# THE FUNDAMENTAL LAWS OF ADDITION AND MULTIPLICATION IN ELEMENTARY ALGEBRA

By Edward V. Huntington

Reprinted from the Annals of Mathematics, Second Series,
Vol. 8, No. 1, October, 1906

For sale by
the Publication Office of Harvard University,
2 University Hall, Cambridge, Mass.
Price, 50 cents

# THE FUNDAMENTAL LAWS OF ADDITION AND MULTIPLICATION IN ELEMENTARY ALGEBRA *

By Edward V. Huntington

CONTENTS.



* This article contains part of a paper presented by the writer to the American Mathematical Society on Dec. 28, 1905.

INTRODUCTION.

Elementary algebra may be regarded, for the purpose of the present paper, as a body of propositions concerning the sums and products of numbers ;* these propositions are not independent, but can all be deduced from a few fundamental propositions, or axioms, which are accepted as self-evident properties of number, just as the propositions of geometry can all be deduced from a few fundamental propositions, or axioms, which are accepted as self-evident properties of space.

The primary object of this paper is to present a list of fundamental propositions for algebra, from which, on the one hand, all the other propositions of algebra can be deduced, and in which, on the other hand, no superfluous items are included,—a list, in short, which is *sufficient*, and *free from redundancies*.

The first propositions which suggest themselves for this purpose are the ten "general laws" numbered $A1$–$A5$, $M1$–$M5$, in §1 ; all these laws will be recognized as familiar and obviously true propositions concerning numbers.

The next step is to see what propositions follow from these laws by logical deduction. But here the question at once arises : How can we be sure that our deduction is rigorous? How can we be sure that we do not employ, in our reasoning, some other properties of numbers besides those expressly stated in the axioms? The only way to avoid this danger is to think of our fundamental laws, not as axiomatic propositions about numbers, but as *blank forms* in which the letters $a$, $b$, $c$, etc. may denote any objects we please and the symbols $+$ and $\times$ any rules of combination ;† such a blank form will become a proposition only when a definite interpretation is given to the letters and symbols—indeed a true proposition for some interpretations and a false proposition for others. (Thus, the blank form "$a + b = b + a$"

---

* It will greatly assist the reader if he will, from the start, think of multiplication, not as repeated addition, but as a separate operation, having no connection with addition except through the distributive law, $a(b + c) = ab + ac$.

Many propositions of algebra concern also the relation of order (or of "greater and less") between two numbers; these propositions are not considered however in the present paper, which stops at the point where the introduction of the relation of order seems necessary.

† A rule of combination is any rule or convention by which two objects determine a third.

is a true proposition if $a$ and $b$ signify numbers, and + the ordinary addition of numbers; but it is a false proposition if $a$ and $b$ signify rotations of a plane about various axes perpendicular to it, and + the succession of two such rotations.) The deductions made from such blank forms must necessarily be purely formal, and hence will not be affected by the troublesome connotations which would be sure to attach themselves to any concrete interpretation of the symbols.

From this point of view our work becomes, in reality, much more general than a study of the system of numbers; it is *a study of any system which satisfies the conditions laid down in the general laws* of §1.* As a matter of fact, there are many such systems, all of which are usually included under the general name of algebra. Thus, there are the various different systems of numbers—the positive integral numbers, the rational numbers, the complex numbers, etc.,—all of which, when + and × are defined in the ordinary way, satisfy all these laws. Then there is the system of points (or vectors) in a plane, with their "sums" and "products" defined as in Argand's diagram (see the end of this introduction). Another striking example is the system of all rational numbers, with the "sum" of $a$ and $b$ defined as $a + b + 1$ and their "product" as $ab + (a + b)$; † a brief computation will show that this strange system also satisfies all the laws of §1.

Every system which has the properties stated in the fundamental laws will have also all the properties formally deduced from those laws. The system of natural numbers, with ordinary addition and multiplication, appears, therefore, as merely a special case of the general class of systems whose properties are here studied.

The object of the paper may now be more precisely stated in the following form: *Given a class of elements with two rules of combination, what conditions must such a system satisfy in order to be formally equivalent to one of the systems of ordinary algebra?* The first conditions which we impose are naturally the ten "general laws" numbered $A1$–$A5$, $M1$–$M5$, in §1; but these laws are to be regarded no longer as "axioms," since they are merely blank forms, not in themselves either true or false, but rather as "postulates," because we

* By a "system," in this connection, we mean any class of entities among which two rules of combination are established.—The entities which belong to the class are called the "elements" of the class, or of the system.

† *Trans. Amer. Math. Soc.*, vol. 6 (1905), p. 225.

"demand," arbitrarily, that the system considered shall conform to these conditions.*

It appears at once, however, that there are many different types of elementary algebra (for example the algebra of the positive integers, the algebra of the rational numbers, the algebra of vectors, etc.), and that the ten general laws of §1 are not sufficient to determine any particular type. We therefore add, in §4, a list of special laws (postulates $E1$–$E6$), which serve to distinguish the various types from one another. This §4 thus completes the main object of the paper. Special attention may be called to the discussion of the notion of isomorphism between two systems, and the notion of a sufficient, or categorical, set of postulates for a particular type of algebra (see page 26), which are of fundamental importance in this connection.

Finally, in §5, the *independence* of the general laws is established, so that we may be sure that the list contains no redundancies. The method for establishing the independence of a set of postulates consists in exhibiting, in the case of each postulate, an example of a system which satisfies all the other postulates of the set, but not the one in question.† These systems may be called pseudo-algebras, since they fail to be true algebras in respect to some single item in the specifications.‡

Incidentally, the paper contains a rigorous development of the rational number-system, starting from the sequence of the natural numbers. The various kinds of numbers are introduced primarily as operators, to indicate repeated addition, repeated multiplication, etc., performed on the elements of the original system; but rules of combination are defined among these operators in such a way that they become themselves examples of systems which satisfy all the laws of §1. Moreover, all the examples used in §5 are constructed out of material offered by these number-systems, so that no part of the paper (except the introduction, and the proof of the final paragraph in §4) presupposes any knowledge of mathematics whatever, beyond the ability to recite the familiar sequence of natural numbers: 1, 2, 3, etc.

* Any set of consistent postulates might be used as the basis of an abstract deductive theory; but only those sets of postulates are worth studying which are capable of some interesting concrete interpretation. If preferred, the postulates may be called "assumptions," or "hypotheses;" cf *Trans. Amer. Math. Soc.*, vol. 5 (1904), p. 288.

† This method has become familiar in the last ten years through the works of Peano, Pieri, Padoa, Hilbert, and others.

‡ It is customary, however, to extend the word algebra so as to include any system which satisfies postulates $A1, 2, 3, 4, 5$; $M1, 4$; and $E1$.

The signs "=" and "$\neq$" are used to denote equality and inequality, respectively; two elements are said to be equal when either can replace the other in every proposition in which it occurs.

It is needless to add that the paper contains no new theorems in so old a subject as elementary algebra; the only part of the paper which has any claim to originality is §5, containing the proofs of independence.

For bibliographical references, the reader is referred to the *Transactions of the American Mathematical Society*, vol. 3 (1902), p. 264; vol. 5 (1904), p. 288; vol. 6 (1905), p. 209; to H. Hankel's *Theorie der complexen Zahlensysteme* (1867); to Stolz and Gmeiner's *Theoretische Arithmetik* (1902); and to articles in the *Encyclopädie der mathematischen Wissenschaften.*

*Illustrative example.*

In order to have before the reader a concrete example of a system which satisfies all the postulates, we cite at once the familiar geometric example of the ordinary complex quantities, or vectors in the plane (Argand's diagram). In this system the class of elements considered is the class of all the points in the plane, including a special point $O$, called the origin, and another special point $U$, whose distance from $O$ is called the unit-distance.

The point $A + B$ is defined as the point arrived at by starting from $A$ and taking a step equal in length and direction to the step from $O$ to $B$.

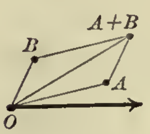


FIG. 1.

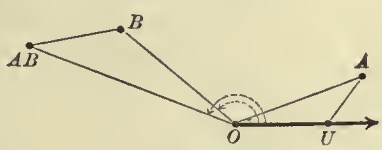


FIG. 2.

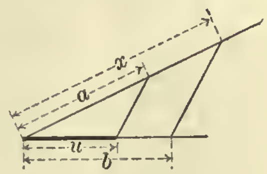


FIG. 3.

The point $A \times B$ is defined as the point whose "angle" (from $OU$) is the *sum* of the "angles" of $A$ and $B$ and whose "distance" (from $O$) is the *product* of the "distances" of $A$ and $B$. Here if $a$ and $b$ are the distances of $A$ and $B$ respectively, then the "product," $x$, of $a$ and $b$, is to be constructed geometrically from the proportion $x : a = b : u$, where $u$ is the unit-distance (see figure 3).

With an elementary knowledge of plane geometry, including the properties of similar triangles, one can readily show that this system satisfies all the postulates $A1$–$A5$, $M1$–$M5$, in §1, and also the "existence-postulates" $E1$–$E5$, in §4; the proof for $E6$, however, is more difficult.

[The "product" of two distances, $a$ and $b$, with respect to the unit-distance $u$, may also be defined as follows: In the special case in which $a$ and $b$ are commensurable with $u$, say $a = (\kappa/\mu)u$ and $b = (\lambda/\nu)u$, their product is defined as $(\kappa\lambda/\mu\nu)u$. In any case, there are sequences of commensurable distances which approach $a$ and $b$ as limits:

$$a = \lim \left[\lambda_1 \frac{u}{2}, \lambda_2 \frac{u}{2^2}, \lambda_3 \frac{u}{2^3}, \cdots\right], b = \lim \left[\mu_1 \frac{u}{2}, \mu_2 \frac{u}{2^2}, \mu_3 \frac{u}{2^3}, \cdots\right];$$

then the product of $a$ and $b$ is defined as the limit of the sequence

$$\lambda_1\mu_1 \frac{u}{2^2}, \lambda_2\mu_2 \frac{u}{2^4}, \lambda_3\mu_3 \frac{u}{2^6}, \cdots.$$

If this definition appears less simple than the geometric definition given above, it may be remembered that the properties of similar triangles, on which the geometric construction depends, are usually established by the consideration of limits of infinite sequences of precisely this character.]

### §1. THE GENERAL LAWS OF ADDITION AND MULTIPLICATION.

We consider a *class of elements*, denoted by $a$, $b$, $c$, etc., and *two rules of combination*, called addition ($+$) and multiplication ($\times$); and upon this system we impose the following conditions, expressed in the postulates numbered I, $A1$–$A5$, $M1$–$M5$.

The *consistency* of these postulates is shown by the examples given in the introduction and in §3; their *independence* will be established by the examples given in §5.

Any system which satisfies these postulates $A1$–$A5$, $M1$–$M5$ is said to *obey the general laws of elementary algebra* as regards addition and multiplication. Various *special types* of systems of this kind will be distinguished by means of further postulates in §4.

In order to exclude the obviously trivial cases of an empty class and a class containing only a single element, we adopt, first of all,

POSTULATE I. *The class contains at least two elements.*

This postulate will be assumed without further mention throughout the paper.

*The laws of addition.*

POSTULATE $A1$. *If $a$ and $b$ are elements of the class ($a = b$ or $a \neq b$), then $a + b$ is likewise an element of the class, uniquely determined by $a$ and $b$ in their given order, and called the "sum, $a$ plus $b$."*

The operation of finding $a + b$ when $a$ and $b$ are given is called "addition;" the elements $a$ and $b$ are called the "terms" of the sum $a + b$.

Any system which satisfies this postulate $A1$ may be called a *closed system with respect to addition*, since the successive addition of any number of elements does not take us outside the system. When sums of three or more elements are considered, parentheses are employed with obvious significance, as in $[(a + b) + c] + d$, etc. It should be noticed, however, that as far as postulate $A1$ is concerned, $a + b$ is not necessarily the same element as $b + a$ (see postulate $A5$).

POSTULATE $A2$. *Throughout the system,*

$$(a + b) + c = a + (b + c).$$

This is the *associative law for addition.** In view of this law, parentheses may be removed or inserted at pleasure in a sum of any number of terms.

POSTULATE $A3$. (1) *If* $a + x = a + y$, *then* $x = y$.
(2) *If* $x + a = y + a$, *then* $x = y$.

These may be called the *laws of cancelation for addition.*† Either (1) or (2) is deducible from the other by the aid of the commutative law for addition (see postulate $A5$), but so many theorems can be proved from $A1$, 2, 3 without the aid of that law that it has seemed worth while to state both parts of $A3$ in this manner.

POSTULATE $A4$. *If $\mu x = \mu y$, where $\mu$ is any positive integer, then $x = y$.*

This postulate will be used first in connection with theorem 26; the notation, which indicates repeated addition, will be explained in theorem 21. The postulate may be called the *law of non-circularity*, since, as we shall see

* The words "associative," "commutative," and "distributive" have been in general use since the middle of the nineteenth century. See H. Hankel, *Theorie der complexen Zahlensysteme* (1867), p. 3, foot-note.

