# A SET OF POSTULATES FOR FIELDS*

BY

NORBERT WIENER

## INTRODUCTION

Huntington† has developed a set of thirteen independent postulates for fields. These postulates make use of the undefined notions of multiplication and addition. They thus represent a state of the theory of postulates for fields analogous to that prevailing in boolean algebras before the work of Sheffer.‡ Sheffer showed that the three operations of disjunction, conjunction, and negation could be derived by iterating the operation $\bar{a} \odot \bar{b}$, and that the logical constants $z$ and $u$ could be obtained in like manner. It is the purpose of this paper to perform an analogous task for ordinary algebra. Our undefined operation, which we shall symbolize by $x \,@\, y$, will turn out to have the formal properties characteristic of $1 - x/y$.

## POSTULATE SET FOR FIELDS

We assume:

I. A class $K$,

II. A binary $K$-rule of combination @.

III. The following properties of $K$ and @:

1. Whatever $x$ may be, there is a $K$-element $y$ such that $x \,@\, (y \,@\, y)$ is not a $K$-element.

2. If $x$ and $y$ are $K$-elements, but $x \,@\, y$ is not a $K$-element, there is a $K$-element $z$ such that $y = z \,@\, z$.

3. Whenever $x$ and $y$ are distinct $K$-elements, either $x \,@\, y$ or $y \,@\, x$ is a $K$-element.

4. Whenever $x$, $y$, $u$, $v$, and their indicated combinations are $K$-elements, and $x \,@\, y = u \,@\, v$, then $x \,@\, u = y \,@\, v$.

*Definition.* $Z = x \,@\, x$, if $x$ and $x \,@\, x$ belong to $K$, and $x \,@\, x$ is unique in the system.

* Presented to the Society, December 30, 1919.

† E. V. Huntington, *Note on the definitions of abstract groups and fields by sets of independent postulates*, these Transactions, vol. 6 (1905), pp. 181–193.

‡ H. M. Sheffer, *A set of five independent postulates for boolean algebras, with application to logical constants*, these Transactions, vol. 14 (1913), pp. 481–488. Sheffer's terminology and method of exposition are followed closely here.

5. If $x$, $y$, $x \mathbin{@} y$, and $Z$ are $K$-elements, and $x \mathbin{@} y = Z$, then $x = y$.

6. If $x$, $y$, $z$, $Z$, and their indicated combinations belong to $K$,

$$[(x \mathbin{@} y) \mathbin{@} (Z \mathbin{@} y)] \mathbin{@} z = [(x \mathbin{@} z) \mathbin{@} (Z \mathbin{@} z)] \mathbin{@} y.$$

*Definition.* $U = Z \mathbin{@} x$, if $x$, $Z$, and $Z \mathbin{@} x$ belong to $K$, and $Z \mathbin{@} x$ is unique in the system.

*Definition.* $x \odot y = \{U \mathbin{@} \{[(\overline{U \mathbin{@} y} \mathbin{@} U) \mathbin{@} x] \mathbin{@} U\}\} \mathbin{@} U$, if all the indicated expressions belong to $K$. Otherwise, if $Z$ belongs to $K$, $x \odot y = Z$.

*Definition.* $x \sim y = x \odot (y \mathbin{@} x)$.

7. If $x$, $y$, $u$, $v$, and all their indicated combinations belong to $K$, we have $(x \sim y) \sim (u \sim v) = (x \sim u) \sim (y \sim v)$.

*Definition.* $x \oplus y$ is defined as $u$, the unique $K$-element for which $x = u \sim y$, if such a unique $K$-element exists, and as $Z$, if $Z$ is a $K$-element, and if there is no $K$-element $u$ for which $x = u \sim y$.

## Classification of postulates 1–7

Postulate 1 is a simple existence-postulate. Postulates 2 and 3, while in form hypothetical existence-postulates, function as $K$-closing postulates in a limited sense, for they narrow the class of cases where $x$ and $y$ are $K$-elements, while $x \mathbin{@} y$ fails to be a $K$-element. Postulates 6 and 7 are simple equivalence-postulates, for they assert that two expressions shall always have the same meaning when they are significant. Postulates 4 and 5 are hypothetical equivalence-postulates, with equivalences for hypotheses. Thus our set consists of one simple existence-postulate, two hypothetical existence-$K$-closing postulates, two simple equivalence-postulates, and two hypothetical equivalence-postulates.

