DEFINITIONS OF A FIELD BY SETS OF INDEPENDENT POSTULATES*

BY

EDWARD V. HUNTINGTON

Introduction.

The fundamental concept involved in the following paper is that of a *class* (assemblage, set, Menge, ensemble) in which two *rules of combination* (operations, Verknüpfungen), which we shall denote by $\oplus$ are $\odot$, are defined. †

Thus, if a and b belong to the class, $a \oplus b$ denotes an object uniquely determined by a and b according to the first rule, and $a \odot b$ denotes an object uniquely determined by a and b according to the second rule. These objects $a \oplus b$ and $a \odot b$ do not necessarily belong to the class unless such condition is expressly stated. (We may think of $a \oplus b$ as the "sum" and $a \odot b$ as the "product" of the two elements a and b.)

A class in which the rules of combination $\oplus$ and $\odot$ are so defined as to satisfy any one of the eight sets of postulates given below shall be called a *field* (Körper) ‡ with respect to $\oplus$ and $\odot$. (A field may be thought of, briefly, as any assemblage in which the rational operations of algebra can all be performed.)

The object of the paper is to show (1) that any one of these eight definitions of a field agrees with the definition usually given; and (2) that the postulates of each set are mutually independent, that is, that no postulate of any one set is deducible from the other postulates of that set.

The simplest definition of a field is that supplied by the first set, which contains only seven postulates: $A1$, $A2$, $A3$, $M1$, $M2$, $M3$, D.

An example of an infinite field is the system of all rational numbers (positive, negative and 0), with $a \oplus b = a + b$ and $a \odot b = ab$.

---

* Presented to the Society at the Evanston meeting, September 2, 1902. Received for publication, November 16, 1902.

† On the fundamental concepts, cf. STOLZ and GMEINER, *Theoretische Arithmetik*, 1901, § 4, and the writer's paper on the postulates of magnitude, Transactions, vol. 3 (1902), p. 264.

‡ On the concept of a field (first employed by DEDEKIND), see H. WEBER, *Algebra*, vol. 1 (1898), p. 491; E. H. MOORE, *Mathematical Papers read at the Chicago Congress of 1893*, p. 211; L. E. DICKSON, *Linear groups with an exposition of the Galois Field theory*, 1901.

An example of a finite field is the system of p integers $0, 1, 2, \cdots, p-1$ (p being any prime number), with $a \oplus b \equiv a + b \pmod{p}$ and $a \odot b \equiv ab \pmod{p}$.

Another example of a finite field is the system of the four digits 0, 1, 2, 3, with $a \oplus b$ and $a \odot b$ defined by the following "multiplication tables":

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

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

As a matter of fact, any set of n objects can be made a field by suitable definitions of $\oplus$ and $\odot$, provided the number of elements, n, is a power of a prime.*

List of postulates from which the eight sets are selected.

To avoid repetition, we give here a list of seventeen postulates from which our eight sets are selected. In this list the letters A and M are intended to suggest "addition" and "multiplication;" the figures 1 and 2 indicate the commutative law and the associative law respectively, while D denotes the distributive law. The figure 3 indicates a postulate which demands the existence of an element satisfying some condition.

The postulates A 1, 2, 3 or A 1′, 2′, 3′, 4′ are the same as those used by the writer to define an Abelian group.†

$A1$. If a, b and $b \oplus a$ belong to the class, then $a \oplus b = b \oplus a$.

$A2$. If a, b, c, $a \oplus b$, $b \oplus c$ and $a \oplus (b \oplus c)$ belong to the class, then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

$A3$. For every two elements a and b ($a = b$ or $a \neq b$) there is an element x such that $a \oplus x = b$.

$A1'$. If a, b, $a \oplus b$ and $b \oplus a$ all belong to the class, then $a \oplus b = b \oplus a$.

$A2'$. If a, b, c, $a \oplus b$, $b \oplus c$, $(a \oplus b) \oplus c$ and $a \oplus (b \oplus c)$ all belong to the class, then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

$A3'$. For every two elements a and b ($a = b$ or $a \neq b$) there is an element x' such that $(a \oplus x') \oplus b = b$.

