NOTE ON THE DEFINITIONS OF ABSTRACT GROUPS AND FIELDS BY SETS OF INDEPENDENT POSTULATES*

BY

EDWARD V. HUNTINGTON

CONTENTS.

Introduction.

The theory of groups † was first studied in connection with the algebraic solution of equations, the leaders in the early development being LAGRANGE (1770), RUFFINI (1799), CAUCHY (1814), ABEL (1824), and especially GALOIS (1831). The first discussion of the theory from an abstract point of view was by CAYLEY ‡ in 1854, and the earliest explicit sets of postulates for abstract groups were

* Presented to the Society, under a slightly different title, December 30, 1904. Received for publication February 9, 1905.

† The most recent bibliography is given by B. S. EASTON, *The constructive development of group-theory*, Philadelphia, 1902 ; and the most recent text-book is the *Éléments de la théorie des groupes abstraits*, by J. A. DE SÉGUIER, Paris, 1904.

Cf. also G. A. MILLER's two reports on recent progress in group-theory, Bulletin of the American Mathematical Society, vol. 5 (1898-1899), pp. 227–251, and vol. 7 (1900–1901), pp. 121–130.

‡ A. CAYLEY, Philosophical Magazine, vol. 7 (1854), p. 40 ; see also Proceedings of the London Mathematical Society, vol. 9 (1878), p. 126, or American Journal of Mathematics, vol. 1 (1878), p. 51. [Collected Papers, vol. 2, p. 123 ; vol. 10, p. 324, or p. 401.] Cf. W. Dyck, Mathematische Annalen, vol. 20 (1882), p. 1.

given by KRONECKER * in 1870 and WEBER † in 1882. WEBER's definition, as finally formulated, ‡ is substantially as follows:

A. There is a rule of combination among the elements of the given set, such that every two elements, a and b, determine uniquely a third element c, called the result of the composition; in symbols: $ab = c$.

B. The associative law holds throughout the set; that is, $(ab)c = a(bc)$.

C. 1) If $ab = ab'$, then $b = b'$.

2) If $ab = a'b$, then $a = a'$.

D. 1) Given a and c, there is an element b such that $ab = c$.

2) Given b and c, there is an element a such that $ab = c$.

E. In the case of abelian groups, the commutative law also holds; that is $ab = ba$.

WEBER notes that if the group is finite, *D* is a consequence of *A*, *B*, and *C*.

This definition was somewhat simplified by BURNSIDE § in 1897, and, more explicitly, by Professor PIERPONT ‖ in 1900. PIERPONT replaced conditions *C* and *D* by the following:

C'. There exists a unique element 1, called the identity, such that $a1 = 1a = a$ for every element a.

D'. For every element a there exists an element a^{-1}, called the inverse of a, such that $aa^{-1} = a^{-1}a = 1$.

The equivalence of the two definitions is readily established. PIERPONT's definition, like most of the earlier definitions, was stated only for the case of finite groups; but essentially the same definition had been used for groups in general by Professor MOORE in lectures ¶ in 1897.

The earliest discussion of the *independence* of the postulates for abstract groups was, as far as I know, that contained in a paper of my own ** in 1902. I noticed in the first place that WEBER's postulate *C* was deducible from his *A*, *B*, and *D*, †† and further, that by a peculiar wording of the associative law,

* L. KRONECKER, Monatsberichte der königlich preussischen Akademie der Wissenschaften zu Berlin (1870), p. 882.

† H. WEBER, Mathematische Annalen, vol. 20 (1882), p. 302. *Cf.* also G. FROBENIUS in Crelle's Journal für die reine und angewandte Mathematik, vol. 100 (1887), p. 179, and in the Sitzungsberichte der königlich preussischen Akademie der Wissenschaften zu Berlin (1895), p. 163.

‡ H. WEBER, Mathematische Annalen, vol. 43 (1893), p. 521; or *Algebra*, second edition, vol. 2 (1899), p. 3.

§ W. BURNSIDE, *Theory of groups of finite order*, 1897, p. 11.

‖ J. PIERPONT, Annals of Mathematics, ser. 2, vol. 2 (1900–01), p. 47. (From a course of lectures delivered in 1896 at the Buffalo Colloquium of the American Mathematical Society.)

¶ *Cf.* E. H. MOORE, Transactions, vol. 3 (1902), p. 488, footnote.

** E. V. HUNTINGTON, Bulletin of the American Mathematical Society, vol. 8 (1901–02), pp. 296–300, revised in Transactions, vol. 4 (1903), p. 30. See also a second definition, in Bulletin, loc. cit., pp. 388–391, and two corresponding definitions for abelian groups, in Transactions, loc. cit., pp. 27–29.

†† For the case of Abelian groups, cf. § 4, below.

postulate A also could be made redundant. Since postulate A is the fundamental postulate of the whole theory, the resulting definition (comprising only D and a modified form of B) had obvious disadvantages. Revised forms of this definition, however, in which the rule of combination is replaced by a relation, as suggested by Professor BÔCHER* in his address at the St. Louis Congress of 1904, have considerable logical interest, and will be presented in §§ 5–6 of this note.

More convenient definitions by sets of independent postulates were given in the same year (1902) by Professor MOORE.† The first of these definitions is of the type published by PIERPONT, differing from WEBER's definition in the use which it makes of the identity and the inverse elements. A second definition given at the end of the paper is a modification of the first, embodying a further analysis of the identical element, and demanding, in particular, the existence of an "idempotent" element i such that $ii = i$. A note by MOORE on this second definition appears in the present number of the Transactions.

Another modification of MOORE's first definition, reverting more nearly to PIERPONT's original form, has been recently given by Professor DICKSON, and will also be found in this number of the Transactions.