## Consistency of postulates 1–7

With the following interpretation of $K$ and @ postulates 1–7 are satisfied: $K$ consists of all rational numbers, and $x \mathbin{@} y = 1 - x/y$.

## Independence of postulates 1–7

With each of the interpretations of $K$ and @ given in (1)–(7) below, all postulates except the one correspondingly numbered are satisfied; that postulate is therefore independent of the remaining six.

(1) $K$ contains only one element $m$; $m \mathbin{@} m = m$.

(2) $K$ contains only two elements, $m$ and $n$; $m \mathbin{@} m = m$; $n \mathbin{@} m = n$; $m \mathbin{@} n$ and $n \mathbin{@} n$ do not belong to $K$.

(3) $K$ contains only two elements, $m$ and $n$; $m \mathbin{@} m = m$; $n \mathbin{@} n = n$; $m \mathbin{@} n$ and $n \mathbin{@} m$ do not belong to $K$.

(4) $K$ contains only three elements, $l_4 = l_1$, $l_2$, and $l_3$; $l_k \mathbin{@} l_{k+1}$ does not belong to $K$; otherwise $l_j \mathbin{@} l_k = l_{k+1}$.

(5) $K$ contains only two elements, $m$ and $n$; $m \mathbin{@} m = m \mathbin{@} n = n \mathbin{@} m = n$; $n \mathbin{@} n$ does not belong to $K$.

(6) $K$ contains only three elements, $l$, $m$, and $n$; @ is defined by the following table (for example: $l \mathbin{@} m = n$; $l \mathbin{@} l$ does not belong to $K$).

| @ | $l$ | $m$ | $n$ |
|---|---|---|---|
| $l$ | | $n$ | $m$ |
| $m$ | | $l$ | $n$ |
| $n$ | | $m$ | $l$ |

(7) $K$ consists of all complex numbers;

$$(x + iy) \mathbin{@} (u + iv) = 1 - \frac{x - iy}{u - iv}.$$

## Deductions from the postulates

Theorem I. *$K$ contains at least two elements.*

Theorem II. *$K$ contains an element answering to the definition of $Z$.*

Theorem III. *If $x$ and $y$ belong to $K$, and $y \neq Z$, $x \mathbin{@} y$ belongs to $K$.*

Theorem IV. *$K$ contains no elements of the form $x \mathbin{@} Z$.*

Theorem V. *$K$ contains an element distinct from $Z$, answering to the definition of $U$.*

Theorem VI. *If $x$, $y$, and $z$ belong to $K$ and $y \neq Z$, $z \neq Z$, then*

$$[(x \mathbin{@} y) \mathbin{@} U] \mathbin{@} z = [(x \mathbin{@} z) \mathbin{@} U] \mathbin{@} y.$$

Theorem VII. *If $x$ is a $K$-element, $(x \mathbin{@} U) \mathbin{@} U = x$.*

Theorem VIII. *If $y \neq Z$ and $x = y \odot z$, then $z = (x \mathbin{@} y) \mathbin{@} U$, and conversely.*

Theorem IX. *If $x$ and $y$ belong to $K$, $x \odot y$ belongs to $K$.*

Theorem X. $x \odot y = y \odot x$.

Theorem XI. *If $x \odot y = Z$, $x = Z$ or $y = Z$, and vice versa.*

Theorem XII. *If $x$ and $y$ belong to $K$, $x \oplus y$ belongs to $K$.*

Theorem XIII. *If $x \oplus x = x$, $x = Z$ and vice versa.*

Theorem XIV. *If $u \odot x = u \odot y$ and $u \neq Z$, then $x = y$.*

Theorem XV. $(x \odot y) \odot z = x \odot (y \odot z)$.

Theorem XVI. $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$.

Theorem XVII. $x \oplus y = y \oplus x$.

