4, it is 1; in Example 5, it is 1. We now turn to the situation for an arbitrary group and a proof of the following theorem:

Theorem 4a. Given the group consisting of the set A and operation $\cdot$, there is a unique element e of A which satisfies the following condition:

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

for all $a \in A$.

The element e is called the identity element of the group.

Proof of Theorem 4a: We fix an element $b \in A$. That there is at most one element e having the stated property follows from the fact that e is a solution of the equation $b \cdot x = b$ which has precisely one solution.

Now let e denote the solution of $b \cdot x = b$ and let us verify that $a \cdot e = a$ for all a in A. Given $a \in A$, let c satisfy $c \cdot b = a$. That is, c is the unique solution of $y \cdot b = a$. Our reason for introducing c is that, if we write a as $c \cdot b$, we are in a position to relate the product ae (which we should like to show is equal to a) to the product $b \cdot e$ about which we have information. Specifically,

$$\begin{aligned} a \cdot e &= (c \cdot b) \cdot e \\ &= c \cdot (b \cdot e) \\ &= c \cdot b \\ &= a . \end{aligned}$$

The proof of the theorem will be complete when we show that we also have $e \cdot a = a$ for all a in A. Given $a \in A$, let d denote the unique solution of the equation $y \cdot a = a$. In order to relate d and e, we introduce

f the unique solution of the equation $a \cdot x = e$ (thereby linking the elements a and e). From $d \cdot a = a$ and $a \cdot f = e$, we have

$$(d \cdot a) \cdot f = a \cdot f$$
$$= e .$$

From the associative law and $a \cdot f = e$, we have.

$$(d \cdot a) \cdot f = d \cdot (a \cdot f)$$
$$= d \cdot e .$$

Taken together these equalities yield

$$d \cdot e = e .$$

Now e satisfies the equation $y \cdot e = e$. (Recall that $a \cdot e = a$ for all a in A, in particular for $a = e$. This yields $e \cdot e = e$) Since e and d both satisfy the equation $y \cdot e = e$ and since this equation has a unique solution, $e = d$. Hence on taking account of the relation $d \cdot a = a$, we have $e \cdot a = a$. The proof of the theorem is now complete.

The notation "e" will be reserved for the identity element.

Inverse element. Given $a \in A$, let us consider the two equations

$$a \cdot x = e \quad \text{and} \quad y \cdot a = e .$$

Since we do not have the commutative law at our disposal, it is not obvious that the solutions x and y of these respective equations are equal. Let us see whether it is true, in spite of the non-availability of the commutative law, that $x = y$. Let us multiply each side of $a \cdot x = e$ on the left by y. We obtain

$$y \cdot (a \cdot x) = y \cdot e .$$

Using the associative law and the basic property of the identity, we obtain

$$(y \cdot a) \cdot x = y .$$

Hence

$$e \cdot x = y .$$

Since

$$e \cdot x = x ,$$

we conclude that $x = y$. The common solution of $a \cdot x = e$ and $y \cdot a = e$ is called simply the inverse of a. It is denoted a^{-1}.

Exercises 4

1. Determine the inverse element of an arbitrary element for each of the groups examined in Section 3. The answer is to be stated in terms of the special interpretation of a group given by the example. Thus in Example 1, the answer is "the inverse of a is -a."

2. Show that $a^{-1} \cdot b$ is the solution of $a \cdot x = b$, and that $b \cdot a^{-1}$ is the solution of $y \cdot a = b$.

3. Which of the multiplication tables considered in Section 2 satisfy the group requirements? In case of failure, state the reason. In the case(s) where a group is specified, exhibit the identity element and the inverse of each element.

4. Let A denote a non-empty set, and $\cdot$ an operation in A. Show that there is at most one element $e \in A$ such that $a \cdot e = e \cdot a = a$ for all $a \in A$.

5. Let A denote a non-empty set, and $\cdot$ an operation in A. Suppose that $\cdot$ satisfies the associative law. Suppose that there exists an element $e \in A$ such that $a \cdot e = e \cdot a = a$ for all $a \in A$. (The element e is unique by Exercise 4.) Suppose that for each $a \in A$, there exists $x \in A$ such that $a \cdot x = e$ and that there exists $y \in A$ such that $y \cdot a = e$. Show that A together with $\cdot$ is a group. Hint: With x satisfying $a \cdot x = e$ and y satisfying $y \cdot a = e$, show that $a \cdot z = b$ is satisfied by $x \cdot b$, and, by multiplying each side by y, that the only possible solution is $y \cdot b$. Hence conclude that there is precisely one solution. Treat the remaining case similarly.

6. Construct multiplication tables for operations in a set A of three elements so that the group postulates G 1 and G 2 are satisfied. Hint: We may assume that one of the elements is e, the identity, and we may call one of the remaining elements a and the other b. The construction of a multiplication table can be carried out in only one way when account is taken of the nature of the identity element and the group postulates.

5. An Example of a Non-Abelian Group.

It is not hard to give an example of a group which is not abelian by means of a specifically constructed multiplication table. However, there is greater interest in constructing an example which is meaningful in terms of our earlier experience and which at the same time is important in terms of our future study of mathematics. The elements which we consider are the non-

constant linear functions; that is, the functions ℓ defined for all real numbers by the formulas of the form

5a $$\ell(x) = \alpha x + \beta ,$$

where α and β are real numbers and $\alpha \neq 0$. Our set A is taken to be the set whose elements are the functions ℓ.

It should be observed that a given linear function is defined by precisely one formula of the form 5a. That is, if

$$\alpha x + \beta = \gamma x + \delta \qquad \alpha \neq 0 \text{ and } \gamma \neq 0$$

for all real x, then $\alpha = \gamma$ and $\beta = \delta$. This is seen by first setting $x = 0$ and inferring that $\beta = \delta$ and then that $\alpha = \gamma$.

