DEFINITIONS OF A FIELD BY INDEPENDENT POSTULATES*

BY

LEONARD EUGENE DICKSON

Introduction.

The English term *field*, equivalent to the German term *Körper*, has the same significance as the terms *domain of rationality* and *realm of rationality*, but is to be preferred to the latter as a designation for the concept apart from its applications.

The ordinary definition of a field is as follows.† A set of elements forms a field if the elements can be combined by operations called addition and multiplication, subject to the associative, commutative, and distributive laws, as well as by the inverse operations called subtraction and division, the divisor not being the unique element having the additive and multiplicative properties of zero; and and if the resulting sum, product, difference, or quotient is uniquely determined as an element of the set. A field may therefore be defined by the property that *the rational operations of algebra can be performed within the field.*

Under the operation addition, the elements of a field form a *commutative group;* under the operation multiplication, the elements other than zero form a commutative group.

The preceding definition involves numerous redundancies since it includes various properties which can be deduced from a portion of the properties. The present paper gives two definitions free from redundancies. Between the first definition, by means of nine independent postulates, and the second definition, by means of eleven independent postulates, the same contrast exists as between the (second) definition of a group by HUNTINGTON‡ and the definition of a group by MOORE.§ My second definition of a field has two advantages over my first, the greater ease|| in deriving the further properties of a field and the

* Presented to the Society at Evanston September 2, 1902. Received for publication July 21, 1902.

† Compare, MOORE, *Mathematical Papers*, Chicago Congress of 1893; DICKSON, *Linear Groups*, p. 5.

‡ Bulletin, second series, vol. 9 (1902), p. 389.

§ Transactions, vol. 3 (1902), pp. 485–492.

|| To emphasize this point, I have derived the desired properties from the two sets of postulates independently, although either set of postulates is readily derived from the other.

suitableness in testing for the field property a given set of elements and laws of combination. To test by the first definition, one would naturally test 4′ and 4″ (from which 4 follows, but not inversely) and 8′ and 8″ (from which 8 follows, but not inversely), for the reason that x in either 4 or 8 might depend upon both a and b (compare S_3 and S_7 below).

First Definition of a Field.

A set of elements with two rules of combination denoted by $\circ$ and $\square$ is called a *field* if the following nine postulates hold:

1. If a and b belong to the set, then $a \circ b$ belongs to the set.

2. $a \circ b = b \circ a$, whenever $a \circ b$ and $b \circ a$ belong to the set.

3. $(a \circ b) \circ c = a \circ (b \circ c)$, whenever $a \circ b$, $b \circ c$, $(a \circ b) \circ c$, and $a \circ (b \circ c)$ belong to the set.

4. For any two elements a and b of the set, there exists in the set an element x such that $(a \circ x) \circ b = b$.

5. If a and b belong to the set, then $a \square b$ belongs to the set.

6. $a \square b = b \square a$, whenever $a \square b$ and $b \square a$ belong to the set.

7. $(a \square b) \square c = a \square (b \square c)$, whenever $a \square b$, $b \square c$, $(a \square b) \square c$, and $a \square (b \square c)$ belong to the set.

8. For any two elements a and b of the set, such that* $c \square a \neq a$ for at least one element c of the set, there exists in the set an element x such that $(a \square x) \square b = b$.

9. $a \square (b \circ c) = (a \square b) \circ (a \square c)$, whenever $b \circ c$, $a \square b$, $a \square c$, $a \square (b \circ c)$, and $(a \square b) \circ (a \square c)$ belong to the set.

Properties Derived from the Nine Postulates.

10. For any two elements a and b of the set there exists in the set an element y such that $a \circ y = b$.

In view of 4, take x so that $(a \circ x) \circ b = b$. Then $a \circ (x \circ b) = b$ by 3. Then $y \equiv x \circ b$ belongs to the set, by 1, and makes $a \circ y = b$.

11. If $a \circ z = a$ for a particular element a, then $b \circ z = b$ for every element b of the set.

In view of 10, take y so that $a \circ y = b$. Then $y \circ a = b$ by 2. Then $y \circ (a \circ z) = b$ by hypothesis. Hence $(y \circ a) \circ z = b$ by 3, so that $b \circ z = b$.

12. If $a \circ b = a \circ b'$, then $b = b'$.

In view of 10, take y so that $b' \circ y = b$. Then $a \circ (b' \circ y) = a \circ b'$ by

* Another definition is obtained by replacing 8 by the postulate: For any two elements a, b, such that $c \circ a \neq c$ for at least one element c, there exists an element x such that $(a \square x) \square b = b$. In the proofs of independence given below, system S_3 must now be modified.

hypothesis. Then $(a \circ b') \circ y = (a \circ b')$ by 3. Hence $b' \circ y = b'$ by 11, so that $b = b'$.