Theorem XVIII. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Theorem XIX. *If $x$ is a $K$-element, there is a $K$-element $y$ such that $y \oplus x = Z$.*

Theorem XX. *If $x$ and $y$ are $K$-elements, there is a $K$-element $u$ such that $u \oplus x = y$.*

## Proofs of the preceding theorems

*Proof of I.* If $K$ contains only one element $x$, it follows by 2 that $x @ x = x$. Hence $x @ (x @ x) = x$ and is a $K$-element. As this contradicts 1, $K$ contains at least two elements.

*Proof of II.* (1) $K$ contains an element of the form $x @ x$ [by 1 and 2].

If $x$ and $y$ are $K$-elements, $x @ y$ or $y @ x$ is a $K$-element [by 3].

If $x @ y$ is a $K$-element, $x @ y = x @ y$. Then, if $x @ x$ and $y @ y$ are $K$-elements,

(2) $$x @ x = y @ y.$$

Similarly, if $y @ x$, $x @ x$, and $y @ y$ are $K$-elements,

(3) $$x @ x = y @ y.$$

Hence $K$ contains a unique term $Z$ [by (1), (2), (3) and the definition of $Z$].

*Proof of III.* This theorem follows directly from II and 2.

*Proof of IV.* This theorem follows directly from II and 1.

*Proof of V.* $[(Z @ y) @ (Z @ y)] @ z$ belongs to $K$ unless $y = Z$ or $z = Z$ [by III]. Therefore, if $y \neq Z$, $z \neq Z$,

$$[(Z @ y) @ (Z @ y)] @ z = [(Z @ z) @ (Z @ z)] @ y \text{ [by 6 and II]}.$$

(1) $\therefore Z @ z = Z @ y$ [by II].

(2) $Z @ Z$ is not a member of $K$ [by IV].

(3) $U$ is a member of $K$ [by (1), (2) and the definition of $U$].

If $Z = U$, then if $x$ is a $K$-element other than $Z$, $Z @ x = Z$ [by III and the definition of $U$]. Then $Z = x$, which is impossible [by 5]. But $K$ contains an element other than $Z$ [by I].

(4) $\therefore Z \neq U$.

Statements (3) and (4) constitute the theorem.

Theorems I–V inclusive will be used in the following proofs without explicit citation.

*Proof of VI.* This theorem follows directly from V and 6.

*Proof of VII.* $[(x @ U) @ U] @ x = [(x @ x) @ U] @ U$ [by VI], $= (Z @ U) @ U = U @ U = Z$.

$$\therefore (x @ U) @ U = x.$$

*Proof of VIII.* Let $x = y \odot z$ and $x \neq Z$, $y \neq Z$, $z \neq Z$. Then

$$Z @ U \neq z @ z \text{ [by V, 5]}.$$

$$\therefore U @ z \neq Z @ z \text{ [by 4]}.$$

(1) $$\therefore (U @ z) @ U \neq Z \text{ [by 5]}.$$

$$\therefore [(\overline{U @ z} @ U) @ y] @ U \neq Z.$$

(2) $\therefore \{U @ \{[(\overline{U @ z} @ U) @ y] @ U\}\} @ U$ belongs to $K$.

$x = \{U @ \{[(\overline{U @ z} @ U) @ y] @ U\}\} @ U$ [Definition of $\odot$].

$x @ U = \{\{U @ \{[(\overline{U @ z} @ U) @ y] @ U\}\} @ U\} @ U$

$= U @ \{[(\overline{U @ z} @ U) @ y] @ U\}.$

$\therefore U @ x = [(U @ z) @ U] @ y$ [by 4, VII].

$\therefore U @ z = y @ x$ [by 4, VII].

$\therefore x @ y = z @ U$ [by 4].

(3) $\therefore (x @ y) @ U = (z @ U) @ U = z$ [by VII].

(4) If $y = Z$ or $z = Z$, then $x = Z$ [by the definition of $\odot$].

If $x = Z$, then $\{U @ \{[(\overline{U @ z} @ U) @ y] @ U\}\} @ U$ is not a $K$-element [by (1)].

