DOCUMENT RESUME

ED 175 688 SE 028 676

AUTHOR Schaaf, William L., Ed.
TITLE Reprint Series: Structure of Algebra. RS-1.
INSTITUTION Stanford Univ., Calif. School Mathematics Study Group.
SPONS AGENCY National Science Foundation, Washington, D.C.
PUB DATE 66
NOTE 45p.; For related documents, see SE 028 677-690

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS *Algebra; Curriculum; *Enrichment; *History; *Instruction; Mathematics Education; *Number Systems; Secondary Education; *Secondary School Mathematics; Supplementary Reading Materials
IDENTIFIERS *School Mathematics Study Group

ABSTRACT

This is one in a series of SMSG supplementary and enrichment pamphlets for high school students. This series makes available expository articles which appeared in a variety of mathematical periodicals. Topics covered include: (1) axioms in algebra; (2) the foundations of algebra; and (3) noncommutative algebra. (MP)

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

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

Some classes and many individual students, however, may find time to pursue mathematical topics of special interest to them. The School Mathematics Study Group is preparing pamphlets designed to make material for such study readily accessible. Some of the pamphlets deal with material found in the regular curriculum but in a more extended manner or from a novel point of view. Others deal with topics not usually found at all in the standard curriculum.

This particular series of pamphlets, the Reprint Series, makes available expository articles which appeared in a variety of mathematical periodicals. Even if the periodicals were available to all schools, there is convenience in having articles on one topic collected and reprinted as is done here.

This series was prepared for the Panel on Supplementary Publications by Professor William L. Schaaf. His judgment, background, bibliographic skills, and editorial efficiency were major factors in the design and successful completion of the pamphlets.

PREFACE

The history of mathematics covers several thousand years. About 2000 B.C. there began a slow development of arithmetic and numbers as well as empirical geometry. The history of geometry during this period is quite familiar, although the work that was done in arithmetic and numbers is not nearly so well known. Indeed, few significant advances were made in algebra until about the third century A.D., when some interest was shown in the methods of solving "story problems." Since very few symbols had been developed up to that time, no general methods were discovered and the rules of grammatical syntax were still observed.

Between 400 A.D. and 1100 A.D. some development in mathematics occurred in Arabia and Persia. The resulting body of knowledge was called *algebra*. The term was derived from the words *al-jaber w'al muqâbalah*, which mean "restoration and opposition," and which allude to the solution of simple equations by sheer manipulation. (In Spain, during the Middle Ages, an *algebrista* was a "restorer"; that is, a man who reset broken bones, usually a barber.)

The middle years of the Renaissance were distinguished by the emergence of *symbolic algebra*. By the twelfth century, the algebra of the Arabs had become known in Europe. The new movement stimulated men such as Fibonacci, Pacioli, Cardan, Bombelli, Rudolf, Stifel, Stevin, Vieta, Clavius, Recorde, Harriot, Oughtred, and Wallis, who contributed to a continual and very valuable improvement in the symbols that were used. This made possible not only greater facility in manipulation, but also something of far greater importance: new insights and ideas. This in turn led to a recognition of patterns and eventually what today is called the *structure* of algebra.

Much of the work of these men and others was concerned with the solution of polynomial equations. To a seventeenth-century mathematician, "solving" an equation meant either one of two things: (1) finding a numerical approximation to a root by a geometrical construction or an appropriate computation; or (2) finding a solution by means of radicals, that is, expressing the roots of a polynomial equation in terms of its rational coefficient using only elementary operations of addition, subtraction, multiplication, division, and the extraction of roots a finite number of times. By this time solutions of the latter type were known for equations of the 2nd, 3rd, and 4th degree, but no solution was known for equations of the 5th degree or higher. Many formal procedures for manipulating algebraic expressions were devised and many ingenious methods were used, but no attention was given to any underlying principle or generalization.

After many unsuccessful attempts to solve the general 5th degree equation, or general quintic, mathematicians began to suspect that the quintic was not "solvable." In 1824 the Norwegian mathematician, Abel, proved that a solution to the 5th degree equation was impossible. A few years later the French mathematician Galois discovered the conditions under which it is possible to solve any polynomial equation by radicals. These two mathematicians achieved their success, which was a tremendous breakthrough in the development of mathematics, by searching for general properties of equations. They did not confine their attention to particular numerical coefficients or to the manipulation of symbols; instead, they initiated a study of the *structure of mathematical systems*. In the course of his work, Galois developed a theory of groups, a group being one of the basic units in algebraic structure. It is generally realized today that the nature of algebra is more clearly revealed by studying the structure of a particular system than it is by manipulating symbols. In fact, modern mathematicians study many different algebraic structures and refer to "algebras and their arithmetics."

To appreciate the full meaning of this statement, it is important to understand the nature of mathematics. Contemporary twentieth century mathematics rests fundamentally on an axiomatic basis. This means that in any branch of mathematics, we first identify or recognize a few basic terms which are left undefined. As one can quickly realize, there comes a point where things can no longer be defined, since new words will of necessity be used in that definition. There must then be a few words (the fewer the better) which are "first" terms and which must therefore be left undefined. Next, a set of assumptions about these undefined terms, or primitives, is agreed upon. Thereafter, all subsequent terms are defined in terms of the primitives, and the theorems are deduced from the assumptions by logical procedures. When we speak of a mathematical system, we mean a specified set of elements together with one or more operations defined with respect to these elements and the accompanying set of assumptions. The elements in question need not be numbers: they may be points, lines, or other geometric configurations. The operations do not have to be the familiar operations of arithmetic: they may be movements, rotations, reflections, or an assortment of other possibilities.

It is important to note that every mathematical science has a distinctive pattern or structure which is established arbitrarily by man. By changing the assumptions, a new system with different characteristics and possessing a different structure can be created.

The study of the structure of algebra is extremely important at the present time. Not only does this study give tremendous insight into what has been done in the past, but it also provides a very fruitful path to new discoveries. The essays that follow are concerned with structure. It is to be hoped that they will shed generous light on the meaning of this concept and contribute to the reader's appreciation of its significance.

—William L. Schaaf

CONTENTS

ACKNOWLEDGMENTS

The School Mathematics Study Group takes this opportunity to express its gratitude to the authors of these articles for their generosity in allowing their material to be reproduced in this manner: John K. Baumgart, of Manchester College, North Manchester, Indiana; Charles Brumfiel, of Ball State Teachers College, Muncie, Indiana; Arnold Wendt, of Western Illinois University, Macomb, Illinois; and Clarence Perisho, of Mankato State College, Mankato, Minnesota.

The School Mathematics Study Group is also pleased to express its sincere appreciation to the several editors and publishers who have been kind enough to allow these articles to be reprinted, namely:

THE MATHEMATICS TEACHER:

(1) John K. Baumgart, "*Axioms in Algebra; Where Do They Come From?*" vol. 54 (March 1961), p. 155-160.

(2) Charles Brumfiel, "*The Foundations of Algebra,*" vol. 50 (November 1957), p. 488-492.

(3) Arnold Wendt, "*A Simple Example of a Non-commutative Algebra,*" vol. 52 (November 1959), p. 534-540.

SCHOOL SCIENCE AND MATHEMATICS:

(1) Clarence Perisho, "*A Non-Commutative Algebra,*" vol. 58 (December 1958), p. 727-730.

FOREWORD

Modern mathematics started in the half century that began with the appearance of Descartes' *GEOMETRIE* (1637) and ended with the publication of Newton's *PRINCIPIA* (1687). At about the same time, modern arithmetic became prominent with the work of Fermat (1630-1665). During the next 150 years mathematicians were largely concerned with extending the number system of algebra. It was not until Gauss appeared (1800-1830) that modern *abstract arithmetic and algebra* can be said to have begun.

Yet it was the brilliant creation of Lobachewsky's non-Euclidean geometry (c. 1830) that gave the impetus to the unconscious search for mathematical structure. Thus the beginning of the abstract approach to algebra paralleled the acceptance of non-Euclidean geometries. Mathematicians once again followed the clue suggested by Euclid more than two thousand years earlier: begin with definitions and postulates, then deduce the theorems.

The door to the creation of mathematical structure was opened by the invention of quaternions by Hamilton (1843), when he took the daring step of rejecting the commutative law of multiplication. With this deliberate abandoning of a restrictive "law," an entirely new approach was possible. Henceforth algebra and arithmetic were liberated. Mathematicians were now free to create self-consistent algebras as they had shortly before learned to create "contradictory" but self-consistent geometries.