In § 1 of the present note I propose a further modification of the PIERPONT-MOORE type of definition, in the direction indicated by the latter part of MOORE's paper. Although the points of difference are so slight as to seem almost trivial, yet the introduction of postulate 4, demanding explicitly the uniqueness of the identical element, and the "weakened" forms in which postulates 5 and 6 are now stated, will be found very convenient when one has to test a given system for the group property.‡

Closely connected with the theory of groups is the theory of fields, § suggested by GALOIS, and due, in concrete form, to DEDEKIND ‖ in 1871. The word *field* is the English equivalent for DEDEKIND's term *Körper*: KRONECKER's term *Rationalitätsbereich*, ¶ which is often used as a synonym, had originally a some-

*M. BÔCHER, Bulletin of the American Mathematical Society, vol. 11 (1904–05), p. 126, footnote.

†E. H. MOORE, Transactions, vol. 3 (1902), pp. 485–492, revised in the present number of the Transactions, p. 179.

‡Further analysis of the postulates, such as I have attempted in Transactions, vol. 6 (1905), pp. 34–36, does not seem likely to lead to practical advantage, except possibly in the case of the associative law.

§See parts of *Linear Groups, with an exposition of the Galois Field theory*, by L. E. DICKSON, in the TEUBNER series of mathematical text-books, 1901; and parts of the *Éléments de la théorie des groups abstraits*, by J. A. DE SÉQUIER, Paris, 1904. [See review by DICKSON in the Bulletin of the American Mathematical Society, vol. 9 (1904–05), pp. 159–162.]

‖P. G. L. DIRICHLET, *Vorlesungen über Zahlentheorie*, edited, with supplementary material, by R. DEDEKIND; 2d edition (1871), p. 424; 4th edition (1894), p. 452.

¶L. KRONECKER, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, 1882, Crelle, vol. 92 (1882), p. 1; Werke, vol. 2, p. 237. Cf. J. KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grösszen*, 1903, p. 183.

what different meaning. The earliest expositions of the theory from the general or abstract point of view were given independently by WEBER* and by MOORE,† in 1893, WEBER'S definition of an abstract field being substantially as follows:

I. There are two rules of combination among the elements of the given set, the one called addition, and the other multiplication.

II. The set forms a group with respect to addition (see conditions A, B, C, D, above). The result of the composition of two elements is here called their sum $(a+b)$, the identity of the group being called zero (0), and the inverse operation subtraction.

III. If the identity of the additive group is excluded, the remaining elements form a group with respect to multiplication. The result of the composition of two elements is here called their product $(a \times b$, or $a \cdot b$, or $ab)$, the identity being called unity (1), and the inverse operation division (the divisor being different from zero).

IV. Addition and multiplication are both commutative.

V. Addition is distributive with respect to multiplication; that is, $a(b+c) = (ab) + (ac)$.

VI. $a(-b) = -(ab)$.

As consequences of this definition,‡ WEBER proves that $a \times 0 = 0 \times a = 0$ for every a, and that a product cannot be zero unless at least one of its factors is zero; but he makes no attempt to free the definition from redundant statements.

The earliest sets of *independent* postulates for abstract fields were given in 1903 by Professor DICKSON§ and myself;‖ all these sets were natural extensions of the sets of independent postulates that had already been given for groups.

In § 2 of the present note I propose another set of postulates for fields, based on the postulates for groups given in § 1, and possessing similar advantages.

Still other sets will be found in § 4, and in the paper by Professor DICKSON (already referred to) in the present number of the Transactions.

---

* H. WEBER, Mathematische Annalen, vol. 43 (1893), p. 526.

† E. H. MOORE, Mathematical Papers read at the International Mathematical Congress at Chicago in 1893 (published in 1896), p. 210; abstract in the Bulletin of the New York Mathematical Society, vol. 3 (1893–94), p. 75. MOORE'S theorem that every existent finite field is the abstract form of some Galois Field is established in this paper; but the term *Galois Field* as here used must not be confused with the term *Galois'scher Körper*, introduced by DEDEKIND (loc. cit., 2d edition, p. 455).

‡ The most familiar and important example of an infinite field is furnished by the rational numbers, under the operations of ordinary addition and multiplication. In fact, a field may be briefly described as a system in which the rational operations of algebra may all be performed (excluding division by zero). A field may be finite, provided the number of elements (called the order of the field) is a prime or a power of a prime.

§ L. E. DICKSON, Transactions, vol. 4 (1903), pp. 13–20.

‖ E. V. HUNTINGTON, Transactions vol. 4 (1903), pp. 31–37.

§ 1. *A definition of groups and abelian groups.*

As already stated, the definition of abstract groups contained in this section is a modification of the definition given by Professor MOORE in 1902.

We consider a class K, and a rule of combination, subject to the following conditions (the result of combining a and b being denoted by ab):

POSTULATE 1. If a and b are elements of the class, then there is an element c in the class such that $ab = c$; and this element c is uniquely determined by a and b.*

POSTULATE 2. The associative law holds throughout K; that is,

$$(ab)c = a(bc),$$

whenever a, b, c, ab, bc, $(ab)c$, and $a(bc)$ are elements of K.

POSTULATE 3. There is at least one element i such that $ii = i$.

POSTULATE 4. There is not more than one element i such that $ii = i$; that is, if x and y are elements such that $xx = x$ and $yy = y$, then $x = y$.

POSTULATE 5. If there is a unique element i such that $ii = i$, then either $ia = a$ for every element a, or else $ai = a$ for every element a.

POSTULATE 6. If there is a unique element i such that $ii = i$, then for every element a there is either an element a_r such that $aa_r = i$, or else an element a_l such that $a_l a = i$.