13. It follows from 10 and 12 that *for any given elements a and b an element y is uniquely determined by* $a \circ y = b$. Hence, by 2, *the same element y is uniquely determined by* $y \circ a = b$.

14. For any two elements a and b such that $c \square a \neq a$ for at least one element c, there exists in the set an element y such that $a \square y = b$.

In view of 8, take x so that $(a \square x) \square b = b$. Then $a \square (x \square b) = b$ by 7. Then $y \equiv x \square b$ belongs to the set, by 5, and makes $a \square y = b$.

15. If $a \square u = a$ for a particular element a and if $c \square a \neq a$ for at least one element c, then $b \square u = b$ for any element b.

In view of 14, take y so that $a \square y = b$. Then $y \square a = b$ by 6. Hence $y \square (a \square u) = b$ by hypothesis. Then $(y \square a) \square u = b$ by 7. Hence $b \square u = b$.

16. If $a \square b = a \square b'$ and $c \square a \neq a$ for at least one element c, then $b = b'$.

Let first $k \square b' \neq b'$ for at least one element k. In view of 14, take y so that $b' \square y = b$. Then $a \square (b' \square y) = a \square b'$ by hypothesis. Then by 7

$$(e) \qquad (a \square b') \square y = (a \square b').$$

If $c \square (a \square b') \neq (a \square b')$ for some element c, then $b' \square y = b'$ follows from (e) by 15, so that $b = b'$. In the contrary case, $c \square (a \square b') = a \square b'$ for every element c. But $c \square (a \square b') = (c \square a) \square b' = (a \square c) \square b'$ by 7 and 6, and the latter equals b' for a suitable value of c by 8. Hence $a \square b' = b'$, so that (e) becomes $b' \square y = b'$, whence $b = b'$.

Similarly, if $k \square b \neq b$ for at least one element k, then $b = b'$.

Finally, if $k \square b' = b'$ and $k \square b = b$ for every element k, we take $k = a$ and apply the hypothesis, and get $b = b'$.

17. We conclude from 14 and 16 that *for any given elements a and b such that* $c \square a \neq a$ *for at least one element c, an element y is uniquely determined by* $a \square y = b$; whence by 6, *the same element y is uniquely determined by* $y \square a = b$.

18. If $c \circ b = c$, then $l \circ (a \square b) = l$ for all elements l and a.

By 9, $(a \square c) \circ (a \square b) = a \square (c \circ b) = a \square c$. Hence $l \circ (a \square b) = l$ by 11.

19. If $c \circ b = c$, then $a \square b = b$ for every element a.

By 18 for $l = c$, $c \circ (a \square b) = c = c \circ b$. Then $a \square b = b$ by 12.

20. If $k \circ (a \square b) = k$ and $c \square a \neq a$ for at least one element c, then $l \circ b = l$ for every element l.

By 19, $x \square (a \square b) = (a \square b)$ for every element x. But

$$x \square (a \square b) = (a \square x) \square b$$

by 6 and 7. In view of 8, take x so that $(a \square x) \square b = b$. Then $b = a \square b$. Applying the hypothesis, $k \circ b = k$. Hence $l \circ b = l$ by 11.

21. If $c \square a = a$ for every c, then $l \circ a = l$ for every l.

By 6, $a \square c = a$. Then by 9 for $b = c$, $a = a \circ a$. Hence $l \circ a = l$ by 11.

Consistency of the Nine Postulates.

There exist sets of elements with two rules of combination $a \circ b$ and $a \square b$ for which the nine postulates hold. We may take as elements all the rational numbers and take $a \circ b = a + b$, $a \square b = a \times b$. Again, we may take as elements $0, 1, 2, \cdots, p - 1$, where p is a prime number, and take $a \circ b$ and $a \square b$ to be the least positive residues modulo p of $a + b$ and $a \times b$ respectively.

Comparison with the Ordinary Definition of a Field.

