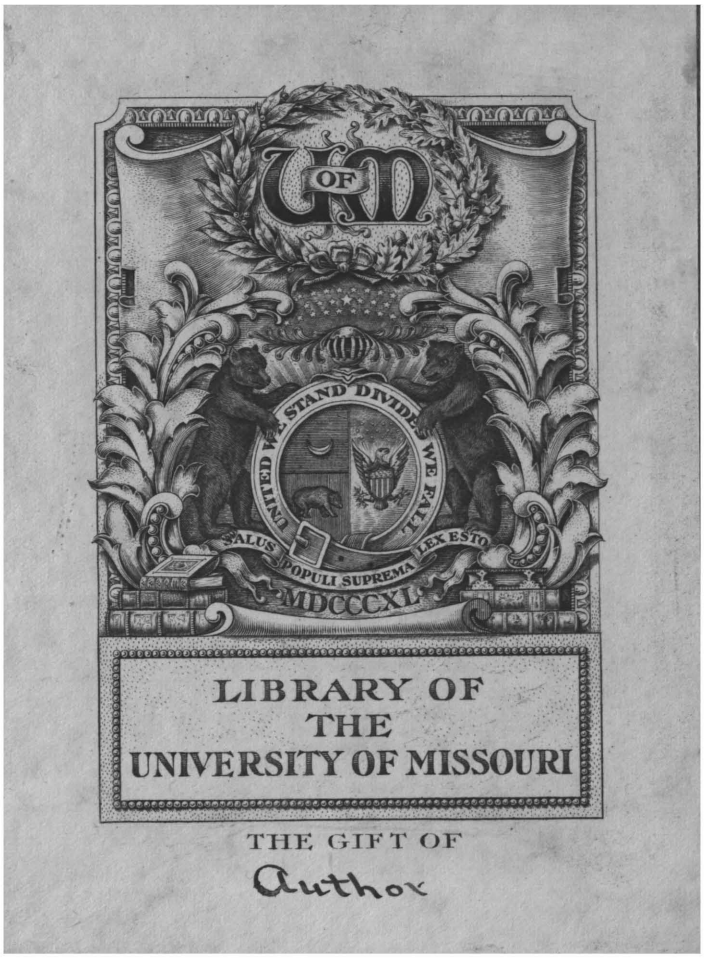

1906

DEFINITION OF IMPROPER GROUPS BY MEANS OF AXIOMS.

A Dissertation.

Respectfully submitted to the Graduate Conference of the University of Missouri, in partial satisfaction of the requirements for the degree of Master of Arts.

BY

W. A. HURWITZ.

INTRODUCTION. ASSEMBLAGES, SETS, AND FIELDS.

(2)

Introduction.

1. If we suppose given, as a principle of classification, some statement, such that its truth or falsehood with respect to every object in the universe is conceivably determinable, an assemblage is said to be defined. Every object in the universe, with respect to which the statement is true, is said to belong to the assemblage, or to be an element of the assemblage.

2. There may be supposed given a rule of combination, by which naming of any two objects in the universe, in a definite order, uniquely* determines some object of the universe. This object will be called the combination, or frequently the product of the two objects which determine it.

3. These two ideas may be combined; any assemblage with which there is associated a rule of combination will be called a combinatorial set, or mor briefly, a set.

The rule of combination may be conceivably pre-defined in such a case for every pair of objects in the universe. Or the rule may be pre-defined only for elements of the assemblage, or for any other selectionof objects. In such cases, the convention will be made, that the combination of two objects, for which the rule is not defined, may be considered anything whatever, according

*But see Chapter I., #6, Art.4.

to the demands of the problem in hand, with the understanding that in any one discussion, it is to be uniquely determined for all cases needed.

4. If the association of the assemblage and the rule of combination is such that the combination of two elements of the set is always an element of the set, the set will be called an abstract field, or simply a field.

The elements of such sets as are to be discussed here will generally be denoted by letters of the alphabet. The rule of combination of two elements will be denoted either by the sign O , placed between them, or by the omission of sign, when there is no ambiguity.

5. If a, b, c be elements of a set (in particular, of a field), and if the rule of combination be such that $(a \circ b) \circ c = a \circ (b \circ c)$, then a, b, c are said to be associative in the order named. If every three elements are associative in every order, the set(or field) is itself said to be associative.

If a, b be elements of a set (or field), and if the rule of combination be such that $a \circ b = b \circ a$, then a, b are said to be commutative.* If every two elements of the set (or field) are commutative, then the set (or field) is itself said to be commutative.

Just as in algebra, the definition of adding leads to the search for a solution of the equations, $x + a = b$, $a + x = b$ and just as the general definition of powers brings up the problem of finding a solution of

*See note *, next page.

$x^a = b$, and $a^x = b$,--so here will arise the question of finding an x so that $x \circ a = b$ or $a \circ x = b$. The process by which x is thought of as determined by a and b (when it is so determined) from either equation will be spoken of as the inverse combination.

*"Permutable".--Burnside, Theory of Groupsof Finite Order.

CHAPTER I. DEFINITION OF A GROUP.

#1. Weber's definition of a finite group.

#2. Weber's general definition of a group.

#3. Pierpont's definition.

#4. A definition by Moore.

#5. A definition by Huntington.

#6. The Burnside-Pierpont-Moore definition generalized by Dickson.

#7. The Burnside-Pierpont-Moore definition generalized by Huntington and Moore.

#8. The non-field definition of Huntington.

#9. Extension to Abelian groups, fields, and relational notation.

Chapter I. Definition of a Group.

#1.

1. Essentially, a group is an associative field, in which the inverse combinations are uniquely possible. This is a concise statement of the classical definition of a group. The conditions which it connotes will be used here as a convenient starting point for comparing various definitions of a group. It should be said, at the outset, that the accurate definition of a group will be a somewhat different question according as a finite or an infinite, or an unspecified number of objects is to be dealt with. Conditions which are sufficient in one case may be found insufficient in the others.

Let us first consider a definition of a finite group adapted from that given by Weber,* and a few of the consequences of this definition. To this I shall in future reduce any other definitions of a finite group which may be given, as authority for the fact that a group in the ordinary sense is being defined.