From these postulates 1–6 the following theorems can be deduced, the proofs for which will be given in § 7:

Theorem I. If i is the unique element described in postulates 3 and 4, then $ia = ai = a$ for every element a.

Theorem II. If $ab = ab'$, then $b = b'$; if $ab = a'b$, then $a = a'$.

From these theorems we have at once two further theorems, by the aid of postulate 6:

Theorem III. Every element a determines uniquely an element a^{-1} such that $aa^{-1} = a^{-1}a = i$, where i is the element described in postulates 3 and 4.

Theorem IV. Every two elements a and b determine uniquely an element x,

---

* If c were not uniquely determined by a and b, then the expression ab would have to be regarded as a multiple-valued function of a and b, and the assertion: $ab = c$, would mean merely that *one of the values* of ab is equal to c. Similarly, $(ab)c$ would mean the multiple-valued function obtained by combining (ab), itself multiple valued, with the element c; and the equation $(ab)c = a(bc)$ would assert merely that *one* of the values of $(ab)c$ is equal to *one* of the value of $a(bc)$.

With this understanding of the notation, a system which satisfies all the postulates except the last half of (1) may be constructed as follows: Let $K =$ any finite or infinite class which contains a special element X and at least one other element; and define the rule of combination so that if $a \neq b$, ab may have any value within the class; while if $a = b$, $aa = X$.

Hence the second part of postulate 1 is essential to the definition. In fact, it is only the uniqueness of the symbol ab which gives this notation any advantage over the relational notation employed in §§ 5–6.

namely $x = a^{-1}b$, such that $ax = b$; and also an element y, namely $y = ba^{-1}$, such that $ya = b$.

Thus we see that any system which satisfies the postulates 1–6 will be a *group* with respect to the given rule of combination. The element i is the *identity* of the group, and the element a^{-1} is the *inverse of* a.

If we wish to make the group *abelian*, we must add another postulate, namely:

POSTULATE 7 (for abelian groups). The commutative law holds throughout K; that is,

$$ab = ba,$$

whenever a, b, ab, and ba are elements of K.

These seven postulates are independent, as will be shown by the examples constructed in § 3; so that no one of them can be deduced from the remaining six.

If we wish to make the group *finite*, we must add the following postulate:

POSTULATE N (for finite groups). The number of elements in the class is some positive integer, n.

After the introduction of this postulate N, postulates 3 and 6 become redundant (see § 7), so that *the five postulates*

$$1,\ 2,\ 4,\ 5,\ \textit{and}\ N$$

are sufficient for finite groups. The independence of these postulates, when $n > 2$, is established in § 3.

§ 2. *A definition of fields.*

The following set of postulates for abstract fields is suggested immediately by the postulates given in § 1 for groups.

We consider a class K, and two rules of combination, called addition and multiplication, subject to the following conditions ($A1 - A6$, $M1 - M4$, $M6$, $M7$, and D):*

POSTULATE $A1$. If a and b are elements of the class, then their "sum" $a + b$, is an element of the class, and is uniquely determined by a and b.

POSTULATE $A2$. The associative law for addition holds throughout the class:

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

POSTULATE $A3$. There is at least one element z such that $z + z = z$.

POSTULATE $A4$. There is not more than one element z such that $z + z = z$.

POSTULATE $A5$. If there is a unique element z such that $z + z = z$, then either $z + a = a$ for every element a, or else $a + z = a$ for every element a.

* The letters A and M in the designation of the postulates are intended to suggest addition and multiplication respectively, while D indicates the distributive law for addition with respect to multiplication.

POSTULATE $A6$. If there is a unique element z such that $z + z = z$, then for every element a there is either an element a_r' such that $a + a_r' = z$, or else an element a_l' such that $a_l' + a = z$.

From these postulates $A1$–$A6$ we have at once, by § 1, the following theorem:

Theorem 1. *The class K is a group with respect to addition.*

The identity, z, of this group, is called the *zero-element* of the field, and is denoted by 0; while the inverse of an element a is here called the *negative of* a, and is denoted by $-a$.

POSTULATE $M1$. If a and b are elements of the class, then their "product," $a \times b$ (or $a \cdot b$, or ab), is an element of the class, and is uniquely determined by a and b.

POSTULATE $M2$. The associative law for multiplication holds throughout the class:

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

POSTULATE $M3$. There is at least one element u such that $u \times u = u$ and $u + u \neq u$.

POSTULATE $M4$. There is not more than one element u such that $u \times u = u$ and $u + u \neq u$.

Lemma $M5$. If there is a unique element u such that $u \times u = u$ and $u + u \neq u$, then either $u \times a = a$ for every element a, or else $a \times u = a$ for every element a.

This lemma $M5$ is not included in the list of postulates, since it will prove to be deducible from $A1$–$A6$, $M1$–$M4$, $M6$, $M7$, and D (see § 7); it is assumed for the moment, however, as are also lemmas $M7'$ and D', below, in order to show exactly how much of the postulates $M7$ and D is required for the proof of theorem 3.

POSTULATE $M6$. If there is a unique element u such that $u \times u = u$ and $u + u \neq u$, then for every element a, provided $a + a \neq a$, there is either an element a_r'' such that $a \times a_r'' = u$, or else an element a_l'' such that $a_l'' \times a = u$.

Lemma $M7'$. If 0 is the zero-element of the system (theorem 1), and u the element in postulates $M3$–$M4$, then $0 \times u = u \times 0$.

This lemma will appear as a special case of postulate $M7$.

Lemma D'. If 0 is the zero-element of the system (theorem 1), then either $0 \times a = 0$ for every element a, or else $a \times 0 = 0$ for every element a.

This lemma will prove to be an immediate consequence of postulate D, in view of $A3$–$A4$, taking $b = c = 0$.