Composition. Suppose that we are given non-constant linear functions ℓ and m where $\ell(x) = \alpha x + \beta$ and $m(x) = \gamma x + \delta$. It is often of interest to construct a function from the given functions ℓ and m in the following manner. Starting with input x our first function ℓ yields output $\ell(x)$. Suppose that we now use $\ell(x)$ as input with the function m. The output is $m(\ell(x))$. We see that for each real x the quantity $m(\ell(x))$ is unambiguously specified. Thus we have a function determined by the requirement that to each real x there is assigned $m(\ell(x))$. This function is called the composition of m and ℓ. It is denoted by $m \cdot \ell$. Let us determine $m(\ell(x))$ explicitly. We have

5b $$\begin{aligned} m(\ell(x)) &= \gamma(\ell(x)) + \delta \\ &= \gamma(\alpha x + \beta) + \delta \\ &= \alpha\gamma x + (\beta\gamma + \delta) . \end{aligned}$$

This computation shows that the function $m \cdot \ell$ is a non-constant linear function, for the coefficient of x in the last line of Formula 5b is not zero. The rule which assigns to the ordered pair (m,ℓ) of non-constant linear functions the composition function $m \cdot \ell$ is an operation in A. By analogy with what we did with sum and product, we denote the operation of composition by $\cdot$. Let us pause to consider a numerical example before we continue our study of the structure we have just introduced.

Thus, suppose

$$\ell(x) = 2x + 1 \text{ and } m(x) = -2x + 3 .$$

We have for $\ell \cdot m$:

$$\ell(m(x)) = 2m(x) + 1 = 2(-2x + 3) + 1 = -4x + 7 .$$

We have for $m \cdot \ell$:

$$m(\ell(x)) = -2\ell(x) + 3 = -2(2x + 1) + 3 = -4x + 1 .$$

This example shows that with the specific choices made for ℓ and m, we have

$$\ell \cdot m \neq m \cdot \ell .$$

We recall that two functions which have the same input sets (i.e., domain) are different if they assign different outputs for some member of their common input set. In our example $\ell \cdot m$ and $m \cdot \ell$ assign different outputs for each real x. Hence they are distinct functions.

This example shows us that the commutative law does not hold for the operation of composition of (non-constant) linear functions.

How do we show that the structure consisting of the non-constant linear functions together with the operation of composition is a group? We simply verify that G 1 and G 2 are fulfilled with the operation of composition.

G 1. Suppose that ℓ, m, and n are three given (non-constant) linear functions. Given x as input, $\ell \cdot (m \cdot n)$ assigns as output the ℓ output for input $m \cdot n(x)$, i.e., the output for input $m(n(x))$. Given x as input, $(\ell \cdot m) \cdot n$ assigns as output the $\ell \cdot m$ output for input $n(x)$, that is,

$$\ell \cdot m(n(x)) .$$

But $\ell \cdot m(n(x))$ is the ℓ output for input $m(n(x))$. Hence for each real x as input, $\ell \cdot (m \cdot n)$ and $(\ell \cdot m) \cdot n$ assign the same output. Hence the functions $\ell \cdot (m \cdot n)$ and $(\ell \cdot m) \cdot n$ are equal. The associative law G 1 is verified for composition.

G 2 : Given two members of A, ℓ and m, we ask: Is there a member n satisfying

5c $$\ell \cdot n = m ;$$

is there just one such member? Let us try to approach the question in an exploratory way. Let

$$\ell(x) = \alpha x + \beta , \quad m(x) = \gamma x + \delta .$$

Suppose that

$$n(x) = \lambda x + \mu \qquad (\lambda \neq 0)$$

satisfies 5c. From 5b we have

$$\ell \cdot n(x) = \alpha\lambda x + (\beta + \alpha\mu) .$$

Hence if $\ell \cdot n = m$, we have, using the fact that a linear function may be represented by only one formula of the form 5a,

$$\alpha\lambda = \gamma \ , \ \beta + \alpha\mu = \delta \ .$$

Hence

5d $$\lambda = \frac{\gamma}{\alpha} \ , \ \mu = \frac{(\delta - \beta)}{\alpha}$$

We conclude that there is at most one such member n. On the other hand, if we take λ and μ as given by 5d the function n defined by

$$n(x) = \lambda x + \mu$$

does satisfy 5c. Hence 5c has a unique solution.

The treatment of the other equation, $n \cdot \ell = m$, where ℓ and m are given members of A, is similar. Thus we see that the set of non-constant linear functions together with the operation of composition is a non-abelian group.

Exercises 5.

1. Furnish the details concerning the equation $n \cdot \ell = m$, where ℓ and m are given members of A.
2. Determine the identity element of the group which we have studied in this section.
3. Determine the inverse of ℓ if $\ell(x) = \alpha x + \beta$, $\alpha \neq 0$.
4. Show by direct computation that $n = \ell^{-1} \cdot m$ satisfies $\ell \cdot n = m$ and that $n = m \cdot \ell^{-1}$ satisfies $n \cdot \ell = m$ where $\ell(x) = \alpha x + \beta$ and $m(x) = \gamma x + \delta$, $\alpha \neq 0$, $\gamma \neq 0$.
5. Show that $\ell \cdot m = m \cdot \ell$ for the functions of Exercise 4 if and only if $(\alpha - 1)\delta = (\gamma - 1)\beta$.
6. Let A denote the set of ordered pairs of real numbers with non-zero first components. Given (a,b), (c,d) in A, let $(a,b) \cdot (c,d)$ be defined as $(ac, ad + b)$. Show that $(A, \cdot)$ is a group. What is the identity element? What is the inverse of the element (a,b) of A? Is there any relation between this group and the group of non-constant linear functions treated in this section? (Hint: Use No. 5 of Exercises 4.