When expressed in the terminology used in the ordinary definition of a field, the postulates 1–9 and the derived properties 10–21 include all the properties required by the ordinary definition. For comparison we write $a + b$ for $a \circ b$, $a \times b$ for $a \square b$, $b - a$ for the unique element y determined by $a \circ y = y \circ a = b$ (§ 13), b/a for the unique element y determined by $a \square y = y \square a = b$, provided $c \square a \neq a$ for at least one element c (§ 17). By 11, $a - a$, $b - b$, $c - c, \cdots$ all equal the same element z, called a *zero*. Then $a + z = a$ for every a. There is a single zero by 13. By 19, $a \times z = z$ for every a. Hence z has the additive and multiplicative properties of zero. If $c \times a = a$ for every c, then $a = z$ by 21, so that there is a single element having the multiplicative property of zero. Hence the set is a field according to the ordinary definition given in the introduction.

Independence of the Nine Postulates.

For $k = 1, \cdots, 9$ is exhibited a system S_k of elements with rules of combination $a \circ b$ and $a \square b$, such that the kth postulate is not satisfied while the remaining eight postulates are satisfied.

S_1. The set of elements $0, +1, -1$, with $a \circ b = a + b$, $a \square b = a \times b$.

S_2. All positive rational numbers, with $a \circ b = b$, $a \square b = a \times b$.

S_3. All rational numbers, with $a \circ b = -a - b$, $a \square b = a \times b$.

Here 3 fails since $-(-a-b)-c \neq -a-(-b-c)$ in general. Postulate 4 is satisfied if we take $x = 2b - a$.

S_4. All positive rational numbers, with $a \circ b = a + b$, $a \square b = a \times b$.

S_5. The set of all numbers $n\sqrt{2}$ in which n is rational, with $a \circ b = a + b$, $a \square b = a \times b$.

Here $n\sqrt{2} \square m\sqrt{2} = 2mn$ is not in the set unless $m = n = 0$. For 8,

$$(n\sqrt{2} \square x) \square m\sqrt{2} = m\sqrt{2}$$

is satisfied by $x = \frac{1}{2n}\sqrt{2}$ if $n \neq 0$.

S_6. All rational numbers, with $a \circ b = a + b$, $a \square b = b$.

Here 8 holds but has no content, since $c \square a = a$ for every c. [We may also take the totality of quaternions with $a \circ b = a + b$, $a \square b = a \times b$.]

S_7. All complex numbers $a_1\epsilon_1 + a_2\epsilon_2$, where a_1 and a_2 take all real values, positive, negative, or zero, and

$$\epsilon_1^2 = \epsilon_1, \qquad \epsilon_1\epsilon_2 = -\epsilon_2, \qquad \epsilon_2\epsilon_1 = -\epsilon_2, \qquad \epsilon_2^2 = -\epsilon_1,$$

while $a \circ b = a + b$, $a \square b = a \times b$.

Evidently postulates 1, 2, 3, 4 are satisfied; 7 is not satisfied, since

$$(\epsilon_2\epsilon_2)\epsilon_1 = -\epsilon_1^2 = -\epsilon_1, \qquad \epsilon_2(\epsilon_2\epsilon_1) = -\epsilon_2^2 = +\epsilon_1.$$

To show that 5, 6, 8, and 9 are all satisfied, we form the product

$$(a_1\epsilon_1 + a_2\epsilon_2)(b_1\epsilon_1 + b_2\epsilon_2) = (a_1b_1 - a_2b_2)\epsilon_1 + (-a_1b_2 - a_2b_1)\epsilon_2.$$

Hence, if $a = a_1\epsilon_1 + a_2\epsilon_2$ and $b = b_1\epsilon_1 + b_2\epsilon_2$, then $ab = ba$. Given a and c, where a_1 and a_2 are not both zero, we can find b_1 and b_2 so that $ab = c$:

$$b_1 = \frac{a_1c_1 - a_2c_2}{a_1^2 + a_2^2}, \qquad b_2 = \frac{-a_2c_1 - a_1c_2}{a_1^2 + a_2^2}.$$

It follows readily that 8 can be satisfied. Evidently 9 holds.

S_8. All positive and negative integers and zero, with $a \circ b = a + b$ and $a \square b = a \times b$. [We may also take a complete set of residues modulo n, where n is a composite number, $a \circ b$ and $a \square b$ being the residues of $a + b$ and $a \times b$ respectively.]

S_9. All rational numbers, with $a \circ b = a \square b = a + b$. [Again, all positive rational numbers, with $a \circ b = a \square b = a \times b$.]

Second Definition of a Field.

A set of elements with two rules of combination designated $\circ$ and $\square$ is called a field if the following eleven postulates hold: 1, 2, 3, 5, 6, 7, 9, and

4′. There exists in the set an element z such that $z \circ b = b$ for every element b.

4″. If elements z of character 4′ exist, then for some such element z and for every element a, there exists in the set an element x for which $a \circ x = z$.