The propositions $A1$–$A6$, $M1$–$M6$, $M7'$, and D' are now sufficient (see § 7) to establish theorems 2–3, without requiring the more general postulates $M7$ and D; and until these postulates $M7$ and D are introduced, the fourteen propositions just mentioned are all independent (see § 3).

The theorems in question concern the group-property of the field with regard to multiplication, as follows:

Theorem 2. $a \times 0 = 0 \times a = 0$, *for every element* a.

Theorem 3. *If the zero-element is excluded, the remaining elements form a group with respect to multiplication.*

The identity, u, of this group is called the *unit-element* of the field and is denoted by 1; while the inverse of any element a in this group is called the *reciprocal of* a and is denoted by $1/a$.

The remaining postulates for a field are the following:

POSTULATE $M7$. The commutative law for multiplication holds throughout the class; that is,

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

POSTULATE D. Either the left-hand or else the right-hand distributive law for multiplication with respect to addition holds throughout the class; that is, either

$$a \times (b + c) = (a \times b) + (a \times c),$$

or else

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

From $M7$ and D, in view of $A1$ and $M1$, we have at once:

Theorem 4. *Multiplication is commutative and distributive.*

To show that $a \times (-b) = -(a \times b)$, we have only to put $b + c = 0$ in postulate D, using $M7$ and theorem 2.

Finally, by a method due to HILBERT (see § 7), we can deduce the commutative law for addition:

Theorem $A7$. *Throughout the class,* $a + b = b + a$.

Thus we see that any system $(K, +, \times)$ which satisfies the postulates $A1$–$A6$, $M1$–$M4$, $M6$, $M7$, and D, will be a field with respect to the rules of combination $+$ and $\times$.

All these postulates are independent, as will be shown by the examples constructed in § 3.

§ 3. *Proof of the independence of the postulates of* §§ 1–2.

In this section, the symbols $+$, $\times$, 0, and 1 are used only in their ordinary arithmetical meanings, the general operations of "addition" and "multiplication" being denoted by $\oplus$ and $\odot$, and the "zero-" and "unit-" elements by z and u respectively. *

The independence of the thirteen postulates of § 2, for abstract fields, is

* The symbols $\oplus$ and $\odot$ were first used in this connection in Transactions, vol. 4 (1903), p. 31; cf. vol. 5 (1904), p. 292, and vol. 6 (1905), pp. 19 and 22.

established by the existence of the following systems $(K, \oplus, \odot)$, each of which satisfies all the other postulates, but not the one for which it is numbered.

The first six of these systems, together with any non-abelian group, serve also to show the independence of the seven postulates of § 1 for abstract groups.

---

*For A*1. $K =$ all real numbers; $a \oplus b = a + b$ when a or b or $a + b$ is zero, otherwise $a \oplus b$ not in the class; $a \odot b = a \times b$.

*For A*2. $K =$ all real numbers; $a \oplus b = a + b$ except that $a \oplus a = 0$; $a \odot b = a \times b$.

*For A*3. $K =$ all positive real numbers; $a \oplus b = a + b$; $a \odot b = a \times b$.

*For A*4. $K =$ all real numbers, together with an extra element ∞; $a \oplus b = a + b$ and $a \odot b = a \times b$, understanding that $\infty \oplus \infty = \infty$, $\infty \oplus a = a \oplus \infty = \infty$, and $a \odot \infty = \infty$, $\infty \odot a = a \odot \infty = \infty$. Here $z = 0$ or ∞ and $u = 1$.

*For A*5. $K =$ all real numbers; $a \oplus b = 0$; $a \odot b = a \times b$.

*For A*6. $K =$ all positive real numbers with 0; $a \oplus b = a + b$; $a \odot b = a \times b$.

*For M*1. $K =$ all real numbers; $a \oplus b = a + b$; $a \odot b = a \times b$ when a or b is 1 or when $a \times b$ is 1 or 0, otherwise $a \odot b$ not in the class.

*For M*2.* $K =$ all complex numbers of the form $(\alpha, \beta, \gamma) = \alpha + \beta i + \gamma j$, where α, β, and γ, are real numbers; $\oplus = +$; $\odot = \times$, the multiplication-table for the three principal units being the following:

$\odot$	1	i	j
1	1	i	j
i	i	-1	1
j	j	1	-2

Here $z = (0, 0, 0)$ and $u = (1, 0, 0)$. To find the reciprocal, (X, Y, Z) of (α, β, γ), take $X = \alpha/\Delta$, $Y = -\beta/\Delta$, $Z = -\gamma/\Delta$, where $\Delta = \alpha^2 + (\beta - \gamma)^2 + \gamma^2$. The associative law fails, since $(ii)j \neq i(ij)$.

*For M*3. $K =$ all even integers (positive, negative, and zero); $\oplus = +$; $\odot = \times$.

*For M*4. $K =$ all complex numbers (α, β), where α and β are real; $\oplus = +$; $(\alpha_1, \beta_1) \odot (\alpha_2, \beta_2) = (\alpha_1\alpha_2, \beta_1\alpha_2 + \alpha_1\beta_2 + \beta_1\beta_2)$.

Here $z = (0, 0)$, and $u = (1, 0)$ or $(0, 1)$ or $(1, -1)$.

*For M*6. $K =$ all integers; $\oplus = +$; $\odot = \times$. The following system may also be used: $K =$ all complex numbers (α, β), where α and β are real; $\oplus = +$; $(\alpha_1, \beta_1) \odot (\alpha_2, \beta_2) = (\alpha_1\alpha_2, \beta_1\alpha_2 + \alpha_1\beta_2)$.

* This system was suggested to me by Professor DICKSON.

For M7. $K =$ all quaternions, $a + \beta i + \gamma j + \delta k$, where a, β, γ, and δ are real numbers; $\oplus = +$; $\odot = \times$.