7. Suppose that A is the set of ordered pairs of rational numbers with non-zero first components and that $\cdot$ is defined as in Exercise 6. Show that $(A, \cdot)$ is a group. Show that a corresponding result holds when A is the set of ordered pairs of complex numbers with non-zero first components and again $\cdot$ is defined as in Exercise 6.

6. Field.

We now turn to the consideration of an algebraic structure which is present in very many areas of mathematical study. We refer to the notion of a field. Once the definition of a field is stated, it will be clear that each of the following number systems is a field:

(a) The rational numbers with the usual addition and multiplication.
(b) The real numbers with the usual addition and multiplication.
(c) The complex numbers with the usual addition and multiplication.

Let A denote a set containing more than one member. Let $+$ and $\cdot$ denote two operations in A. Then $(A, +, \cdot)$ is called a field provided that the following postulates are satisfied:

F 1. The structure $(A, +)$ is an abelian group. (The identity element of this group is called "zero", and is denoted by "0" in accordance with the usage employed for the number systems which we have studied earlier; the inverse of the element a is denoted by $-a$, and the solution of $a + x = b$ by $b - a$).

F 2. Let B denote the set obtained from A by the removal of the element 0. It is required

(1) that $\cdot$ be an operation in B -- i.e., if $b_1, b_2 \in B$, then $b_1 \cdot b_2 \in B$; and

(2) that the structure $(B, \cdot)$ be an abelian group. (The identity element of this group is called "one" and is denoted by "1". When we speak of $\cdot$ as an operation in B, we actually refer, not to the full operation $\cdot$ in A, but rather to the function obtained from $\cdot$ by restricting attention to inputs of the form (b_1, b_2) where b_1 and b_2 are members of B.)

F 3. The two distributive laws

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a,$$

hold, a, b, and c being arbitrary elements of A.

Some remarks are in order.

Given a field $(A, +, \cdot)$, it is sometimes convenient in order to avoid unnecessarily clumsy modes of expression to use the phrase "the field A" and to mean either

(1) the set A, or

(2) the field in the strict sense: $(A, +, \cdot)$.

Which meaning is intended will be clear from context. When we speak of the elements of the field, we mean of course the elements of A.

We shall also agree to write, as is usual, "ab" for "$a \cdot b$".

Of course, it is possible to state the required postulates in alternative form and in detail. The group concept, however, permits us to separate off in individual compartments a description of the action of each of the given operations $+$ and $\cdot$. It is now clear that if the two operations are to be interrelated in a serious sort of way, some condition pertaining to both $+$ and $\cdot$ must be in effect. In the postulates which we have listed, it is F 3 which links $+$ and $\cdot$. In particular, it is natural to turn to F 3 to see how 0 acts in multiplication.

We have

$$0 + 0 = 0,$$

and hence if a is an arbitrary element of A,

$$a(0 + 0) = a0,$$

and

$$(0 + 0)a = 0a.$$

Applying the distributive laws, we obtain

$$a0 + a0 = a0$$

and

$$0a + 0a = 0a,$$

relations which state that $a0$ and $0a$ are each the zero of A; i.e.,

$$a0 = 0a = 0, \qquad a \in A.$$

Postulate F 2 pertains only to B. Are the commutative and associative laws in effect for $\cdot$ in A? The only case that need concern us is when one of the given elements is zero, but then we see that the two laws are in effect, for each side is zero if one of the given elements is.

Since $1 \cdot 0 = 0$ and $1 \cdot a = a$, $a \neq 0$, we see that 1 is an identity element for $\cdot$ in A. The element 1 is the only element in A with this property. If $e \in A$ satisfies $a \cdot e = a$ for all $a \in A$, we have

$$1 \cdot e = 1$$

and

$$1 \cdot e = e.$$

Hence

$$1 = e.$$

Consider equation $a \cdot x = b$. If $a = 0$ and $b \neq 0$, then there is no solution. If $a = 0$ and $b = 0$, then every element of A is a solution. Suppose that $a \neq 0$. Here we see, using the same argument that we used in the study of a group, that if $a \neq 0$, the equation has the unique solution $a^{-1} \cdot b$. Again, following our earlier practice for number systems, we shall denote the solution of $a \cdot x = b$, $a \neq 0$, by $\frac{b}{a}$.

We now see that the identities and theorems which were obtained for the rational number system, the real number system, or the complex number system, and whose proofs depended only on the structural laws which hold for an arbitrary field, continue to hold for an arbitrary field. Thus, if a, b, c, d are members of an arbitrary field and $b \neq 0$ and $d \neq 0$, then

6a $$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Exercises 6

1. Verify that Equation 6a holds for an arbitrary field.
2. Given that a, b, c, d are elements of a field and that $b \neq 0$, $c \neq 0$, $d \neq 0$. Show that $\frac{(\frac{a}{b})}{c} = \frac{a}{bc}$ and that $\frac{(\frac{a}{b})}{(\frac{c}{d})} = \frac{ad}{bc}$.
3. Show that if a, b, c, d, e, f are arbitrary elements of a field and $ae - bd \neq 0$, then the system of equations

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

has a unique solution (x,y) whose components are elements of the field. Give explicit formulas for the solution.