2. A set of elements will be called a group if the following conditions are satisfied:-

W.(I).† If a, b are elements of the set, then $a \circ b$ is an element of the set. (That is to say, the set is a field).

---

*Lehrbuch der Algebra, II., 3-4.

†See note *, next page

W.(II).* If a, b, c are elements of the set, then

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

(That is, the set is associative).

W.(III.1). If a, b, b' be any elements of the set, such that $a \circ b = a \circ b'$, then $b = b'$.

W.(III.2). If a, b, b' be any elements of the set, such that $b \circ a = b' \circ a$, then $b = b'$.

W.(IV). The set contains a finite number of elements.

3. Before considering the compatibility and independence of these axioms, it will be advantageous to derive some of the conclusions which follow from them, and which we are justified in stating, whether or not any set exists satisfying the axioms.

Theorem. W. (V.1). If a, b be elements of the set, there is in the set an element x, such that

$$a \circ x = b$$

Suppose all the elements written out in order:-

$$x_1, x_2, \ldots\ldots x_n, \qquad (1).$$

Form the set of elements

$$a \circ x_1, a \circ x_2, \ldots\ldots a \circ x_n. \qquad (2).$$

Since every $a \circ x_i$ is an element of the original set (1), by W.(I/), the set (2) satisfies W.(I-IV.) and is therefore a group, contained in the group (1).

*Throughout this chapter any axiom will be denoted, for convenience of reference, by the initial of the author to whom it seems chiefly due, and one or more numbers.

But it contains the same number of elements as (1); hence, unless some of the elements of (2) are equal, (1) and (2) must contain precisely the same elements.

Now no two elements of (2) are equal; for if $a \circ x_i = a \circ x_j$, we should have $x_i = x_j$, by W.(III.1). Hence the elements of (2) must be simply those of (1). But b is an element of (1), therefore an element of (2). Therefore there is some x_i , such that

$$a \circ x_i = b;$$

and the theorem is proved.

In precisely the same fashion we might prove:-

Theorem. W(V2) If a, b be elements of the set, there is in the set an element y, such that

$$y \circ a = b.$$

We may also note, that by W.(III.1), the x determined in W(V.1) is unique; for if $a \circ x = b = a \circ x'$ then $x = x'$. Likewise, by W. (III.2), the y determined in W.(IV.2) is unique. We may then say:-

Corollary. The inverse combination is always uniquely possible.

4. Select any element a of the group. By W.(III.1) there exists in the group an element u, such that

$$a \circ u = a$$

It can now be shown that for any other element b of the group

$$b \circ u = b.$$

For, by W.(IV.2) there is an element y for which

$$y \circ a = b.$$

Then

$$b \circ u = (y \circ a) \circ u$$

But by W.(II), $(y \circ a) \circ u = y \circ (a \circ u)$, and as shown above, $y \circ (a \circ u) = y \circ a = b$.

Hence $b \circ u = b$.

We are now able to state:-

Theorem. W.(VI.1). There is a right-hand identity element u, such that whatever element a may be,

$$a \circ u = a.$$

Similarly:-

Theorem.W.(VI.2). There is a left-hand identity element v, such that, whatever element a may be,

$$v \circ a = a.$$

Theorem.W.(VII). The right-hand and left-hand identity elements are the same element.

Denote the two identity elements by u, v, in the order named. Then by W.(VI.1).,

$$v \circ u = v,$$

and by W(VI.2), $v \circ u = u$.

Therefore, $u = v$.

We denote the identity element by 1 *.

5. Making use once more of W.(III.1,2) there are elements a', a'' such that

$$a \circ a' = 1.$$
$$a'' \circ a = 1.$$

These elements are called the right-hand and left-hand inverses of a respectively.

---

*Sometimes by I. Cf.Dickson, Theory of Algebraic Equations.

Theorem.W.(VIII.1). For every element a there is a right-hand inverse a', such that

$$a \circ a' = 1.$$

Theorem.W.(VIII.2). For every element a there is a left-hand inverse a'', such that

$$a'' \circ a = 1.$$

Theorem.W.(IX). The right-hand and left-hand inverses of an element a are equal.

We know that $a \circ a' = 1$, $a'' \circ a = 1$.

By W.(VI.2), $(a \circ a') \circ a = 1 \circ a = a$.

By W.(VI.1), $a \circ (a'' \circ a) = a \circ 1 = a$.

Therfore $(a \circ a') \circ a = a \circ (a'' \circ a)$.

But by W.(II.), $(a \circ a') \circ a = a \circ (a' \circ a)$,

so that $a \circ (a' \circ a) = a \circ (a'' \circ a)$,

Now applying successively W.(III.1), W.(III.2), we obtain

$$a' = a''.$$

6. In order to prove the consistency of the system W.(I.-IV.), it is sufficient to produce a set satisfying the conditions.

One such set is that of all integers less than a definite integer n, where the rule of combination is

$a \circ b = a + b$ when $a + b \leq n$.

$a \circ b = a + b - n$ when $a + b > n$.*

Another example, for $n = 6$, is the group of transformations of a variable,

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

---

* Huntington, Bull. AM. Math. Soc., 8,299.

where the rule of combination is the direct succession of one transformation on the other.*

We may arbitrarily construct others ad libitum, of purely arbitrary character,-- for example, a set of two symbols A, B, with the rule of combination, $A \circ A = B \circ B = A$, $A \circ B = B \circ A = B$.

7. The independence of the axioms W.(I-IV) will be shown by adducing sets which fail to satisfy each axiom in turn, but do satisfy all the others.

I. Consider the set of all positive integers $\leqq n$, with the rule of combination $a \circ b = a + b$. Evidently, W.(II-IV) are satisfied, while W.(I) is not.

II. Consider the set of all positive integers $\leqq n$, with the rule of combination, $a \circ b = a - b$, when $a > b$; $a \circ b = n + a - b$, when $a \leqq b$. This set satisfies W.(I.,III.1,2,IV.), but does not in general satisfy W.(II.)

III.1. Consider the set of positive integers $\leqq n$, with the rule of combination, $a \circ b = a$. W.(I.) is at once seen to be satisfied. As for W.(II.) we have

$$a \circ (b \circ c) = a \circ b = a,$$

and

$$(a \circ b) \circ c = a \circ c = a,$$

so that $(a \circ b) \circ c = a \circ (b \circ c)$.