† Cf. *Trans. Amer. Math. Soc.*, vol. 6 (1905), p. 212.

in theorem 26, it prevents a repeated summation from returning, so to speak, into itself. (For a "weaker" postulate, which can be used, under certain conditions, in place of postulate $A4$, see appendix 1.)

[POSTULATE $A5$. *Throughout the system,*

$$a + b = b + a.]$$

This is the *commutative law for addition.** This postulate is placed in brackets, because it will prove to be deducible from $A1$, 2, 3, with the aid of some of the laws of multiplication, and is therefore redundant when the list of postulates is taken as a whole (see page 25.)

*The laws of multiplication.*

POSTULATE $M1$. *If $a$ and $b$ are elements of the class ($a = b$ or $a \neq b$), then $a \times b$ (written also $a \cdot b$ or simply $ab$) is likewise an element of the class, uniquely determined by $a$ and $b$ in their given order, and called the "product, $a$ times $b$."*

The operation of finding $a \times b$ when $a$ and $b$ are given is called "multiplication;" the elements $a$ and $b$ are called the "factors" of the product $ab$. Parentheses are used as in addition.

POSTULATE $M2$. *Throughout the system,*

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

This is the *associative law for multiplication.* In view of this law, parentheses may be removed or inserted at pleasure in a product of any number of factors.

POSTULATE $M3$. (1) *If $ax = ay$ and $a + a \neq a$, then $x = y$.*
(2) *If $xa = ya$ and $a + a \neq a$, then $x = y$.*

These are the *laws of cancelation for multiplication.* Either (1) or (2) is deducible from the other by the aid of the commutative law for multiplication (postulate $M5$); both parts are included, however, for the sake of the deductions which can be made from $M1$, 2, 3 without the aid of $M5$. The restriction "$a + a \neq a$" may be written "$a \neq \mathbf{0}$" after the definition of the zero-element is obtained, in theorem 1. (For a "weaker" postulate which can be used, under certain conditions, in place of postulate $M3$, see appendix 1.)

---

* See footnote * on preceding page.

POSTULATE $M4$. *Throughout the class,*

$$(1)\quad a(b+c)=ab+ac, \textit{ and}$$
$$(2)\quad (b+c)a=ba+ca.$$

These are called the *distributive laws * for multiplication* with respect to addition. Either (1) or (2) is deducible from the other by the aid of $M5$; both parts are included, however, for the same reason as in the case of postulate $M3$.

POSTULATE $M5$. *Throughout the system,*

$$a \times b = b \times a.$$

This is the *commutative law for multiplication.* Unlike the commutative law for addition, this postulate is independent of all the preceding postulates.

These ten postulates, $A1$–$A5$, $M1$–$M5$, are the general laws of addition and multiplication in elementary algebra. The immediate consequences of these laws are developed in the next section.

## §2. DEDUCTIONS FROM THESE LAWS.

Sections 2–3 contain the most important of the deductions which can be drawn from the postulates $A1$–$A5$, $M1$–$M5$. The precise postulates on which the proof of each theorem depends are stated in brackets after the number of the theorem; to avoid interruption in reading the paper, the proofs themselves, whenever needed, are collected in §6 below.

### *The zero-element.*

*Theorem* 1, *and Definition.* [$A1$, 2, 3.] It follows from postulates $A1$, 2, 3 that there cannot be more than one element $z$ such that $z+z=z$; if there is any such element, it is called the *zero-element* of the system, and denoted by $\mathbb{0}$; that is,

$$\mathbb{0}+\mathbb{0}=\mathbb{0}.$$

(Proof on p. 35; on the use of the symbols $\mathbb{0}$ and 0, see §3, below.)

This definition of the zero-element, which is suggested by Benjamin Peirce's definition of an "idempotent" element,† is somewhat simpler than the more usual definition, which is based on the property here stated as theorem 2.

* See footnote * on page 7.

† B. Peirce, *Linear Associative Algebra*, 1874.

*Theorem* 2. [$A$1, 2, 3.] If there is a zero-element, $\mathbb{0}$, then

$$a + \mathbb{0} = a \text{ and } \mathbb{0} + a = a$$

for every element $a$; and conversely, if $a + x = a$ or $x + a = a$, then $x = \mathbb{0}$. (Proof on p. 36.)

On account of this additive property, the zero-element is often called the "modulus" of addition.*

*Theorem* 3. [$A$1, 2, 3; $M$1, 4.] If there is a zero-element, $\mathbb{0}$, then

$$a \times \mathbb{0} = \mathbb{0} \text{ and } \mathbb{0} \times a = \mathbb{0}$$

for every element $a$. (Proof on p. 36.)

This theorem expresses the multiplicative property of the zero-element.

*Theorem* 4. [$A$ 1, 2, 3; $M$ 1, $3_1$ or $3_2$, 4.] If $ab = \mathbb{0}$ then either $a = \mathbb{0}$ or $b = \mathbb{0}$. In other words, a product $ab$ cannot be the zero-element, unless at least one of its factors, $a$ or $b$, is the zero-element. (Proof on p. 36.)

This theorem is of considerable importance, and may be called the *law of the zero product* (compare appendix 1).

### *The unit-element.*

*Theorem* 5, *and Definition*. [$M$1, 2, 3.] It follows from postulates $M$1, 2, 3 that there cannot be more than one element $u$, different from the zero-element, and such that $u \times u = u$; if there is any such element, it is called the *unit-element* of the system, and denoted by $\mathbb{1}$; that is,

$$\mathbb{1} \times \mathbb{1} = \mathbb{1} \quad (\mathbb{1} \neq \mathbb{0}).$$

(Proof on p. 36; on the use of the symbols $\mathbb{1}$ and 1, see §3, below.)

*Corollary*. If $a \times a = a$ and $a \neq \mathbb{0}$, then $a = \mathbb{1}$.

This definition of the unit-element is due to B. Peirce (loc. cit.); the more usual definition is here given as theorem 6.

*Theorem* 6. [$M$1, 2, 3.] If there is a unit-element, $\mathbb{1}$, then

$$a \times \mathbb{1} = a \text{ and } \mathbb{1} \times a = a$$

for every element $a$. (Proof on p. 36.)

On account of this property, the unit-element is often called the "modulus" of multiplication.

---

* Cf. H. Hankel, loc. cit., p. 23; also Stolz and Gmeiner, *Theoretische Arithmetik* (1902), p. 54.

*Theorem* 7. [$A$1, 2, 3; $M$1, 2, 3, 4.] Conversely, if $ax = a$ or $xa = a$, and $a \neq \mathbb{0}$, then $x = 1$. (Proof on p. 36.)

*Opposite elements. Subtraction.*

*Lemma.* [$A$1, 2, 3.] It follows from postulates $A$1, 2, 3 that if $a + b = \mathbb{0}$, then $b + a = \mathbb{0}$; hence we may speak of two elements as having a zero sum, without ambiguity in regard to the order of the terms, even before assuming the commutative law $A5$. (Proof on p. 36.)

*Theorem* 8, *and Definition.* [$A$1, 2, 3.] Given any element $a$, there cannot be more than one element $x$ such that the sum of $x$ and $a$ is $\mathbb{0}$; if there is any such element, it is called the *opposite of* $a$, and denoted by $\mathbb{0} - a$, or simply by $-a$; that is,

$$a + (-a) = (-a) + a = \mathbb{0}.$$

Any two elements whose sum is the zero-element are called a pair of opposite elements.

*Corollary.* If there is a zero-element, then $-\mathbb{0} = \mathbb{0}$; and if $a$ is an element which has an opposite, then $-(-a) = a$.

The opposite of an element $a$ is commonly called the "negative" of $a$; it seems preferable, however, to reserve the term negative for use in the phrase "positive and negative elements." *

Concerning the multiplication of opposites we have:

*Theorem* 9. [$A$1, 2, 3; $M$1, 4.] If $a$ and $b$ are elements which have opposites, then

$$(-a) \times b = a \times (-b) = -ab, \quad \text{and} \quad (-a) \times (-b) = ab.$$

(Proof on p. 36.)

The following theorems are the first which require the commutative law for addition (postulate $A5$):

*Theorem* 10. [$A$1, 2, 3, 5.] If $a$ and $b$ are elements which have opposites, then

$$(-a) + (-b) = -(a + b).$$

(Proof on p. 36.)

---

* The distinction between positive and negative elements involves the notion of *order*, and will therefore not be discussed in the present paper. (An element $a$ is called positive or negative according as $a + a > a$ or $a + a < a$.) It should be mentioned, however, that in many cases the relation of order is definable in terms of addition, or of addition and multiplication; see especially O. Veblen, *Trans. Amer. Math. Soc.*, vol. 7 (1906), pp. 197–199.

*Theorem* 11, *and Definition*. [$A$1, 3, 5.] Given any elements $a$ and $b$, there cannot be more than one element $x$ such that $a = b + x = x + b$; if there is any such element it is called the *remainder*, *a minus b*, and denoted by $a - b$; that is,

$$a = b + (a - b) = (a - b) + b.$$

The operation of finding $a - b$ when $a$ and $b$ are given is called "subtraction;" the definition of $\mathbf{0} - a$ in theorem 8 is a special case.

*Theorem* 12. [$A$1, 2, 3, 5.] If the remainders in question exist, then $a + (b - c) = (a + b) - c$; $a - (b + c) = (a - b) - c$; and $a - (b - c) = (a - b) + c$. Moreover, if there is a zero-element, then $a - \mathbf{0} = a$ and $a - a = \mathbf{0}$; and if $-x$ exists, then

$$a + (-x) = a - x \text{ and } a - (-x) = a + x.$$

(Proof on p. 36.)

*Theorem* 13. [$A$1, 3, 5; $M$1, 4.] If $b - c$ exists, then

$$a(b - c) = ab - ac \text{ and } (b - c)a = ba - ca.$$

(Proof on p. 37.)

*Reciprocal elements. Division.*

*Lemma*. [$M$1, 2, 3.] It follows from postulates $M$1, 2, 3 that if $ab = \mathbf{1}$, then $ba = \mathbf{1}$; hence we may speak of two elements as having a unit product, without ambiguity in regard to the order of the factors, even before assuming the commutative law $M$5. (Proof on p. 37.)

*Theorem* 14, *and Definition*. [$M$1, 2, 3.] Given any element $a$, there cannot be more than one element $y$ such that the product of $y$ and $a$ is $\mathbf{1}$; if there is any such element, it is called the *reciprocal of a*, and denoted by $\frac{\mathbf{1}}{a}$, or $\mathbf{1}/a$; so that

$$a\left(\frac{\mathbf{1}}{a}\right) = \left(\frac{\mathbf{1}}{a}\right)a = \mathbf{1}.$$

(Proof on p. 37.) Any two elements whose product is the unit-element are called a pair of reciprocal elements.

*Remark*. In view of theorem 3, it is evident that *if $a = \mathbf{0}$, then no reciprocal of $a$ exists* in any system that satisfies postulate $M$4.

*Theorem* 15. [$A$1, 2, 3; $M$1, 2, 3, 4.] If $a$ is an element which has an opposite and a reciprocal, then

$$\frac{1}{-a} = -\frac{1}{a}.$$

(Proof on p. 37.)

The following theorems are the first which require the commutative law for multiplication (postulate $M5$):

*Theorem* 16. [$M$1, 2, 3, 5.] If $a$ and $b$ are elements which have reciprocals, then

$$\frac{1}{a} \times \frac{1}{b} = \frac{1}{ab}.$$

(Proof on p. 37.)

*Theorem* 17, *and Definition.* [$M$ 1, 3, 5.] Given any elements $a$ and $b$, $b$ not zero, then there cannot be more than one element $y$ such that $a = by = yb$; if there is any such element it is called the *quotient, a divided by b*, and is denoted by $\frac{a}{b}$, or $a/b$; so that

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

The operation of finding $a/b$ when $a$ and $b$ are given is called "division;" the element $a$ is called the "numerator," and $b$ the "denominator," of the quotient $a/b$. The special case in which the numerator is the unit-element agrees with the definition of $1/a$ given in theorem 14.

*Remark.* From theorem 3 it is evident that if $b = 0$ there is no (uniquely determined) element $y$ such that $a = by$; hence *division by the zero-element* is impossible in any system which satisfies postulate $M4$. On the other hand, if $b \neq 0$, then $0/b = 0$.

*Theorem* 18. [$M$ 1, 2, 3, 5.] If the quotients in question exist, then

$$\frac{ac}{bc}=\frac{a}{b};\ \left(\frac{a}{b}\right)\times c = \frac{ac}{b};\ \left(\frac{a}{b}\right)/c = \frac{a}{bc};\ \frac{a}{b}\times\frac{c}{d} = \frac{ac}{bd};\ \left(\frac{a}{b}\right)/\left(\frac{c}{d}\right) = \frac{ad}{bc}.$$

Moreover, if there is a unit-element, then $a/1 = a$ and $a/a = 1$. (Proof on p. 37.)