4. Let A consist of the numbers $0, 1, 2$. Let an operation $+$ be defined in A by the requirement that if $a, b \in A$, then $a + b$ is to be the remainder obtained when the number $a + b$ ($+$ being the conventional addition) is divided by 3. Thus if $a = 2$ and $b = 2$, then $a + b$ is the remainder obtained when $4 = 2 + 2$ is divided by 3; i.e., 1. Similarly, let an operation $\cdot$ be defined in A by the requirement that, if $a, b \in A$, then $a \cdot b$ is to be the remainder when the number ab (reference being made to conventional multiplication) is divided by 3. Display the tables for $+$ and $\cdot$. Verify that the structure $(A, +, \cdot)$ is a field. This exercise yields an example of a field which has precisely 3 elements.

5. Let A consist of two distinct elements a, b. Let $+$ and $\cdot$ be the operations in A given by the following tables.

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

Show that the structure $(A, +, \cdot)$ is a field. Specify the additive identity and the multiplicative identity of this field.

7. Subfield.

Given a field whose elements constitute a set A. It is natural to consider subsets B of A which taken together with $+$ and $\cdot$ make up a field; that is, subsets B which have the following two properties:

(1) When $+$ and $\cdot$ are restricted to ordered pairs (b_1, b_2), whose components are in B, they define operations in B.

(2) B together with $+$ and $\cdot$ so restricted is a field.

Such a subset B of A is called a subfield of A. Of course, one can also call such a B taken together with its two operations a subfield of the given field. The meaning which is intended will be clear from context.

With this notion we can proceed to find out something about the architecture of the complex number system. Let Q denote the set of rational numbers; let R denote the set of real numbers, and let C denote the set of complex numbers. We know that Q is a subset of R and that R is a subset of C; in the notation of the theory of sets,

$$Q \subset R \subset C.$$

We may ask whether there are any intermediate subfields between R and C or between Q and R, and whether there is any subfield of the complex number system which is a proper part of Q.

Suppose that A is a subfield of the complex number system which contains R. Suppose that A contains an element not already in R. Then such an element must be of the form $a + bi$ where a and b are real and $b \neq 0$. Since $a \in A$, $(a + bi) - a = bi \in A$. Since $b \in A$, $i \in A$. Hence given arbitrary real numbers c and d, we have $di \in A$ and therefore $c + di \in A$. That is, $C \subset A$. We need to recall that if $A \subset C$ and $C \subset A$, then $A = C$. Hence $A = C$. We are led to the following conclusion:

Theorem 7a. If A is a subfield of the complex number system containing R, then either $A = R$ or $A = C$.

This theorem states that there is no subfield of the complex number system which contains R as a proper subset and at the same time is a proper subset of C.

A second result that is easy to obtain is the following:

Theorem 7b. Every subfield of the complex number system contains Q.

Proof: Let A denote a subfield of the complex number system. We note that if a and b belong to A and $b \neq 0$, then $\frac{a}{b} \in A$. Now $1 \in A$. It is a consequence of the additive closure of A and the well-ordering property of the natural number system that every natural number is a member of A.* Suppose that there are one or more natural numbers not in A and let m be the minimal member of the set of natural numbers not in A (the well-ordering property assures us there is such a minimal member). Then $m - 1$ is a member of A, but our hypothesis tells us m is not. Since $m = (m - 1) + 1$ and $m - 1$ and 1 are in A, it follows from the additive closure of A that m itself is in A. This contradiction proves that the set of natural numbers not in A is empty. It now follows that every integer is a member of A, since for each natural number n, $-n$ is a member of A. Since A contains the quotients of its members, it follows that A contains every quotient of the form $\frac{p}{q}$ where p and q are integers and $q \neq 0$. This says that every rational number is a member of A. In other words, $Q \subset A$. The theorem is established.

---

* See G. Birkhoff and S. MacLane, A Survey of Modern Algebra; N.Y., MacMillan, 1946; p. 9

Subfields intermediate to Q and R. There is a vast hierarchy of subfields between Q and R. Their study is a large undertaking. We shall content ourselves to see that certain intermediate fields can be exhibited in a simple way.

Let A denote the set of real numbers of the form

$$a + b\sqrt{2} ,$$

where a and b are both rational numbers. What can be said about the sum and product of elements of A ? Given that a , b , c , d are rational numbers, we see that

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} ,$$

and since a + c and b + d are rational numbers, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) \in A .$$

Similarly,

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} ,$$

and since ac + 2bd and ad + bc are rational numbers, we have

$$(a + b\sqrt{2})(c + d\sqrt{2}) \in A .$$

Suppose that $a + b\sqrt{2} = 0$ where a and b are rational numbers. Then $b = 0$, otherwise $\sqrt{2}$ would be a rational number. It follows that also $a = 0$. Therefore, a member $a + b\sqrt{2}$ of A (a and b rational numbers) is equal to zero if and only if $a = 0$ and $b = 0$. This implies that if $a + b\sqrt{2} \neq 0$, then $a^2 - 2b^2 \neq 0$. Otherwise we should have

$$0 = a^2 - 2b^2 = (a + b\sqrt{2})(a + (-b)\sqrt{2}) ,$$

so that either $a + b\sqrt{2} = 0$ or $a + (-b)\sqrt{2} = 0$. From $a + (-b)\sqrt{2} = 0$, we have $a = 0$ and $-b = 0$ and consequently $a + b\sqrt{2} = 0$. That is, if $a^2 - 2b^2 = 0$ then $a + b\sqrt{2} = 0$.

We now have by a familiar rationalization method,

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})}$$

$$= \frac{(ac - 2bd)}{c^2 - 2d^2} + \frac{(bc - ad)\sqrt{2}}{c^2 - 2d^2}$$

This tells us that the quotient of two members of A is also a member of A.

It is now easy to verify that A is a subfield of the real number system. We leave the details as an exercise.