For W.(III.2), if $b \circ a = b' \circ a$ we have

$$b = b \circ a = b' \circ a = b',$$

And W.(IV.) is of course true. But it may be and in general is true that $a \circ b = a = a \circ b'$, without $b = b'$, so that W.(III.1.) is not satisfied.

*Burnside, Theory of Groups, Ch.I. Art. 17.
~~Weber, Lehrbuch der Algebra, I., 139-141.~~

III.2. Similarly, the set of positive integers $\leqq n$, with the rule of combination $a \circ b = b$, satisfies W.(I.,II.,III.1,IV.), but does not satisfy W.(III.2.)

IV. Finally, the set of all integers, including zero, satisfies W.(I.-III.), but does not satisfy IV.

The axioms, thus grouped, are therefore mutually independent.

#2.

1. We proceed now to the definition of a group, with an unspecified number of elements. For this purpose, following Weber as before, I shall use the following system of axioms, all of which appeared, either as axioms or theorems, in #1.

W.(I.). If a, b are elements of the set, then $a \circ b$ is an element of the set.

W.(II.). If a, b, c are elements of the set, then

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

W.(III.1.). If a, b, b' be any elements of the set, such that $a \circ b = a \circ b'$, then $b = b'$.

W.(III.2.). If a, b, b' be any elements of the set, such that $b \circ a = b' \circ a$, then $b = b'$.

W.(V.1). If a, b be elements of the set, there is in the set an element x, such that $a \circ x = b$.

W.(V.2). If a, b be elements of the set, there is in set an element y, such that $y \circ a = b$:

2. It is unnecessary to develop at length the group properties studied in the last section, since it may be noted that the only occasion for the use of W.(IV.), which does not appear in the present system, was as a means for the proof of W.(V.1,2), which are assumed in the first place here. All the facts of #1, exceptW.(IV) are necessarily true in the present instance.

It is decidedly worth while to note that the system W.(I-III.) and W.(IV!) The set contains an infinite number of elements. is by no means sufficient to define a group. This might be suspected from the fact that the proof given in #1 of W.(V.1,2) absolutely necessitates the use of W.(IV.) To show accurately the insufficiency of the system W.(I-IV!), consider the set of all positive integers, with the rule of combination $a \circ b = a + b$. The system W.(I-IV.') is satisfied, but W.(V.1,2) are both violated whenever $a \geqq b$.

On the other hand the system W.(I.-III.,IV!., V.1,2) certainly does define an infinite group. It will be seen later that neither of the systems W.(I.-III.,V.1,2), W.(I.-III.,IV.',V.1,2) consists of mutually independent axioms.

3. In order to show the consistency of either system it is sufficient to produce a set satisfying W.(I.-III.,IV.',V.1,2), for such a set satisfies, a fortiori , the smaller set W.(L.,-III.,V.1,2). Such a setis the set of all integers, including zero, with the rule of combination, $a \circ b = a + b$. Another is the set of all rational numbers, except zero, with the rule of

combination, $a \circ b = ab$.

#3.

1. I shall next give another definition of a group, which is used almost as often as that of Weber, as a basis for the study of groups. In particular, it is used by Pierpont in his discussion of the Galois theory.* The system is as follows, the number of elements being unspecified:-

P.(I.) If a, b are elements of the set, then $a \circ b$ is an element of the set.

P.(II.) If a, b, c are elements of the set, then $(a \circ b) \circ c = a \circ (b \circ c)$.

P.(III.) There is in the set an element 1, such that for every element a,

$$a \circ 1 = 1 \circ a = a$$

P.(IV.) For every element a of the set there is an element a^{-1}, such that

$$(a \circ a^{-1}) = (a^{-1} \circ a) = 1.$$

The specification of the group as finite or infinite is accomplished by the adjunction of

P.(V.) The set contains a finite number of elements.

P.(V'.) The set contains an infinite number of elements.

---

*Annals of Math.,2,p.47. The definition is not unlike that of Burnside, except that the latter deals explicitly with groups of operations, and makes use of this fact. Cf.#5.

The system just stated possesses the important disadvantage that the axiom P.(IV.) involves in its statement the truth of P.(III.); any discussion of the independence of these two axioms in their present form is thus meaningless. A method of obviating this, and similar difficulties, will be made clear in the future discussion of other systems.

2. We have to show that the set defined by P.(I.-IV.) is co-extensive with that defined by W.(I.-III.,V.): this will also show that P.(I.-V.), P.(I.-V'.) are co-extensive respectively with W.(I.-III.,IV.), W.(I.-III.,IV'.,V.), and will show the consistency of each of the systems P.(I.-IV.),P.(I.-V.), P.(I.-V'.).

To show that P.(I.-IV.) will be true if W.(I.-III.,V.) is true. Note that all of P.(I.-IV.) have been seen either as axioms or theorems in the W. system,- the correspondence being as follows,-

	P.(I.)	is	W.(I.)
	P.(II.)	"	W.(II.)
	P.(III.)	"	W.(~~VI.~~ 1, 2, ~~VII.~~)
	P.(IV.)	"	W.(~~VIII.~~ 1, 2, ~~IX.~~)
And also	P.(V.)	"	W.(IV.)
and	P.(V'.).	"	W.(IV'.)

3. It is still necessary to show that P.(I.-IV.) suffice to establish W.(I.-III.,V.). In the first

place, as noted before, W.(I.) is the same as P.(I.), W.(II.) the same as P.(II.). Hence W.(III.1,2,V.1,2) must be deduced.

Theorem. P.(VI.1) If a, b, b' be any elements of the set, such that $a \circ b = a \circ b'$, then $b = b'$.

This is the same as W.(III.1). To prove it, select the element a^{-1} determined by P.(IV.).

We have $a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ b')$.

But by P.(II.), $a^{-1} \circ (a \circ b) = (a^{-1} \circ a) \circ b$,

and $a^{-1} \circ (a \circ b') = (a^{-1} \circ a) \circ b'$.

Using P.(IV.), $1 \circ b = 1 \circ b'$,

or by P.(III.), $b = b'$.

Similarly,

Theorem. P.(VI.2). If a, b, b' be any elements of the set, such that $b \circ a = b' \circ a$, then $b = b'$.