*Theorem* 19. If the required quotients and remainders exist, then:

(1) [$A$1; $M$ 1, 2, 3, 4, 5.] $\quad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$;

(2) [$A$1, 3, 5; $M$1, 2, 3, 4, 5.] $\quad \frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$.

(Proof on p. 37.)

*The so-called imaginary units.*

*Theorem* 20. [$A$1, 2, 3; $M$1, 2, 3, 4, 5.] In a system containing a unit-element and its opposite ($\mathbf{1}$ and $-\mathbf{1}$), if there is any element $x$ such that $x \times x = -\mathbf{1}$, then there will be another element, namely $-x$, having the same property; but there cannot be more than two such elements. If there are two such elements, they are called the *imaginary units* (or better, the *secondary units*) of the system; and denoted by $i$ and $-i$; that is

$$i \times i = -\mathbf{1} \quad \text{and} \quad (-i) \times (-i) = -\mathbf{1}.$$

(Proof on p. 37.)

The term imaginary is a legacy from the eighteenth century, which has, unfortunately, become firmly fixed in mathematical literature; the elements $i$ and $-i$ are of course no more "imaginary" than any other elements which may exist in the system.*

It is a curious fact concerning these imaginary units, that no distinction can be made between them in terms of addition and multiplication; that is, there is no true proposition concerning $i$, and expressible in terms of addition and multiplication alone, which does not remain a true proposition when $-i$ is put in place of $i$.

## §3. FURTHER DEDUCTIONS: USE OF NUMERICAL OPERATORS.

*Multiples of an element. Use of integral numbers as coefficients.*

*Theorem* 21, *and Definition.* [$A$1, 2.] If $a$ is any element of the system, then the elements

$$a, \quad a+a, \quad a+a+a, \quad a+a+a+a, \quad \cdots$$

belong to the system, and are called the *multiples of* $a$. In order to secure a

* For a sketch of the history of the imaginary quantities, see H. Hankel, loc. cit., p. 71.

convenient notation for these successive multiples, we employ, in the manner explained below, the familiar sequence of Arabic numerals,

$$1,\ 2,\ 3,\ \cdots;$$

no knowledge of these symbols is presupposed, however, beyond a rule by which, when any one of them is given, the next following one can be written down, the rule being of such a nature that each new symbol is different from all that have gone before it. Thus:

the element $a$ is denoted by $1a$;
the element $1a + a$ is denoted by $2a$;
the element $2a + a$ is denoted by $3a$;

and so on; in general,

the element $\nu a + a$ is denoted by $\nu' a$,

where $\nu'$ is the numeral next following $\nu$. In this way the element $\mu a$, where $\mu$ is any Arabic numeral, is defined, and is called the $\mu^{th}$ *multiple of* $a$.

The Arabic numerals are called, in mathematical language, the *positive integral numbers*, or the *positive integers*, and when used in the manner just described they are called *coefficients;* thus, in $\mu a$, the number $\mu$ is the coefficient of the element $a$.

It must be noticed that $\mu a$ is not a product in the sense of postulate $M1$, since the number $\mu$ is merely a symbol of operation and not an element of the system $a, b, c, \cdots$. In particular, the positive integral number 1 must not be confused with the unit-element, $\mathbf{1}$, of theorem 5.

The statement of many theorems in regard to multiples of an element can be much simplified by the aid of the following conventions in regard to the positive integral numbers.

If $\lambda$ is any positive integer, then the integer next following $\lambda$ is called the *successor* of $\lambda$, and denoted by $\lambda + 1$; the successor of $\lambda + 1$ is denoted by $\lambda + 2$; the successor of $\lambda + 2$ is denoted by $\lambda + 3$; and so on; in general, the successor of $\lambda + \nu$ is denoted by $\lambda + \nu'$, where $\nu'$ is the successor of $\nu$; that is,

$$(\lambda + \nu) + 1 = \lambda + (\nu + 1).$$

In this manner, we can define, by successive steps, a positive integer

$$\lambda + \mu,$$

for any two positive integers $\lambda$ and $\mu$; this integer $\lambda + \mu$ is called the *sum*, $\lambda$ *plus* $\mu$.

Further, if $\lambda$ is any positive integer, $\lambda + \lambda$ is denoted by $2\lambda$; $2\lambda + \lambda$ is denoted by $3\lambda$; and so on; in general, $\nu\lambda + \lambda$ is denoted $\nu'\lambda$, where $\nu'$ is the successor of $\nu$; that is,

$$\nu\lambda + \lambda = (\nu + 1)\lambda;$$

moreover, to complete the series, we set $1\lambda = \lambda$.

In this manner we can define, by successive steps, a positive integer

$$\mu\lambda \text{ (written also } \mu \times \lambda \text{ or } \mu\cdot\lambda)$$

for any two positive integers $\lambda$ and $\mu$; this integer $\mu\lambda$ is called the *product*, $\mu$ *times* $\lambda$.

Finally, if $\lambda$ comes later than $\mu$ (or $\mu$ earlier than $\lambda$) in the succession of positive integers, we write $\lambda > \mu$ (or $\mu < \lambda$).

From these definitions it follows, by "mathematical induction," that the sums and products of the positive integral numbers obey the associative, commutative, and distributive laws for addition and multiplication, and also the laws of cancelation (proof on p. 37); in other words, *the system of positive integers, with addition and multiplication defined as above, is itself an example of a system satisfying postulates $A1$–$A5$, $M1$–$M5$*, so that all the definitions and theorems of §2 can be applied to it.' Thus, the system contains a unit-element (namely the number 1), but no zero-element; the remainder, $\lambda - \mu$, will exist in the system when and only when $\lambda > \mu$. The fact that the number-system satisfies the ten postulates is incidental, however, in the present discussion, since the numbers appear merely as symbols of operation, not as elements of the class $a, b, c, \cdots$ whose properties are primarily under consideration.

The usefulness of these definitions concerning the positive integral numbers is shown by the following theorems concerning multiples of an element of the original system:

*Theorem* 22. [$A1$, 2.] If $a$ be any element of the system, and $\lambda$, $\mu$ any positive integers, then

$$\lambda a + \mu a = (\lambda + \mu)a \quad \text{and} \quad \lambda(\mu a) = (\lambda\mu)a.$$

(Proof on p. 38.)

The first part of this theorem shows that the sum of any two multiples of $a$ is again a multiple of $a$, and that $\lambda a + \mu a = \mu a + \lambda a$; that is, *the* *system of multiples of any element a is a closed system with respect to addition, and obeys the commutative law.* Hence we may use the notion of subtraction within this system (theorems 11–12), so that we have, on the basis of postulates $A1$, 2, 3 alone:

*Theorem* 23. [$A1$, 2, 3.] If $\lambda > \mu$, then

$$\lambda a - \mu a = (\lambda - \mu)a.$$

(Proof on p. 39.)

*The negative integral numbers and the zero-number.*

Concerning multiples of opposite elements, we have:

*Theorem* 24. [$A1$, 2, 3.] If $a$ is any element which has an opposite, then

$$\mu(-a) = -(\mu a),$$

where $\mu$ is any positive integer. Hence, any element of this form may be denoted without ambiguity by $-\mu a$. (Proof on p. 39.)

This theorem suggests the use of the composite symbol $-\mu$ as an operator analogous to the operators already used; such a symbol $-\mu$, where $\mu$ is any positive integer, is called a *negative integral number*, or a *negative integer*. Moreover, we may define sums and products of positive and negative integers as follows (the purpose being to devise such definitions that the formulæ in theorem 22 shall remain true when $\lambda$ or $\mu$ or both are negative):

$$(-\lambda) + (-\mu) = -(\lambda + \mu)\,; \quad \lambda + (-\mu) = (-\mu) + \lambda = \begin{cases} \lambda - \mu \text{ when } \lambda > \mu, \\ -(\mu - \lambda) \text{ when } \lambda < \mu\,; \end{cases}$$

$$(-\lambda) \times (-\mu) = \lambda\mu\,; \qquad \lambda \times (-\mu) = (-\lambda) \times \mu = -(\lambda\mu).$$

These definitions are only partially satisfactory, however, since there is no meaning attached to a sum of the form $\lambda + (-\lambda)$. To obviate this difficulty, we introduce a new operator called the *zero-number*, 0, with the convention that

$$0a = \mathbb{0}$$

for every element $a$, and the following definitions as to sums and products:

$$\lambda + (-\lambda) = 0\,;\ \lambda + 0 = 0 + \lambda = \lambda\,;\ (-\lambda) + 0 = 0 + (-\lambda) = -\lambda\,;\ 0 + 0 = 0\,;$$

$$\lambda \times 0 = 0 \times \lambda = 0\,; \quad (-\lambda) \times 0 = 0 \times (-\lambda) = 0\,; \quad 0 \times 0 = 0.$$

This zero-number, 0, which is merely an operator, must be carefully distinguished from the zero-element, $\mathbb{0}$, of theorem 1.

The positive and negative integers, together with the zero-number, make up the system of *all integral numbers*. *The system of all integral numbers is, incidentally, another example of a system which satisfies all the postulates $A1$–$A5$, $M1$–$M5$*; it contains a unit-element (the number 1), and a zero-element (the number 0); and subtraction is always possible. The usefulness of these definitions is shown by the following theorem:

*Theorem* 25. [$A1$, 2, 3.] If $a$ is any element which has an opposite, then the formulæ of theorem 22 hold true when $\lambda$ and $\mu$ are any integral numbers (positive, negative or zero).

*Submultiples and rational fractions of an element. Use of the rational numbers as coefficients.*

The following theorems depend on the postulate of non-circularity ($A4$), which has not hitherto been required.

*Theorem* 26. [$A1$, 2, 3, 4.] If $\mu a = \mathbb{0}$ (where $\mu$ is any positive integer), then $a = \mathbb{0}$. In other words, if any multiple of $a$ is the zero-element, then $a$ itself is the zero-element. (Proof on p. 39.)

*Corollary*. If $\lambda \neq \mu$, and $a \neq \mathbb{0}$, then $\lambda a \neq \mu a$. In other words, if $a$ is not the zero-element, then every multiple of $a$ is different from every other multiple of $a$; this justifies the name "law of non-circularity" proposed for postulate $A4$.

In view of this theorem, we notice that every system which satisfies postulates $A1$–$A4$, and contains more than a single element, must be infinite.

*Theorem* 27, *and Definition*. [$A1$, 2, 3, 4.] If $a$ is any element, and $\mu$ any positive integer, then there cannot be more than one element $x$ such that $\mu x = a$; if there is any such element, it is called the $\mu^{th}$ *submultiple of* $a$, and denoted by $\frac{a}{\mu}$, or $a/\mu$; that is,

$$\mu\left(\frac{a}{\mu}\right) = a.$$

In particular, $a/1 = a$.

*Corollary*. If $\lambda \neq \mu$, and $a \neq \mathbb{0}$, then $a/\lambda \neq a/\mu$.

*Theorem* 28, *and Definition*. [$A1$, 2, 3, 4.] If $a/\mu$ exists, then

$$\lambda\left(\frac{a}{\mu}\right) = \frac{\lambda a}{\mu},$$

where $\lambda$ and $\mu$ are any positive integers. Any element of this form is called a *rational fraction of* $a$, and may be denoted without ambiguity by $\frac{\lambda}{\mu}a$. In particular, $\frac{\lambda}{1}a = \lambda a$, and $\frac{1}{\mu}a = \frac{a}{\mu}$. (Proof on p. 39.)

*Corollary.* If $\lambda\mu_1 = \mu\lambda_1$, then $\frac{\lambda}{\mu}a = \frac{\lambda_1}{\mu_1}a$.

This theorem 28 suggests the use of the composite symbol $\frac{\lambda}{\mu}$ as an operator analogous to the operators already used; such a symbol $\frac{\lambda}{\mu}$, where $\lambda$ and $\mu$ are any positive integers, is called a *positive rational number*.

In order to make these symbols as useful as possible, we agree, in the first place, to set $\frac{\lambda}{1} = \lambda$, and to call $\frac{\lambda}{\mu} = \frac{\lambda_1}{\mu_1}$ wherever $\lambda\mu_1 = \mu\lambda_1$; with this convention, if $\xi$ and $\eta$ are any positive rational numbers, we shall have $\xi a = \eta a$ whenever $\xi = \eta$.

Further, we define the sum and product of two positive rational numbers by the formulæ

$$\frac{\lambda}{\mu} + \frac{\lambda_1}{\mu_1} = \frac{\lambda\mu_1 + \mu\lambda_1}{\mu\mu_1}, \qquad \frac{\lambda}{\mu} \times \frac{\lambda_1}{\mu_1} = \frac{\lambda\lambda_1}{\mu\mu_1},$$

these definitions reducing to the previous definitions for positive integers when $\mu = \mu_1 = 1$.

Finally, we agree to write $\frac{\lambda}{\mu} > \frac{\lambda_1}{\mu_1}$ whenever $\lambda\mu_1 > \mu\lambda_1$.