For D. $K =$ all integers; $a \oplus b = a + b$; $0 \odot a = a \odot 0 = 0$; when $a \neq 0$ and $b \neq 0$, $a \odot b$ is defined as follows: let $A = a$ or $a + 1$, according as a is positive or negative, and let $B = b$ or $b + 1$, according as b is positive or negative; then $a \odot b = A + B$ when $A + B$ is positive, and $a \odot b = A + B - 1$ when $A + B$ is negative or zero.

The independence of the postulates is thus established. Since each of the systems is infinite, the postulates will remain independent even when we add the demand that the group or field shall be infinite.

In regard to the lemmas $M5$, and $M7'$, and D', we notice that all the systems just given satisfy them; further, the following systems show that they cannot be proved without the aid of $M7$ or D.

For M5 and D. Let $K =$ all real numbers; $\oplus = +$; $a \odot b = 1$, except that $a \odot 0 = 0 \odot a = 0$.

For M7' and M7. $K =$ a class of two elements, 0 and 1, with $a \oplus 0 = 0 \oplus a = a$, $1 \oplus 1 = 0$, and $a \odot b = a$; or the same system, with $a \odot b = b$. No system of this kind exists that has more than two elements.

For D' and D. Let $K =$ all real numbers; $\oplus = +$; $a \odot b = a + b - 1$.

It remains to prove the independence of the postulates 1, 2, 4, 5, N, for finite groups* of order $n > 2$ (§1).† To show the independence for the first four cases, let $K =$ the class of n integers from 0 to $n - 1$ inclusive, and define the rule of combination as follows:

For 1. $a \oplus b = 0$ when $a + b = n$, and $a \oplus 0 = 0 \oplus a = a$; otherwise $a \oplus b$ not in the class.

For 2. $a \oplus b = 0$ except that $a \oplus 0 = 0 \oplus a = a$.

For 4. $a \oplus b = 0$ except that $a \oplus a = a$.

For 5. $a \oplus b = 0$.

To show the independence of postulate N, consider any infinite group, or an empty class K.

---

* I have not attempted to get a set of independent postulates for *finite fields*. All that has been done in this direction will be found in Professor DICKSON'S paper in the present number of the Transactions.

† If $n = 1$, postulate 1 is sufficient; if $n = 2$, postulates 1, 2, 4, 5 are independent, the non-group systems for 1 and 2 being the following:

	0	1
0	1	X
1	X	0

and

	0	1
0	1	1
1	1	0

In regard to the independence of the commutative law in the case of finite groups of order n, Professor DICKSON has just proved the following interesting theorem: Let $n = A \cdot B \cdot C \cdots$, where $A = a^\alpha$, $B = b^\beta$, $C = c^\gamma$, $\cdots$, the a, b, c, $\cdots$, being distinct primes; then

(1) if any one of the exponents α, β, γ, $\cdots$ is greater than 2, there is a non-abelian group of order n; and

(2) if any one of the expressions $A-1$, $B-1$, $C-1$, $\cdots$ is divisible by any one of the primes a, b, c, $\cdots$, there is a non-abelian group of order n.

If neither of these conditions is satisfied, every group of order n is abelian.

§ 4. *A shorter definition of a field.*

This section contains a shorter definition of a field, by means of ten postulates, the independence of which, however, is not completely established.*

POSTULATES 1–7. The same as $A1$, $A2$, $A7$; $M1$, $M2$, $M7$; D. (See § 2.)

POSTULATE 8. Given a and b, there is an x such that $a + x = b$.

POSTULATE 9. Given a and b, and $a+a \neq a$, there is a y such that $a \times y = b$.

POSTULATE 10. There are at least two elements in the class.

Five of these postulates, namely 1, 2, 3, 8, and 10, constitute a definition of abelian groups; but for the purpose of testing a given system, neither of these shorter definitions is so convenient as those given in § 1.

The following theorems, proved in § 7, show that any system which satisfies the postulates 1–10 is a field with respect to $+$ and $\times$:

Theorem I. There is a unique element 0 such that $0 + a = a + 0 = a$ for every element a. (From 1, 2, 3, 8, 10.)

Theorem II. If $a + b = a + b'$, then $b = b'$. (From 1, 2, 3, 8, 10.)

Theorem III. There is a unique element 1, different from 0, such that $1a = a1 = a$ for every element a.

Theorem IV. If $a \times b = a \times b'$, and $a \neq 0$, then $b = b'$.

Theorem V. If $a \neq 0$ and $b \neq 0$, then $a \times b \neq 0$.

The independence of all the postulates, except 1 and 4, is established by the following systems:

[*For* 1 *and* 8. K = all real numbers; $a \oplus b = a + b$ when a and b are integers, otherwise $a \oplus b$ not in the class; $\odot = \times$.]

For 2. K = all real numbers; $a \oplus b = 2(a + b)$; $\odot = \times$.

For 3. K = all real numbers; $a \oplus b = b$; $\odot = \times$.

[*For* 4 *and* 9. K = all real numbers; $\oplus = +$; $a \odot b = a \times b$ when a and b are rational, otherwise $a \odot b$ not in the class.]

For 5. K = all complex numbers (α, β), where α and β are real; $\oplus = +$; $(\alpha_1, \beta_1) \odot (\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\beta_2, -\alpha_1\beta_2 - \alpha_2\beta_1)$.

* Compare a similar set of thirteen postulates, all independent, in a paper of mine on complex algebra, in the present number of the Transactions.

In the geometrical representation of this system, $\odot$ is the ordinary multiplication followed by reflection in the axis of reals.

For 6. $K =$ all real numbers; $\oplus = +$; $a \odot b = b$.