Exercises 7

1. Show that A is a subfield of the real number system.
2. Let B denote the set of real numbers of the form $a + b\sqrt{3}$ where a and b are rational numbers. Show that B is a subfield of the real number system.
* 3. Show that the only real numbers belonging to both A and B are rational numbers. In particular, $\sqrt{3}$ does not belong to A. Hence, A is intermediate in the strict sense to Q and R. That is, Q is a proper part of A, and A is a proper part of R.

References:

1. Birkhoff, Garrett and Saunders MacLane, A Survey of Modern Algebra (rev. ed.), Macmillan Company.
2. Books cited in the bibliography of Reference 1 above.

ANSWERS TO PROBLEMS

Exercise 2.

1.

	a	b
a	a	b
b	a	a

,

	a	b
a	a	a
b	b	a

,

	a	b
a	b	a
b	a	a

,

	a	b
a	a	a
b	b	b

,

	a	b
a	a	b
b	a	a

,

	a	b
a	b	b
b	a	a

,

	a	b
a	b	a
b	b	a

,

	a	b
a	b	a
b	a	b

,

	a	b
a	a	b
b	b	b

,

	a	b
a	b	a
b	b	b

,

	a	b
a	b	b
b	a	b

,

	a	b
a	b	b
b	b	a

.

2. That $\cdot$ is an operation in A follows from the fact that the product in the conventional sense of members a and b of A is itself a member of A. The multiplication table is:

$\cdot$	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Exercises 3.

1. Here only Example 4 calls for comment. Suppose that α and β are nth roots of 1. From $\alpha^n = 1$ and $\beta^n = 1$, we have $(\alpha\beta)^n = 1$ and $(\frac{\alpha}{\beta})^n = 1$. That is, $\alpha\beta$ and $\frac{\alpha}{\beta}$ are each nth roots of 1. From the fact that $\alpha\beta$ is an nth root of 1, we see that $\cdot$ is an operation in A. From the fact $\frac{\alpha}{\beta}$ is an nth root of 1, we see that Postulate G 2 is fulfilled, the uniqueness of solution of the equation $\beta z = \alpha$ in A being guaranteed by the uniqueness of the solution of $\beta z = \alpha$ in C. The associative law follows automatically from the fact that multiplication in the complex number system is associative. Note that $\cdot$ is commutative. Consequently the equation $z\beta = \alpha$ has exactly the same solution set in A as does $\beta z = \alpha$.

2. Not every equation of the form $\alpha z = \beta$ where α and β are given complex numbers has a solution; e.g., take $\alpha = 0$; $\beta = 1$.

3. Given a, b, c, d integers, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in A ,$$

since $a + c$ and $b + d$ are integers. Also the equation

$$(a + b\sqrt{2}) + x = c + d\sqrt{2}$$

has the unique solution

$$(c - a) + (d - b)\sqrt{2} .$$

in R., and moreover this solution is a member of A since $c - a$ and $d - b$ are both integers. The remaining details are readily furnished.

4. See Section 7 of this booklet, "Subfields intermediate to Q and R."

Exercises 4.

1. Example 2: the inverse of a is $\frac{1}{a}$.

Example 3: the inverse of (a, b, c) is $(-a, -b, -c)$.

Example 4: the inverse of $\alpha = \cos(\frac{2\pi k}{n}) + i \sin(\frac{2\pi k}{n})$, $k = 0, 1, \ldots, n - 1$, is $\frac{1}{\alpha} = \cos(\frac{2\pi k}{n}) - i \sin(\frac{2\pi k}{n})$.

Example 5: the inverse of a is $\frac{1}{a}$.

Exercise 3: the inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2}$.

Exercise 4: the inverse of $a + b\sqrt{2}$ is

$$\left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2} .$$

2.
$$\begin{aligned} a \cdot (a^{-1} \cdot b) &= (a \cdot a^{-1}) \cdot b \\ &= e \cdot b \\ &= b . \end{aligned}$$

$$\begin{aligned} (b \cdot a^{-1}) \cdot a &= b \cdot (a^{-1} \cdot a) \\ &= b \cdot e \\ &= b. \end{aligned}$$

3. The table for $\{0,1\}$ does not satisfy the group requirements. The equation $0 \cdot x = 1$ does not have a solution in $\{0,1\}$. The first three tables given for $\{a,b\}$ do not satisfy the group requirements, for in the cases of the first and third tables the equation $a \cdot x = b$ has no solution in A and in the case of the second table the equation $b \cdot x = a$ has no solution in A.

The fourth table for $\{a,b\}$ does satisfy the group requirements. That G 2 is satisfied may be seen by noting that each new row and each column of the body of the table contain each of the elements a and b (without repetition).

Notice that we cannot be cavalier about the associative law! We must examine the 8 cases afforded by the distinct ordered triples with components in A. The confirmation of the associative law is given by the following table.

c_1	c_2	c_3	$c_1 \cdot (c_2 c_3)$	$(c_1 c_2) \cdot c_3$
a	a	a	$a \cdot (aa) = a \cdot a = a$	$(aa) \cdot a = a \cdot a = a$
a	a	b	$a \cdot (ab) = ab = b$	$(aa) \cdot b = a \cdot b = b$
a	b	a	$a(ba) = ab = b$	$(ab)a = ba = b$
a	b	b	$a(bb) = aa = a$	$(ab)b = bb = a$
b	a	a	$b(aa) = ba = b$	$(ba)a = ba = b$
b	a	b	$b(ab) = bb = a$	$(ba)b = bb = a$
b	b	a	$b(ba) = bb = a$	$(bb)a = aa = a$
b	b	b	$b(bb) = ba = b$	$(bb)b = ab = b$

Each of the indicated reductions in the second and third columns of the body of the table is carried out by use of the multiplication table with which we are concerned.

We have: $e = a$, $a^{-1} = a$, $b^{-1} = b$.