With these definitions of addition and multiplication, the system of positive rational numbers is, incidentally, *a system which satisfies all the postulates* $A1$–$A5$, $M1$–$M5$; it contains a unit-element (the number 1), but no zero-element; the remainder, $\xi - \eta$, exists in the system when and only when $\xi > \eta$; but division is always possible.

The usefulness of these definitions is apparent from the following theorems (compare theorems 22–23):

*Theorem* 29. [$A1$, 2, 3, 4.] If $a$ be any element all of whose submultiples exist, and if $\xi$, $\eta$ are any positive rational numbers, then

$$\xi a + \eta a = (\xi + \eta)a \quad \text{and} \quad \xi(\eta a) = (\xi\eta)a.$$

The first part of this theorem shows that the sum of any two rational fractions of $a$ is again a rational fraction of $a$, and that $\xi a + \eta a = \eta a + \xi a$; that is, the system of rational fractions of any element $a$ is a closed system with respect to addition, and obeys the commutative law ($A5$). Hence we may use the notion of subtraction within this system (see theorems 11–12), so that we have, on the basis of postulates $A1$, 2, 3, 4 alone:

*Theorem* 30. [$A1$, 2, 3, 4.] If $a$ is an element all of whose submultiples exist, and if $\xi$, $\eta$ are positive rational numbers such that $\xi > \eta$, then $\xi a - \eta a = (\xi - \eta)a$.

*The negative rational numbers.*

Concerning rational fractions of opposite elements we have:

*Theorem* 31. [$A1$, 2, 3, 4.] If $a$ is any element which has an opposite and all its submultiples, then

$$\frac{\lambda}{\mu}(-a) = -\left(\frac{\lambda}{\mu}a\right),$$

where $\frac{\lambda}{\mu}$ is any positive rational number. Hence, any element of this form may be denoted without ambiguity by $-\frac{\lambda}{\mu}a$.

This theorem suggests that we add the symbol $-\frac{\lambda}{\mu}$ to our list of operators; such a symbol $-\frac{\lambda}{\mu}$, where $\lambda$ and $\mu$ are any positive integers, is called a *negative rational number*. The negative rational numbers bear the same relation to the positive rational numbers that the negative integers bear to the positive integers. The positive and negative rational numbers, together with the zero-number, constitute the set of *all rational numbers*, and the sum and product of any two rational numbers are defined by precisely the same conventions as in the case of all integers (page 17.)

*The system of all rational numbers, with addition and multiplication defined in this way, is still another example of a system which satisfies all the postulates* $A1$–$A5$, $M1$–$M5$; this system contains a unit-element (the number 1), and a zero-element (the number 0); every element has an opposite, and every element except zero has a reciprocal, so that subtraction and division are always possible, except division by zero.

The usefulness of these definitions is shown by

*Theorem* 32. [$A1$, 2, 3, 4.] If $a$ is any element which has an opposite and all its submultiples, then the formulæ of theorem 22 hold true when $\lambda$ and $\mu$ are replaced by any rational numbers (positive, negative, or zero).

*Further theorems on the use of numerical coefficients.*

*Theorem* 33. [$A$1, 2; $M$ 1, 4.] If $\lambda$, $\mu$ are any positive integers, and $a$, $b$ any elements, then

$$(\lambda a)(\mu b) = (\lambda\mu)ab.$$

*Theorem* 34. [$A$1, 2, 3; $M$ 1, 4.] If $\xi$, $\eta$ are any integral numbers, and $a$, $b$ any elements which have opposites, then

$$(\xi a)(\eta b) = (\xi\eta)ab.$$

*Theorem* 35. [$A$1, 2, 3, 4; $M$ 1, 4.] If $\xi$, $\eta$ are any rational numbers, and $a$, $b$ any elements which have opposites and submultiples, then

$$(\xi a)(\eta b) = (\xi\eta)ab.$$

(Proofs on p. 39.)

To avoid further repetition, the following theorems are stated at once for the general case, in which $\xi$, $\eta$ and $\theta$ stand for any rational numbers, and $a$, $b$, $x$, $y$ for any elements which have opposites and submultiples:

*Theorem* 36. [$A$1, 2, 3, 4.] If $\theta x = \theta y$ and $\theta \neq 0$, then $x = y$; and if $\xi a = \eta a$ and $a \neq \mathbf{0}$, then $\xi = \eta$. (Proof on p. 40.)

*Theorem* 37. [$A$1, 2, 3, 4.] If $\xi a = \mathbf{0}$, then either $\xi = 0$ or $a = \mathbf{0}$. (By theorem 36.)

*Theorem* 38. [$A$1, 2, 3, 4, 5.] $\xi(a + b) = \xi a + \xi b$. (Proof on p. 40.)

*Theorem* 39. [$A$1, 2, 3, 4, 5.] $\xi(a - b) = \xi a - \xi b$. (Proof on p. 40.)

*Theorem* 40. [$A$1, 2, 3, 4; $M$1, 2, 3, 4, 5.] If $\eta \neq 0$ and $b \neq \mathbf{0}$, then

$$\frac{\xi a}{\eta b} = \left(\frac{\xi}{\eta}\right)\frac{a}{b}.$$

(Proof on p. 41.)

*Powers of an element.*

*Use of the integral numbers as exponents.*

*Theorem* 41, *and Definition.* [$M$1, 2.] If $a$ is any element of the system, then the elements

$$a, \quad a \times a, \quad a \times a \times a, \quad a \times a \times a \times a, \; \cdots$$

belong to the system and are called the *powers of a*.

The element $a$ is denoted by $a^1$;
the element $a^1 \times a$ is denoted by $a^2$;
the element $a^2 \times a$ is denoted by $a^3$;

and so on; in general,

the element $a^\nu \times a$ is denoted by $a^{\nu'}$,

where $\nu'$ is the positive integer next following $\nu$. In this way the element $a^\mu$, where $\mu$ is any positive integer, is defined, and is called the *$\mu^{th}$ power of a*.

The positive integers when used in this manner are called *exponents*; thus, in $a^\mu$, the positive integer $\mu$ is the exponent of the element $a$.

By the use of the definitions for the sum and product of two positive integers, we have:

*Theorem* 42. [$M$1, 2.] If $a$ is any element of the system, then

$$a^\lambda \times a^\mu = a^{\lambda+\mu} \quad \text{and} \quad (a^\lambda)^\mu = a^{\lambda\mu},$$

when $\lambda$, $\mu$ are any positive integral numbers (compare theorem 22).*

The first part of this theorem shows that the product of any two powers of $a$ is again a power of $a$, and that $a^\lambda \times a^\mu = a^\mu \times a^\lambda$; that is, *the system of powers of any element a is a closed system with respect to multiplication, and obeys the commutative law.* Hence we may use the notion of division within this system (theorems 17–18), so that we have, on the basis of postulates $M$1, 2, 3 alone:

*Theorem* 43. [$M$1, 2, 3.] If $\lambda > \mu$, then $a^\lambda/a^\mu = a^{\lambda-\mu}$. (Compare theorem 23).

Concerning powers of reciprocal elements, we have:

*Theorem* 44. [$M$1, 2, 3.] If $a$ is any element which has a reciprocal, then

$$\left(\frac{1}{a}\right)^\mu = \frac{1}{a^\mu}.$$

where $\mu$ is any positive integer.

These theorems suggest the use of the *negative integral numbers and the zero-number as exponents*, operating on any element which has a reciprocal; thus, if we agree to define

* The proofs of theorems 41–45 are similar to the proofs of theorems 21–25, and may well be left to the reader.

$$a^{-\mu} = \frac{1}{a^{\mu}} \quad \text{and} \quad a^0 = 1,$$

we shall have:

*Theorem* 45. [$M$1, 2, 3.] If $a$ is any element which has a reciprocal, then the formulæ of theorem 42 hold true when $\lambda$ and $\mu$ are any integral numbers (positive, negative, or zero).

*On the use of rational exponents.*

The analogy between these theorems 41–45 on powers and the theorems 21–25 on multiples suggests the possibility of carrying the parallel one step further and introducing also the use of *rational* numbers as exponents. The attempt to do this is complicated, however, by the fact that we have, in general, no law for multiplication corresponding to the law of non-circularity for addition (see theorem 26); that is, if $a$ and $\mu$ are given, there may well be more than one element $x$ such that $x^{\mu} = a$. If, therefore, we define $a^{1/\mu}$ to signify an element $x$ such that $x^{\mu} = a$, we must understand that we are introducing a symbol whose value is, in general, *not uniquely determined*. Such multiple-valued symbols can indeed be used, as is well known, to good advantage, and their properties can be made to conform, approximately, to the laws of theorem 42; but the study of them would carry us beyond the limits of the present paper.

*Further theorems on the use of numerical exponents.*

*Theorem* 46. [$M$ 1, 2, 3, 5.] If the requisite reciprocals and quotients exist, then

$$(ab)^{\mu} = a^{\mu} b^{\mu} \quad \text{and} \quad \left(\frac{a}{b}\right)^{\mu} = \frac{a^{\mu}}{b^{\mu}},$$

when $\mu$ is any integer (positive, negative, or zero).

Since the rational numbers form a system which satisfies the postulates $A$1–$A$5, $M$1–$M$5 with respect to their addition and multiplication, the definitions of $a^{\mu}$, $a^{-\mu}$, and $a^0$ will apply equally when the element $a$ is replaced by any rational number $\xi$ (provided $\xi \neq 0$ in $\xi^{-\mu}$). Using this notation we have:

*Theorem* 47. [$A$1, 2, 3, 4; $M$1, 2, 3, 4.] If the requisite reciprocals exist, then

$$(\xi a)^{\mu} = (\xi^{\mu}) a^{\mu},$$

when $\mu$ is any integer, and $\xi$ any rational number (provided $\xi \neq 0$ when $\mu$ is negative).

Concerning a power of a sum of two terms, we have the following important theorem, known as the binomial theorem for positive integral exponents:

*Theorem* 48. [$A$1, 2; $M$1, 2, 4, 5.] If $\mu$ is any positive integer, then

$$(a+b)^{\mu} = a^{\mu} + \frac{\mu}{1} a^{\mu-1} b + \frac{\mu(\mu-1)}{1 \cdot 2} a^{\mu-2} b^2 + \frac{\mu(\mu-2)(\mu-3)}{1 \cdot 2 \cdot 3} a^{\mu-3} b^3 + \cdots + b^{\mu}.$$

(Proof by induction.)

Concerning the subtraction of two powers, we have:

*Theorem* 49. [$A$1, 2, 3, 5; $M$1, 2, 4, 5.] If $a - b$ exists, then

$$a^{\mu+1} - b^{\mu+1} = (a-b)(a^{\mu} + a^{\mu-1} b + a^{\mu-2} b^2 + \cdots + ab^{\mu-1} + b^{\mu}),$$

where $\mu$ is any positive integer.

*Equations of the $\mu^{th}$ degree in x.*

A conditional equation of the form

$$c_0 x^{\mu} + c_1 x^{\mu-1} + c_2 x^{\mu-2} + \cdots + c_{\mu-1} x + c_{\mu} = \mathbf{0},$$

where $\mu$ is any given positive integer, and $c_0 \, (\neq \mathbf{0})$, $c_1$, $c_2$, $\cdots$, $c_{\mu}$ are any elements of the system, is called *an equation of the $\mu^{th}$ degree in x*: any element $x$ which satisfies the condition is called a *root* of the equation; the left-hand side of the equation is called a *polynomial of the $\mu^{th}$ degree in x*; and the given elements $c_0$, $c_1$, $\cdots$, $c_{\mu}$ are called the *coefficients* of the polynomial (or of the equation.)

*Lemma.* If $x = a$ is a root of an equation of the $\mu^{\text{th}}$ degree in $x$, then the equation can be written in the form

$$(x - a) \times (\text{a polynomial of next lower degree in } x) = \mathbf{0},$$

provided the system is one in which subtraction and division (except division by $\mathbf{0}$) are always possible.

*Theorem* 50. [$A$1, 2, 3, 4, 5; $M$1, 2, 3, 4, 5.] If the system is one in which every equation of the $\mu^{th}$ degree has at least one root, then every such equation can be written in the form

$$(x - a_1)(x - a_2)(x - a_3) \cdots (x - a_{\mu}) = \mathbf{0},$$

Each of the elements $a_1$, $a_2$, $\cdots$ $a_\mu$ will be a root of the equation, and the equation cannot have any other roots. (Proof by successive applications of the lemma.)

*Redundancy of the commutative law for addition.*

It remains to prove, as stated above, that the commutative law for addition (postulate $A5$) is redundant when the list of postulates is taken as a whole.

*Theorem.* The commutative law for addition,

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

is a consequence of postulates $A1$, 2, 3 ; $M1$, $3_1$ or $3_2$, 4.

This theorem was given first by H. Hankel in 1867 ; the proof is here modified so as not to require the existence of a unit-element.