From then on into the beginning of the twentieth century the development of mathematical structures continued at an accelerated pace. It permeated arithmetic, algebra, geometry, analysis. There followed in rapid succession Grassmann's *AUSDEHNUNGSLEHRE*, or generalized quaternions (1844); Cayley's matrices; J. Willard Gibbs' vector analysis (1880); the contributions of Abel and Galois to the theory of algebraic equations and to group theory; Boole's mathematical logic (c. 1850); and the contributions of Dedekind and Kronecker to abstract algebra (1870-1890).

Thus, since 1900, we may say that mathematics in general, and algebra in particular, have been "arithmetized"; that is to say, great emphasis is now put upon the formalization of postulates and meticulous attention is given to the structure of the system deduced from the postulates. While the term "structure" is not easily defined, it is fairly simple to tell what is meant by "same structure." It is hoped that this and the other articles will make these ideas more meaningful.

Axioms in Algebra—Where Did They Come From?[1]

John K. Baumgart

Today we hear a great deal about revision of the mathematics curriculum on both the high school and college levels. At the high school level some proposals involve the presentation of algebra from a more axiomatic viewpoint—in much the same way as geometry has been built logically from a set of axioms. It is interesting and instructive to trace the development of the axioms for algebra.

Every mathematics teacher has seen in at least one algebra book a set of "rules" such as

$$a + b = b + a,$$

$$ab = ba,$$

$$a(b + c) = ab + ac,$$

and so on. Sometimes the reaction has been "Why bother to list such obvious statements?"

We shall try to show that these "obvious statements" were abstracted from a system of arithmetic and algebra (and, in fact, from geometry, too) which just grew, like Topsy. But the system grew to fulfill a need for that kind of mathematical structure which it eventually became; this structure is now called a *field*.

Consider, for example, the property $a + b = b + a$. In rudimentary and concrete terms this was obvious even to primitive man. He knew that it made no difference whether he first made three vertical marks on a wall and then two, or first two and then three. This was the intuitive level of using the commutative law: $3 + 2 = 2 + 3$.

The Egyptians (as early as 1850 B.C.) showed a curious awareness that something was involved in assuming that $ab = ba$. A. B. Chace in his commentary on the Rhind Papyrus remarks that the Egyptian method of multiplication emphasized a distinction between multiplicand and mul-

[1] Written while on an NSF Science Faculty Fellowship at the University of Michigan. Many helpful suggestions were made by Professor Phillip S. Jones.

tiplier, but it was known that if the two were interchanged the product would be the same [1].[2] An example of this interchange of factors occurs in Problem 26 of the Rhind Papyrus [2]. The problem has additional interest as an example of the Egyptian method of solving what we would today call an algebra problem. The method used is known as the method of *false position;* that is, a solution is guessed at and then revised.

It seems worth while to give the problem just as it appears in the Rhind Papyrus, which includes the statement of the problem, its solution, and a verification. (The English translation uses modern notation for numbers.)

Problem 26

A quantity and its ¼ added together become 15. What is the quantity? Assume 4.

√	1	4
√	¼	1
	total	5.

As many times as 5 must be multiplied to give 15, so many times 4 must be multiplied to give the required number. Multiply 5 so as to get 15.

√	1	5
√	2	10
total	3.	

Multiply 3 by 4.

	1	3
	2	6
√	4	12;

the quantity is

	12
¼	3
total	15.

Notice in the above problem that the Egyptian scribe determines that 4 must be multiplied by 3. Then to get the product he multiplies 3 by 4, the reverse order. The probable reason for this is that the Egyptian did all his multiplication by doubling; consequently it was easier to multiply

[2] Numbers in brackets refer to the references given at the end of the paper.

by powers of 2 than by other numbers. Actually to multiply 4 by 3, the Egyptian would have to double *and* add:

√	1	4
√	2	9
totals	3	12.

The Egyptians also freely used the distributive law, $a(b + c) = ab + ac$, but apparently without recognizing anything basic. An illustration of this occurs in Problem 68 of the Rhind Papyrus [3]. To double the number 3 21/64, which the scribe writes as $3 + 1/4 + 1/16 + 1/64$, he simply doubles each term and gets $6 + 1/2 + 1/8 + 1/32$, which, of course, is equal to 6 21/32. Note the use of *unit fractions* (fractions with unit numerators), which was standard procedure.

The ancient Babylonians (*ca.* 1700 B.C.) also used the commutative and distributive laws. These laws were tacitly assumed in their rhetorical algebra when, in effect, they used such formulas as $(a+b)^2 = a^2 + 2ab + b^2$. Van der Waerden gives some excellent examples of Babylonian algebra where these ideas are implied [4]. He writes:

The formulas

(11) $$(a + b)^2 = a^2 + 2ab + b^2$$

and

(12) $$(a - b)^2 = a^2 - 2ab + b^2$$

must also have been known to the Babylonians. For the old-Babylonian text BM 13901 contains the following problem: "I have added the areas of my two squares: 25,25.[3] (the side of) the second square is ⅔ of that of the first plus 5 GAR."

That is to say:

$$x^2 + y^2 = 25, 25,$$
$$y = (2/3)x + 5.$$

In order to substitute the value of y, obtained from the second equation, in the first equation, formula (11) has to be used:

$$(0; 40x + 5)^2 = 0; 40^2x^2 + 2 \cdot 0; 40 \cdot 5x + 5^2.$$

This leads to a quadratic equation

$$ax^2 + 2bx = c$$

[3] The Babylonian numerals employ 60 for a base. Hence 25,25 means $25 \cdot 60 + 25$. Again, 1;26,40 means $1 + 26/60 + 40/60^2$.

for x, in which

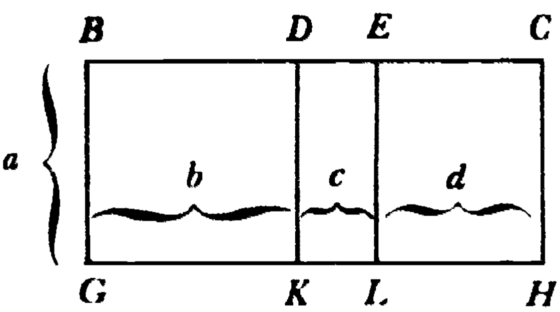
$$a = 1 + 0;40^2 = 1;26,40,$$
$$b = 5 \cdot 0;40 = 3;20,$$
$$c = 25,25 - 5^2 = 25,0.$$

The text first calculates the three coefficients a, b, c; then the quadratic equation is solved by use of the correct formula:

$$x = a^{-1}(\sqrt{ac + b^2} - b),$$

and finally $y = (2/3)x + 5$ is determined. It follows that the method of elimination, described above, was used and that the formula (11) was known.

Looking at Greek mathematics, we see that Euclid (320 B.C.) was more aware of the explicit nature of the distributive law. In his geometric algebra of Book II he states and proves Proposition 1: "If there be two



straight lines, and one of them be cut into any number of segments whatever, the rectangle contained by the two straight lines is equal to the rectangles contained by the uncut straight line and each of the segments [5]." That is (See the figure above.),

$$\text{area } BGHC = \text{area } BGKD + \text{area } DKLE + \text{area } ELHC,$$

or

$$a(b + c + d) = ab + ac + ad.$$

Although Euclid was quite explicit on the distributive property as applied to areas, we find that in Book VII, where Euclid deals with numbers as such, it does not occur to him to discuss the same distributive property. Perhaps he regarded this property as "only natural" for numbers and felt that no specific mention was necessary.

The question naturally arises as to when mathematicians began to recognize as axioms the properties which had been previously taken for granted.

Of the axioms for arithmetic and algebra, we first want to consider three in particular:

The associative law: $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

The commutative law: $a + b = b + a$ and $ab = ba$.

The distributive law: $a(b + c) = ab + ac$.

These axioms received the above names during the first sixty years of the nineteenth century [6]. Interestingly enough, the last two were given their present names by Servois in a discussion involving *functions* [7].

Servois comments that if $f\phi z = \phi f z$, where f and ϕ are functions and z an independent variable, then the functions are called *commutative*. He also says that if $f(x + y + \cdots) = fx + fy + \cdots$, then the function is called *distributive*. (He used parentheses more sparingly than we do today.)

The associative law was mentioned by Hamilton in 1853 in his *Lectures on Quaternions*. In the preface he stated, "to this associative property or principle I attach much importance [8]." Of course the associative law was used long before it was named, and it was already explicitly noted in 1830 when Legendre called attention to it in his *Théorie des Nombres*. Legendre wrote, "One ordinarily supposes that in multiplying a given number C by another number N which is the product of two factors A and B, one gets the same result whether he multiplies C by N all at once, or C by A and then by B." Symbolically, Legendre wrote: $C \times \overline{AB} = \overline{CA} \times B$ [9].

It is now only natural to ask, "What are the other axioms which in the past have been tacitly assumed when working with arithmetic and algebra?" To answer this question it is desirable from both historical and logical considerations to talk about a *group*.