The table

$\cdot$	a	b
a	b	b
b	a	a

yields an example of a non-associative operation. In fact, $(aa)b = bb = a$ and $a(ab) = ab = b$, so that $(aa)b \neq a(ab)$, a being distinct from b.

4. Suppose that e and f are elements of A satisfying for each $a \in A$.

$$ae = ea = a ,$$
$$af = fa = a .$$

Then setting $a = f$ in the first line, we obtain

$$fe = f ,$$

and setting $a = e$ in the second line, we obtain

$$fe = e .$$

Hence

$$e = f .$$

It follows that there is at most one element $e \in A$ satisfying for all $a \in A$: $ae = ea = a$.

5. We have

$$a(xb) = (ax)b = eb = b ,$$

so that xb is a solution of $az = b$. Thus $az = b$ has at least one solution. If z is any solution of $az = b$, we have

$$yb = y(az) = (ya)z = ez = z ,$$

so the only possibility for z is the element yb . Thus $az = b$ has at most one solution in A . Hence the equation $az = b$ has a unique solution in A .

The equation $wa = b$ is similarly treated.

Corollary. $x = y$.

We found (i) xb satisfies $az = b$, (ii) no member of A besides yb satisfies $az = b$. It follows that $xb = yb$. But b is arbitrary. Taking $b = e$, we obtain $x = y$. (Thus a "right" inverse is also a "left" inverse -- even if our operation is non-commutative, provided each of them exists. We neither knew nor needed this fact in solving Exercise 4, No. 4, however.)

6. Since e is the identity element, the following part of the table is evident:

	e	a	b
e	e	a	b
a	a		
b	b		

Consider the product aa. It is not possible that $aa = a$, for $ae = a$ and the equation $ax = a$ has a unique solution.

It is not possible that $aa = e$, for if $aa = e$, then

$$ab = b$$

since the equation $ax = b$ has a solution in A and this solution would have to be distinct from e and a. Since

$$eb = b,$$

and the equation $yb = b$ has a unique solution, we should be forced to conclude that $a = e$. This is impossible. We must reject $aa = e$. Hence necessarily $aa = b$.

At this stage we are assured that our table contains the following entries:

·	e	a	b
e	e	a	b
a	a	b	
b	b		

Since the element a has an inverse of a^{-1} and neither e nor a is the inverse of a (as we see from the second line of the table as far as it has been constructed), $a^{-1} = b$. Hence $ab = ba = e$. We have at this stage

·	e	a	b
e	e	a	b
a	a	b	e
b	b	e	

We now see, since the equation $bx = a$ has a solution in A and this solution is different from e and a, that $bb = a$. Conclusion: If we have a group containing precisely three elements: e, a, b, and e is the identity element, the multiplication table is

(*)

·	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We must note that we have merely shown that, if $(A, \cdot)$ is a group, then the multiplication table is given by (*). There remains to be shown that (*) does respect the group axioms.

G 2. Since each row and column of the body of (*) contains each of the elements of A precisely once, G 2 is satisfied.

G 1. We may break down the checking of the associative law into two cases.

Case 1. At least one of the factors is e. This case is disposed of by noting

$$(ec_2)c_3 = c_2c_3 = e(c_2c_3), \quad c_2, c_3 \in A;$$
$$(c_1e)c_3 = c_1c_3 = c_1(ec_3), \quad c_1, c_3 \in A;$$
$$(c_1c_2)e = c_1c_2 = c_1(c_2e), \quad c_1, c_2 \in A.$$

Case 2. No factor is e. We list all the possibilities and compute the desired products employing (*).

c_1	c_2	c_3	$(c_1c_2)\cdot c_3$	$c_1\cdot(c_2c_3)$
a	a	a	(aa)a = ba = e	a(aa) = ab = e
a	a	b	(aa)b = bb = a	a(ab) = ae = a
a	b	a	(ab)a = ea = a	a(ba) = ae = a
a	b	b	(ab)b = eb = b	a(bb) = aa = b
b	a	a	(ba)a = ea = a	b(aa) = bb = a
b	a	b	(ba)b = eb = b	b(ab) = be = b
b	b	a	(bb)a = aa = b	b(ba) = be = b
b	b	b	(bb)b = ab = e	b(bb) = ba = e

Exercises 5.

1. Here $n \cdot \ell(x) = \lambda(\alpha x + \beta) + \mu$. From $n \cdot \ell = m$, we conclude that $\lambda\alpha = \gamma$ and $\lambda\beta + \mu = \delta$. Hence $\lambda = \frac{\gamma}{\alpha}$, $\mu = \delta - (\beta\frac{\gamma}{\alpha})$. With λ and μ so taken $n \cdot \ell = m$.
2. The identity element is the linear function e given by $e(x) = 1 \cdot x + 0 = x$.
3. From $\ell \cdot n = e$, we have $\lambda = \frac{1}{\alpha}$, $\mu = -\frac{\beta}{\alpha}$.

4. $\ell(x) = \alpha x + \beta$, $m(x) = \gamma x + \delta$; $\ell^{-1}(x) = \frac{1}{\alpha}x + (\frac{-\beta}{\alpha})$.

$\ell^{-1} \cdot m(x) = \frac{1}{\alpha}(\gamma x + \delta) + (\frac{-\beta}{\alpha}) = (\frac{\gamma}{\alpha})x + \frac{\delta - \beta}{\alpha}$.

$\ell \cdot (\ell^{-1} \cdot m)(x) = \alpha[(\frac{\gamma}{\alpha})x + \frac{\delta - \beta}{\alpha}] + \beta = \gamma x + \delta$.

$m \cdot \ell^{-1}(x) = \gamma[\frac{1}{\alpha}x + (\frac{-\beta}{\alpha})] + \delta = \frac{\gamma}{\alpha}x + \frac{\alpha\delta - \beta\gamma}{\alpha}$.