$A4'$. If a and b belong to the class, then $a \oplus b$ also belongs to the class.

---

* GALOIS, 1830; see Journal de mathématiques, vol. 11 (1846), pp. 398–407. The theorem that every finite field is necessarily a Galois field of order a power of a prime was first proved by E. H. MOORE, *loc. cit.* See DICKSON, *Linear Groups*, § 18.

† Transactions, vol. 4, pp. 27, 29.

$M1$. If a, b and $b \odot a$ belong to the class, then $a \odot b = b \odot a$.

$M2$. If a, b, c, $a \odot b$, $b \odot c$ and $a \odot (b \odot c)$ belong to the class, then $(a \odot b) \odot c = a \odot (b \odot c)$.

$M3$. For every two elements a and b ($a = b$ or $a \neq b$), provided $a \oplus a \neq a$ and $b \oplus b \neq b$, there is an element y such that $a \odot y = b$.

$M1'$. If a, b, $a \odot b$ and $b \odot a$ all belong to the class, then $a \odot b = b \odot a$.

$M2'$. If a, b, c, $a \odot b$, $b \odot c$, $(a \odot b) \odot c$ and $a \odot (b \odot c)$ all belong to the class, then $(a \odot b) \odot c = a \odot (b \odot c)$.

$M3'$. For every two elements a and b ($a = b$ or $a \neq b$), provided $a \oplus a \neq a$ and $b \oplus b \neq b$, there is an element y' such that $(a \odot y') \odot b = b$.

$M4'$. If a and b belong to the class, and $b \oplus b \neq b$, then $a \odot b$ also belongs to the class.

D. If a, b, c, $b \oplus c$, $a \odot b$, $a \odot c$ and $(a \odot b) \oplus (a \odot c)$ belong to the class, then $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

D'. If a, b, c, $b \oplus c$, $a \odot b$, $a \odot c$, $a \odot (b \oplus c)$ and $(a \odot b) \oplus (a \odot c)$ all belong to the class, then $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

M_0. If a and b belong to the class, and $b \oplus b = b$, then $a \odot b$ also belongs to the class.

The eight definitions of a field.

From the list of postulates just given we form the following eight sets, any one of which may be taken as a definition of a field:

DEF. 1.	$A1$, $A2$, $A3$,	$M1$, $M2$, $M3$,	D.
DEF. 2.	$A1$, $A2$, $A3$,	$M1$, $M2$, $M3$,	D', M_0.
DEF. 3.	$A1$, $A2$, $A3$,	$M1'$, $M2'$, $M3'$, $M4'$,	D.
DEF. 4.	$A1$, $A2$, $A3$,	$M1'$, $M2'$, $M3'$, $M4'$,	D', M_0.
DEF. 5.	$A1'$, $A2'$, $A3'$, $A4'$,	$M1$, $M2$, $M3$,	D.
DEF. 6.	$A1'$, $A2'$, $A3'$, $A4'$,	$M1$, $M2$, $M3$,	D', M_0.
DEF. 7.	$A1'$, $A2'$, $A3'$, $A4'$,	$M1'$, $M2'$, $M3'$, $M4'$,	D.
DEF. 8.	$A1'$, $A2'$, $A3'$, $A4'$,	$M1'$, $M2'$, $M3'$, $M4'$,	D', M_0.

It will be noticed that Def. 1 involves seven postulates; Defs. 2, 3 and 5 each involve eight, Defs. 4, 6 and 7 each involve nine and Def. 8 involves ten.

Remark. In Def. 4 and in Def. 8 we might replace $M4'$ and M_0 by a single postulate requiring that $a \odot b$ shall always belong to the class whatever elements a and b may be, and thus reduce the number of postulates in each of these sets by one.*

* The latter definition thus obtained is essentially the same as the first of two definitions proposed by L. E. DICKSON; see p. 14 of the present number of the Transactions.