This of course establishes W.(III.2).

Theorem. P.(VII.1). If a, b be elements of the set, there is in the set an element x, such that $a \circ x = b$.

Theorem. P.(VII.2). If a, b be elements of the set, there is in the set an element y, such that $y \circ a = b$.

These are identical with W.(V.1,2). I shall prove only the former, since the other may be proved similarly. The element x sought is in fact given by

$$x = a^{-1} \circ b,$$

which by P.(I.) is in the set.

For then $a \circ x = a \circ (a^{-1} \circ b)$,

and by P.(II.), $a \circ x = (a \circ a^{-1}) \circ b$,

That is, by P.(IV.), $a \circ x = 1 \circ b$,

or by P.(III.), $a \circ x = b$.

#4.

1. A system much like the preceding, differing in fact only in the accuracy and independence of the several axioms, and in the narrowness of the conditions which demand associativity, has been given by Moore.* It is as follows:-

M.(I.) If a, b are elements of the set, then $a \circ b$ is an element of the set.

M.(II.) If $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$, and $a \circ (b \circ c)$ are in the set, then

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

M.(III.1) There is in the set an element u, such that for every element a, $u \circ a = a$. This is the left-hand identity.

M.(III.2) There is in the set an element v, such that for every element a, $a \circ v = a$. This is the right-hand identity.

M.(IV.1). If there is a right-hand identity v, then for every element a, there is a left-hand inverse a', such that $a' \circ a = v$.

To indicate the finite or infinite character, we add

M.(V.) The set contains a finite number of elements; or

M.(V.') The set contains an infinite number of elements.

Of course, M.(IV.1) is replaceable by an axiom in which the words right and left are interchanged, and other similar

*Trans. Am. Math. Soc., 3.pp.485-486.

changes made. Either of these axioms follows as a theorem from the other together with M.(I-III.)

2. I shall prove that the one stated above involves the other.

Theorem. M.(IV.2) If there is a left-hand identity u, then for every element a, there is a right-hand inverse a'', such that

$$a \circ a'' = u .$$

The element a'' demanded is the element a' determined in M.(IV. 1,). To prove this, repeat the process of M.(IV.1), obtaining (say) an element $\bar{a}$. Then

$$a' \circ a = v.$$
$$\bar{a} \circ a' = v$$

Assume for the present, that $u = v$; this will be proved in the next paragraph entirely independently of the theorem now in question. Under this assumption we have $\bar{a} \circ a' = u.$

Now
$$\begin{aligned} a \circ a' &= u \circ (a \circ a'), && \text{by M.(III.1),} \\ &= (\bar{a} \circ a') \circ (a \circ a'), && \text{by definition of } \bar{a}, \\ &= [(\bar{a} \circ a') \circ a] \circ a', && \text{by M.(II)), } \\ &= [\bar{a} \circ (a' \circ a)] \circ a', && \text{by M.(II.),} \\ &= [\bar{a} \circ v] \circ a', && \text{by definition of } a', \\ &= \bar{a} \circ a' && \text{, by definition of } v, \\ &= v && \text{, by definition of } \bar{a}, \\ &= u && \text{, assumed from the next} \end{aligned}$$

paragraph.

3. All the statement of M.(I.-III.,IV.1) have been

seen to be true in the previous systems. Ishall deduce P.(I.-IV.) from M.(I.-III.,IV.1), M.(I.) is the same as P.(I.), and by properly assigning the meaning of the rule of combination* between objects not in the set†, M.(II.) is the same as P.(II.). In the last paragraph I have proved P.(IV.), contingently on the truth of a statement, which if true, likewise involves the subsistence of P.(III.),- that is to say, the statement $u = v$. This I proceed to justify

Theorem. M.(VI.) The right-hand and left-hand identities are equal.

For by M.(III.1), $u \circ v = u$.

And by M.(III.2), $u \circ v = u$.

Hence . $u = v$.

4. The proof of the independence of the axioms will be conducted as in #1. They are independent for $n > 2$ or for infinite sets

(I) From any ordinary group, omit any number of elements except 1, and their inverses. Then M.(II.-IV.1,V. or V.′) are satisfied, but, M.(I.) is not.

(II) Consider the first n integers, or all integers. Let $a \circ b = a$, unless $a = b$, $a = 1$, or $b = 1$,

$a \circ a = 1$,

and $a \circ 1 = 1 \circ a = a$.

Evidently M.(I.) is satisfied. For M.(III.1,2), take $u = v = 1$. For M.(IV.1), take $a' = a$. The two cases mentioned satisfy M.(V. or V.′). But for M.(II.),

*Cf. Introduction, #t. 3 . This is possible, since †examples previously given effects this assignment.

take $a \neq b, a \neq 1, b \neq 1;$

then $a \circ (a \circ b) = a \circ a = 1,$

while $(a \circ a) \circ b = 1 \circ b = b.$

In order to be able to find two unequal numbers a, b, neither being the identity, in a finite set, we must have $n \geqq 3$.

(III.1) Consider the first n integers or all integers. Let

$$a \circ b = a$$

M.(I.,II.,V. or V'.) are evidently satisfied. In M.(III.2), take any member of the set, and in M.(IV.1), take $a' = v$. As for M.(III.1), no element u will make

$$u \circ a = a$$

except for the value $u = a$. Hence M.(III.2) is untrue if there are two different elements in the set,- that is (for a finite set), if $n \geqq 2$.

(III.2) Consider the first n integers or all integers. Let

$$a \circ b = b$$

As before M.(I.,II.,V. or V'.) hold. In M.(III.2), take u any member of the set. Just as before M.(III.1) is untrue for $n \geqq 2$. As for M.(IV.1), the hypothecated conditions for its subsistence are untrue,-the fact as it is stated is true, simply because the accasion for a trial of its falsity could never occur. In such a case, - and it is one of by no means infrequent occurence in the general theory of definition by means of axioms,- the axiom is said to be satisfied, or to hold, or to be true, <u>vacuously</u>.

(IV.1) Consider the first n integers, or all integers. Let

$a \circ b = k$ unless $a = 1$ or $b = 1$, where $a \circ 1 = 1 \circ a = a$. | k is a fixed integer $\neq 1$.