$(m \cdot \ell^{-1}) \cdot \ell(x) = \frac{\gamma}{\alpha}(\alpha x + \beta) + \frac{\alpha\delta - \beta\gamma}{\alpha} = \gamma x + \delta$.

5. We have $\ell \cdot m(x) = \alpha\gamma x + (\beta + \alpha\delta)$ and $m \cdot \ell(x) = \gamma\alpha x + (\delta + \gamma\beta)$. Hence $\ell \cdot m = m \cdot \ell$ if and only if $\beta + \alpha\delta = \delta + \gamma\beta$. This latter equality holds if and only if $\alpha\delta - \delta = \gamma\beta - \beta$. The assertion follows.

6. Note that, if (a,b) , $(c,d) \in A$, then $(a,b) \cdot (c,d) = (ac\,,\, ad + b) \in A$ since $ac \neq 0$. Given elements (a_1, b_1) , (a_2, b_2) , $(a_3, b_3) \in A$, we have

$$((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) = (a_1a_2\,,\, a_1b_2 + b_1) \cdot (a_3, b_3)$$
$$= (a_1a_2a_3\,,\, a_1a_2b_3 + (a_1b_2 + b_1)) ,$$

and

$$(a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)) = (a_1, b_1) \cdot (a_2a_3\,,\, a_2b_3 + b_2)$$
$$= (a_1a_2a_3\,,\, a_1(a_2b_3 + b_2) + b_1) .$$

The associative law now follows.

Note that for every $(a,b) \in A$, we have

$$(a,b) \cdot (1,0) = (1,0) \cdot (a,b) = (a,b) .$$

Hence A has an identity element, namely $(1,0)$. Further, $(\frac{1}{a}, -\frac{b}{a})$ satisfies both

$$(a,b) \cdot (x,y) = (1,0)$$

and

$$-(x,y) \cdot (a,b) = (1,0) .$$

The conditions of Exercise 4, No. 5 are fulfilled. $(\frac{1}{a}, -\frac{b}{a})$ is the inverse of (a,b) .

A $(1,1)$ correspondence between A and the set of non-constant linear functions is defined by the rule which assigns to $(a,b) \in A$ the linear function given by

$$\ell(x) = ax + b .$$

This correspondence has the property that if m corresponds to $(c,d) \in A$, then $m \cdot \ell$ corresponds to $(c,d) \cdot (a,b)$. That is, "product corresponds to product." This is an instance of an isomorphism. The structure $(A, \cdot)$ was, of course, constructed in an obvious way from the group of non-constant linear functions with composition as the operation. The object of the exercise was to construct a group isomorphic to an important group of common occurrence but having elements and rules of a different nature.

7. This exercise is straightforward. It suffices to note in either case that $\cdot$ is an operation, that $(1,0) \in A$ is the identity element, that, if $(a,b) \in A$, then $(\frac{1}{a}, -\frac{b}{a}) \in A$ and that the verification of the associative law remains valid for the case where A consists of the set of ordered pairs of complex numbers with non-zero first components.

Exercises 6.

1. We note that $(bd)(b^{-1}d^{-1}) = 1$, so that $(bd)^{-1} = b^{-1}d^{-1}$. Hence

$$\begin{aligned}\frac{ad + bc}{bd} &= (bd)^{-1}(ad + bc), \\ &= b^{-1}d^{-1}(ad + bc) \\ &= (b^{-1}d^{-1})(ad) + (b^{-1}d^{-1})(bc) \\ &= b^{-1}a + d^{-1}c \\ &= \frac{a}{b} + \frac{c}{d}.\end{aligned}$$

The details are readily supplied.

2. The argument may be based on the use of reciprocals. Thus

$$\begin{aligned}\frac{(\frac{a}{b})}{c} &= c^{-1} \cdot (b^{-1}a) \\ &= (b^{-1}c^{-1}) \cdot a \\ &= (bc)^{-1}a \\ &= \frac{a}{bc}.\end{aligned}$$

The second part may be treated as follows.

$$\frac{(\frac{a}{b})}{(\frac{c}{d})} = \frac{(b^{-1}a)}{(d^{-1}c)}$$

$$= (d^{-1}c)^{-1}(b^{-1}a)$$

$$= ((d^{-1})^{-1}c^{-1})(b^{-1}a)$$

$$= (bc)^{-1}(ad)$$

$$= \frac{ad}{bc} .$$

The following points should be emphasized:

(a) The indicated calculations in the asserted identity are all meaningful, there being no divisions by zero.

(b) $(d^{-1})^{-1} = d$.

(c) A corresponding result holds for an arbitrary abelian group.

3. The given pair of equations imply

$$\begin{cases} e(ax + by) = ce \\ b(dx + ey) = bf \end{cases} \qquad \begin{cases} d(ax + by) = cd \\ a(dx + ey) = af \end{cases}$$

and subtraction gives (respectively)

$$(ae - bd)x = ce - bf , \qquad (ae - bd)y = af - cd .$$

Since $ae - bd \neq 0$, we conclude

$$x = \frac{ce - bf}{ae - bd} , \qquad y = \frac{af - cd}{ae - bd} ;$$

so that <u>if</u> our system has any solution (x,y) it must be

$$\left(\frac{ce - bf}{ae - bd} , \frac{af - cd}{ae - bd}\right)$$

Substitution in the original equations verifies that this couple is indeed a solution:

$$a \cdot \frac{ce - bf}{ae - bd} + b \cdot \frac{af - cd}{ae - bd} = \frac{ace - abf + abf - bcd}{ae - bd} = c$$

$$d \cdot \frac{ce - bf}{ae - bd} + e \cdot \frac{af - cd}{ae - bd} = \frac{cde - bdf + aef - cde}{ae - bd} = f .$$

4.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Both commutative laws follow from the very construction of the addition and multiplication tables. On turning to the table (*) of Exercise 4, No. 6, we see on taking $e = 0$, $a = 1$, $b = 2$, that $(A, +)$ is a group whose identity element is 0. The postulate F 1 is verified. The postulate F 2 is readily checked from the multiplication table. (Be sure that the associative law is verified.)