For 7. $K =$ all real numbers; $\oplus = +$; $\odot = +$.

For 8. $K =$ all positive real numbers; $\oplus = +$; $\odot = \times$.

For 9. $K =$ all integers; $\oplus = +$; $\odot = \times$.

For 10. $K =$ an empty class; or $K =$ a class containing a single element a, with $a \oplus a = a$ and $a \odot a = a$.

The independence of postulates 1 and 4 is still an open question, unless postulates 8 and 9 are artificially "weakened".

§§ 5–6. *Definitions of groups in terms of a triadic relation, R.*

The sets of postulates for abstract groups given in §§ 5–6 are modifications of the writer's first definition of 1902 (loc. cit.), expressed in terms of the triadic relation suggested by Professor BÔCHER (loc. cit.).

The fundamental concepts are here a *class*, K, and a *relation*, R; instead of writing "$ab = c$," which means "the combination of a and b equals c," we write "$R(abc)$," which means "the three elements a, b, and c satisfy the given relation R."

The use of this notation suggested the more explicit division of the first postulate of § 1 into its two component statements, namely postulates IV in § 5, and postulate IV′ in § 6.

§ 5.

One set of postulates for which, however, the proofs of independence are not complete, is the following (a, b, c, etc. denoting elements of K):

POSTULATE I. The class K is not an empty class.

POSTULATE II. Given b and c there is an a such that $R(abc)$.

POSTULATE III. Given a and c there is a b such that $R(abc)$.

POSTULATE IV. Given a and b there is a c such that $R(abc)$.

POSTULATE V. If $R(abp)$, $R(pcM)$, $R(bcq)$, and $R(aqN)$, then $M = N$.

From these postulates I–V the following theorems are deduced (see § 7):

Theorem 1. If $R(abc)$ and $R(a'bc)$, then $a = a'$.

Theorem 2. If $R(abc)$ and $R(ab'c)$, then $b = b'$.

Theorem 3. If $R(abc)$ and $R(abc')$, then $c = c'$.

If now we write $ab = c$ in place of $R(abc)$, postulate V gives us the associative law: $(ab)c = (p)c = M$; $a(bc) = a(q) = N$; and all the conditions in WEBER's definition of a group are clearly satisfied.

The independence of all the postulates except IV is established by the systems used in § 6; but the question of the independence or deducibility of postulate IV is undecided.

§ 6.

Another set of postulates, less symmetrical than that given in § 5, but admitting complete proofs of independence, is the following:

POSTULATES I–III. The same as in § 5.

POSTULATE IV′. If $R(abc)$ and $R(abc')$, then $c = c'$.

POSTULATE V′. Either (1): If $R(abp)$, $R(bcq)$, and $R(pcM)$, then $R(aqM)$; or else (2): If $R(abp)$, $R(bcq)$, and $R(aqN)$, then $R(pcN)$.

From these postulates we can prove (see § 7) the theorems 1–2 of § 5, and also

Theorem 3′. Given a and b there is a c such that $R(abc)$.

Hence the two definitions are clearly equivalent.

The proofs of independence are as follows:

For I. $K =$ an empty class.

For II–III. $K =$ any class of more than two elements; for II, let $R(abc)$ mean $b = c$; for III, let $R(abc)$ mean $a = c$.

For IV′. $K =$ any class of more than two elements, with $R(abc)$ true for all values of a, b, and c.

For V′. $K =$ all real (or all rational) numbers, with $R(abc)$ signifying $a + b = 2c$; or again, $K =$ the n positive integers ($n > 2$) from 0 to $n - 1$ inclusive, with $R(abc)$ holding whenever $c = n - s$, where s is congruent to $a + b$ modulo n. In this last system, $(11)2 \neq 1(12)$.

It may be noticed that the postulates I–III, IV, and V′ are independent,* but not sufficient to define a group, as witness the systems in which $R(abc)$ is always true.

The postulates I–III, IV′, and V are likewise independent, but their sufficiency is still an open question.

§ 7. *Proofs of theorems in the preceding sections.*

To avoid interruption in reading, a number of theorems in the preceding sections have been stated without proof; the requisite demonstrations are here supplied.

In § 1: *Proof of theorem* I. If i is the element described in postulates 3 and 4, we have the following lemmas:

Lemma 1. If $ab = i$, then $ba = i$. (By 1–5.) For, if $ab = i$, then $(ba)(ba) = b(ab)a = bia = ba$; whence $ba = i$, by 4.

Lemma 2. For every element a there is at least one element α such that $a\alpha = \alpha a = i$. (By postulate 6 and lemma 1.)

The proof of the main theorem is then as follows: Suppose $ia = a$ for every element a, and take α so that $a\alpha = \alpha a = i$; then

$$ai = i(ai) = i[a(\alpha a)] = i[(a\alpha)a] = i(ia) = (ii)a = ia = a.$$

*To show the independence of IV in this set, let $R(abc)$ signify $a = b$.

Similarly, if we suppose $ai = a$ for every element a, then

$$ia = (ia)i = [(a\alpha)a]\,i = [a(\alpha a)]\,i = (ai)i = a(ii) = ai = a.$$

In § 1: *Proof of theorem* II. By lemma 2, take α so that $\alpha a = i$, and β so that $b\beta = i$. Then if $ab = ab'$,

$$b = ib = (\alpha a)b = \alpha(ab) = \alpha(ab') = (\alpha a)b' = ib' = b';$$

and similarly, if $ab = a'b$,

$$a = ai = a(b\beta) = (ab)\beta = (a'b)\beta = a'(b\beta) = a'i = a'.$$

In § 1: *Proof of postulates* 3 *and* 6 *for finite groups.* (The proof of 3 depends merely on 1, 2, and N; that for 6 requires 1, 2, 4, 5, and N.)