Agreement with the accepted definition of a field.

It is easy to see that every field in the usual sense will satisfy all our eight definitions, hence the postulates of each of our eight sets are *consistent.* We now show, conversely, that every system $S(\oplus, \odot)$, which satisfies any one of our eight definitions will be a field in the usual sense.

Since all the definitions include either the three postulates A 1, 2, 3 or the four postulates A 1′, 2′, 3′, 4′, we have:

THEOREM I. *The elements of S form a commutative group with respect to $\oplus$.*

Hence,* the sum $a \oplus b$ of any two elements will itself be an element of the class; subtraction † will always be possible and the result uniquely determined; and a peculiar element 0 will exist having the additive property of zero: $a \oplus 0 = 0 \oplus a = 0$ for every element a.

In particular, $a \oplus a = a$ when and only when $a = 0$. (Compare $M3$, $M3'$, $M4'$, M_0.)

Again, all the definitions include either M 1, 2, 3 or M 1′, 2′, 3′, 4′; hence if we can prove:

$$1^\circ) \text{ in } M3: y \neq 0; \qquad 2^\circ) \text{ in } M3': y' \neq 0;$$

$$3^\circ) \text{ in } M4': a \odot b \neq 0 \text{ when } a \neq 0, b \neq 0;$$

then we shall have:

THEOREM II. *The elements of S exclusive of 0 form a commutative group with respect to $\odot$.*

Hence will follow: The product $a \odot b$ of two elements not 0 will itself be an element not 0; within the sub-class of elements not 0, division ‡ will always be possible, and the result uniquely determined; and a peculiar element 1 will exist, having, within this sub-class, the multiplicative property of unity: $a \odot 1 = 1 \odot a = a$, when $a \neq 0$.

Proof of (1°). Considering first the Definitions 1, 2, 5, 6, we see that in $M3$, $y \neq 0$. For if we suppose $y = 0$, then, by D or D',

$$b = a \odot y = a \odot (y \oplus y) = (a \odot y) \oplus (a \odot y) = b \oplus b,$$

which contradicts the hypothesis that $b \neq b \oplus b$.

Thus Theorem II is established for Definitions 1, 2, 5, 6.

Before passing to the proof of (2°) and (3°) we establish next, for all the definitions, the multiplicative property of 0 (Theorem III).

---

* See p. 28, where proofs of the fundamental group properties here used may be found.

† Definition of $b - a$: If $a \oplus x = b$ then $x = b - a$.

‡ Definition of b/a: If $a \odot x = b$ then $x = b/a$.

Lemma 1. The product $c \odot 0$ is an element of the class when $c \neq 0$.

In case of Defs. 2, 4, 6, 8 the lemma follows at once from M_0.—In case of Defs. 1, 3, 5, 7 the proof is as follows: Let c be any element not 0, and take c' so that $c \oplus c' = 0$, where clearly $c' \neq 0$. Then $c \odot c$ and $c \odot c'$ will belong to the class (by Theorem II in case of Defs. 1 and 5; by $M4'$ in case of Defs. 3 and 7). Applying D, $c \odot (c \oplus c') = (c \odot c) \oplus (c \odot c')$; therefore $c \odot 0$ will belong to the class.

Lemma 2. The product $0 \odot c$ will be an element of the class when $c \neq 0$.

This follows by $M4'$ in the case of Defs. 3, 4, 7, 8; and by Lemma 1 and $M1$ in the case of Defs. 1, 2, 5, 6.

Lemma 3. The product $0 \odot 0$ is an element of the class.

In case of Defs. 2, 4, 6, 8 this follows at once from M_0.—In case of Defs. 1, 3, 5, 7 take c and c' as in Lemma 1. Then $0 \odot c$ and $0 \odot c'$ are elements of the class, by Lemma 2. Applying D, $0 \odot (c \oplus c') = (0 \odot c) \oplus (0 \odot c')$, whence $0 \odot 0$ will belong to the class.