Proof. Let $c$ be any element different from [illegible] (by postulate I). Then

$$(a+b)(c+c) = (a+b)c+(a+b)c = ac+bc+ac+bc, \qquad \text{by } M4_1 \text{ and } M4_2;$$

but also

$$(a+b)(c+c) = a(c+c)+b(c+c) = ac+ac+bc+bc, \qquad \text{by } M4_2 \text{ and } M4_1;$$

hence

$$bc+ac+bc = ac+bc+bc, \qquad \text{by } A3_1,$$

and therefore

$$bc+ac = ac+bc, \qquad \text{by } A3_2.$$

Hence

$$(b+a)c = (a+b)c, \qquad \text{by } M4_2,$$

and therefore

$$b+a = a+b, \qquad \text{by } M3_2.$$

In order to use $M3_1$ instead of $M3_2$ in the proof, we should have merely to start with $(c+c)(a+b)$ instead of $(a+b)(c+c)$.

## §4. SPECIAL LAWS OF ADDITION AND MULTIPLICATION. PARTICULAR TYPES OF ELEMENTARY ALGEBRA.

The postulates $A1$–$A5$, $M1$–$M5$ may be satisfied, as we have seen, by many different systems ; for example, the system of positive integers, with addition and multiplication defined as on page 15, or the system of all rational numbers, with addition and multiplication defined as on page 20, Two systems satisfying these general laws are said to be *isomorphic* with respect to addition and multiplication when the following conditions are satisfied:

1) the elements of the two systems can be brought into *one-to-one correspondence* (so that each element of one class is paired with one and only one element of the other class, and reciprocally each element of the second class is paired with one and only one element of the first class); and

2) this correspondence can be set up in such a way that whenever $a$ and $b$ in one class correspond to $a'$ and $b'$ in the other class, *then* $a + b$ *will correspond to* $a' + b'$, *and* $a \times b$ *will correspond to* $a' \times b'$.

Two systems satisfying the general laws of §1, and isomorphic with each other, are said to belong to the *same type of algebra;* two systems satisfying the same general laws, but not isomorphic with each other are said to belong to *different types of algebra.* The various systems of numbers employed as operators in §2 afford examples of several different types of algebra.

Two algebras of the same type are *formally identical* as far as addition and multiplication are concerned; that is, they cannot be distinguished by any properties expressible in terms of addition and multiplication alone.

The set of postulates $A1$–$A5$, $M1$–$M5$ is clearly not sufficient to determine any one type of algebra, since all these postulates can be satisfied by various systems, non-isomorphic with one another. In order to obtain, for each of the more important types of elementary algebra, a set of postulates which shall *completely determine* that type, we add certain further postulates, given in the present section. *Each of the resulting sets of postulates determines completely one type of algebra*, in the sense that any two systems which satisfy all the postulates of that set will be *isomorphic* with respect to addition and multiplication.

A set of postulates which is sufficient to determine a particular type of system in this manner has been called a *categorical* set of postulates.* This

* The earliest set of postulates having this character is probably the set of five postulates for the system of natural numbers with respect to succession, given by G. Peano in 1891. [*Rivista di Matematica*, vol. 1 (1891), p. 87; *Formulaire de Mathématiques*, vol. 2 (1898), p. 2.] Other sets of postulates of the same kind, for the systems of positive real, positive rational, and positive integral numbers with respect to addition, were given by the present writer in 1902. [*Trans. Amer. Math. Soc.*, vol. 3, pp. 264–284, especially theorems II, II′, III″, on pp. 277, 282, 283. See also *ibid.*, vol. 6 (1905), p. 41.] The name categorical was introduced in 1904 by O. Veblen, who has made important use of the notion in his sets of postulates for geometry. [*Trans. Amer. Math. Soc.*, vol. 5 (1904), p. 346.]

name has been criticised by Couturat as inappropriate;* but whether or not the name has been happily chosen, the notion itself is of fundamental importance. Any categorical set of postulates includes, by implication, all the properties of the type of system which it determines, as far as they concern the operations in question; thus, in case of a categorical set of postulates for a type of algebra every proposition which is expressible in terms of addition and multiplication alone must either be a consequence of the postulates of such a set, or else be in contradiction with them. This is not true of a non-categorical set of postulates, like the set $A1$–$A5$, $M1$–$M5$; for example, the proposition "there is an element $z$ in the system, such that $z + z = z$" is neither deducible from these postulates nor in contradiction with them; it is true in some systems which satisfy the postulates, and false in others.

*The object of the present section is, then, to give a sufficient, or categorical, set of postulates for each of the types of algebra here considered.* (Other types of algebra—like the algebra of all real numbers, or the algebra of all complex numbers—require for their characterisation properties which involve the notion of order, and are therefore not discussed in the present paper.)

The new postulates all concern the existence, in the system, of elements satisfying certain conditions, and are therefore designated by the letter $E$.

*The algebra of positive integers and the algebra of positive integers with zero.*

The first of the special laws which we add to the general laws of §1 is the following:

POSTULATE $E1$. *There is a unit-element in the system* (*see theorem* 5).

All the multiples of this unit-element will exist in the system, by postulates $A1$, 2, and may be called the *positive integral elements* of the system. By theorems 22 and 33, these positive integral elements form a closed system with respect to addition and multiplication (see postulates $A1$ and $M1$); hence, to obtain a sufficient, or categorical, set of postulates for this type of algebra, we have only to add the following postulate:

POSTULATE $F$. *There are no elements in the system besides those required by the other postulates.*

---

* L. Couturat, *Les principes des Mathématiques*, 1905, p. 169.

That is, the *algebra of positive integers* is completely determined by postulates

$$A1,\ 2;\ M1,\ 2,\ 3,\ 4;\ E1;\ F.$$

Every system which satisfies these eight conditions will be formally identical with the system of positive integers, as far as addition and multiplication are concerned. (The other postulates of §1 become redundant after $E1$ and $F$ are added.)

Further, if we add

POSTULATE $E2$. *There is a zero-element in the system* (*see theorem* 1), then the postulates

$$A1,\ 2,\ 3;\ M1,\ 2,\ 3,\ 4;\ E1,\ 2;\ F$$

completely determine the *algebra of positive integers with zero*. Every system which satisfies these ten conditions will be formally identical with the system of positive integers with zero, as far as addition and multiplication are concerned.

This postulate $F$ may be called, for lack of a better name, the law of non-superfluity.* The "other postulates" referred to mean, of course, in each case, the other postulates of the set considered in that case.

### *The algebra of all integers.*

Besides postulates $E1$ and $E2$ we may add also

POSTULATE $E3$. *The opposite of the unit-element exists in the system* (*see theorem* 8).

When this postulate is added, the system will contain $\mathbf{1}$, $\mathbf{0}$, and $-\mathbf{1}$, and all the multiples of $\mathbf{1}$ and $-\mathbf{1}$; these elements form a closed system with respect to addition and multiplication (by theorems 25 and 34), and may be called the *integral elements* of the system.

Hence the *algebra of all integers* is completely determined by postulates

$$A1,\ 2,\ 3;\ M1,\ 2,\ 3,\ 4;\ E1,\ 2,\ 3;\ F.$$

* This postulate is much less vague than Hilbert's "Axiom of Completeness" (Axiom der Vollständigkeit), which is apparently intended to serve a similar purpose. [*See Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 8 (1900), part 1, p. 184.] Hilbert does not use the notion of isomorphism, however, and his "Axioms of geometry," as a matter of fact, do not form a categorical set.

Every system which satisfies these eleven conditions will be isomorphic with the system of all integers, with respect to addition and multiplication.

*The algebra of positive rationals, and the algebra of positive rationals with zero.*

We now introduce another postulate,

POSTULATE $E4$. *All the submultiples of the unit-element exist in the system.*

By virtue of this postulate, all the rational fractions of the unit-element (theorem 28) will exist in the system, and may be called the *positive rational elements* of the system. Moreover, these elements form a closed system with respect to addition and multiplication, by theorems 29 and 35.

Hence, the *algebra of the positive rationals* is completely determined by postulates

$$A1, 2, 3, 4;\ M1, 2, 3, 4;\ E1, 4;\ F.$$

The isomorphism of any two systems which satisfy these eleven conditions is established by means of the fact that the sum and product of two elements of the form $\frac{\lambda}{\mu}1$ and $\frac{\lambda_1}{\mu_1}1$ are wholly determined by the numbers $\lambda$, $\mu$, $\lambda_1$, and $\mu_1$ (see theorems 29 and 35).

Similarly, the *algebra of positive rationals with zero* is completely determined by the postulates

$$A1, 2, 3, 4;\ M1, 2, 3, 4;\ E1, 2, 4;\ F.$$

Here, and below, postulate $M5$ becomes redundant when the later postulates are added.

*The algebra of all rationals.*

The *algebra of all rationals* (positive, negative, or zero) is completely determined by postulates

$$A1, 2, 3, 4;\ M1, 2, 3, 4;\ E1, 2, 3, 4;\ F.$$

Every system which satisfies these thirteen conditions will be formally identical with the system of all rational numbers, with respect to addition and multiplication. This type of algebra is the simplest type in which the four operations of addition, multiplication, subtraction, and division (except division by zero) are always possible.

It will be noticed that in all the types of algebra so far considered, the isomorphism between two systems of the same type can be set up in only one way, since the unit-elements of the two systems must be made to correspond.

*The algebras of complex quantities.*

We now consider postulates $E1, 2, 3$, with

Postulate $E5$. *There is a pair of imaginary units in the system (see theorem* 20).

An imaginary unit, $i$, defined by the equation $i^2 = -\mathbf{1}$, cannot be an integral or rational element of the system, because if it were, then $i^2$ could not be $-\mathbf{1}$. Hence, by $A1$, the addition of this postulate $E5$ introduces a new class of elements of the form $\xi\mathbf{1} + \eta i$, where $\xi$ and $\eta$ are integral or rational numbers. Elements of this form are called *complex elements* of the system, with integral or with rational coefficients. No further elements are introduced by multiplication, however, since

$$(\xi\mathbf{1} + \eta i)(\xi_1\mathbf{1} + \eta_1 i) = (\xi\xi_1 - \eta\eta_1)\mathbf{1} + (\xi\eta_1 + \eta\xi_1)i.$$

Hence a definite type of algebra, which may be called the *algebra of complex quantities with integral coefficients* is completely determined by postulates

$$A1, 2, 3;\ M1, 2, 3, 4;\ E1, 2, 3, 5;\ F.$$

In a similar way another type of algebra, called the *algebra of complex quantities with rational coefficients* is completely determined by postulates

$$A1, 2, 3, 4;\ M1, 2, 3, 4;\ E1, 2, 3, 4, 5;\ F.$$

It will be noticed that in the case of either of the complex algebras, the isomorphism between two systems of either type can be set up in two ways, on account of the ambiguity in the choice of the element $i$ (see theorem 20).

An example of a system which satisfies all the postulates for the algebra of complex quantities with integral [or rational] coefficients is the class of all ordered pairs of integral [or rational] numbers, $(\xi, \eta)$, with addition and multiplication defined as follows:

$$(\xi_1, \eta_1) + (\xi_2, \eta_2) = (\xi_1 + \xi_2, \eta_1 + \eta_2),$$

$$(\xi_1, \eta_1) \times (\xi_2, \eta_2) = (\xi_1\xi_2 - \eta_1\eta_2, \xi_1\eta_2 + \eta_1\xi_2).$$

Here $\mathbf{0} = (0, 0)$, $\mathbf{1} = (1, 0)$, $i = (0, 1)$ or $(0, -1)$, and $(\xi, \eta) = \xi\mathbf{1} + \eta i$. The system thus constructed is called the system of *ordinary complex numbers* with integral [or rational] coefficients; the construction of some example of this kind is necessary to establish the *consistency* of the last two sets of postulates.

*The algebra of all algebraic quantities.*

Any equation of the $\mu^{\text{th}}$ degree in $x$, in which the coefficients are integral elements of the system, may be written in the form

$$\lambda_0 x^\mu + \lambda_1 x^{\mu-1} + \lambda_2 x^{\mu-2} + \cdots + \lambda_{\mu-1} x + \lambda_\mu \cdot \mathbb{1} = \mathbb{0},$$

where $\lambda_0 (\neq 0)$, $\lambda_1, \cdots \lambda_\mu$ are integral numbers; such an equation is called an *algebraic equation with integral coefficients*, and any root of such an equation is called an *algebraic element* of the system.

It is easy to show that if $x$ and $y$ are algebraic elements, then $x + y$ and $xy$ are also algebraic elements; that is, the algebraic elements of a system form a closed system with respect to addition and multiplication.*

Further, if the coefficients in any equation of the form

$$c_0 x^\mu + c_1 x^{\mu-1} + c_2 x^{\mu-2} + \cdots + c_{\mu-1} x + c_\mu \cdot \mathbb{1} = \mathbb{0}$$

are algebraic elements, then all the roots of such an equation (in so far as they exist in the system) are also algebraic elements.*

Hence, in order to obtain a system in which every such equation has a root, we need to add merely the following postulate:

POSTULATE $E6$. *Every algebraic equation of the $\mu^{th}$ degree with integral coefficients has at least one root.*

Then the postulates

$$A1, 2, 3, 4;\ M1, 2, 3, 4, 5;\ E1, 2, 6;\ F$$

determine completely a type of algebra called the *algebra of all algebraic quantities.* All the other types of algebra which have been considered in this section are sub-algebras within this algebra of algebraic quantities.