(5) Then $y = Z$ or $z = Z$ [by (2)]. $\therefore$ If $y \neq Z$, $x = z = Z$ [by (4) and (5)].

(6) Then $(x @ y) @ U = Z = z$.

Statements (3) and (6) constitute the theorem, and all the steps taken are reversible.

*Proof of IX.* This follows immediately from II and the definition of $\odot$.

*Proof of X.* Let $x = y \odot z$ and $y \neq Z$, $z \neq Z$, then

$Z = [(x @ y) @ U] @ z$ [by VIII],

$= [(x @ z) @ U] @ y$ [by VI].

(1) Consequently $x = z \odot y$ [by VIII, 5].

If $y = Z$ or $z = Z$, $\{U @ \{[(\overline{U @ z} @ U) @ y] @ U\}\} @ U$ is not a $K$-element, and by the definition of $\odot$, $y \odot z = z \odot y = Z$.

This fact and (1) constitute the proof of X.

*Proof of XI.* Suppose $x \odot y = Z$. Then $x = Z$ or

$y = (Z @ x) @ U = U @ U = Z$ [by VIII].

The converse of this proposition follows from the definition of $\odot$.

*Proof of XII.* If $x \oplus y$ does not belong to $K$, there are two distinct $K$-elements, $u$ and $v$, such that

(1) $x = u \sim y = v \sim y$ [by definition of $\oplus$].

Then either $u \sim y = Z$ or $(u \sim y) \sim (v \sim y) = Z$ [by XI, definition of $\sim$].

Then either $u \sim y = Z$ or $u \sim v = Z$ or $y = Z$ or

$(u \sim v) \sim (y \sim y) = Z$ [by 7].

If $m \sim n = Z, m = n$, and if $m = n \neq Z, m \sim n = Z$ [by definition of $\sim$].

$$\therefore \quad u = y \quad \text{or} \quad u = v \quad \text{or} \quad y = Z.$$

$$v = y \quad \text{or} \quad v = u \quad \text{or} \quad y = Z.$$

$$\therefore \quad u = v \quad \text{or} \quad y = Z. \tag{2}$$

If $y = Z, x = u \odot U = v \odot U$ [by (1)].

(3) Then $u = (u @ U) @ U = (v @ U) @ U = v$ [by VII, VIII, X].

Statements (2) and (3) constitute the theorem.

*Proof of XIII.* If $x \oplus x = x$ and $x \neq Z$, then $x \sim x = x$ [by definitions of $\odot$, $\sim$, and $\oplus$].

(1) Then $x = x \odot (x @ x) = x \odot Z = Z$ [by XI].

(2) $Z \oplus Z = Z$ [by XI and the definitions of $\sim$ and of $\oplus$].

Statements (1) and (2) constitute the theorem.

*Proof of XIV.* Suppose $z = u \odot x = u \odot y$ and $u$ is a $K$-element other than $Z$. Then $x = (z @ u) @ U = y$ [by VIII].

*Proof of XV.* Suppose $u = (x \odot y) \odot z$, $v = x \odot y$, and $x \neq Z$, $y \neq Z$, $z \neq Z$. Then $y = (v @ x) @ U$ and $v = (u @ z) @ U$ [by VIII, X].

$$\therefore \quad y = \{[(u @ z) @ U] @ x\} @ U$$

$$= \{[(u @ x) @ U] @ z\} @ U \text{ [by VI].}$$

The steps already taken are reversible, and by retracing them after the interchange of $x$ and $z$, it appears that if $x \neq Z$, $y \neq Z$, $z \neq Z$,

$$(x \odot y) \odot z = (z \odot y) \odot x = x \odot (y \odot z) \text{ [by X].} \tag{1}$$

If $x$, $y$, or $z = Z$, by XI,

$$(x \odot y) \odot z = Z = x \odot (y \odot z). \tag{2}$$

Statements (1) and (2) constitute the theorem.

*Proof of XVI.*

LEMMA. $x \odot (u \sim v) = (x \odot u) \sim (x \odot v)$, if both sides belong to $K$, unless $x = Z$.