THEOREM III. *For every element a, $a \odot 0 = 0 \odot a = 0$.*

For $a \odot 0$ and $0 \odot a$ are always elements of the class, by Lemmas 1, 2, 3. Applying D or D', $a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0)$; hence $a \odot 0 = 0$. Then by $M1$ or $M1'$, $0 \odot a = 0$.

Using Theorem III we can now complete the proof of Theorem II for Definitions 3, 4, 7, 8, as follows:

Proof of (2°).—In $M3'$, $y' \neq 0$. For, if $y' = 0$, we should have $b = (a \odot y') \odot b = 0 \odot b = 0$, which contradicts the hypothesis.

Proof of (3°).—In $M4'$, $a \odot b \neq 0$ when $a \neq 0$ and $b \neq 0$. For, by $M4'$ and Theorem III, every product will be an element of the class; hence if $a \odot b = 0$, we should have $b = (a \odot y') \odot b = (a \odot b) \odot y' = 0 \odot y' = 0$, by $M3'$, $M1'$, $M2'$.

Thus Theorem II is established for all cases.

Combining the immediate consequences of Theorem II with Theorem III we have: The product $a \odot b$ will always be an element of the class; division will always be possible when the divisor is not 0, and the quotient will be uniquely determined; and there will be a peculiar element 1 such that $a \odot 1 = 1 \odot a = a$ whatever the element a.

These results, together with the commutative, associative and distributive laws, show that our system S will have all the characteristic properties of a field in the accepted sense.*

---

*See, for example, DICKSON, *Linear Groups*, §5. Since the operations $\oplus$ and $\odot$ are thus shown to obey the familiar laws of addition $(+)$ and multiplication $(\cdot)$, the circles around these symbols are conveniently omitted in further developments of the abstract field theory.

Independence of the postulates.

The independence of the postulates of each of the eight sets may be established by the use of the following systems. For example, the system marked $(A1)$ fails to satisfy the postulate $A1$, but will be found to satisfy all the other postulates of any set in which this postulate occurs.*

$(A1)$ or $(A1')$. The system of all positive rational numbers, with $a \oplus b = b$ and $a \odot b = ab$.

In proving that this system satisfies $A3$, $A3'$, $M3$, $M3'$, take $x = b$, $x' =$ any element, $y = b/a$, $y' = 1/a$.

$(A2)$ or $(A2')$. The system of all positive real numbers, with $a \oplus b = \sqrt{ab}$ and $a \odot b = ab$.

Postulates $A2$, $A2'$ fail, for $(2 \oplus 2) \oplus 8 = 4$ while $2 \oplus (2 \oplus 8) = \sqrt{8}$. In $A3$ and $A3'$ take $x = b^2/a$, $x' = b^2/a$. Postulates D and D' are satisfied, since $a \odot (b \oplus c) = a\sqrt{bc} = (a \odot b) \oplus (a \odot c)$.

$(A3)$ or $(A3')$. The system of all positive rational numbers, with $a \oplus b = a + b$ and $a \odot b = ab$.

To show that $A3$ and $A3'$ fail, consider $a = 5$, $b = 2$.

$(A4')$. The system of all rational numbers, with $a \oplus b$ defined as follows: when $a + b = 0$ or $a = 0$, then $a \oplus b = a + b$; otherwise, $a \oplus b = \sqrt{2}$; and always, $a \odot b = ab$.

Here $A4'$ clearly fails, since $\sqrt{2}$ is not an element of the system. In $A3'$ take $x' = -a$. In $M3$, $M3'$ take $y = b/a$, $y' = 1/a$, which will always belong to the system when $a \oplus a \neq a$, that is, when $a \neq 0$. Postulate D holds whenever the conditions stated are fulfilled. (We notice in passing that this system does not satisfy $A1$, $A2$ or $A3$; as a matter of fact, $A4'$ is deducible from $A1$, $A2$, $A3$.)

$(M1)$ or $(M1')$. The system of all integral numbers, with $a \oplus b = a + b$ and $a \odot b = b$.