In this algebra, the opposite of the unit-element, and all the submultiples of the unit-element, exist (since the equations $x + \mathbb{1} = \mathbb{0}$ and $\lambda x - \mathbb{1} = \mathbb{0}$ have roots in the system); moreover, there is a pair of imaginary units, namely,

---

* For the proofs of these theorems, which are due to R. Dedekind (1877), and involve merely an elementary knowledge of determinants, the reader is referred to P. Bachmann's *Zahlentheorie*, vol. 5 (*Allgemeine Arithmetik der Zahlenkörper*, 1905), pp. 3–6. Another method of proof, depending on elementary properties of symmetric functions, is given in Borel and Drach's *Théorie des nombres et l'algèbre supérieure*, 1895, p. 184.

the roots of the equation $x^2 + 1 = 0$. Hence *all* the postulates $E1-E6$ are satisfied.

This type of algebra is the simplest type in which the operations of addition, multiplication, subtraction, and division (except division by the zero-element) are always possible, and in which every equation of the $\mu^{th}$ degree in $x$ (the coefficients being any elements of the system) always has a root; it therefore forms a suitable stopping-place for the discussion in the present paper.

The problem of constructing an example of a system of this type is an interesting one, into which we cannot enter here;* the *consistency* of the postulates is usually established by the fact that the algebra of algebraic quantities is a sub-algebra within the algebra of vectors described in the introduction.

## §5. EXAMPLES OF SYSTEMS WHICH SATISFY SOME BUT NOT ALL OF THE GENERAL LAWS OF §1. PROOFS OF INDEPENDENCE.

In this section we establish the independence of the postulates $A1-A4$, $M1-M5$, by exhibiting, in the case of each of the postulates, a system which satisfies all the other postulates, but not the one for which it is numbered. No one of the postulates, therefore, is deducible from the remaining postulates; for, if it were, then any system which possessed all the other properties would possess this property also, which, as the examples show, is not the case.

The rules of combination in these pseudo-algebraic systems we denote by $\oplus$ and $\odot$, reserving the symbols $+$ and $\times$ for use between numbers, in the sense explained in §3. In describing each system, we must give: (1) the class of elements considered, (2) the rule of combination called $\oplus$, and (3) the rule of combination called $\odot$.

*List of the postulates of* §1 (*general laws*).

$A1$. $a \oplus b$ in the system.

$A2$. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

$A3$. (1) If $a \oplus x = a \oplus y$, then $x = y$.

(2) If $x \oplus a = y \oplus a$, then $x = y$.

$A4$. If $\mu x = \mu y$, then $x = y$.

[$A5$. $a \oplus b = b \oplus a$.]

*See É. Borel and J. Drach, *Théorie des nombres et l'algèbre supérieure*, 1895, p. 157. For an early statement of the problem, compare H. Hankel, loc. cit., 1867, §12.

*M*1. $a \odot b$ in the system.

*M*2. $(a \odot b) \odot c = a \odot (b \odot c)$.

*M*3. (1) If $a \odot x = a \odot y$ and $a \oplus a \neq a$, then $x = y$.

(2) If $x \odot a = y \odot a$ and $a \oplus a \neq a$, then $x = y$.

*M*4. (1) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

(2) $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$.

*M*5. $a \odot b = b \odot a$.

*Examples of pseudo-algebras.*

The examples which prove the independence of the several postulates are the following, all of which are constructed out of numerical classes with which the reader has already been made familiar in §3.

*All except* $A1$. The class of all rational numbers, with $\oplus$ and $\odot$ defined as follows: $a \oplus b = a + b$ whenever $a + b = 0$; otherwise, $a \oplus b$ not in the class. $a \odot b = ab$, where $ab$ denotes the ordinary product.

*All except* $A2$. The class of all rational numbers. $a \oplus b = 2(a + b)$. $a \odot b = ab$.

*All except* $A3_1$ *and* $A5$. The class of positive rational numbers. $a \oplus b = a$. $a \odot b = ab$.

*All except* $A3_2$ *and* $A5$. The class of positive rational numbers. $a \oplus b = b$. $a \odot b = ab$.

*All except* $A3_1$ *and* $A3_2$. The class of all rational numbers. $a \oplus a = a$ but if $a \neq b$, then $a \oplus b = 0$. $a \odot b = ab$.

*All except* $A4$. A class consisting of nine elements, 0, 1, 2, $\cdots$, 8, with $\oplus$ and $\odot$ defined by means of the following tables:

| $\oplus$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | | | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | | | | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | | | | | 8 | 6 | 1 | 2 | 0 |
| 5 | | | | | | 7 | 2 | 0 | 1 |
| 6 | | | | | | | 3 | 4 | 5 |
| 7 | | | | | | | | 5 | 3 |
| 8 | | | | | | | | | 4 |

| $\odot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | | | 1 | 6 | 8 | 7 | 3 | 5 | 4 |
| 3 | | | | 4 | 7 | 1 | 8 | 2 | 5 |
| 4 | | | | | 2 | 3 | 5 | 6 | 1 |
| 5 | | | | | | 8 | 2 | 4 | 6 |
| 6 | | | | | | | 4 | 1 | 7 |
| 7 | | | | | | | | 8 | 3 |
| 8 | | | | | | | | | 2 |

For example, $3 \oplus 7 = 7 \oplus 3 = 1$; $3 \odot 7 = 7 \odot 3 = 2$

This system (which is a Galois Field of order $3^2$) satisfies also all the existence postulates $E1$, 2, 3, 4, 5. Thus,

$$\mathbf{0} = 0, \quad \mathbf{1} = 1, \quad -\mathbf{1} = 2, \quad i = 4 \text{ or } 8.$$

*All except* $M1$. The class of all rational numbers. $a \oplus b = a + b$. $a \odot b = ab$ when $ab = 1$; otherwise $a \odot b$ not in the class.

*All except* $M2$. The class of complex numbers of the form $ae_1 + be_2$, where $a$ and $b$ are any rational numbers, and the "units," $e_1$ and $e_2$, are connected by the following "multiplication table:"*

$$e_1 e_1 = e_1; \; e_1 e_2 = e_2 e_1 = -e_2; \; e_2 e_2 = -e_1.$$

| | $e_1$ | $e_2$ |
|---|---|---|
| $e_1$ | $e_1$ | $-e_2$ |
| $e_2$ | $-e_2$ | $-e_1$ |

*All except* $M3_1$ *and* $M5$. The class of all complex numbers of the form $ae_1 + be_2$ where $a$ and $b$ are positive rational numbers or zero, and *

$$e_1 e_1 = e_1; \; e_1 e_2 = e_1; \; e_2 e_1 = e_2; \; e_2 e_2 = e_2.$$

| | $e_1$ | $e_2$ |
|---|---|---|
| $e_1$ | $e_1$ | $e_1$ |
| $e_2$ | $e_2$ | $e_2$ |

*All except* $M3_2$ *and* $M5$. The same class as the preceding, with

$$e_1 e_1 = e_1; \; e_1 e_2 = e_2; \; e_2 e_1 = e_1; \; e_2 e_2 = e_2.$$

| | $e_1$ | $e_2$ |
|---|---|---|
| $e_1$ | $e_1$ | $e_2$ |
| $e_2$ | $e_1$ | $e_2$ |

*All except* $M3_1$ *and* $M3_2$. The class of all complex numbers of the form $ae_1 + be_2$, where $a$ and $b$ are any rational numbers and *

$$e_1 e_1 = e_1; \; e_1 e_2 = e_2 e_1 = e_2; \; e_2 e_2 = e_2.$$

| | $e_1$ | $e_2$ |
|---|---|---|
| $e_1$ | $e_1$ | $e_2$ |
| $e_2$ | $e_2$ | $e_2$ |

* It is understood that the "sum" of two complex numbers $ae_1 + be_2$ and $a'e_1 + b'e_2$ is $(a + a')e_1 + (b + b')e_2$ their "product" is $aa'e_1e_1 + ab'e_1e_2 + ba'e_2e_1 + bb'e_2e_2$, where the expressions $e_1e_1$, $e_1e_2$, $e_2e_1$ and $e_2e_2$ are to be simplified, in any given case, according to the "multiplication-table" adopted in that case. In any such system of complex numbers, both the distributive laws ($M4$) will clearly be satisfied; moreover, the associative and commutative laws for multiplication ($M2$, $M5$) will hold throughout the system whenever they hold for the "multiplication-table" of the $e$'s.

*All except* $M4_1$ *and* $M5$. The class of all couples of the form $(a, b)$, where $a$ and $b$ are positive rational numbers, with $\oplus$ and $\odot$ defined as follows:

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 + b_2);$$

$$(a_1, b_1) \odot (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1).$$

*All except* $M4_2$ *and* $M5$. The same class as the preceding, with $\oplus$ defined in the same way, and $\odot$ defined as follows:

$$(a_1, b_1) \odot (a_2, b_2) = (a_1 a_2, b_1 a_2 + b_2).$$

*All except* $M4_1$ *and* $M4_2$. The class of all rational numbers.

$$a \oplus b = a + b. \qquad a \odot b = a + b + 1.$$

*All except* $M5$. The class of all complex numbers of the form $ae_1 + be_2 + ce_3 + de_4$, with the following "multiplication table" for the "units" $e_1$, $e_2$, $e_3$, and $e_4$:

| | $e_1$ | $e_2$ | $e_3$ | $e_4$ |
|---|---|---|---|---|
| $e_1$ | $e_1$ | $e_2$ | $e_3$ | $e_4$ |
| $e_2$ | $e_2$ | $-e_1$ | $e_4$ | $-e_3$ |
| $e_3$ | $e_3$ | $-e_4$ | $-e_1$ | $e_2$ |
| $e_4$ | $e_4$ | $e_3$ | $-e_2$ | $-e_1$ |

This is the system of quaternions with rational coefficients.

Thus the independence of all the postulates of §1 (except $A5$) is established. The redundancy of postulate $A5$ is proved on page 25.

## §6. PROOFS OF THEOREMS IN §§2–4.*

The proofs of a number of theorems in §§2–4, were postponed to the present section, to avoid interruption in reading.

*Page* 9.

Proof of theorem 1. Suppose $z + z = z$ and $z' + z' = z'$. Then $z + z + z' = z + z' + z'$, by $A1, 2$; hence $z + z' = z' + z'$, by $A3_1$, and therefore $z = z'$, by $A3_2$.

* I am indebted to Mr. P. W. Bridgman and Mr. G. C. Evans for assistance in verifying the demonstrations in this and the preceding section.

Proof of theorem 2. If $\mathbf{0} + \mathbf{0} = \mathbf{0}$, then $a + \mathbf{0} + \mathbf{0} = a + \mathbf{0}$ and $\mathbf{0} + \mathbf{0} + a = \mathbf{0} + a$, by $A1$, 2; hence $a + \mathbf{0} = a$, by $A3_2$, and $\mathbf{0} + a = a$, by $A3_1$.

Conversely, if $a + x = a$ or $x + a = a$, then $a + x + x = a + x$ or $x + x + a = x + a$, by $A1$, 2; hence, $x + x = x$, by $A3$.

Proof of theorem 3. By $M1$, $4_1$, $a \times \mathbf{0} = a \times (\mathbf{0} + \mathbf{0}) = (a \times \mathbf{0}) + (a \times \mathbf{0})$, whence $a \times \mathbf{0} = \mathbf{0}$, by theorem 1; again, by $M1$, $4_2$, $\mathbf{0} \times a = (\mathbf{0} + \mathbf{0}) \times a = (\mathbf{0} \times a) + (\mathbf{0} \times a)$, whence $\mathbf{0} \times a = \mathbf{0}$, by theorem 1.

Proof of theorem 4. If $a \times b = \mathbf{0}$, then $a \times b = a \times \mathbf{0}$, by theorem 3; hence, if $a \neq \mathbf{0}$, then $b = \mathbf{0}$, by $M3_1$. Or thus: if $a \times b = \mathbf{0}$, then $a \times b = \mathbf{0} \times b$, by theorem 3; hence, if $b \neq \mathbf{0}$, then $a = \mathbf{0}$, by $M3_2$.

Proof of theorem 5. Suppose $uu = u$ and $u'u' = u'$, with $u \neq \mathbf{0}$ and $u' \neq \mathbf{0}$. Then $uuu' = uu'u'$, by $M1$, 2; hence $uu' = u'u'$, by $M3_1$, and therefore $u = u'$, by $M3_2$.

Proof of theorem 6. If $\mathbf{1} \times \mathbf{1} = \mathbf{1}$, then $a \times \mathbf{1} \times \mathbf{1} = a \times \mathbf{1}$ and $\mathbf{1} \times \mathbf{1} \times a = \mathbf{1} \times a$, by $M1$, 2; hence $a \times \mathbf{1} = a$, by $M3_2$, and $\mathbf{1} \times a = a$, by $M3_1$, since $\mathbf{1} \neq \mathbf{0}$.