A group is defined to be a set of elements (say numbers) and an operation (say addition) with the properties:

1. *Closure* (i.e., the sum of two numbers in the set is also in the set);

2. *Associativity:* $(a + b) + c = a + (b + c)$;

3. *Existence of an identity element,* zero (0), such that $a + 0 = 0 + a = a$ for every number a in the set;

4. *Existence of an inverse element* $(-a)$ for each a in the set such that $a + (-a) = (-a) + a = 0$.

If we add the property

5. *Commutativity:* $a + b = b + a$, we say the group is a *commutative group*.

For example, the integers (positive, negative, and zero) under ordinary addition form a communtative group since all five of the above axioms hold. But the odd integers under ordinary addition do not form a group, since the closure property does not hold—the sum of two odd integers is *not* an odd integer. Axiom 3 also fails, since zero is not among the odd integers; and as a result Axiom 4 also fails to hold.

Of course, all five of the above axioms were known and used long before the formal definition of a commutative group was given. Let us look at each of the five axioms more closely.

The first axiom (of closure) was what early mathematicians were really concerned with when they saw that fractions were needed to make division always possible. They had no trouble dividing 12 by 4 or 15 by 3, but to divide 2 by 3 they needed a fraction ⅔. (The idea of using fractions to represent "parts" seems fairly natural, but a general reluctance to do so is still evident in using, for example, 12 ounces in place of ¾ pound.)

The second axiom (of associativity) seems, at first glance, to be the least interesting of the five. One is inclined to say for addition, "Of course $(3+5)+2=3+(5+2)$," or to say for multiplication, "Of course $(3\cdot5)\cdot2=3\cdot(5\cdot2)$." The associative law (for both addition and multiplication) continues to hold as we enlarge the number system from integers to the rational numbers (integers and fractions) and then to the real numbers (the rationals and the irrationals). In fact, the associative law still holds for the complex numbers — numbers like $3+4i$ with one real part and one imaginary part. It even holds for Hamilton's *quaternions* — hypercomplex numbers like $3+2i+5j+4k$ with one real part and three different imaginary parts. But the associative law finally breaks down when multiplying Cayley numbers (one real part and seven imaginary parts).

With respect to the third axiom which states the existence of an identity element, we have already mentioned zero when speaking of *addition* of numbers. The story of zero is a fascinating one. The symbol and concept of zero were achieved in response to several needs. The role of zero in the principle of position is fairly well known. Another role was played in the solution of equations such as $5+x=5$. It was in this setting that a need was sensed for an identity element: something which added to 5 gives 5 again.

The fourth axiom stating the existence of inverse elements, requires negative numbers (when the group operation is addition). Although the Chinese had some understanding of negative numbers (and wrote positive coefficients in red, negative in black), the first mention of negative numbers in an occidental work is by Diophantus (*ca.* 275). He gave "rules" for operating with "forthcomings" and "wantings" in situations where the final result was a "forthcoming," but he apparently had no conception of a negative number in the abstract, and regarded the equation $4x + 20 = 4$ as absurd because it had $x = -4$ as a root [10]. Cardan, in his *Ars Magna* (1545), recognized negative roots and stated laws governing negative numbers. The solution of an equation like $x + 7 = 0$, with a root $x = -7$, was preliminary to stating essentially the same idea in more sophisticated terms: the (additive) inverse of 7 is -7.

The fifth axiom (of commutativity) was, as we have seen, tacitly assumed and used for a long time. Its basic character was perhaps most dramatically revealed when Hamilton discovered that his newly invented quaternions did not necessarily obey the commutative law (for multiplication).

Hamilton's discovery that his new "numbers" (beyond the complex numbers, hence sometimes called hypercomplex numbers), quaternions, did not obey one of the expected properties of numbers should have been enough to raise the question, "What axioms are needed to define various systems?"

But the answer came, in part, in response to a somewhat different line of inquiry. It was in connection with the algebraic solution of equations that the theory of groups was first studied [11]. The pioneers in this undertaking were Lagrange (1770), Ruffini (1799), Cauchy (1814), Abel (1824), and especially Galois (1831). The first discussion of the theory of groups from an abstract point of view was by Cayley in 1854, and the earliest explicit sets of axioms were given by Kronecker in 1870 and H. Weber in 1882.

It was noted above that the integers form a group if the group operation is addition. But if we had chosen multiplication as the group operation the integers would *not* form a group, since 7, for example, would not have an inverse in the set of integers; that is, Axiom 4 would not hold since it is impossible to find an integer x such that $7 \cdot x = x \cdot 7 = 1$. (Our identity element for multiplication is 1, since $N \cdot 1 = 1 \cdot N = N$.)

But the rational numbers (the integers and the fractions) *do* form a commutative group under multiplication—except for zero, which has no inverse. This is easily seen by checking the five group axioms using nonzero fractions. The rational numbers (zero now included) also form a commutative group under addition. Moreover, these two groups are "connected" by the distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c$, and we say that multiplication is distributive over addition.

Taking inventory of our axioms up to this point we see that we now have eleven axioms.

Additive group:

1. Closure: $a + b$ is in the set.

2. Associativity: $(a + b) + c = a + (b + c)$.
3. Identity element, zero (0), such that $a + 0 = 0 + a = a$.
4. Inverse element, $(-a)$, such that $a + (-a) = (-a) + a = 0$ for every element a in the set.
5. Commutativity: $a + b = b + a$.

Multiplicative group:

6. Closure: $a \cdot b$ is in the set.
7. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
8. Identity element, one (1), such that $a \cdot 1 = 1 \cdot a = a$.
9. Inverse element, a^{-1}, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ for every nonzero element a in the set.
10. Commutativity: $a \cdot b = b \cdot a$.

The distributive law:

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

We say that these eleven axioms determine a *field*. This means, for example, that the rational numbers under ordinary addition and multiplication form a field, since all eleven axioms are satisfied. The real numbers, under addition and multiplication, also constitute a field; so do the complex numbers.

The theory of fields was suggested by Galois and was given a concrete formulation by Dedekind in 1871. The earliest expositions of the theory from the general or abstract point of view were given independently by H. Weber and E. H. Moore in 1893 [12].

As we have seen above, the "natural," or expected, properties of the rational numbers (as summarized by the eleven field axioms) still hold when we enlarge the system to include the irrational numbers. And if we take this larger system (the real number field) and add to it the imaginary numbers, the resulting system (the system of complex numbers) is again a field (the complex number field).

Can we continue this process? Are there larger number fields than the complex number field? The answer is *no*; it is not possible to extend the complex number field to a larger field. Both Hamilton's and Cayley's hypercomplex numbers fail to satisfy all of the field axioms, as was pointed out above.

References

1. A. B. Chace, *The Rhind Mathematical Papyrus* (Oberlin: Mathematical Association of America, 1927), I, 6.
2. *Ibid.*, p. 68.
3. *Ibid.*, p. 104.

4. B. L. VAN DER WAERDEN, *Science Awakening* (Groningen, Holland: P. Noordhoff, Ltd., 1954), pp. 68-69.

5. T. L. HEATH, *The Thirteen Books of Euclid's Elements* (Cambridge, England: University Press, 1908), I, 375.

6. G. A. Miller, "A Third Lesson in the History of Mathematics," *National Mathematics Magazine*, 15 (1940-1941), 234-244.

7. F. SERVOIS, "Essai sur les principes du calcul différentiel," *Annals de Mathématiques Pures et Appliquées*, 5 (1814), 98.

8. W. R. HAMILTON, *Lectures on Quaternions* (Dublin: Hodges and Smith, 1853), p. 61 of preface.

9. A. M. LEGENDRE, *Théorie des Nombres* (Paris: Librairie Scientifique A. Hermann, 1900), I, 2.

10. D. E. SMITH, *History of Mathematics* (New York: Ginn and Co., 1953), II, 257-259.

11. E. V. HUNTINGTON, "Note on the Definitions of Abstract Groups and Fields by Sets of Independent Postulates," *Transactions American Mathematical Society*, 6 (1905), 181.

12. *Ibid.*, p. 183.

FOREWORD

The author here shows us very clearly how a number system can be developed "from scratch" by beginning with the natural numbers and zero, setting up eleven basic assumptions and two binary operations called *addition* and *multiplication*. The assumptions are here called "postulates," but for our purpose, *postulate, assumption* and *axiom* are synonomous terms. (The two assumptions for closure are stated verbally, not with symbols.)

The essay is somewhat "sophisticated" inasmuch as it is a formal, abstract presentation. Yet this is precisely the way in which mathematicians have developed various algebras and number systems. Moreover, it is also an excellent example of the use of deductive reasoning to derive a variety of theorems from the basic assumptions by formal proofs. This is one of the essential hallmarks of modern mathematics. And to help the reader appreciate this distinctive feature of mathematics, he is invited to work some simple exercises at the end of the essay.