Let a be any element, and form the sequence of elements

$$a_1 = aa,\ a_2 = a_1a_1,\ a_3 = a_2a_2,\ \cdots,\ a_{k+1} = a_ka_k.$$

Since the class is finite, this sequence must eventually contain repetitions; that is, there must be indices p and $p+q$ such that $a_p = a_{p+q}$. The element

$$x = a_pa_{p+1}a_{p+2}\cdots a_{p+q-1}$$

will then be such that $xx = x$, which establishes postulate 3. *

Now this element x is simply the combination of a certain number, say m, † of the a's:

$$aaa\cdots a = i;$$

hence the combination of $m-1$ of the a's will be an element a' such that $aa' = i$, which establishes postulate 6.

In § 2: *Proof* ‡ *of lemma* $M5$.

a) $a\times 0 = 0$. (From $A1$, $A3$–$A4$, $M1$, $M7$, D.) For,

$$a\times 0 = a\times(0+0) = (a\times 0) + (a\times 0),$$

whence $a\times 0 = 0$, by $A4$.

b) If $u\times x = 0$, then $x = 0$. (From $A1$, $A2$–$A4$, $M1$–$M4$, $M6$–$M7$, D.) For suppose $x \neq 0$, and take x'' by $M6$ so that $x''\times x = u$. Then by a), $u = u\times u = u\times(x\times x'') = (u\times x)\times x'' = 0\times x'' = 0$, which is impossible.

c) $a\times(b-c) = (a\times b) - (a\times c)$. (From $A1$–$A6$, $M1$–$M4$, $M6$–$M7$, D.) For, $a\times(-c) + a\times c = a\times(-c+c) = a\times 0 = 0$, whence

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

* This proof for 3, which suggested the proof for 6, is taken from the paper by E. H. MOORE, loc. cit. (1902), p. 490.

† Here $m = 2^p(2^q-1)$.

‡ I am indebted to Mr. G. D. BIRKHOFF for this demonstration.

d) If $u \times a = x$, then $u \times x = x$. (From $M1$–$M4$.) For,

$$u \times x = u \times (u \times a) = (u \times u) \times a = u \times a = x.$$

From *c*) and *d*) we can now prove the lemma, as follows: Let $u \times a = x$; then $u \times (a - x) = (u \times a) - (u \times x) = x - x = 0$, whence $a - x = 0$, or $x = a$.

In § 2: *Proof of theorem* 2. (The proof depends on $A3$–$A4$, $M1$–$M5$, $M7'$ and D', but not on $M6$.)

If the first part of D' is true, $0 \times a = 0$ for every element a. Then $(a \times 0) \times (a \times 0) = a \times (0 \times a) \times 0 = a \times 0 \times 0 = a \times 0$, whence, by $M4$, $a \times 0 =$ either 0 or u.

But the second alternative, $a \times 0 = u$, must be rejected, in view of $M7'$. For, suppose $a \times 0 = u$ for any particular value of a. Then $u \times c = (a \times 0) \times c = a \times (0 \times c) = a \times 0 = u$, for every element c, so that first half of $M5$ cannot be true. Therefore, by the second half of $M5$, $c \times u = c$ for every element c. Then, for every c, $c \times c = (c \times u) \times c = c \times (u \times c) = c \times u = c$, whence, by $M4$, every c must be either 0 or u. But if 0 and u are the only elements in the class, then $u \times 0 = 0 \times u$, by $M7'$, or $u \times 0 = 0$.

Therefore $a \times 0 = 0$ for all values of a.

If the second part of D' is true, instead of the first part, the theorem is proved in a similar way.

In § 2: *Proof of theorem* 3.

(1°) If $a \times b = u$, then $b \times a = u$. For, if $a \times b = u$, then $(b \times a) \times (b \times a) = b \times (a \times b) \times a = b \times u \times a = b \times a$, whence, by $M4$, $b \times a$ is either u or 0. But it cannot be 0, since if it were we should have $u \times u = (a \times b) \times (a \times b) = a \times (b \times a) \times b = a \times 0 \times b = 0$ (by theorem 2), which is impossible by $M5$.

(2°) For every element a, provided $a \neq 0$, there is at least one element α such that $a \times \alpha = \alpha \times a = u$ [by (1°) and $M6$]; and any such element α will be $\neq 0$ when $a \neq 0$ [by theorem 2, since $0 \neq u$].

(3°) If $a \neq 0$, then $u \times a = a \times u = a$. [This follows from (1°) and (2°), as in the proof of theorem I in § 1.]

(4°) If $a \neq 0$ and $b \neq 0$, then $a \times b \neq 0$. For, suppose $a \times b = 0$ and $a \neq 0$; then taking α so that $\alpha \times a = u$ we have

$$b = u \times b = (\alpha \times a) \times b = \alpha \times (a \times b) = \alpha \times 0 = 0.$$

Thus all the conditions for a group (see § 1) are satisfied.

In § 2: *Proof* of theorem A7*. (The proof depends on $A1$–$A6$, $M1$–$M6$,

*D. HILBERT, *Über den Zahlbegriff*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 8 (1899–1900), p. 183.

and both parts of D). Since the system is a group with respect to addition, we know that from $a + b = a + b'$ follows $b = b'$, and from $a + b = a' + b$ follows $a = a'$ (theorem 2, § 1). By D, in view of $M7$, we have

$$(a + b) \times (1 + 1) = a \times (1 + 1) + b \times (1 + 1) = a + a + b + b,$$

$$= (a + b) \times 1 + (a + b) \times 1 = a + b + a + b.$$

Therefore $a + a + b = a + b + a$, and hence $a + b = b + a$.

In § 4: *Proof of theorems* I–V.