*Proof.* Suppose $u \neq Z$, $v \neq Z$. Let $x \odot u = m$ and $x \odot v = n$. Then $m \neq Z$, $n \neq Z$ [by XI]. Then $u = (m @ x) @ U$ and $v = (n @ x) @ U$ [by VIII]. Hence $u @ m = [(m @ x) @ U] @ m = [(m @ m) @ U] @ x$ [by VI] $= U @ x = v @ n$ [by VI, as before].

(1) Therefore $v @ u = n @ m$ [by 4].

$$x \odot (u \sim v) = x \odot [u \odot (v @ u)] \text{ [by definition of } \sim],$$

$$= (x \odot u) \odot (v @ u) \text{ [by XV],}$$

$$= m \odot (n @ m) \text{ [by (1)],}$$

$$= m \sim n \text{ [by definition of } \sim]. \tag{2}$$

(3) If $u = Z$, $m = Z$, and neither $x \odot (u \sim v)$ nor $m \sim n$ is a $K$-element, by the definition of $\sim$.

If $u \neq Z$, and $v = Z$, then $n = Z$, so that $x \odot (u \sim v) = m \odot (v \mathbin{@} u)$ [as before], $= m \odot U = m \odot (n \mathbin{@} m)$

(4) $\qquad = m \sim n$ [as before].

Statements (2), (3), and (4) constitute the lemma.

Let $y \oplus z = p$. If $p \neq Z$, then $y = p \sim z$ [def. of $\oplus$, (1) of VIII]. Then $x \odot y = (x \odot p) \sim (x \odot z)$ [by (2) and (4)].

(5) $\qquad \therefore\ x \odot p = (x \odot y) \oplus (x \odot z)$ [by XII, def. of $\oplus$].

If $p = Z$, there is no $K$-element $q$ such that $y = q \sim z$ [def. of $\oplus$]. Then if $x \neq Z$ there is no $q$ such that $x \odot y = (x \odot q) \sim (x \odot z)$ [by the Lemma, XI, XIV].

(6) Then $x \odot p = (x \odot y) \oplus (x \odot z)$ [by the def. of $\oplus$].

(7) If $x = Z$, the theorem becomes, by XII, $Z = Z \oplus Z$, which is an immediate consequence of the definition of $\oplus$.

Statements (5), (6), and (7) constitute the theorem.

*Proof of XVII.* Suppose $x \oplus y = u$, $u \neq Z$. Then $x = u \sim y$ [def. of $\oplus$], $= u \odot (y \mathbin{@} u)$ [def. of $\sim$].

This proposition is equivalent to $(x \mathbin{@} u) \mathbin{@} U = y \mathbin{@} u$, or to [by VII, VIII]; $(y \mathbin{@} u) \mathbin{@} U = x \mathbin{@} u$ [by VI].

Reversing our former reasoning, $y = u \sim x$, and

(1) $\qquad u = y \oplus x$ [by def. of $\oplus$, XII].

(2) If $x \oplus y = Z$, $y \oplus x = Z$ [by def. of $\oplus$, XII, (1)].

Statements (1) and (2) constitute the theorem.

*Proof of XVIII.* Let $x \oplus y = m$, $y \oplus z = n$, $m \oplus z = u$, and $x \oplus n = v$.

*Case I.* Suppose $x$, $y$, $z$, $m$, $n$, $u$, and $v$ are all distinct from $Z$. Then $x = m \sim y$, $z = n \sim y$, $x = v \sim n$, $z = u \sim m$ [by def. of $\oplus$, XVII].

$\therefore\ x \sim z = (m \sim y) \sim (n \sim y) = (v \sim n) \sim (u \sim m)$ [def. of $\sim$].

$\therefore\ m \sim n = (v \sim n) \sim (u \sim m)$ [by 7, def. of $\sim$].

$\therefore\ u \sim m = (v \sim n) \sim (m \sim n)$ [by XVII, defs. of $\oplus$ and $\sim$].

$= v \sim m$ [by 7, def. of $\sim$].