The Foundations of Algebra

Charles Brumfiel

In the years immediately ahead we shall undoubtedly see much experimentation in the teaching of algebra. The trend will be toward a presentation that stresses the importance of assumptions, definitions, proofs, and the logical concepts utilized in proofs. How quickly can we move in this direction? Teachers will be encouraged to experiment if suitable materials are placed in their hands.

This article is not to be considered a teachable unit in beginning algebra. But it illustrates the kind of reasoning we should like to obtain from algebra students. In a teaching situation many numerical examples should precede the theorems. Someone has remarked pessimistically that the per cent of young people in our schools who can follow careful deductive reasoning is vanishingly small. However, we always have a few who can do so. It is hoped that some teachers of mathematics will be able to use the ideas in this article to construct experimental algebra units. We need to find out how far we can go in our presentation of algebra as a logical structure rather than a hodgepodge of rules and descriptions.

As a basis for the construction of the complex number system studied in high school algebra, let us assume the existence of a set

$$S = \{0, 1, 2, 3, 4, \cdots\}$$

that consists of zero and the natural numbers. Also let us agree that operations called addition and multiplication are defined so that every ordered pair of numbers in S has a unique sum and product. In particular, sums and products of natural numbers are natural numbers. We now postulate that these operations have the following properties:

For all numbers a, b, c in S it is true that:

A 1. $a + b = b + a$	M 1. $ab = ba$
A 2. $(a + b) + c = a + (b + c)$	M 2. $(ab)c = a(bc)$
A 3. $a + 0 = a$	M 3. $a \cdot 1 = a$
A 4. $a + b = a + c \rightarrow b = c$	M 4. $ab = ac$ and $a \neq 0 \rightarrow b = c$

D. $a(b + c) = ab + ac$

The above postulates can be used to illustrate the processes of deductive reasoning. If the teacher is skillful, the development of algebra from these postulates should not involve logical difficulties greater than those encountered in geometry. We present below a collection of theorems, definitions, and problems that might be useful to the algebra teacher who would like to follow the advice of modern algebraists and stress the importance of definition, proof, and logical structure in algebra.

We sketch proofs of a few theorems that are a consequence of the nine basic postulates above. All variables range over S, that is, letters are used to represent numbers in S alone. One remark is in order. The sign "=" will only be used to indicate *identity*. The statement "$a = b$" means that "a" and "b" are symbols for the same number in S. Hence, it is needless to remark that $x = y = z \rightarrow x = z$.

Theorem 1: For every x in S, $1 \cdot x = x$.

Proof:	$1 \cdot x = x \cdot 1$	M 1
	$x \cdot 1 = x.$	M 3

The reader may wonder why anything as obvious as Theorem 1 needs proof. Even the simple statement, $1 \cdot 2 = 2$, does not occur among our postulates. However, we can find the two statements, $1 \cdot 2 = 2 \cdot 1$ and $2 \cdot 1 = 2$. Our proof consists of calling attention to the fact that we have made these two assumptions, and together they imply that $1 \cdot 2 = 2$.

Theorem 2: For every a in S, $a \cdot 0 = 0$.

Proof:	$a(1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0$	D and M 3
	$a(1 + 0) = a \cdot 1 = a + 0$	A 3 and M 3
	$a + 0 = a + a \cdot 0 \rightarrow 0 = a \cdot 0$	A 4

Theorem 3: $(a + b) + (c + d) = (a + (c + d)) + b$.

Proof:	$(a + b) + (c + d) = a + (b + (c + d))$	A 2
	$a + (b + (c + d)) = a + ((c + d) + b)$	A 1
	$a + ((c + d) + b) = (a + (c + d)) + b.$	A 2

Many theorems like Theorem 3 can be proved using the commutative laws A 1, M 1 and the associative laws A 2, M 2. Indeed, a proof employing mathematical induction enables one to establish general associative and commutative laws, showing that if arbitrarily many numbers of S are to be added they can be reordered in any desired manner (commutativity) and then grouped by parentheses in any fashion (associativity). It follows that the order of performing a series of additions need not be indicated by parentheses, and we may write without ambiguity "$a + b + \cdots + l$," since any insertion of parentheses leads to the same sum. We observe that in adding three numbers, $a + b + c$, parentheses may be inserted in *two* ways, as: $(a + b) + c$ or $a + (b + c)$. Four numbers may be associated for addition in five ways. In how many different ways may parentheses be inserted in a sum involving five numbers? six? Can you find a general formula that gives the number of different ways that n numbers may be associated for addition—of course without changing the order of the numbers?

Let us illustrate how definitions are used to call attention to interesting concepts. Definitions in mathematics are no more than agreements to replace certain symbols, whose meaning is understood, by other symbols. These new symbols are to have precisely the same meaning as the old. Definitions usually enable us to express mathematical ideas more concisely, but the real test for a definition is whether it can be used as a tool in proofs.

Definition 1: When we write "$a > b$," we mean that there is a number c in S with $c \neq 0$ such that $a = b + c$. We read this new symbol as "a is greater than b."

Theorem 4: If $a \neq 0$ then $a > 0$.

Proof: $a = 0 + a$. — A 3, A 1 and Def. 1

Theorem 5: $a > b \rightarrow a + c > b + c$.

Proof:

$a > b \rightarrow a = b + t$ with $t \neq 0$	Def. 1
$a = b + t \rightarrow a + c = (b + c) + t$	A 1, A 2
$a + c = (b + c) + t \rightarrow a + c > b + c.$	Def. 1

Theorem 6: $a + c > b + c \rightarrow a > b$.

Proof:

$a + c > b + c \rightarrow a + c = (b + c) + t$	Def. 1
$a + c = (b + c) + t \rightarrow a + c = (b + t) + c$	A 1, A 2
$a + c = (b + t) + c \rightarrow a = b + t$	A 4
$a = b + t \rightarrow c > b.$	Def. 1

Definition 2: When we write "$x < y$" we mean $y > x$, and we read "$x < y$" as "x is less than y."

Theorem 7: $x < y$ and $y < z \rightarrow x < z$.

Proof:

$x < y \rightarrow y = x + a$	Def. 1, 2
$y < z \rightarrow z = y + b$	Def. 1, 2
So, $z = (x + a) + b = x + (a + b)$	A 2
And, $z > x$, so $x < z$.	Def. 1, 2

Definition 3: When we write "$a - b = c$" we mean $a = b + c$. We read this new symbol as "a minus b is c." The process of determining c when a and b are known is called subtraction. If $b > a$ the expression "$a - b$" is assigned no meaning.

Theorem 8: If $x - y = z$ then $x - z = y$.

Proof:

$x - y = z \rightarrow x = y + z$	Def. 3
$x = y + z \rightarrow x = z + y$	A 1
$x = z + y \rightarrow x - z = y$	Def. 3

Theorem 9: If $y < x$ then $(x - y) + y = x$.

Proof:

Set $x - y = t$, then $x = y + t$	Def. 3
Hence, $(x - y) + y = t + y = y + t = x$.	A 1

Theorem 10: $(a + b) - b = a$.

Proof: Obvious by Def. 3 and A 1.

Theorem 11: If $s < r$ then $r - (r - s) = s$.

Proof:

$r = (r - s) + s$	Theorem 9
$r - (r - s) = s$.	Def. 3

Theorem 12: If $a + b < c$ then $c - (a + b) = (c - a) - b$.

Proof:

$c = (a + b) + t = a + (b + t)$	Def. 2, A 2
$c = a + (b + t) \rightarrow c - a = b + t$	Def. 3
$c - a = b + t \rightarrow (c - a) - b = t$	Def. 3
$c = (a + b) + t \rightarrow c - (a + b) = t$	Def. 3
So, $c - (a + b) = (c - a) - b$.	

Theorem 13: $b < a$ and $c < b \rightarrow (a - c) - (b - c) = a - b$.

Proof:

$(a - c) - (b - c) = a - (c + (b - c))$	Theorem 12
$a - (c + (b - c)) = a - b$.	A 1, Theorem 9

Theorem 14: $a - a = 0$.

Proof:

$a = a + 0$.	A 3, Def. 3

Theorem 15: $b < a$ and $c < b \rightarrow a - (b - c) = (a - b) + c$.