*Pages* 11–12.

Proof of theorem 7. If $ax = a$ or $xa = a$, then $axx = ax$ or $xxa = xa$, by $M1$, 2; hence $xx = x$, by $M3$, so that $x = \mathbf{0}$ or $\mathbf{1}$. But $x \neq \mathbf{0}$, since if $x = \mathbf{0}$, then $a = \mathbf{0}$, by theorem 3; therefore $x = \mathbf{1}$.

Proof of lemma to theorem 8. If $a + b = \mathbf{0}$, then $b + a + b = b + \mathbf{0} = b = \mathbf{0} + b$, by $A1$, 2, and theorem 2; hence $b + a = \mathbf{0}$, by $A3_2$.—Theorem 8 follows from this lemma by $A3$.

Proof of theorem 9. By $M4_1$ and theorem 3, $a(-b) + ab = a(-b + b) = a \times \mathbf{0} = \mathbf{0}$, so that $a(-b)$ and $ab$ are opposite elements; again, by $M4_2$ and theorem 3, $(-a)b + ab = (-a + a)b = \mathbf{0} \times b = \mathbf{0}$, so that $(-a)b$ and $ab$ are opposite elements. Hence, further, $(-a) \times (-b) = -[(-a) \times b] = -[-(ab)] = ab$, by the corollary to theorem 8.

Proof of theorem 10. By $A2$, 5, $(-a) + (-b) + (a + b) = (-a) + a + (-b) + b = \mathbf{0} + \mathbf{0} = \mathbf{0}$, so that $(-a) + (-b)$ and $(a + b)$ are opposite elements.

Proof of theorem 12. First, $[a + (b - c)] + c = a + [(b - c) + c] = a + b = [(a + b) - c] + c$; hence $a + (b - c) = (a + b) - c$, by $A3_2$. The second equation is proved in a similar way by adding $b + c$ to both sides, and the third equation by adding $b$.

Proof of theorem 13. By $M4_1$, $ac + a(b - c) = a[c + (b - c)] = ab = ac + (ab - ac)$; hence $a(b - c) = ab - ac$, by $M3_1$. Similarly for the second part of the theorem.

Proof of lemma to theorem 14. If $a \neq 0$ and $ab = 1$, then $aba = 1 \times a = a \times 1$, whence $ba = 1$, by $M3_1$. If $b \neq 0$ and $ab = 1$, then $bab = b \times 1 = 1 \times b$, whence $ba = 1$, by $M3_2$. If both $a$ and $b$ are $0$, then in any case $ab = ba$.

Proof of theorem 14. If $ay = 1$ and $ay' = 1$, then, by the lemma, $y' = 1 \times y' = ya \times y' = y \times ay' = y \times 1 = y$.

*Pages* 13–14.

Proof of theorem 15. $a\left(\frac{1}{a}\right) = 1 = (-a)\left(\frac{1}{-a}\right) = a\left[-\left(\frac{1}{-a}\right)\right]$, by theorem 9; hence $\frac{1}{a} = -\left(\frac{1}{-a}\right)$, by $M3_1$.

Proof of theorem 16. $\frac{1}{a} \times \frac{1}{b} \times ab = \frac{1}{a} \times a \times \frac{1}{b} \times b = 1 \times 1 = 1$, so that $\frac{1}{a} \times \frac{1}{b}$ and $ab$ are reciprocal elements.

Proof of theorem 18. Multiply the five equations by $bc$, $b$, $bc$, $bd$, $c/d$, respectively; then use $M3$.

Proof of theorem 19. Multiply the equations by $bb'$, and reduce by $M4$; then use $M3$, since $b$, and $b'$ must be different from $0$.

Proof of theorem 20. First, in any system containing the elements $1$ and $-1$, every element will have an opposite, since, if $x$ is any element, then $(-1) \times x$ will exist in the system, by $M1$, and $(-1) \times x = -x$, by theorems 9 and 6; moreover, if $xx = -1$, then $(-x) \times (-x) = -1$, by theorem 9. Secondly suppose $xx = -1$ and $yy = -1$; then $xx - yy = 0$, whence $(x + y)(x - y) = 0$, by $M4$, 5, and therefore either $x + y = 0$ or $x - y = 0$, by theorem 4; that is, $x = -y$ or $x = y$.

*Page* 16.

*Proof of the laws of addition and multiplication for the positive integers.*

1) $\underline{(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)}$.

This is true when $\gamma = 1$, by definition. Also, if it is true when $\gamma = \nu$, then it will be true when $\gamma = \nu'$, where $\nu'$ is the successor of $\nu$; for,

$$(\alpha+\beta)+\nu' = [(\alpha+\beta)+\nu]+1 = [\alpha+(\beta+\nu)]+1 = \alpha+[(\beta+\nu)+1] = \alpha+(\beta+\nu').$$

Hence, putting successively $\nu = 1, 2, 3, \cdots$, we see that the formula is true when $\gamma$ is any positive integer. This method of proof is called induction from $\gamma = \nu$ to $\gamma = \nu'$, when $\nu'$ is the successor of $\nu$; or briefly, induction on $\gamma$.

2) Lemma. $a+1 = 1+a$. By induction on $a$:

$$\nu'+1 = (\nu+1)+1 = (1+\nu)+1 = 1+(\nu+1) = 1+\nu'.$$

3) $\underline{a+\beta = \beta+a.}$ For, by induction on $\beta$:

$$a+\nu' = (a+\nu)+1 = (\nu+a)+1 = \nu+(a+1) = \nu+(1+a) = (\nu+1)+a = \nu'+a.$$

4) $\underline{a(\beta+\gamma) = a\beta+a\gamma.}$ For, by induction on $a$:

$$\nu'(\beta+\gamma) = \nu(\beta+\gamma)+(\beta+\gamma) = \nu\beta+\nu\gamma+\beta+\gamma = \nu\beta+\beta+\nu\gamma+\gamma = \nu'\beta+\nu'\gamma.$$

5) $\underline{(\beta+\gamma)a = \beta a+\gamma a.}$ For, by induction on $\gamma$:

$$(\beta+\nu')a = [(\beta+\nu)+1]a = (\beta+\nu)a+a = \beta a+\nu a+a = \beta a+\nu' a.$$

6) $\underline{(a\beta)\gamma = a(\beta\gamma).}$ For, by induction on $a$:

$$(\nu'\beta)\gamma = (\nu\beta+\beta)\gamma = (\nu\beta)\gamma+\beta\gamma = \nu(\beta\gamma)+\beta\gamma = \nu'(\beta\gamma).$$

7) Lemma. $1a = a\cdot 1$ For, by induction on $a$:

$$1\nu' = 1(\nu+1) = 1\nu+1\cdot 1 = \nu\cdot 1+1 = \nu'\cdot 1.$$

8) $\underline{a\beta = \beta a.}$ For, by induction on $a$:

$$\nu'\beta = \nu\beta+\beta = \beta\cdot\nu+\beta\cdot 1 = \beta(\nu+1) = \beta\nu'.$$

9) Lemma. If $a \neq \beta$, then either $a = \beta + \xi$ or $\beta = a + \xi$, where $\xi$ is some positive integer. For, if $a > \beta$, then $a$ will be found in the sequence $\beta + 1, \beta + 2, \beta + 3, \cdots$; and if $\beta > a$, then $\beta$ will be found in the sequence $a + 1, a + 2, a + 3, \cdots$.

10) Lemma. $a + \beta \neq a$. For, $a + \beta$ will be found in the sequence $a + 1, a + 2, a + 3, \cdots$, and each of these numbers is different from $a$.

11) $\underline{\text{If } a + \xi = a + \eta, \text{ then } \xi = \eta.}$ For, if $\xi \neq \eta$, then we should have $\xi = \eta + \zeta$, say, whence $a + (\eta + \zeta) = a + \eta$, or $(a + \eta) + \zeta = (a + \eta)$, which is impossible.

12) $\underline{\text{If } a\xi = a\eta, \text{ then } \xi = \eta.}$ For, if $\xi \neq \eta$, then we should have $\xi = \eta + \zeta$, say, whence $a(\eta + \zeta) = a\eta$, or $a\eta + a\zeta = a\eta$, which is impossible.

Proof of theorem 22. By definition, $\lambda a + a = (\lambda + 1)a$; hence $\lambda a + \mu a = (\lambda + \mu)a$, by induction on $\mu$, since $\lambda a + \nu' a = \lambda a + (\nu a + a) = (\lambda a + \nu a) + a = (\lambda + \nu)a + a = [(\lambda + \nu) + 1]\, a = (\lambda + \nu')a$.

Again, $1(\mu a) = (1\mu)a$; hence $\lambda(\mu a) = (\lambda\mu)a$, by induction on $\lambda$, since

$$\nu'(\mu a) = \nu(\mu a) + \mu a = (\nu\mu)a + \mu a = (\nu\mu + \mu)a = (\nu'\mu)a.$$

*Pages* 17–19.

Proof of theorem 23.

$$(\lambda a - \mu a) + \mu a = \lambda a = [(\lambda - \mu) + \mu]a = (\lambda - \mu)\, a + \mu a\text{; hence}$$

$$\lambda a - \mu a = (\lambda - \mu)a, \text{ by } A3_2.$$

Proof of theorem 24. By definition, $1(-a) + 1a = \mathbb{O}$; hence $\mu(-a) + \mu a = \mathbb{O}$, by induction on $\mu$, since

$$\nu'(-a) + \nu' a = (-a) + [\nu(-a) + \nu a] + a = (-a) + \mathbb{O} + a = \mathbb{O};$$

therefore $\mu(-a)$ and $\mu a$ are opposite elements.

Proof of theorem 26. If there is a zero-element, $\mathbb{O}$, then every multiple of $\mathbb{O}$ is $\mathbb{O}$; that is, when $\mu$ is any positive integer, $\mu\mathbb{O} = \mathbb{O}$, whence the theorem, by $A4$.

Proof of the corollary. Suppose $\lambda a = \mu a$, and $\lambda > \mu$; then $\lambda = \mu + \xi$, so that $(\mu + \xi)a = \mu a$, whence $\mu a + \xi a = \mu a$; therefore $\xi a = \mathbb{O}$, by theorem 2, and hence $a = \mathbb{O}$, by theorem 26.

Proof of theorem 28. $\mu\left[\lambda\left(\dfrac{a}{\mu}\right)\right] = \lambda\left[\mu\left(\dfrac{a}{\mu}\right)\right] = \lambda a = \mu\left[\dfrac{\lambda a}{\mu}\right]$; hence $\lambda\left(\dfrac{a}{\mu}\right) = \dfrac{\lambda a}{\mu}$, by $A4$.

Proof of theorem 29. Put $\xi = \dfrac{\lambda}{\mu}$, $\eta = \dfrac{\lambda_1}{\mu_1}$; take the $(\mu\mu_1)^{\text{th}}$ multiple of both sides of the equation, and use theorem 27.

*Page* 21.

Proof of theorems 33–35. Let $\lambda$, $\mu$ be any positive integers. We prove first that $a(\mu b) = \mu(ab)$; thus, $a(1\cdot b) = 1\cdot(ab)$, and by induction,

$$a(\nu' b) = a(\nu b + b) = a(\nu b) + ab = \nu(ab) + ab = \nu'(ab),$$

where $\nu'$ is the successor of $\nu$. Then it follows that $(\lambda a)(\mu b) = (\lambda\mu)(ab)$; for, $(1\cdot a)(\mu b) = (1\cdot\mu)(ab)$; and by induction,

$$\begin{aligned}(\nu' a)(\mu b) = (\nu a + a)(\mu b) = (\nu a)(\mu b) + a(\mu b) &= (\nu\mu)(ab) + \mu(ab)\\ &= (\nu\mu + \mu)\, ab = (\nu'\mu)(ab).\end{aligned}$$

To prove that $\left(\frac{\lambda}{\mu}a\right)\left(\frac{\lambda_1}{\mu_1}b\right)\left(\frac{\lambda}{\mu}=\frac{\lambda_1}{\mu_1}\right)(ab)$, take the $(\mu\mu_1)^{\text{th}}$ multiple of both sides. The proof for negative coefficients follows from theorem 24 and theorem 9.

Proof of theorem 36. Let $\lambda$, $\mu$ be any positive integers.

1) If $\lambda x = \lambda y$, then $x = y$, by $A4$.

If $\frac{\lambda}{\mu}x = \frac{\lambda}{\mu}y$, then $\lambda x = \left(\mu\frac{\lambda}{\mu}\right)x = \mu\left(\frac{\lambda}{\mu}x\right) = \mu\left(\frac{\lambda}{\mu}y\right) = \left(\mu\frac{\lambda}{\mu}\right)y = \lambda y$, and therefore $x = y$ as above.