As far as F 3 is concerned we may put aside the case where $a = 0$ since we know that the product 0 and any element of A is 0. Further since multiplication is commutative, it suffices to consider only the first of the two distributive laws. The check may be tabulated as follows:

a	b	c	a · (b + c)	a · b + a · c
1	0	0	1 · 0 = 0	0 + 0 = 0
1	0	1	1 · 1 = 1	0 + 1 = 1
1	0	2	1 · 2 = 2	0 + 2 = 2
1	1	0	1 · 1 = 1	1 + 0 = 1
1	1	1	1 · 2 = 2	1 + 1 = 2
1	1	2	1 · 0 = 0	1 + 2 = 0
1	2	0	1 · 2 = 2	2 + 0 = 2
1	2	1	1 · 0 = 0	2 + 1 = 0
1	2	2	1 · 1 = 1	2 + 2 = 1
2	0	0	2 · 0 = 0	0 + 0 = 0
2	0	1	2 · 1 = 2	0 + 2 = 2
2	0	2	2 · 2 = 1	0 + 1 = 1
2	1	0	2 · 1 = 2	2 + 0 = 2
2	1	1	2 · 2 = 1	2 + 2 = 1
2	1	2	2 · 0 = 0	2 + 1 = 0
2	2	0	2 · 2 = 1	1 + 0 = 1
2	2	1	2 · 0 = 0	1 + 2 = 0
2	2	2	2 · 1 = 2	1 + 1 = 2

This is, quite frankly, tedious. If the division algorithm has been developed, as well as the result that if a prime number divides a product of integers it divides one of the factors, it is not hard to generalize this exercise to the case where 3 is replaced by an arbitrary prime p, A is replaced by $\{0,1,\ldots,p - 1\}$ and "addition" and "multiplication" are defined as in the exercise save that we operate with remainders obtained on division by p. If p is replaced by a natural number which is not a prime, the resulting structure is not a field.

5. The verification of F 1 and F 2 is immediate. cf. Exercise 4, No. 3. The additive identity is a and the multiplicative identity is b . Note that B consists simply of the element b . It suffices to verify

$$b(c_1 + c_2) = bc_1 + bc_2 , \quad c_1 , c_2 \in A ,$$

to be assured that F 3 holds. Since $b = 1$,

$$b(c_1 + c_2) = c_1 + c_2$$

and

$$bc_1 + bc_2 = c_1 + c_2 .$$

Exercises 7.

1. From our formulas for sum and product we see that the usual addition and multiplication define operations in A . The difference of two elements of A is an element of A , as is easily checked. We have seen that the same holds true for quotients of elements of A . The commutative, associative and distributive laws hold for $(A, +, \cdot)$ since they hold for the real number system. The verification of the field postulates is now routine.
2. The details parallel those of the first exercise and are readily furnished.
3. Suppose that x is a real number belonging to both A and B . Since $x \in A$, $x = a + b\sqrt{2}$ where a and b are rational. Since $x \in B$, $x = c + d\sqrt{2}$ where c and d are rational. It is essential to recall that $\sqrt{2}$ and $\sqrt{3}$ are both irrational. We start with the equality

$$a + b\sqrt{2} = c + d\sqrt{3}$$

and draw the consequences.

Case 1. $d = 0$. Here x is a rational number.

Case 2. $d \neq 0$. Here we conclude that

$$\sqrt{3} = \frac{a - c}{d} + \frac{b}{d}\sqrt{2} ,$$

that is, $\sqrt{3}$ is of the form

$$\alpha + \beta\sqrt{2}$$

where α and β are both rational numbers. On taking squares, we have

$$3 = (\sqrt{3})^2 = (\alpha + \beta\sqrt{2})^2 .$$

$$\alpha^2 + 2\beta^2 + (2\alpha\beta)\sqrt{2} .$$

Since

$$3 = 3 + 0\sqrt{2} ,$$

we conclude, by the uniqueness property established in Section 7 concerning the representation of the members of A in the form $a + b\sqrt{2}$, a and b rational numbers, that

$$3 = \alpha^2 + 2\beta^2$$

and

$$0 = 2\alpha\beta .$$

Now $\beta \neq 0$ since $\sqrt{3}$ is an irrational number. Hence from $0 = 2\alpha\beta$, we conclude that $\alpha = 0$ and

(**) $$3 = 2\beta^2 .$$

At this point we make use of the fact that β may be written in the form $\frac{p}{q}$ where p and q are natural numbers which are not both divisible by a natural number greater than one. In particular, p and q cannot both be even. From (**) we obtain

$$3 = 2\left(\frac{p}{q}\right)^2$$

and hence

(***) $$3q^2 = 2p^2 .$$

Now q must be even, otherwise the left-hand side of (***) would be odd and the right-hand side even. Hence $q = 2r$, where r is a natural number. From (***) we obtain

$$3(2r)^2 = 2p^2 ,$$

and hence

$$6r^2 = p^2 .$$

We now see that p is even. This is impossible, for p is odd. Hence the hypothesis $\alpha \neq 0$ must be rejected.

Conclusion: x is a rational number; i.e., $A \cap B \subset Q$.

Since $Q \subset A \cap B$, we have $Q = A \cap B$.

Note: $A \cap B$ means the intersection of sets A and B.