Proof:

$(a - (b - c)) + (b - c) = a$.	Theorem 9
$((a - b) + c) + (b - c) = (a - b) + (c + (b - c))$	A 2
$(a - b) + (c + (b - c)) = (a - b) + b$	A 1, Theorem 9
$(a - b) + b = a$	Theorem 9
So, $(a - (b - c)) + (b - c) = ((a - b) + c) + (b - c)$	
And, $a - (b - c) = (a - b) + c$.	A 4

The numerical examples below illustrate some of these theorems:

1. $(987 - 653) + 653 =$ Theorem 9
2. $6423 - (6423 - 854) =$ Theorem 11
3. $97 - 43 = (97 - 40) - 3 =$ Theorem 12
4. $(5000 - 2416) - (4000 - 2416) = 5000 - 4000 =$ Theorem 13
5. $90 - 59 = (90 - 60) + 1 =$ Theorem 15

Definition 4: If $a = bc$ and $b \neq 0$ we write "$a \div b = c$" and say "a divided by b equals c." The process of determining c when a and b are known is called division. If $a \div b = c$ we say "b divides a" and write this as "b/a."

Theorem 16: If $a \div b = c$ and $c \neq 0$ then $a \div c = b$.

Proof: $a \div b = c \rightarrow a = bc \rightarrow a = cb \rightarrow a \div c = b$. Def. 4, M 1

Theorem 17: If y/x then $(x \div y) \cdot y = x$.

Proof: Set $x \div y = t$, then $x = yt$. Def. 4

Hence. $(x \div y) \cdot y = ty = yt = x$ M 1

Theorem 18: $ab \div b = a$.

Proof: Obvious by Def. 4 and M 1.

Theorem 19: If s/r then $r \div (r \div s) = s$.

Proof: $r = (r \div s) \cdot s$ Theorem 17

$r \div (r \div s) = s$ Def. 4

Theorem 20: If ab/c then $c \div (ab) = (c \div a) \div b$.

Proof: $c = (ab)t = a(bt)$ Def. 4, M 2

$c = a(bt) \rightarrow c \div a = bt$ Def. 4

$c \div a = bt \rightarrow (c \div a) \div b = t$ Def. 4

$c = (ab)t \rightarrow c \div ab = t$ Def. 4

So. $c \div ab = (c \div a) \div b$.

The reader may have noticed a curious duality between the set of Theorems 9, 10, 11, 12 and the last four, 17, 18, 19, 20. This is the type of duality encountered in projective geometry and Boolean algebra. We restate some of these theorems for comparison:

Theorem 9: $y < x \rightarrow (x - y) + y = x$.

Theorem 17: $y/x \rightarrow (x \div y) \cdot y = x$.

Theorem 11: $s < r \rightarrow r - (r - s) = s$.

Theorem 19: $s/r \rightarrow r \div (r \div s) = s$.

Theorem 12: $a + b < c \rightarrow c - (a + b) = (c - a) - b$.

Theorem 20: $ab/c \rightarrow c \div (ab) = (c \div a) \div b$.

This duality extends to the proofs of these theorems. That is, if in the proof of Theorem 12 the signs "<," "−," "+" are replaced by "/," "÷," "•" respectively, then the proof of Theorem 20 results. The reader may now construct and prove the dual theorems on division corresponding to Theorems 13, 14, and 15.

The following list of exercises offers opportunities to use the concepts that have been developed.

Exercises

1. $(20 - (20 - 12)) - (12 - 7) =$
2. $(80 \div (80 \div 16)) \div (16 \div 2) =$
3. Is it true that for every pair of numbers, a, b with $a > b$, we have $(a - b) + (2b - a) = b$?
4. Show that if $(a - b) = (c - b) + t$ with $t > 0$ then $a > c$.
5. Show that if $a > b$ then $a - (a - (a - (a - b))) = b$.

Determine whether or not the following equations have solutions in S. We remark that to *solve* an equation relative to the set S means to indicate all numbers in S that make the equation a true statement.

6. $15 - (5 - x) = 5x - (5 - x)$
7. $12 - (x - 4) = 4x - (x - 4)$
8. $2x - (2x - 4) = 2x - 20$
9. $(t + 1) \cdot 5 = 0$
10. $(3t + 8) - 5t = 0$
11. $(3a - 30) \cdot (40 - 5a) = 0$
12. $2r + (2r - 7) = 2r$
13. $(5s + 4) \div (3s - 8) = 5s + 4$
14. $(s - 2) \div 5 = s - 2$
15. $x - (x - (x - 4)) = x - 4$
16. $(8 - x) + x = 8$

Are these statements true or false?

17. There is no number x in S such that $3(x - 4) = 2x - 12$.
18. If $3x - (x + y) = 12 - y$ then $x = 6$.
19. If $x, y, x - y, 2y - x$ and $4 - x$ are all natural numbers then $x = 3$ and $y = 2$.
20. If $2x - 3 < 8$ and $3x - 4 > 9$ then $x = 5$.
21. If $ab = 0$ then either $a = 0$ or $b = 0$.

22. For all numbers, a, b, c in S with $b > c$ it is true that $a(b - c) = ab - ac$.
23. The only root of the equation $(t - 2)(3t - 9) = 0$ is the number 3.
24. 8/4.
25. a/b and $b/a \rightarrow a = b$.
26. 0/4.
27. $2/(6a + 4)$ for every a in S.
28. If b is any number in S then $2/b(b + 1)$.

Complete the following statements.

29. If $xyz = t$ then $t \div xz =$ . . . .
30. If $x \div t = 4$ and $y \div t = 3$ then
$(x + y) \div t =$ . . . . and $xy \div t =$ . . . .
31. If $a \div b = 27$ and $c \div b = 9$ then
$(a + 2c) \div b =$ . . . . and
$(a - c) \div b =$ . . . . and
$3ac \div b =$ . . . . and
$a \div c =$ . . . .
32. If b/a and $b = a - 1$ then $a =$ . . . .
and $b =$ . . . .
33. If x/y and $x < y$ and $3x > y$ then $y \div x =$ . . . .
34. If $rs \neq 0$ then $5rrs \div rs =$ . . . .
35. If $3/ab$, and if the statement, $3/a$, is false then . . . .
36. If $a \neq 1$ and $b \div a = b$ then . . . .

We comment upon a few of the problems above.

The statement in problem 3 is false. To see this take $a = 10$, $b = 2$ and remember that we are dealing only with numbers in S. Statements about numbers are always made relative to a specified number system. A statement may be true when it refers to the integers and false when it refers to fractions. As an example, consider:

There is no number x greater than 3 and less than 4.

The equations in (7), (9), (12) have no solutions in S. The equation in (11) has no solution. The equation in (16) has nine solutions. The statements in (17) and (23) are true.

FOREWORD

As we have already mentioned, not all groups need to be commutative. This concept bothered nineteenth-century mathematicians for quite some time. Indeed, the brilliant Irish mathematician Sir William Rowan Hamilton, inventor of quaternions, spent some fifteen years of his life wrestling with this problem. In a letter to his son, he once wrote that for years he only knew how to *add* "triplets"; finally, one day, in a flash of intuition, he realized that to multiply triplets he would have to give up the commutative property; then it would be possible to multiply triplets, obtaining the relation $i^2 = j^2 = k^2 = ijk = -1$.

Today, the matter of structure is clear. A *group* is a system in which addition and subtraction are always possible, wi[illegible] closure, as for example, the integers.

A *ring* is a system in which addition, subtraction and multiplication are always possible. In other words, such a system has two binary operations. It is a commutative group with respect to addition. Both addition and multiplication are associative, and multiplication is distributive with respect to addition. It can be shown that in any system having a ring structure that $x + 0 = x$ and $x \cdot 0 = 0$.

A *field* is a system in which addition, subtraction, multiplication and division are always possible, except that division by zero is excluded.

Here the author gives us an example of an algebra that is noncommutative, using a system in which the elements, instead of being numbers, are 2×2 matrices of real numbers.

A Simple Example of a Noncommutative Algebra

Arnold Wendt

Introduction

NOWADAYS TEACHERS are encouraged to give more attention to the postulational nature of algebra. Often this emphasis takes the form of an abstraction of a notion with which the students are already familiar. Many students remain singularly unimpressed by attempts to postulate or prove an idea they have long ago accepted as a fact holding universally in mathematics. So long as we remain in the algebra of the real or complex numbers, the same old rules apply.

We have found that one way to get students to appreciate more fully our rules of arithmetic is to expose them to an easily understandable, yet mathematically important, example of an algebra in which not all the usual laws hold. Such an example is the algebra of 2×2 (read 2 by 2) matrices with real numbers as elements. They are easily understandable, because in performing operations with or on these matrices we make use of ordinary arithmetic. Much of what follows can be readily followed by high school students, if not all of it.