M.(I.,II.,V. or V.') are seen to be satisfied. In M.(III.1,2), take $u = v = 1$. There is evidently no other right-hand identity except 1. Thus M.(IV.1) is untrue; for if $a \neq 1$, then

$$x \circ a = k \text{ or } a$$

according as $x \neq 1$ or $= 1$, so that x cannot $= a'$, such that

$$a' \circ a = 1.$$

Here again we require $n \geq 2$.

M.(V. or V.'). Consider an infinite or a finite group respectively.

Thus, the axioms M.(I.-IV.1,V.') are independent, as grouped; and the axioms M.(I.-IV.1,V.), as grouped are independent for $n \geq 3$.

5. For the sake of completing the theory, let us consider separately the two cases passed over. Suppose first $n = 1$. The axioms M.(I.,V.) serve to determine the group; for since we must have $a \circ a = a$, M.(II.,III.,IV.) are necessarily satisfied.* Also M.(I.,V.) are independent, as may be seen from the two sets:-

(I) The number 1; with $a \circ b = a + b$.

(V) Any group of more than one element, or any infinite group.

*For M.(III.1,2,IV.) take $u = v = a' = a$

Suppose next that $n=2$. Then the axioms M.(III.1,2;IV.1,V.) determine the group, as I shall show. Let the elements be α, β, and let $u=\alpha$. Then $\alpha \circ \alpha = \alpha$, , $\alpha \circ \beta = \beta$, by M.(III.1). The element v cannot be β, for $\alpha \circ \beta = \beta \neq \alpha$; hence $v=\alpha$, by M.(V.). Hence $\beta \circ \alpha = \beta$. Finally, if $\alpha' \circ \alpha = \beta$, $\beta' \circ \beta = \alpha$, where α', β' are in the set, by M.(IV.1),

$\alpha' \neq \beta$, for $\beta \circ \alpha = \beta \neq \alpha$,

$\beta' \neq \alpha$, for $\alpha \circ \beta = \beta \neq \alpha$.

Hence $\alpha' = \alpha$, $\beta' = \beta$. The "multiplication table" of the set is therefore

	α	β
α	α	β
β	β	α

,

which shows that we have a group*, and that, therefore, the other properties are satisfied. The independence of the three axioms is seen from the sets defined by the following "multiplication tables":-

(III.1).

	α	β
α	α	α
β	β	β

Take $v=\alpha$ or β. $a'=v$.

(III.2).

	α	β
α	α	α
β	β	β

Take $u=\alpha$ or β.

M.(IV.1) holds vacuously.

(IV.1).

	α	β
α	α	α
β	α	β

Take $u=v=\beta$.

---

*Cf. #1, Art. 6, last example.

#5.

1. A system which resembles the ones just studied, in that it is a systematizing of the Burnside definition, and which furthermore is closely related to the Weber definition, is due to Huntington.* It consists of the following four axioms:-

H.(I.) If a and b are elements of the set, then $a \circ b$ is an element of the set.

H.(II.) If $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$, and $a \circ (b \circ c)$ are in the set, then

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

H.(III.1). If a, b be any two elements of the set, there is in the set an element a', such that

$$b \circ (a' \circ a) = b .$$

H.(III.2) If a, b be any two elements of the set, there is in the set an element a'', such that

$$(a \circ a'') \circ b = b .$$

We may add

H.(IV.) The set contains a finite number of elements,

or

H.(IV'). The set contains an infinite number of elements.

2. H.(I.-III.) are plainly consequences of W.(I.-III.,V.). I shall deduce the latter from the former in a few theorems.

Theorem. H.(V.1) If a be any element of the set, there is in the set an element a', such that for any

*Bull. Am. Math. Soc., 8, p.388.

element b,

$$b \circ (a' \circ a) = b.$$

Theorem. H.(V.2) If a be any element of the set, there is in the set an element a'', such that for any element b,

$$(a \circ a'') \circ b = b.$$

In substance, these theorems indicate that the elements a', a'', determined by a, b in H.(III.) are really independent of b, and depend wholly upon a, I shall prove H.(V.1).

For a special element b, choose a', by H.(III.1), so that

$$b \circ (a' \circ a) = b.$$

Let c be any other element. To show that

$$c \circ (a' \circ a) = c,$$

choose b', by H.(III.1), so that

$$c \circ (b' \circ b) = c.$$

Then
$$\begin{aligned} c \circ (a' \circ a) &= [c \circ (b' \circ b)] \circ (a' \circ a), \\ &= [(c \circ b') \circ b] \circ (a' \circ a), && \text{by H.(II.)}, \\ &= (c \circ b') \circ [b \circ (a' \circ a)], && \text{by H.(II.)}, \\ &= (c \circ b') \circ b && \text{by definition of } a', \\ &= c \circ (b' \circ b) && \text{by H.(II.)}, \\ &= c && \text{by definition of } b'. \end{aligned}$$

Theorem. H.(VI.1) If a, b, c be any elements of the set, such that $a \circ b = a \circ c$, then $b = c$.

Theorem. H.(VI.2) If a, b, c be any elements of the set, such that $b \circ a = c \circ a$, then $b = c$.

I shall prove H.(VI.1)

Put $a \circ b = a \circ c = s$.

Let $x = b'' \circ c$,

and $y = b \circ s'$.

Then $(y \circ s) \circ x = y \circ (s \circ x)$, by H.(I.,II.)

I shall show that $y \circ (s \circ x) = b$ and $(y \circ s) \circ x = c$.

$s \circ x = (a \circ b) \circ (b'' \circ c)$, by H.(II.),

$= a \circ [b \circ (b'' \circ c)]$, by H.(II.),

$= a \circ [(b \circ b'') \circ c]$, by definition of b''.

$= a \circ c$, by hypothesis.

$= s$

Then $y \circ (s \circ x) = y \circ s$, as just proved.

$= (b \circ s') \circ s$, by hypothesis,

$= b \circ (s' \circ s)$, by H.(II.),

$= b$, by definition of s'.

Now let us consider $(y \circ s) \circ x$.

$y \circ s = (b \circ s') \circ s = b$, as just seen.

$(y \circ s) \circ x = b \circ x = b \circ (b'' \circ c)$,

$= (b \circ b'') \circ c$, by H.(II.)