I. Let c be any fixed element and a any other element. Take z so that $c + z = c$, and x so that $x + c = a$. Then $a+z = (x+c) + z = x+(c + z) = a$. Further, if $a + z_1 = a$ for every a, and also $a + z_2 = a$ for every a, then $z_2 + z_1 = z_2$ and $z_1 + z_2 = z_1$, whence by postulate 3, $z_1 = z_2 = 0$.

II. Take x so that $x+a=0$; then $b=0+b=x+a+b=x+a+b'=0+b'=b'$.

III. Let c be any fixed element not 0, and a any element not 0. Take u so that $cu = c$ and y so that $yc = a$. Then $au = (yc)u = y(cu) = yc = a$.

IV. Take y so that $ya = u$; then $b = ub = yab = yab' = yb' = b'$.

V. Suppose $ab = 0$ and $a \neq 0$, and take y so that $ya = 1$. Then $b = 1b = yab = y0 = 0$.

In § 5: *Proof of theorem* 1. Given $R(abc)$ and $R(a'bc)$.

Take z and x so that $R(za'a)$ and $R(zcx)$; and y so that $R(cya')$. Then from $R(za'a)$, $R(abc)$, $R(a'bc)$, $R(zcx)$, follows $c = x$; and from $R(zcc)$, $R(cya')$, $R(cya')$, $R(za'a)$, follows $a' = a$.

In § 5: *Proof of theorem* 2. Given $R(abc)$ and $R(ab'c)$.

Take z and x so that $R(b'zb)$ and $R(czx)$; and y so that $R(ycb')$. Then from $R(ab'c)$, $R(czx)$, $R(b'zb)$, $R(abc)$, follows $c = x$; and from $R(ycb')$, $R(b'zb)$, $R(czc)$, $R(ycb')$, follows $b = b'$.

In § 5: *Proofs of theorem* 3. Given $R(abc)$ and $R(abc')$.

First proof (using only II, IV, and V): Take x, β, and y so that $R(xab)$, $R(ax\beta)$, and $R(\beta ay)$. Then from $R(ax\beta)$, $R(\beta ay)$, $R(xab)$, $\left\{\begin{smallmatrix} R(abc) \\ R(abc') \end{smallmatrix}\right\}$, follows $\left\{\begin{smallmatrix} y=c \\ y=c' \end{smallmatrix}\right\}$.

Second proof (using only III, IV, and V): Take x, α, and y so that $R(bx\alpha)$, $R(xb\alpha)$, and $R(b\alpha y)$. Then from $R(bx\alpha)$, $\left\{\begin{smallmatrix} R(abc) \\ R(abc') \end{smallmatrix}\right\}$, $R(xb\alpha)$, $R(b\alpha y)$, follows $\left\{\begin{smallmatrix} y=c \\ y=c' \end{smallmatrix}\right\}$. In either case, $c = c'$.

In § 6: *Proof of theorems* 1–2. In order to show that either half of postulate V' is sufficient, the proof is divided into four steps, (*a–d*):

a) Proof of theorem 1, using $V'(1)$: Given $R(abc)$ and $R(a'bc)$: to prove, $a = a'$. Take z so that $R(za'a)$ and y so that $R(cya')$. From $R(za'a)$,

$R(a'bc)$, $R(abc)$, follows $R(zcc)$; and from $R(zcc)$, $R(cya')$, $R(cya')$, follows $R(za'a')$. Hence, from $R(za'a)$ and $R(za'a')$, we have $a = a'$.

b) Proof of $V'(2)$ from $V'(1)$ and theorem 1: Given, $R(abp)$, $R(bcq)$, and $R(aqN)$. Take P so that $R(PcN)$ and A so that $R(AbP)$. Then from $R(AbP)$, $R(bcq)$, $R(PcN)$, follows $R(AqN)$. From $R(AqN)$ and $R(aqN)$, we have $A = a$; and from $R(abP)$ and $R(abp)$ we have $P = p$. Hence $R(pcN)$.

c) Proof of theorem 2, using $V'(2)$: Given, $R(abc)$ and $R(ab'c)$; to prove $b = b'$. Take z so that $R(bzb')$ and x so that $R(xcb)$. From $R(abc)$, $R(bzb')$, $R(ab'c)$, follows $R(czc)$; and from $R(xcb)$, $R(czc)$, $R(xcb)$, follows $R(bzb)$. Hence, from $R(bzb)$ and $R(bzb')$, we have $b = b'$.

d) Proof of $V'(1)$ from $V'(2)$ and theorem 2: Given, $R(abp)$, $R(bcq)$, and $R(pcM)$. Take Q so that $R(aQM)$, and C so that $R(bCQ)$. Then from $R(abp)$, $R(bCQ)$, $R(aQM)$, follows $R(pCM)$. From $R(pCM)$ and $R(pcM)$ we have $C = c$; and from $R(bcQ)$ and $R(bcq)$ we have $Q = q$. Hence $R(aqM)$.

Thus from either half of postulate V' we can prove the other half, and hence both the theorems 1–2.

In § 6: *Proof of theorem* 3'. Given a and b; take z so that $R(aza)$, b' so that $R(bb'z)$, and c so that $R(cb'a)$. Then c is the required element such that $R(abc)$. For, take β so that $R(a\beta c)$ and β' so that $R(\beta\beta'z)$. Then from $R(a\beta c)$, $R(\beta\beta'z)$, $R(aza)$, follows $R(c\beta'a)$, by $V'(2)$. From $R(c\beta'a)$ and $R(cb'a)$ we have $\beta' = b'$, by theorem 2; and from $R(\beta b'z)$ and $R(bb'z)$ we have $\beta = b$, by theorem 1. Hence $R(abc)$.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.