For future reference let us first list the usual laws of arithmetic satisfied by the real numbers. For all real numbers a, b, c:

1. *Closure laws:* $a + b$ and $a \times b$ are unique real numbers.
2. *Commutative laws:* $a + b = b + a$ and $a \times b = b \times a$.
3. *Associative laws:* $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$.
4. *Distributive law:* $a(b + c) = (a \times b) + (a \times c)$.
5. *Identity elements:* There exists a number 0 such that $a + 0 = a$ for all a, and there exists a number 1 such that $a \times 1 = a$ for all a.
6. *Inverse elements:* For each number a there exists a number $(-a)$ such that $a + (-a) = 0$, and for each $a \neq 0$ there exists a number a^{-1} such that $a \times a^{-1} = 1$.

From these first six laws we can prove the following law, written in two equivalent forms.

7. *Cancellation law:* If $a \times b = a \times c$ and $a \neq 0$, then $b = c$.

7′. (Alternate form): If $a \times b = 0$, then $a = 0$, or $b = 0$, or both.

The laws one through six are usually referred to as postulates for a *field*. They are satisfied by other mathematical entities besides the real and complex numbers.

MATRICES

We now define a new kind of mathematical entity called a *matrix*, plural *matrices*.

Definition: A 2 × 2 matrix is a square array of real numbers represented by

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

The subscripts merely denote the row and column, in that order, in which the number is located. For example, a_{21} means the number or *element* in the second row, first column.

Remarks: 1. Although similar in appearance to a determinant, a matrix is not the same thing as a determinant. *A determinant* (we are assuming the reader is familiar with determinants) *is a number* obtained from a square array of numbers by combining them according to certain rules. On the other hand, a matrix is the array of numbers itself. There is no rule for combining the elements in a matrix.

2. Since the laws in which we are going to be interested can be demonstrated most easily by using 2 × 2 matrices, we shall confine our attention chiefly to them. However, a matrix may have any number of rows and columns and need not be square, i.e., number of rows need not equal number of columns.
3. The elements in a matrix may be almost any mathematical entity, including even matrices themselves.
4. There is no geometrical representation for general matrices as there is for real numbers and complex numbers. One can consider matrices as a generalization of the notions of complex number and vector. They are sometimes referred to as hypercomplex numbers.
5. The fact that we cannot draw a picture of a matrix does not mean matrices have no application in practical problems. The development of the theory of matrices preceded their application to practical problems, as has been the history of many other mathematical systems. Their theory had its beginnings in the 1850's and so can be considered modern mathematics.

Definition: Two matrices will be considered equal if, and only if, the elements in corresponding positions are equal.

Definition of Addition:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

Example: Let

$$A = \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \text{ and } B = \begin{pmatrix} 4 & -1 \\ 0 & 2 \end{pmatrix}.$$

Then

$$A + B = \begin{pmatrix} -1+4 & 3+(-1) \\ 1+0 & 2+2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}.$$

Since addition of real numbers is commutative and associative, it is not difficult to see that laws 1, 2, 3 of the real numbers under + are satisfied by matrices under +.

Also, we have the identity element under addition of Law 5, for the matrix

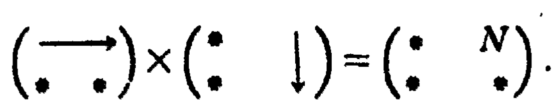
$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

satisfies this property.

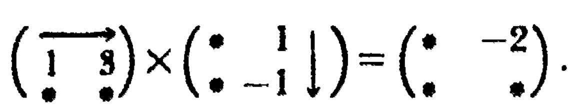
Definition of Multiplication:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Before checking the properties of matrices under multiplication, we shall amplify the definition above. By noting the pattern in the subscripts, we see that the element in the first row, second column of the product matrix, is obtained by adding the products of corresponding elements in the first row of the left factor and the second column from the right factor. Corresponding elements are determined by proceeding from left to right in the row and from top to bottom in the column. Schematically,



Using numbers,



This "over and down" rule is a convenient mnemonic device for matrix multiplication. In general, to get the element in the ith row and jth column of the product matrix we proceed from left to right in the ith row of the *left* factor and down the jth column of the right factor, forming products of corresponding elements determined in this manner. Then the products are added to get the entry.

Example:

$$\begin{pmatrix} 1 & 3 \\ -2 & 2 \end{pmatrix} \times \begin{pmatrix} 4 & 1 \\ 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} (1)(4) + (3)(0) & (1)(1) + (3)(-1) \\ (-2)(4) + (2)(0) & (-2)(1) + (2)(-1) \end{pmatrix}$$

$$= \begin{pmatrix} 4 & -2 \\ -8 & -4 \end{pmatrix}.$$

It follows from the definition of multiplication that matrices cannot be multiplied unless the number of columns in the left factor is the same as the number of rows in the right factor.

That matrices are closed under multiplication should be evident. We check the commutative law by performing two more multiplications in detail.

$$\begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 4 & -1 \\ 0 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} (-1)(4) + (3)(0) & (-1)(-1) + (3)(2) \\ (1)(4) + (2)(0) & (1)(-1) + (2)(2) \end{pmatrix}$$

$$= \begin{pmatrix} -4 & 7 \\ 4 & 3 \end{pmatrix}.$$

On the other hand,

$$\begin{pmatrix} 4 & -1 \\ 0 & 2 \end{pmatrix} \times \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} (4)(-1) + (-1)(1) & (4)(3) + (-1)(2) \\ (0)(-1) + (2)(1) & (0)(3) + (2)(2) \end{pmatrix}$$

$$= \begin{pmatrix} -5 & 10 \\ 2 & 4 \end{pmatrix}.$$

And we see that matrix multiplication is *not* in general commutative. But this does not mean matrix multiplication is useless.

The associative law for matrix multiplication holds, but we shall not prove this fact. We merely illustrate the rule.

$$\begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \times \left[\begin{pmatrix} 4 & -1 \\ 0 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \right]$$

$$= \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 4 & 6 \end{pmatrix} = \begin{pmatrix} 10 & 17 \\ 10 & 13 \end{pmatrix}.$$

$$\left[\begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 4 & -1 \\ 0 & 2 \end{pmatrix} \right] \times \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} -4 & 7 \\ 4 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 10 & 17 \\ 10 & 13 \end{pmatrix}.$$

The distributive law also holds; but since multiplication is not commutative, we have a right distributive law and a left distributive law. That is, for matrices we do *not* have in general

$$A(B + C) = (B + C)A.$$

The identity element for multiplication exists and is denoted by

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The reader may verify that I has the property of a multiplicative identity. In doing so he will note that I commutes with every matrix and so is both a right and left identity.

We have seen that every matrix has an additive inverse and now investigate the existence of multiplicative inverses. Suppose

$$\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$$

is a matrix for which we wish to find an inverse. Then it must be true that

$$\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Applying the definition of matrix multiplication we see it is necessary that

$$\begin{pmatrix} 3b_{11} - b_{21} & 3b_{12} - b_{22} \\ b_{11} + 2b_{21} & b_{12} + 2b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since matrices are equal only if corresponding elements are equal, we have

$$3b_{11} - b_{21} = 1 \quad 3b_{12} - b_{22} = 0$$
$$b_{11} + 2b_{21} = 0 \quad b_{12} + 2b_{22} = 1.$$

These two pairs of simultaneous equations have the solutions $b_{11} = 2/7$, $b_{21} = -1/7$, $b_{12} = 1/7$, $b_{22} = 3/7$, so the proposed inverse is

$$\begin{pmatrix} 2/7 & 1/7 \\ -1/7 & 3/7 \end{pmatrix}.$$

Checking, we see that

$$\begin{pmatrix} 2/7 & 1/7 \\ -1/7 & 3/7 \end{pmatrix} \times \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 2/7 & 1/7 \\ -1/7 & 3/7 \end{pmatrix},$$

so that inverses are both right and left inverses.

While it is true that every real number except zero has a multiplicative inverse, it is not true that every matrix other than the zero matrix has an inverse. For example, let us try to find the inverse of

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

by the method used previously. Then

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

results in the equations

$$a_{11} + 2a_{21} = 1 \qquad a_{12} + 2a_{22} = 0$$
$$2a_{11} + 4a_{21} = 0 \qquad 2a_{12} + 4a_{22} = 1.$$

We see both sets are inconsistent, and so it is simply not possible to find an inverse for this matrix.