$= c$, by definition of b''.

Hence as was to be proved, $b = c$.

Theorem.H.(VII.1) If a, b be any elements of the set, there is in the set an element x such that $a \circ x = b$.

Theorem. H.(VII.2) If a, b be any two elements of the set, there is in the set an element y such that $y \circ a = b$.

In fact, take $x = a'' \circ b$, $y = b \circ a'$.

Then $a \circ x = a \circ (a'' \circ b) = (a \circ a'') \circ b$, by H.(II.),

$= b$

And $y \circ a = (b \circ a') \circ a = b \circ (a' \circ a)$, by H.(II.),

$= b$.

We have now seen that W.(I.-III.,V.) are consequences of H.(I.-III.), as follows,

W.(I.) is H.(I.)

W.(II.) " H.(II.)

W.(III.1)" H.(VI.1).

W.(III.2)" H.(VI.2).

W.(V.1) " H.(VII.1).

W.(V.2) " H.(VII.2).

Also W.(IV.) " H.(IV.).

W.(IV.') " H.(IV.')

Thus H.(I.-IV.) define a finite, H.(I.-IV.') an infinite group.

3. For $n > 2$, or for infinite sets, the axioms H.(I.-IV. or IV.') are independent, as may be seen from the sets which follow.

(I.) When n is odd, take the set of all integers, including zero, from $-\frac{n-1}{2}$ to $+\frac{n-1}{2}$, with $a \circ b = a+b$. In H.(III.) take $a' = a'' = -a$.

When n is odd, take the set of all integers, including zero, from $-\left(\frac{n}{2}-1\right)$ to $+\left(\frac{n}{2}-1\right)$, and an extra element z ; let

$a \circ b = a+b$, unless $a = z$ or $b = z$,

$a \circ z = z \circ a =$ an object not in the set, unless $a = 0$,

$0 \circ z = z \circ 0 = 0$,

$z \circ z = 0$.

In H.(III.), take $a' = a'' = -a$, for $a \neq z$; take $z' = z'' = z$.

For an infinite set, take all integers, except ± 1, with $a \circ b = a+b$.

Here again $a' = a'' = -a$.

In all these cases H.(I.) is untrue, while H.(II.-III.,IV. or IV!) are true.

(II.) Consider all positive integers from 1 to n.

Let $a \circ b = a+b$, unless $a+b = 1, 2, \text{or} > n$,

$a \circ b = a+b-n$, when $a+b > n$, unless $a+b = n+1, n+2$,

$a \circ b = 2$, if $a+b = 1$ or $n+1$,

$a \circ b = 1$, if $a+b = 2$ or $n+2$.

In H.(III.), $a' = a''$ is given by the following table:-

$b \neq 1, 2.$	$a \neq n.$	$a' = a'' = n-a.$
$b \neq 1, 2.$	$a = n.$	$a' = a'' = n.$
$b = 1.$	$a \neq 1.$	$a' = a'' = n+2-a$
$b = 1.$	$a = 1.$	$a' = a'' = 1.$
$b = 2.$	$a < n-1.$	$a' = a'' = n-1-a.$
$b = 2.$	$a = n-1.$	$a' = a'' = n.$
$b = 2.$	$a = n.$	$a' = a'' = n-1.$

Trial will show that H.(III.) is in all cases verified.

But H.(II.) is untrue, for $n > 2$: For when $n > 3$,

$$(101) \circ 2 = 102 = 3, \quad 1 \circ (102) = 103 = 4.$$

and for $n = 3$,

$$(101) \circ 2 = 102 = 3, \quad 1 \circ (102) = 103 = 2,$$

As an example of an infinite set, take all rational numbers, with $a \circ b = \frac{a+b}{2}$. Take $a' = a'' = 2b - a$.

In both cases, all the axioms except H.(III.) are satisfied.

(III.1) Consider all integers $\leqq n$, or all integers, with $a \circ b = b$. If $n \geq 2$, and a, b are chosen unequal, there is no a', such that

$b \circ (a' \circ a) = b$;

(III,2). Similarly consider all integers $\leqq n$, or all integers, with $a \circ b = a$.

(IV). or(IV'). Consider any infinite or finite group respectively.

§6.

1. The Burnside-Pierpont-Moore definition* has been variously modified, by Moore, Huntington, and Dickson. In this section I shall give essentially† the form proposed by Dickson‡. This system of axioms is:-

D.(I.) If a, b are elements of the set, then $a \circ b$ is an element of the set.

D.(II.) If $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$, and $a \circ (b \circ c)$ are elements of the set, then

$$(a \circ b) \circ c = a \circ (b \circ c)$$

D.(III.1) There is in the set an element 1, such that for every element a

$$1 \circ a = a.$$

D.(IV.1). If there is in the set an element 1, such that for every element a, $1 \circ a = a$; then for some such element 1, and for every element a, there is in the set an element a^{-1} such that

$$a \circ a^{-1} = 1,$$

We shall call1 the right-hand identity, and a^{-1} the right-hand inverse of a.

As usual, to specify the finite or infinite character, adjoin

D.(V.) The set contains a finite number of elements;

or D.(V.') The set continas an infinite number of elements.

*see note *, next page. †see note †, next page. ‡see note ‡, next page.

2. The statements are now familiar as properties of an ordinary group. I shall show that they conversely define a group, by proving from them the system P.(I.-IV.). it is only necessary, of course, to prove the"left-hand" statements corresponding to D.(III.1,IV.1). and establish the equivalence of analogous right- and left-hand elements.

Theorem D. (III.') The right-hand identity 1, is a left-hand identity, and is the unique identity of the set.

By D.(IV.1), choose a^{-1}, $\bar{a}$, so that

$$a \circ a^{-1} = 1,$$

$$a^{-1} \circ \bar{a} = 1.$$

By D.(II.-IV), $a = a \circ 1 = a \circ (a^{-1} \circ \bar{a}) = (a \circ a^{-1}) \circ \bar{a} = 1 \circ \bar{a}.$

Hence $a^{-1} \circ a = a^{-1} \circ (1 \circ \bar{a}) = (a^{-1} \circ 1) \circ \bar{a} = a^{-1} \circ \bar{a} = 1.$

And likewise $\bar{a} \circ a^{-1} = 1.$

Therefore $1 \circ a = (1 \circ 1) \circ a = [1 \circ (\bar{a} \circ a^{-1})] \circ a$

$$= [(1 \circ \bar{a}) \circ a^{-1}] \circ a = [(1 \circ \bar{a}) \circ (a^{-1} \circ a)$$

$$= a \circ 1 = a.$$

So that we have

$$a \circ 1 = 1 \circ a = a.$$

Furthermore, 1 is the only such identity element. For if $1'$ be another, then $1 = 1 \circ 1' = 1'$.