8′. There exists in the set an element u such that $u \square b = b$ for every element b.

8″. If elements u of character 8′ exist, then for some such element u and for every element a such that $c \square a \neq a$ for at least one element c, there exists an element x for which $a \square x = u$.

Properties Derived From the Eleven Postulates.

22. For any two elements a and b of the set, there exists in the set an element y such that $a \circ y = b$.

By 4″ take x so that $a \circ x = z$. Then $(a \circ x) \circ b = z \circ b = b$. Hence $a \circ (x \circ b) = b$ by 3. Hence $y \equiv x \circ b$ is an element (by 1) which makes $a \circ y = b$.

23. If $a \circ b = a \circ b'$, then $b = b'$.

Take $a \circ a' = z$ by 4″. Then $a' \circ a = z$ by 2. Hence, by 3 and 4′,

$$a' \circ (a \circ b) = (a' \circ a) \circ b = z \circ b = b, \qquad a' \circ (a \circ b') = b', \qquad b = b'.$$

24. Hence, for any given elements a and b, an element y of the set is uniquely determined by $a \circ y = b$, and, by 2, the same element y is uniquely determined by $y \circ a = b$.

25. For any two elements a and b such that $c \square a \neq a$ for at least one element c, there exists in the set an element y such that $a \square y = b$.

By 8″ take x so that $a \square x = u$. Then by 7 and 8′

$$a \square (x \square b) = (a \square x) \square b = u \square b = b.$$

Hence $y \equiv x \square b$ is an element (by 5) which makes $a \square y = b$.

26. If $a \square b = a \square b'$ and $c \square a \neq a$ for at least one c, then $b = b'$.

Take $a \square x = u$ by 8″. Then $x \square a = u$ by 6. Hence, by 7 and 8′,

$$x \square (a \square b) = (x \square a) \square b = u \square b = b, \qquad x \square (a \square b') = b', \qquad b = b'.$$

27. Hence, for any given elements a and b such that $c \square a \neq a$ for at least one element c, an element y of the set is uniquely determined by $a \square y = b$, and by 6, the same element y is uniquely determined by $y \square a = b$.

28. If $z \circ a = a$ for a particular element a, then $z \circ b = b$ for every element b.

By 22 take y so that $a \circ y = b$. Applying 3 and the hypothesis,

$$(z \circ a) \circ y = b, \qquad z \circ (a \circ y) = b, \qquad z \circ b = b.$$

29. If $u \square a = a$ for a particular element a and if $c \square a \neq a$ for at least one element c, then $u \square b = b$ for every element b.

By 25 take y so that $a \square y = b$. Applying 7 and the hypothesis,

$$(u \square a) \square y = b, \qquad u \square (a \square y) = b, \qquad u \square b = b.$$

Properties 18, 19, 20, 21 follow as before, noting in the proof of 20 that 8 can be deduced from 8′ and 8″.

Independence of the Eleven Postulates.

A system Σ_k is exhibited such that the postulate k does not hold while the remaining ten postulates hold. We take

$$\Sigma_1 = S_1, \qquad \Sigma_2 = S_2, \qquad \Sigma_{4'} = S_4, \qquad \Sigma_6 = S_6, \qquad \Sigma_{8''} = S_8, \qquad \Sigma_9 = S_9,$$

the S_i being defined above, and

$\Sigma_{4''}$. All positive rational numbers, together with zero, with $a \circ b = a + b$ and $a \square b = a \times b$.

$\Sigma_{8'}$. The set of elements 0, 2, -2, with $a \circ b$ and $a \square b$ the residues modulo 6 of $a + b$ and $a \times b$ respectively.

Σ_3. The set of elements * z, r, s, with the rules of combination:

$$z \circ a = a \circ z = a, \text{ for any } a, \qquad r \circ s = s \circ r = z, \qquad r \circ r = z, \qquad s \circ s = z,$$

$$r \square a = a \square r = a, \text{ for any } a, \qquad z \square s = s \square z = z, \qquad z \square z = z, \qquad s \square s = r.$$

Evidently 1, 2, 4′, 4″, 5, 6, 8′ and 8″ are satisfied. But 3 fails, since

$$(r \circ r) \circ s = z \circ s = s, \qquad r \circ (r \circ s) = r \circ z = r.$$

Finally, 7 and 9 are evidently satisfied when $a = r$ or $a = z$, and, by trial, when $a = s$.