$\therefore\ Z = (u \sim m) \sim (v \sim m)$ [by def. of $\sim$]

$= (u \sim v) \sim (m \sim m)$ [by 7, def. of $\sim$]

$= u \sim v$ [by def. of $\sim$]

$= u \mathbin{@} v$ [by def. of $\sim$, XI].

(1) $\qquad \therefore\ v = u$ [by 5].

*Case II.* Let $x$, $y$, or $z = Z$.

(2) $\quad a \oplus Z = Z \oplus a = a$ [by XVII and the defs. of $\oplus$ and $\sim$].

(3) Combining this proposition with XVII, the proof is obvious.

*Case III.* Let $x, y, z, n, u$, and $v$ be all distinct from $Z$, and let $m = Z$. Then $y = n \sim z$, $x = v \sim n$, $z = u \sim Z = u$ [by defs. of $\oplus$ and $\sim$; XVII].

(4) Whatever $p$, $x \neq p \sim y$. Suppose $u \neq v$. Then

$$\begin{aligned} x &= v \sim n \\ &= (v \sim n) \sim (u \sim u) \text{ [by def. of } \sim], \\ &= (v \sim u) \sim (n \sim u) \text{ [by 7]}, \\ &= (v \sim u) \sim y. \end{aligned} \tag{5}$$

(6) Statements (5) and (4) contradict one another. Hence $u = v$.

(7) *Case IV.* Similarly, if $n$ alone is $Z$, $u = v$.

(8) *Case V.* It follows from the cases already considered by XII and the definitions of $\sim$ and $\oplus$ that if $u = Z$, $v = Z$, and vice versa.

Statements (1), (3), (6), (7), and (8) constitute the theorem.

*Proof of XIX.* If $a$, $b$, and $x$ are distinct from $Z$ and from one another,

$$\begin{aligned} (a \sim x) \sim (b \sim x) &= (a \sim b) \sim (x \sim x) \text{ [by 7]}, \\ &= (a \sim b) \odot U \text{ [def. of } \sim, U], \\ &= \{U \mathbin{@} \{[(\overline{U \mathbin{@} U} \mathbin{@} U) \mathbin{@} (a \sim b)] \mathbin{@} U\}\} \mathbin{@} U \\ &\qquad \text{[def. of } \odot], \\ &= \{U \mathbin{@} \{[U \mathbin{@} (a \sim b)] \mathbin{@} U\}\} \mathbin{@} U \text{ [def. of } U], \\ &= \{(a \sim b) \mathbin{@} \{[U \mathbin{@} U] \mathbin{@} U\}\} \mathbin{@} U \text{ [by 4, VI]}, \\ &= a \sim b \text{ [by VII]}. \end{aligned} \tag{1}$$

(2) Then $(a \sim x) \sim a = (b \sim x) \sim b$ [by 7]. Now, $(a \sim x) \sim a$ can never be expressed in the form $u \sim x$. For, suppose $(a \sim x) \sim a = u \sim x$. Then $(a \sim x) \sim u = a \sim x$ [by 7].

(3) $\quad \therefore \ a \sim x = (a \sim x) \odot [u \mathbin{@} (a \sim x)]$ [def. of $\sim$].

But we have just seen in (1) how it can be shown that

(4) $\quad (a \sim x) = (a \sim x) \odot U.$

Hence, $u \mathbin{@} (a \sim x) = U$ [(3), (4), X, XIV], $= Z \mathbin{@} (a \sim x)$ [def. of $U$].

$$\therefore \ U = Z \mathbin{@} u = (a \sim x) \mathbin{@} (a \sim x) = Z.$$

Since this contradicts V,

(5) $$(a \sim x) \sim a \neq u \sim x.$$

From (2) and (5) we conclude that, if $x \neq Z$, there is a unique term

$$\bar{x} = (a \sim x) \sim a,$$

such that whatever $u$, $\bar{x} \neq u \sim x$.

(6) $\therefore\ Z = \bar{x} \oplus x$ [def. of $\oplus$, XII]

(7) $Z = Z \oplus Z$ [def. of $\oplus$, $U$, $\sim$, argument of (1)].