If $\left(-\frac{\lambda}{\mu}\right)x = \left(-\frac{\lambda}{\mu}\right)y$, then $-\left(\frac{\lambda}{\mu}x\right) = -\left(\frac{\lambda}{\mu}y\right)$, whence $\frac{\lambda}{\mu}x = \frac{\lambda}{\mu}y$, and therefore $x = y$ as above.

2) If $\lambda a = \mu a$, then $\lambda = \mu$, by theorem 26.

If $\frac{\lambda}{\mu}a = \frac{\lambda_1}{\mu_1}a$, then $\mu_1\lambda a = \mu_1\mu\left(\frac{\lambda}{\mu}a\right) = \mu\mu_1\left(\frac{\lambda_1}{\mu_1}a\right) = \mu\lambda_1 a$, and therefore $\mu_1\lambda = \mu\lambda_1$ as above; that is, $\frac{\lambda}{\mu} = \frac{\lambda_1}{\mu_1}$.

If $\left(-\frac{\lambda}{\mu}\right)a = \left(-\frac{\lambda_1}{\mu_1}\right)a$, then $\frac{\lambda}{\mu}a = \frac{\lambda_1}{\mu_1}a$, and therefore $\frac{\lambda}{\mu} = \frac{\lambda_1}{\mu_1}$ as above; hence $-\frac{\lambda}{\mu} = -\frac{\lambda_1}{\mu_1}$.

The proof of theorem 37 follows at once from theorem 36.

Proof of theorem 38. Let $\lambda$, $\mu$ be any positive integers.

Clearly, $1(a + b) = 1a + 1b$; hence $\lambda(a + b) = \lambda a + \lambda b$ by induction, since $\nu'(a + b) = \nu(a + b) + (a + b) = \nu a + \nu b + a + b = \nu a + a + \nu b + b = \nu' a + \nu' b$, where $\nu'$ is the successor of $\nu$.

Further, $\frac{\lambda}{\mu}(a + b) = \frac{\lambda}{\mu}a + \frac{\lambda}{\mu}b$, since the $\mu^{\text{th}}$ multiple of each side is $\lambda(a + b)$ or $\lambda a + \lambda b$.

Finally, $\left(-\frac{\lambda}{\mu}\right)(a + b) = \left(-\frac{\lambda}{\mu}\right)a + \left(-\frac{\lambda}{\mu}\right)b$, by the aid of theorem 10.

Proof of theorem 39. $\xi(a - b) + \xi b = \xi(a - b + b) = \xi a = (\xi a - \xi b) + \xi b$; hence $\xi(a - b) = \xi a - \xi b$, by $A3_2$.

Proof of theorem 40.

$$(\eta b)\left(\frac{\xi a}{\eta b}\right) = \xi a = \left(\eta\frac{\xi}{\eta}\right)\left(b\frac{a}{b}\right) = (\eta b)\left(\frac{\xi}{\eta}\cdot\frac{a}{b}\right);\text{ hence } \frac{\xi a}{\eta b} = \frac{\xi}{\eta}\cdot\frac{a}{b}, \text{ by } M3_1,$$

since $\eta b \neq \mathbb{0}$.

The proofs of theorems 41–45 are similar to the proofs of theorems 21–25, and need not be given here in detail.

*Page* 24.

Proof of lemma to theorem 50. If $x = a$ is a root of the equation

$$c_0x^\mu + c_1x^{\mu-1} + c_2x^{\mu-2} + \cdots + c_{\mu-1}x + c_\mu\cdot \mathbb{1} = \mathbb{0},$$

then

$$c_0a^\mu + c_1a^{\mu-1} + c_2a^{\mu-2} + \cdots + c_{\mu-1}a + c_\mu\cdot \mathbb{1} = \mathbb{0};$$

hence, by subtraction, the given equation may be written in the form

$$c_0(x^\mu - a^\mu) + c_1(x^{\mu-1} - a^{\mu-1}) + c_2(x^{\mu-2} - a^{\mu-2}) + \cdots + c_{\mu-1}(x - a) = \mathbb{0},$$

each term of which, by theorem 49, is divisible by $x - a$.

## APPENDIX 1.

The following postulate holds in all the types of algebra which we have considered in this paper:

POSTULATE $E7$. *If $x \neq y$, then there is either an element $v$ such that $x = y + v$, or an element $w$ such that $y = x + w$.*

In the first case, $v = a - b$; in the second, $w = b - a$ (compare theorem 11).

If we add this postulate $E\,7$ to the list of general laws in §1, then postulates $A4$ and $M3$ may be replaced by the following simpler postulates, $A\,4'$ and $M\,3'$:

POSTULATE $A\,4'$. *If $a \neq \mathbb{0}$, then $\mu a \neq \mathbb{0}$, where $\mu a$ is any multiple of $a$ (see theorem 21).*

This is a modified form of the law of non-circularity.

POSTULATE $M3'$. *If $a \neq \mathbb{0}$ and $b \neq \mathbb{0}$, then $ab \neq \mathbb{0}$.*

This is the law of the zero-product (compare theorem 4).

The deduction of postulate $A4$ from $A1$, 2, 3, 5 and $E7$ is as follows:

We are to prove that if $\mu x = \mu y$, then $x = y$. Suppose $x \neq y$, and that

$x = y + v$, by $E7$. Then $\mu x = \mu y + \mu v$, by theorem 38 for positive integers; whence $\mu v = \mathbb{0}$, by hypothesis and theorem 2, so that $v = \mathbb{0}$, by $A4'$. Therefore $x = y$, by theorem 2. — Similarly if $y = x + w$.

The deduction of postulate $M3_1$ from $A1$, 2, 3, $M1$, $3'$, $4_1$, and $E7$ is as follows:

We are to prove that if $ax = ay$ and $a \neq \mathbb{0}$, then $x = y$. Suppose $x \neq y$, and that $x = y + v$, by $E7$. Then $ax = ay + av$, by $M4_1$. whence $av = \mathbb{0}$, by hypothesis and theorem 2, so that $v = \mathbb{0}$, by $M3'$ (since $a \neq \mathbb{0}$). Therefore $x = y$, by theorem 2. — Similarly if $y = x + w$.

The deduction of $M3_2$ follows in like manner from $A1$, 2, 3, $M1$, $3'$, $4_2$, and $E7$.

*Examples.*

An example of a system which satisfies $A1 - A5$ and $M1 - M5$, but not $E7$, is the system of all positive rational numbers > 2, with addition and multiplication defined in the usual way.

An example of a system which satisfies $A$ 1, 2, 3, 4, 5 and $M1$, 2, $3'$, 4, 5, but not $M3$, is the system of all complex numbers of the form $ae' + be''$, or $(a, b)$, where $a$ is zero or any positive rational number, and $b$ is zero or a positive rational > 1, with the following "multiplication table" for the units:

$$e'e' = e'; \; e'e'' = e''e' = e''; \; e''e'' = e''. \qquad \begin{array}{c|cc} & e' & e'' \\ \hline e' & e' & e'' \\ e'' & e'' & e'' \end{array}$$

This system contains a zero-element, $\mathbb{0} = (0, 0)$, and a unit-element, $\mathbb{1} = (1, 0)$. To show that it does not satisfy $M3$, note that $(0, 2) \odot (4, 5) = (0, 18)$ while also $(0, 2) \odot (3, 6) = (0, 18)$. Moreover, as was to be expected, it does not satisfy $E7$; for example, if $a = (2, 7)$ and $b = (3, 6)$, then neither $a - b$ nor $b - a$ exists in the system.

The existence of this system shows that the set of postulates in §1 is "weakened"* when $M3$ is replaced by $M3'$, since $M3$ cannot be deduced from $M3'$ without the aid of an additional postulate, like $E7$.

An example of a system satisfying $A1$, 2, 3, $4'$, 5 and $M$ 1, 2, 3, 4, 5, but not $A4$, would also be interesting; I have not, however, been able to find an

* The notion "weaker" seems to me to be applicable rather to a set of postulates than to a single postulate.

example of this kind. It therefore remains an open question whether the set of postulates in §1 is really "weakened" when $A4$ is replaced by $A4'$.

### APPENDIX 2.

It may be interesting to note here, somewhat more in detail than in the text, what can be done with postulates $A1$, 2, 3; $M1$, 2, 3 without the aid of the distributive laws for multiplication.

*Lemma* 1. If $a \times \mathbf{0} = \mathbf{0}$ or $\mathbf{0} \times a = \mathbf{0}$, then $a \times \mathbf{0} = \mathbf{0} \times a$.

For, if $a\mathbf{0} = \mathbf{0}$, then $\mathbf{0}a\mathbf{0}a = \mathbf{0}\mathbf{0}a$, whence $\mathbf{0}a = \mathbf{0}$, by $M3_2$; and again, if $\mathbf{0}a = \mathbf{0}$, then $a\mathbf{0}a\mathbf{0} = a\mathbf{0}\mathbf{0}$, whence $a\mathbf{0} = \mathbf{0}$, by $M3_1$.

*Lemma* 2. If $a \times \mathbf{0} = a$ or $\mathbf{0} \times a = a$, then $a \times \mathbf{0} = \mathbf{0} \times a$.

For, if $a\mathbf{0} = a$, then $a\mathbf{0}a = aa$, whence $\mathbf{0}a = a$, by $M3_3$; and again, if $\mathbf{0}a = a$, then $a\mathbf{0}a = aa$, whence $a\mathbf{0} = a$, by $M3_2$.

*Theorem A.* In any system which satisfies $A1$, 2, 3; $M1$, 2, 3, if we assume in regard to the multiplicative property of $\mathbf{0}$, merely that

$$\mathbf{0} \times \mathbf{0} = \mathbf{0},$$

then either $a \times \mathbf{0} = \mathbf{0} \times a = \mathbf{0}$ for every element $a$, or else $a \times \mathbf{0} = \mathbf{0} \times a = a$ for every element $a$.

For, since $\mathbf{0}\mathbf{0} = \mathbf{0}$, we have $x\mathbf{0}\mathbf{0}a = x\mathbf{0}a$; therefore, by $M3_2$, if $x\mathbf{0} \neq \mathbf{0}$ for any single element $x$, then $\mathbf{0}a = a$ for every element $a$. Hence the theorem, by lemmas 1 and 2.

*Theorem B.* In any system which satisfies $A1$, 2, 3; $M1$, 2, 3, if $c \times \mathbf{0} = \mathbf{0}$ or $\mathbf{0} \times c = \mathbf{0}$ for *any single element* $c$, not $\mathbf{0}$ or 1, then $a \times \mathbf{0} = \mathbf{0} \times a = \mathbf{0}$ for *every* element $a$.

Proof: If $c\mathbf{0} = \mathbf{0}$, then $cc\mathbf{0}a = c\mathbf{0}a$, whence $\mathbf{0}a = \mathbf{0}$ (for, if $\mathbf{0}a \neq \mathbf{0}$, then $cc = c$, by $M3_2$, and therefore $c = \mathbf{0}$ or 1, by theorem 8); hence the theorem, by lemma 1.

*Theorem C.* In any system which satisfies $A1$, 2, 3; $M1$, 2, 3, if $c \times \mathbf{0} = c$ or $\mathbf{0} \times c = c$ for *any single element* $c$, not $\mathbf{0}$, then $a \times \mathbf{0} = \mathbf{0} \times a = a$ for *every* element $a$.

Proof: If $c\mathbf{0} = \mathbf{0}$, then $c\mathbf{0}\mathbf{0}a = c\mathbf{0}a$, whence $\mathbf{0}a = a$, by $M3_1$; hence the theorem, by lemma 2.

*Examples.*

The following three systems, all of which satisfy $A1, 2, 3, 4, 5$ and $M1$, 2, 3, 5, but not $M4$, will illustrate these theorems. In each of the systems there is a zero-element, namely $\mathbb{0} = 0$.

*Example* 1. The class of all even integers, with addition defined in the usual way, and multiplication defined as follows:

$$a \odot 0 = 0 \odot a = a; \quad \text{otherwise} \quad a \odot b = ab.$$

In this system, the equations $a \odot \mathbb{0} = \mathbb{0} \odot a = \mathbb{0}$ are true when and only when $a = \mathbb{0}$. There is no unit-element.

*Example* 2. The class of all positive integers and zero, with $a \oplus b = a + b$, and $a \odot b$ defined as follows:

$$a \odot 1 = 1 \odot a = a; \quad \text{otherwise} \quad a \odot b = a + b + 2.$$

In this system, there is a unit-element, namely $\mathbb{1} = 1$, and the equations $a \odot \mathbb{0} = \mathbb{0} \odot a = \mathbb{0}$ are true when and only when $a = \mathbb{1}$.

*Example* 3. The class of all positive integers and zero, with $a \oplus b = a + b$, and $a \odot b = a + b + 1$.

In this system, the equations $a \odot \mathbb{0} = \mathbb{0} \odot a = \mathbb{0}$, and also the equations $a \odot \mathbb{0} = \mathbb{0} \odot a = a$, are false for all values of $a$. There is no unit-element.

It should be noticed that all these systems possess the property that a product is never zero unless at least one of its factors is zero.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.