Σ_5. The set of elements † e and f, with the rules of combination:

$$e \circ e = e, \qquad e \circ f = f, \qquad f \circ e = f, \qquad f \circ f = e,$$

$$e \square e = e, \qquad e \square f = f, \qquad f \square f = e, \qquad f \square e \text{ not in set.}$$

Evidently 1, 2, 3, 4′ and 4″ (with $z = e$), 6, 8′ and 8″ (with $u = e$) all hold, while 5 fails. For $a = e$, 7 holds since $e \square b = b$ for every b; for $a = f$ and $b = e$, the first member of 7 is not in the set; for $a = f$, $b = f$, the second member of 7 is $f \square (f \square c)$ and is in the set neither for $c = e$ nor for $c = f$. For $a = e$, 9 is evident; for $a = f$, the cases $b = e$ and $c = e$ have no content; for $a = b = c = f$, the first member of 9 is $f \square (f \circ f) = f \square e$, not in the set.

* Taking $r = 1$, $z = 0$, $s = -1$, $a \square b = a \times b$, we obtain a multiplicative-field. Hence 7 holds.

† Taking $e = 0$, $f = 1$, $a \circ b = a + b \pmod 2$, we obtain an additive-field. Hence 3 holds.

Σ_7. The set of eight * elements e_{ijk}, the suffixes i, j, k being taken modulo 2, with

$$e_{ijk} \circ e_{rst} = e_{i+r\, j+s\, k+t},$$

$$e_{ijk} \square e_{001} = e_{001} \square e_{ijk} = e_{ijk}, \qquad e_{ijk} \square e_{000} = e_{000} \square e_{ijk} = e_{000},$$

$$e_{010} \square e_{010} = e_{000}, \quad e_{011} \square e_{011} = e_{001}, \quad e_{100} \square e_{100} = e_{010}, \quad e_{101} \square e_{101} = e_{011},$$

$$e_{110} \square e_{110} = e_{010}, \quad e_{111} \square e_{111} = e_{011}, \quad e_{010} \square e_{011} = e_{010}, \quad e_{010} \square e_{100} = e_{011},$$

$$e_{010} \square e_{101} = e_{001}, \quad e_{010} \square e_{110} = e_{011}, \quad e_{010} \square e_{111} = e_{001}, \quad e_{011} \square e_{100} = e_{111},$$

$$e_{011} \square e_{101} = e_{100}, \quad e_{011} \square e_{110} = e_{101}, \quad e_{011} \square e_{111} = e_{110}, \quad e_{100} \square e_{101} = e_{110},$$

$$e_{100} \square e_{110} = e_{001}, \quad e_{100} \square e_{111} = e_{101}, \quad e_{101} \square e_{110} = e_{111}, \quad e_{101} \square e_{111} = e_{010},$$

$$e_{110} \square e_{111} = e_{100},$$

with relations derived from the last fifteen by interchanging the elements in their left members. Since the elements from an additive-field under the operation $\circ$, postulates 1, 2, 3, 4′ and 4″ hold. Evidently 5 and 6 hold; while 7 fails since

$$(e_{010} \square e_{010}) \square e_{111} = e_{000} \square e_{111} = e_{000}, \qquad e_{010} \square (e_{010} \square e_{111}) = e_{010} \square e_{001} = e_{010}.$$

Also 8′ and 8″ (with $u = e_{001}$) hold. Finally, 9 is evidently satisfied if a, b, or c is e_{000}, or if $b = c = e_{001}$. For

$$b = e_{001},\ c = e_{010}; \qquad b = e_{001},\ c = e_{100}; \qquad b = e_{001},\ c = e_{110}; \qquad b = e_{010},\ c = e_{100};$$

formula 9 becomes, respectively,

$$a \square e_{011} = a \circ (a \square e_{010}), \qquad a \square e_{101} = a \circ (a \square e_{100}),$$

$$a \square e_{111} = a \circ (a \square e_{110}), \qquad a \square e_{110} = (a \square e_{010}) \circ (a \square e_{100}).$$

From these follow at once (in view of the simple character of the operation $\circ$) all the remaining cases of 9. In this manner 9 is readily seen to hold.

THE UNIVERSITY OF CHICAGO,
July 19, 1902.

*Smaller sets forming additive-fields with respect to the operation $\circ$ do not lead to a system Σ_7. Thus the p elements e_i, where i is taken modulo p, with $e_i \circ e_j = e_{i+j}$ and $e_i \square a = a \square e_i = a$, for every a and a particular e_i, and with 6 and 9 satisfied, form a *field* if p be prime, and do not satisfy 8″ if p be composite. Likewise one or the other conclusion holds for a set of 4 elements combining under $\circ$ as the marks of the $GF[2^2]$ under addition.