We have one more law to check, the cancellation law for multiplication. That it does *not* hold follows immediately from the following example:

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \times \begin{pmatrix} 6 & 2 \\ -3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Consequently, we cannot say that simply because the product of two matrices is the zero matrix, at least one of the two factors must be the zero matrix. We extend the above example to present a counter example to the first form of Law 7, also. Since

$$\begin{pmatrix}1 & 2\\2 & 4\end{pmatrix}\times\begin{pmatrix}-2 & -4\\1 & 2\end{pmatrix}=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix},$$

we have

$$\begin{pmatrix}1 & 2\\2 & 4\end{pmatrix}\times\begin{pmatrix}6 & 2\\-3 & -1\end{pmatrix}=\begin{pmatrix}1 & 2\\2 & 4\end{pmatrix}\times\begin{pmatrix}-2 & -4\\1 & 2\end{pmatrix},$$

but

$$\begin{pmatrix}6 & 2\\-3 & -1\end{pmatrix}\neq\begin{pmatrix}-2 & -4\\1 & 2\end{pmatrix}.$$

Going very deeply into matrix theory is not the primary purpose of this paper. However. the observant reader's curiosity may be aroused by the fact that previously we saw the matrix

$$\begin{pmatrix}1 & 2\\2 & 4\end{pmatrix}$$

had no multiplicative inverse, and now we see it is a proper divisor of zero. Is there any connection between these two observations? The answer is yes. Suppose the matrix A is a proper devisor of zero, i.e., $A \times B = 0$ for some matrix B where B is *not* the zero matrix, and suppose A has an inverse A^{-1}. Then

$$A^{-1} \times (A \times B) = (A^{-1} \times A) \times B = I \times B = B,$$

and also

$$A^{-1} \times (A \times B) = A^{-1} \times 0 = 0.$$

Hence B would be equal to the zero matrix, contrary to the assumption that B is not the zero matrix. Consequently, any proper divisor of zero does not have an inverse. The converse is also true.

Summarizing, we see matrix algebra is the same as the algebra of the real numbers with the following exceptions:

1. Multiplication is not commutative.
2. Not all non-zero matrices have an inverse.
3. The cancellation law for multiplication does not hold.

The algebra of matrices with real elements is an example of a "ring with unit element."

Applications

Despite what at first might appear to be shortcomings, matrices have proved handy things to have around. They are used in every branch of pure mathematics. To attempt to list all their applications in practical problems would be impossible. They are used in physics, chemistry, many branches of engineering, psychology, biology, sociology, economics, game theory, linear programming, and statistics. Matrices are often used because they afford a compact form for recording data.

Suppose we look at a trivial example of an application to a problem in higher finance.

Number of Units Consumed

	Soda	Ice Cream	Candy
John	2	1	3
Mary	1	2	0
Jim	1	1	1

Cost per Unit

Soda	10 cents
Ice Cream	8 cents
Candy	5 cents

We form the matrix product

$$\begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 10 \\ 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 43 \\ 26 \\ 23 \end{pmatrix}$$

and leave to the reader the interpretation of the product matrix. The product

$$(1, 1, 1) \times \left[\begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 10 \\ 8 \\ 5 \end{pmatrix} \right] = (1, 1, 1) \times \begin{pmatrix} 43 \\ 26 \\ 23 \end{pmatrix} = (92)$$

also has an interpretation which the reader should check.

Not all important applications of matrices involve matrix algebra. Often their advantage lies in the compact manner in which the matrix notation can represent information. We note, for example, that the equations

$$\begin{aligned} x + 2y - 3z &= 6 \\ 2x + 5y - 2z &= 4 \\ x + 3y - z &= 0 \end{aligned}$$

can be represented by the matrix

$$\begin{pmatrix} 1 & 2 & -3 & 6 \\ 2 & 5 & -2 & 4 \\ 1 & 3 & -1 & 0 \end{pmatrix}.$$

By performing operations, which correspond to eliminating unknowns, on the rows of this matrix one can obtain an equivalent set of equations represented by

$$\begin{pmatrix} 1 & 0 & 0 & 11 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

The numbers in the last column are the solutions of the equations.

Before leaving this example we should point out that if one had a set of equations with the same coefficients as above, i.e., equations of form

$$\begin{aligned} x + 2y - 3z &= C_1 \\ 2x + 5y - 2z &= C_2 \\ x + 3y - z &= C_3, \end{aligned}$$

then application of matrix algebra would give a convenient method for finding solutions once the inverse of the coefficient matrix has been determined. In the present case the inverse of

$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & 5 & -2 \\ 1 & 3 & -1 \end{pmatrix} \text{ is } \begin{pmatrix} -1/2 & 7/2 & -11/2 \\ 0 & -1 & 2 \\ -1/2 & 1/2 & -1/2 \end{pmatrix},$$

that is, their product in either order is I. Since the above equations may be represented by

$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & 5 & -2 \\ 1 & 3 & -1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix},$$

multiplying both sides on the left by the inverse gives

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1/2 & 7/2 & -11/2 \\ 0 & -1 & 2 \\ -1/2 & 1/2 & -1/2 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}.$$

Thus, substituting different sets of values for the C's will automatically grind out the answers upon performing the indicated multiplication.

Isomorphism

We conclude with a few remarks having no bearing on the body of this paper, but which, in the writer's opinion, may amplify the concept of a matrix as a number.

In the sense that certain subsets of matrices are nothing more than the real numbers and complex numbers in disguise, matrices are an extension, or generalization, of these two number systems. The reader is probably familiar with the following hierarchy:

Complex numbers $\supset$ real numbers $\supset$ rational numbers $\supset$ integers and 0. The symbol $\supset$ means "contain." What we have said above is merely that we can also write

Matrices $\supset$ complex numbers $\supset$, etc.

Considering only 2×2 matrices is sufficient for our purposes.

We have already noted that

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

behaves like the additive identity 0 for the reals and that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

behaves like the multiplicative identity 1 for the reals.

Looking at these two correspondences

$$\begin{matrix} 0 & & 1 \\ \updownarrow & & \updownarrow \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{matrix}$$

suggests that for any real number r we set up the correspondence

$$\begin{matrix} r \\ \updownarrow \\ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}. \end{matrix}$$

Under this correspondence sums and products of corresponding elements again correspond to each other.

Example:

$$\begin{array}{ccccc} 4 & + & 3/4 & = & 4\,3/4 \\ \updownarrow & & \updownarrow & & \updownarrow \\ \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} & + & \begin{pmatrix} 3/4 & 0 \\ 0 & 3/4 \end{pmatrix} & = & \begin{pmatrix} 4\,3/4 & 0 \\ 0 & 4\,3/4 \end{pmatrix}. \end{array}$$

$$\begin{array}{ccccc} 4 & \times & 3/4 & = & 3 \\ \updownarrow & & \updownarrow & & \updownarrow \\ \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} & \times & \begin{pmatrix} 3/4 & 0 \\ 0 & 3/4 \end{pmatrix} & = & \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}. \end{array}$$

Now the complex numbers were formed from the reals by forming pairs of reals and adding $\sqrt{-1}$ to the system in a special way, namely, $a + ib$, where a and b are real numbers. To extend our correspondence of matrices to the complex numbers we will need a matrix to represent i. It turns out that the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \leftrightarrow i$$

will complete our correspondence. For we see

$$\begin{array}{ccc} i^2 & = & -1 \\ \updownarrow & & \updownarrow \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 & = & \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \end{array}$$

and

$$\begin{array}{ccccccc} a & + & i & \times & b & = & a+ib \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} & + & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \times & \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} & = & \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \end{array}$$

The correspondence

$$a + ib \leftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

shows that the complex numbers may be represented by 2×2 matrices with real elements. The reader may check that sums and products are preserved under this correspondence. A one-to-one correspondence preserving sums and products is called an "isomorphism."

Other noncommutative systems

There are other important, noncommutative systems in mathematics.

Noncommutative groups are such a system. For an example the reader is referred to a recent article* in THE MATHEMATICS TEACHER.

Another example is the "cross product" of two vectors. Here we have

$$\vec{A} \times \vec{B} = -\vec{B} \times \vec{A}.$$

There is also a "dot product," denoted by $\vec{A} \cdot \vec{B}$, for vectors that is commutative, however. Vectors are especially important in mechanics.

The quarternions are another example of a noncommutative system, though they are not as important as the others mentioned. They are numbers formed from pairs of complex numbers in much the same way complex numbers are formed from pairs of real numbers. For further information on any of the subjects mentioned in this paper, the reader is referred to the readable books listed below. Information on vector products may be found in a great variety of texts on vectoral mechanics and vector analysis, and in some analytic geometry texts.

* Carl H. Denbow, "To Teach Modern Algebra," THE MATHEMATICS TEACHER, XII (March 1959), 162–170.

SUGGESTED REFERENCES

ANDREE, RICHARD V., *Selections from Modern Abstract Algebra*. New York: Henry Holt and Co., 1958.

BIRKHOFF, GARRETT, and MACLANE, SAUNDERS. *Survey of Modern Algebra* (Rev. ed.). New York: The Macmillan Co., 1953.

HOHN, FRANZ E., *Elementary Matrix Algebra*. New York: The Macmillan Co., 1958.