Thus the theorem is proved.

Theorem D.(IV.'). The right-hand inverse of any element a is a left-hand inverse of a, and is the unique inverse of a.

It was shown above that 1, was both a right-hand and a left-hand identity, and that $a \circ a^{-1} = a^{-1} \circ a = 1$,

*#4,#5. †For the points of difference, see Art. 4 of this section.

‡Trans. Am. Math. Soc., 6,p. 198.

hence a^{-1} is both a right-hand and a left-hand inverse.

If again, a^{-1}, a' were both inverses of a; then

$$a' = a' \circ 1 = a' \circ (a \circ a^{-1}) = (a' \circ a) \circ a^{-1} = 1 \circ a^{-1} = a^{-1}$$

Therefore, the theorem is proved.

3. The following systems establish the mutual independence of the axioms D.(I.-IV.1,V.), and D.(I.-IV.1,V.')

(I.) All integers $\leqq n$, or all integers; with

$a \circ b$ not in the set unless $a = b$ or $b = 1$.

$a \circ a = 1$.

$a \circ 1 = a$.

In D.(IV.1), take $a^{-1} = a$.

(II.) All integers $\leqq n$, or all integers; with

$a \circ b = 1$, unless $a = 1$ or $b = 1$.

$a \circ 1 = a$,

$1 \circ b = 1$.

Take a^{-1} any element of the set except 1.

(III.1). All integers $\leqq n$, or all integers; with

$a \circ b = 1$.

(IV.1). All integers $\leqq n$, or all integers; with

$a \circ b = k$, unless $a = 1$ or $b = 1$,

$a \circ 1 = 1 \circ a = a$,

where k is a fixed element of the set $\neq 1$.

(V. or V.') Any fnfinite or finite set respectively.

4. As a matter of fact, Dickson goes much further into the analysis on the basis of simplicity, than I have indicated. He considers $a \circ b$ as a (potentially) multiple-valued function of a and b. On this basis, any such

espression as $a \circ b$, in D.(II.III.1,IV.1) is to be understood as meaning "one of the (possibly) many values of $a \circ b$. D.(I.) is replaced by the three axioms,-

D.(I.a). If a, b are elements of the set, $a \circ b$ has some value.

D.(I.b). If a, b are elements of the set, $a \circ b$ has not more than one value.

D.(I.c). If a, b are elements of the set, and there is at least one value of $a \circ b$, then some value of $a \circ b$ is in the set.

From these follow readily D.(I.). The following systems show that each of D.(I.,a,b,c) is independent of the others combined with D.(II.,III.,IV.1):-

(I.a) All integers $\leq n$, or all integers; with
$a \circ b$ undefined unless $a = b$ or $b = 1$.
$a \circ a = 1$.
$a \circ 1 = a$

(I.b) All integers $\leq n$, or all integers; with
$a \circ b = a + b$ or 1.

(I.c) All integers $\leq n$, or all integers; with
$a \circ b = 1$, unless $b = 1$.

$a \circ 1$ not in the set unless $a = 1$.

#7.

1. The newer forms of the Burnside-Pierpont-Moore definition given by Moore and Huntington both postulate for the identity element the property which may be called (after Benjamin Peirce,* who applied it, however to unit numbers of a hypercomplex number system, rather than of to

*AM. Journ. Math. IV., p.97.

identity elements of a group) idempotency,--- that is, the property that its square is equal to itself. I shall discuss these two systems in this section. The definition of Moore assumes that such an idempotent element is both a right-hand and a left-hand identity, and that left-hand inverses exist. That of Huntington assumes that the idempotent element is unique, and is either a right-hand or a left-hand identity, and that either right-hand or left-hand inverses exist.

2. Huntington's definition is as follows:-

H.'(I.) If a, b are elements of the set, then $a \circ b$ is an element of the set.

H.'(II.) If $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$, and $a \circ (b \circ c)$ are elements of the set, then

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

H.'(III.1) There is in the set an element u such that $u \circ u = u$.

H.'(III.2). If a, b are elements of the set such that $a \circ a = a$, $b = b = b$, then $a = b$.

(The postulates H.'(III.1,2) state respectively that there is at least one and at most one idempotent element in the set).

H.'(IV.) If there is a unique idempotent element u in the set, then either $u \circ a = a$ for every element a, or else $a \circ u = a$ for every element a.

H.(V) If there is a unique idempotent element in the set, then for every element a there is either an element a' such that $a' \circ a = u$, or else an element a'' such that $a \circ a'' = u$.

We add the usual axioms H.'(VI. or VI.') to determine the order of the group. It is distinctly noteworthy, however, that the assumption of H.'(VI.), making the group

finite, renders H.'(III.1,V.) redundant. Similar facts have been noted in the Weber definitions.* The deduction of H.'(III.1,V.) from the other axioms will be given in Art. 5 of this section.

3. Theorem. H.'(VII.) There element u has the property that for every element a,

$$a \circ u = u \circ a = a .$$

By virtue of H.'(IV.), it is only necessary to prove that if either $u \circ a = a$ or $a \circ u = a$, then the other is true. Suppose defintely that $u \circ a = a$; it will be proved that $a \circ u = a$. By H.'(V.) there exists either a' such that $a' \circ a = u$, or else a'' exists such that $a \circ a'' = u$. Suppose first a' exists. Then $a' \circ a = u$.