Statements (6) and (7) constitute the theorem, unless it is impossible for an $a$ to be found distinct from $Z$ and $x$. In this case $K$ contains only $Z$ and $U$. Here the same result may be obtained by a simple computation.

*Proof of XX.* Let $x$ and $y$ be $K$-elements. Then either $y = Z$ or $y \sim x$ is a $K$-element $v$ [by IX, def. of $\sim$].

(1) If $y = Z$, there is a $K$-element $u$ such that $u \oplus x = y$ [by XIX].

(2) If $y \neq Z$, since $v = y \sim x$, $v \oplus x = y$ [by def. of $\oplus$, XII].

## Postulates 1–7 and the definition of a field

In the article already cited, Huntington gives the following reduced set of postulates for a field, the sufficiency of which he proves, but not their independence.

1. If $a$ and $b$ belong to $K$, $a \oplus b$ belongs to $K$.
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. $a \oplus b = b \oplus a$.
4. If $a$ and $b$ belong to $K$, $a \odot b$ belongs to $K$.
5. $(a \odot b) \odot c = a \odot (b \odot c)$.
6. $a \odot b = b \odot a$.
7. Either $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, or
$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a).$$
8. Given $a$ and $b$, there is an $x$ such that $a \oplus x = b$.
9. Given $a$ and $b$, and $a \oplus a \neq a$, there is $ay$ such that $a \odot y = b$.
10. There are at least two elements in the class.

That the postulates of Huntington are deducible from those of this paper will be seen at once from an inspection of the following table of correspondences. The figures beneath the line refer to Huntington's postulates; those above, to the present article.

| Corresponds to | XII | XVIII | XVII | IX | XV | X | XVI | XX | VII, X | I |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

If for any elements $a$ and $b$ of Huntington's class, we write $a \mathbin{@} b$ for $1 - a/b$, Huntington's set implies set 1–7.

## A SINGLE UNDEFINED NOTION FOR COMPLEX ALGEBRA

The laws of complex algebra cannot be expressed entirely in terms of $+$ and $\times$. Huntington* has given a set of postulates for complex algebra in which the undefined notions are addition, multiplication, the class of all complex numbers, the class of all real numbers, and the order of magnitude among real numbers. He has suggested† how all these notions may be derived from that of the absolute value of the difference between two complex numbers, though he has given no set of postulates for this operation. Apart from this operation, which is rather unlike those on which we are accustomed to base sets of postulates in that it always results in a number of a very special sort—a real number, no single operation has been developed which may serve as the sole foundation of complex algebra.

There are other such operations, however, and one of them is closely allied to the one taken for the fundamental notion of this set of postulates. This operation has already been employed to demonstrate the independence of postulate 7. Denoting $a - ib$, the conjugate‡ imaginary of $a + ib$, by $C(a + ib)$, our operation, which we shall term $x * y$, is

$$1 - C\left(\frac{x}{y}\right).$$

We define $Z$, $U$, and multiplication in terms of $*$ in the same manner in which they have already been defined in terms of @. $C(x)$ is defined as

$$U * [U * (U * x)].$$

We say that $x$ is real if $x = C(x)$. We define $x \wedge y$ as $C(x * y)$, and addition is defined in terms of $\wedge$ as previously in terms of @. If $x$ and $y$ are real, $x$ is said to be larger than $y$ when there is a $K$-element $z$, the product of a real by itself, which when added to $y$ gives $x$.

The formulation of a set of postulates for $*$ is a very difficult matter. Postulates 1–6 of this paper may stand unchanged, but the properties of addition and of the series of reals are so intricate as not to lend themselves readily to independence proofs. In general, independence proofs that are satisfactory when addition and multiplication are assumed separately break down on more than one postulate when translated in terms of $*$. The system of $*$, though fundamentally the same as that of the familiar complex algebra, has a technique of its own of considerable difficulty.

* E. V. Huntington, *A set of postulates for ordinary complex algebra*, these Transactions, vol. 6 (1905), pp. 209–229.

† Ibid., note on p. 210.

‡ This use of the conjugate was suggested to me by an unpublished paper of Sheffer.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
*June*, 1919.