In $A3$, $A3'$ take $x = b - a$, $x' = -a$.

$(M2)$ or $(M2')$.† The system of all couples (α_1, α_2) in which α_1 and α_2

* This is the now familiar method of PEANO and HILBERT.

† This system for proving the independence of $M2$ and $M2'$ was suggested to me by Professor L. E. DICKSON. Another system which may be used for the same purpose is the system of four digits 0, 1, 2, 3, with $a \oplus b$ and $a \odot b$ defined by the following "multiplication tables":

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

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	3	2
2	0	3	2	1
3	0	2	1	3

are rational numbers; with

$$(\alpha_1, \alpha_2) \oplus (\beta_1, \beta_2) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$

and

$$(\alpha_1, \alpha_2) \odot (\beta_1, \beta_2) = (\alpha_1\beta_1 - \alpha_2\beta_2, -\alpha_1\beta_2 - \alpha_2\beta_1).$$

(If we represent these couples by points in the complex plane, $\oplus$ will be the ordinary addition of complex numbers, and $\odot$ will be the ordinary multiplication followed by reflection in the axis of α's.)

Postulates $M2, M2'$ fail, since $[(1,0)\odot(1,1)]\odot(0,1) = (1,-1)$, while $(1,0)\odot[(1,1)\odot(0,1)] = (-1,1)$.

In $M3$, $M3'$, if $a = (\alpha_1, \alpha_2)$ and $b = (\beta_1, \beta_2)$, take

$$y = \left(\frac{\alpha_1\beta_1 - \alpha_2\beta_2}{\alpha_1^2 + \alpha_2^2}, \quad \frac{-\alpha_2\beta_1 - \alpha_1\beta_2}{\alpha_1^2 + \alpha_2^2}\right),$$

$$y' = \left(\frac{\alpha_1(\beta_1^2 - \beta_2^2) - \alpha_2(-2\beta_1\beta_2)}{(\alpha_1^2 + \alpha_2^2)(\beta_1^2 + \beta_2^2)}, \quad \frac{-\alpha_2(\beta_1^2 - \beta_2^2) - \alpha_1(-2\beta_1\beta_2)}{(\alpha_1^2 + \alpha_2^2)(\beta_1^2 + \beta_2^2)}\right).$$

($M3$) or ($M3'$). The system of all integral numbers, with $a \oplus b = a + b$ and $a \odot b = ab$.

($M4'$). The system of all rational numbers, with $a \oplus b = a + b$, and $a \odot b$ defined as follows: when $ab = 0, 1, 2, 3, \cdots$, or $a = 1$, then $a \odot b = ab$; otherwise, $a \odot b = \sqrt{2}$.

Here $M4'$ clearly fails, since $\sqrt{2}$ is not an element of the system. In $M3'$ take $y' = 1/a$. Postulate D holds whenever the conditions stated are fulfilled. (We notice in passing that this system does not satisfy $M1$, $M2$ or $M3$.)

(D) or (D'). The system of all integral numbers, with $a \oplus b = a + b$ and $a \odot b = a + b$.

Here $1 \odot (1 \oplus 1) = 3$ while $(1 \odot 1) \oplus (1 \odot 1) = 4$.

(M_0). In Definitions 2 and 6 consider the system of all rational numbers, with $a \oplus b = a + b$, and $a \odot b$ defined as follows: when $ab \neq 0$, $a \odot b = ab$; when $ab = 0$, $a \odot b = \sqrt{2}$. (This system does not satisfy D or $M4'$.)

In Definitions 4 and 8 consider the same system with $a \odot b = ab$ when $b \neq 0$, while otherwise $a \odot b = \sqrt{2}$. (This system does not satisfy D or $M1$.)

The independence of all the postulates of each set is thus established. Indeed, since each of the systems employed for this purpose is infinite, we see that each of our eight sets of postulates will still be a set of independent postulates even if we add the requirement that the field shall be infinite.

HARVARD UNIVERSITY, CAMBRIDGE, MASS., *August*, 1902.