FOREWORD

In this second essay dealing with a noncommutative algebraic structure, the author illustrates the properties of a noncommutative system by means of a system in which the elements are not numbers or matrices, but processes. Strictly speaking, the structure discussed is a "group," not an "algebra," despite the somewhat misleading title.

The thoughtful reader will appreciate the generality of certain mathematical concepts, namely, that "processes" may mean much more than the ordinary processes of arithmetic; that symbolism plays a crucial role; that mathematics is indeed man-made; and that the mathematics of the future may very well be so different from contemporary mathematics that it may scarcely be recognized as "mathematics."

A Noncommutative Algebra

Clarence R. Perisho

It is often said that one does not properly appreciate something until he has to do without it. This certainly applies to algebra as much as anything else. Any discussion of the commutative, associative and distributive laws often falls rather flat because they appear so "obvious." We are so used to assuming the commutative law $(ab = ba)$ in arithmetic and algebra that we miss its significance unless we work with a system where it does not apply.

It always does apply, of course, in arithmetic and in an algebra where the symbols represent numbers. The existence of noncommutative algebra has been known since 1843 when Hamilton discovered that quaternions did not obey the commutative law.[1] Besides quaternions one might mention the vector product of two vectors and the multiplication of matrices as examples of systems where the commutative law does not necessarily hold. Although these are important examples with many applications, they are rather difficult to explain on an elementary level.

The group of symmetries of a square[2] is an example of a noncommutative system that has the advantage of being easily understood and it can be developed in one class period.

The work can be prefaced by saying that we have been studying algebra where we assume the symbols represent numbers and the laws we use are those which are obeyed by ordinary numbers. There are, however, other kinds of algebra which might obey different sets of laws. Since we are boss of the symbols, we can give any meaning we wish to them. But once the meaning has been decided, it remains for us to determine what laws they obey.

Suppose we let our symbols represent, not numbers, but processes. For convenience, if one process is followed by another we call it *multiplication*. Thus if A means to add three and B means to multiply by six, AB means to add three and then multiply by six, but BA means to multiply by six and then add three. In general, this does not give the same result.

[1] W. T. Bell, *Men of Mathematics* (New York: Simon and Schuster, 1937), p. 360.

[2] Garrett Birkhoff and Saunders MacLane, *A Survey of Modern Algebra* (New York: The Macmillan Company, 1941), pp. 122–132.

We could let our symbols mean to turn a geometric figure in a certain way. We can then see whether these symbols obey the usual laws.

Each student can take a sheet of paper and cut or tear it into a square. The square is then marked so it is easy to tell when it is face up and right way around. Some students write their names at the top on one side or draw a picture of a man.

We find that the square can be placed in eight different positions (with sides parallel to the original) and we can give a symbol to the process that puts it into each position (Fig. 1).

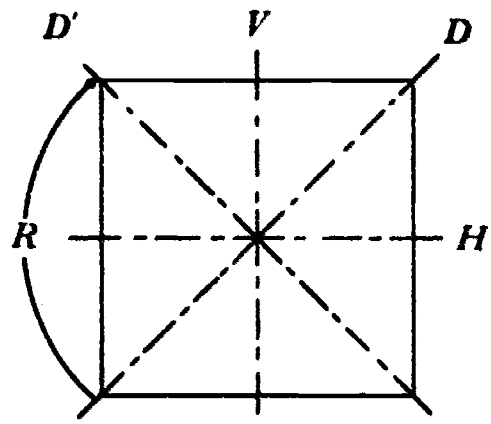


FIG. 1

V means to turn the paper over by rotating it around the vertical center line (face down but right side up).

H means to turn it over a horizontal center line (face down with top at the bottom).

D means to turn it over the diagonal line from upper right to lower left (face down and top to right).

D' means to turn it over the other diagonal (face down and top to left).

R means to turn the paper to the right 90° (face up and top to right).

R' means to turn it 180° (face up and top at bottom).

R'' means to turn it 270° to right (face up and top at left).

These make seven operations. The eighth would be to leave it in the original position. We thus let I be our *neutral element* that means we do nothing but leave the square alone. Of course I could also mean to rotate any multiple of 360°.

Now we can try some multiplication like VV. This means we apply process V and then apply it again. First we turn the paper over so it is right side up and face down, then turn it over again the same way and it is back where it started. Thus $V^2 = I$.

As we try other pairs of operations, we find, for instance, that applying V (leaves it right side up and face down) and then following it with D

(leaves it face up and top to right), produces the same result as applying R in the first place. Thus we can write $VD = R$. Similarly we can find that D (leaves it face down and top to right) followed by V (leaves it face up and top to left) results in the same position as R''. Thus, since $VD = R$ and $DV = R''$, it is evident that the commutative law does *not* hold.

	I	*V*	*H*	*D*	*D'*	*R*	*R'*	*R''*
I	*I*	*V*	*H*	*D*	*D'*	*R*	*R'*	*R''*
V	*V*	*I*	*R'*	*R*	*R''*	*D*	*H*	*D'*
H	*H*	*R'*	*I*	*R''*	*R*	*D'*	*V*	*D*
D	*D*	*R''*	*R*	*I*	*R'*	*H*	*D'*	*V*
D'	*D'*	*R*	*R''*	*R'*	*I*	*V*	*D*	*H*
R	*R*	*D'*	*D*	*V*	*H*	*R'*	*R''*	*I*
R'	*R'*	*H*	*V*	*D'*	*D*	*R''*	*I*	*R*
R''	*R''*	*D*	*D'*	*H*	*V*	*I*	*R*	*R'*

Fig. 2

The multiplication table (Fig. 2) can be well started in one class period and then finished at home. It is understood that the process on the left is performed first followed by the one on top. When the table is finished a number of questions can be answered by examining it.

1. Is the system *closed?* In other words, is the product of two operations always another operation of the set?
2. Is the *associative law* obeyed: $a(bc) = (ab)c$?
3. Is there a *neutral element*[3] e such that $ea = ae = a$ no matter which operation a might represent?
4. Does each element have an *inverse?*[4] That is, can we always find values of x which satisfy the equation $ax = e$ no matter what operation a might represent?
5. Does the *commutative law* hold? That is, does $ab = ba$?

If some student wishes to pursue the matter further, there are several possibilities.

[3] Often called the identity Element. Zero is the familiar identity element for addition since $a + 0 = 0 + a = a$. One is the familiar identity element for multiplication since $a \times 1 = 1 \times a = a$.

[4] Two elements that produce the neutral or identity element are said to be inverses. Thus +2 and −2 are inverses under addition because $+2 + (-2) = 0$. And 2 and ½ are inverses under ordinary multiplication because $2 \times \frac{1}{2} = 1$. In the system described here R and R'' are inverses because $RR'' = I$.

First, it could be pointed out that the system forms a *group*[6] because (a) it is closed, (b) it is associative, (c) it contains a neutral element, and (d) each element has an inverse.

Second, the problem of solving for x in equations like $Rx = H$ and $xR = H$ could be investigated. From examining the multiplication table we find that the solutions are $x = D'$ and $x = D$ respectively. Since the equations have different solutions, it is *not* satisfactory to write the solutions as H/R or $H \div R$. We can, however, solve the first equation systematically by multiplying both sides of the equation on the *left* by the inverse of R (written R^{-1}).

$Rx = H$	[Original problem]
$R^{-1}Rx = R^{-1}H$	[Multiplying both sides of the equation on the *left* by the inverse of R]
$Ix = R^{-1}H$	[From definition of inverse]
$x = R^{-1}H$	[From definition of neutral element]
$R^{-1} = R''$	[Observed from table]
$x = R''H$	[Substituting the inverse of R]
$x = D'$	[Reading the product R'' and H from the table]

In the second equation we should start by multiplying by R^{-1} on the *right*. Thus we see that although H/R is ambiguous, $R^{-1}H$ and HR^{-1} are not and can be used.

Third, the existence of *subgroups* could be pointed out. That is, groups can be formed from less than the full eight transformations. For example, I and H form a subgroup, and I and V form a subgroup.

Fourth, multiplication tables for other groups of geometric transformations could be constructed. A rectangle, equilateral triangle, or regular hexagon could be tried. A very ambitious student might try the group for rotations of a cube. A cube has 24 symmetries and the multiplication table has $24 \times 24 = 576$ entries in it.

[6] Richard V. Andree, *Selections from Modern Abstract Algebra* (New York: Henry Holt Company, 1958), p. 79; *Insights into Modern Mathematics* (Twenty-third yearbook, Washington, D.C.: The National Council of Teachers of Mathematics, 1957), pp. 106, 133; M. Richardson, *Fundamentals of Mathematics* (revised edition; New York: The Macmillan Company, 1958), p. 467.