Also
$$\begin{aligned}(a \circ a') \circ (a \circ a') &= a \circ [a' \circ (a \circ a')] && \text{, by H.(II.)} \\ &= a \circ [(a' \circ a) \circ a'] && \text{, by H.(II.)} \\ &= a \circ [u \circ a'] && \text{, by definition of } a' \\ &= a \circ a' && \text{, by hypothesis}\end{aligned}$$

Thus it appears that the element $a \circ a'$ is indempotent; whence by H.'(III.2), $a \circ a' = u$. Then

$$\begin{aligned}a \circ u &= u \circ (a \circ u) && \text{, by hypothesis} \\ &= u \circ [a \circ (a' \circ a)] && \text{, by definition of } a' \\ &= u \circ [(a \circ a') \circ a] && \text{, by H.'(II.)} \\ &= u \circ [u \circ a] && \text{, as just proved.} \\ &= (u \circ u) \circ a && \text{, by H.'(II).} \\ &= u \circ a && \text{, by definition of } u \\ &= a && \text{, by hypothesis.}\end{aligned}$$

Secondly, suppose that instead of knowing that a' exists, we know that a'' exists. Then $a \circ a'' = u$.

Also
$$\begin{aligned}(a'' \circ a) \circ (a'' \circ a) &= a'' \circ [a \circ (a'' \circ a)] && \text{, by H.'(II.)} \\ &= a'' \circ [(a \circ a'') \circ a] && \text{, by H.'(II.)}\end{aligned}$$

*Cf. #1, #2.

$= a'' o [u o a]$, by definition of a''

$= a'' o a$, by hypothesis.

Hence, as before, $a'' o a = u$. Then

$a o u = u o (a o u)$, by hypothesis

$= u o [a o (a'' o a)]$, as just proved

$= u o [(a o a'') o a]$, by H.'(II).

$= u o [u o a]$, by definition of a''

$= (u o u) o a$, by H.'(II.)

$= u o a$, by definition of u

$= a$, by hypothesis

Thus the theorem is proved, if $u o a = a$. If, instead, $a o u = a$, the proof is precisely similar.

Theorem. H.'(VIII.1) If a, b, c are elements such that $a o b = a o c$, then $b = c$.

Theorem. H.'(VIII.2) If a, b, c are elements such that $b o a = c o a$, then $b = c$.

I shall prove the former. Suppose $a o b = a o c$. By H.'(V.), either $a' o a = u$ or $a o a'' = u$.

In the first case,

$b = u o b$, by H.'(VII).

$= (a' o a) o b$, by hypothesis.

$= a' o (a o b)$, by H.'(II).

$= a' o (a o c)$, by hypothesis.

$= (a' o a) o c$, by H.'(II).

$= u o c$, by hypothesis

$= c$, by H.'(VII.)

In the second case, I have shown, during the proof of H.'(VII.) that if $a o a'' = u$, then $a'' o a = u$, so that a'' may be used just as a' has been used in the preceding proof.

Theorem. H.′(IX.1). If a, b be elements of the set, there is an element x, such that $a \circ x = b$. There is only one such element.

Theorem. H.′(IX.2). If a, b be elements of the set, there is only an element y, such that $y \circ a = b$. There is only one such element.

I prove H.′(IX.1). The element x is given by $a' \circ b$ under the first possibility of H.′(V.), or by $a'' \circ b$ under the second. For denoting either a' or a'', as the case may be, by α, then, as has been shown, $a \circ \alpha = u$. Hence

$$a \circ x = a \circ (\alpha \circ b) = (a \circ \alpha) \circ b = u \circ b = b$$

by the aid of H.′(II.VII.)

The x determined is unique; for, by H.′(IX.1) if $a \circ x = b = a \circ x'$ then $x = x'$.

Thus we have deduced all the Weber axioms, so that the present system defines a group.

4. The axioms H.′(I.-V., VI.′) are independent, To establish this, consider the following sets:-

(I.) Consider all real numbers, with $a \circ b$ not in the set unless $a = 0$, $b = 0$, or $a + b = 0$,

$a \circ b = a + b$ if $a = 0$, $b = 0$, or $a + b = 0$.

Take $u = 0$, and a' or $a'' = -a$.

(II.) Consider all real numbers, with

$a \circ b = a + b$, unless $a = b$,

$a \circ a = 0$.

Take $u = 0$, a' or $a'' = 0$. If a, b are unequal non-zero numbers,

$$(a \circ a) \circ b = 0 \circ b = b,$$
$$a \circ (a \circ b) = a + (a + b) = 2a + b,$$

so that H.'(II.) is violated. The other axioms hold.

(III.1). Consider all positive real numbers, with

$$a \circ b = a + b.$$

Since zero is excluded, there is evidently no element u, such as is demanded in H.'(III.1). H.'(III.2, IV., V.) are satisfied vacuously.

(III.2). Consider all real numbers, and an extra element z, with

$$a \circ b = a + b, \text{ unless } a = z \text{ or } b = z,$$
$$a \circ z = z \circ a = z$$

The elements 0 and z are idempotent.

(IV.) Consider all real numbers, with

$$a \circ b = 0.$$

The unique idempotent element is 0. Select $a' = a'' = 0$. Evidently H.'(IV.) is violated.

(V.) Consider all positive real numbers and zero, with

$$a \circ b = a + b.$$

(VI.') Consider any finite group of the character previously discussed.

5. The axioms H.'(I.-V.,VI.) are of course sufficient to define a finite group; they contain, however, some redundancies. For $n > 2$, axioms H.'(III.1,V.) are deducible from the remainder: for $n = 1$, the system may be still further reduced. In order to prove this, I shall first establish the following

Lemma, proved on the assumption of H.'(I.,II.,VI.).

Define two functions of an element a, denoted by upper and lower subscripts, by the recursion formulae,-

(A). $a_{k+1} = a_k \circ a_k$, $a_1 = a \circ a$.

(B). $a^{k+1}_{\ k} = a^k \circ a$, $a^1 = a$.

I shall prove the following two properties:-

(1). $a^m \circ a^n = a^{m+n}$

(2). $a_m^{\ m} = a^{2^m}$ *.

Suppose that (1) is true for some value of n, $n = n_1$,

$$a^m \circ a^{n_1} = a^{m+n_1}$$

Then $a^m \circ a^{n_1+1} = a^m \circ (a^{n_1} \circ a)$, by definition of (A).

$= (a^m \circ a^{n_1}) \circ a$, by H.(II).

$= a^{m+n_1} \circ a$, by hypothesis,

$= a^{m+n_1+1}$, by definition (A).

so that (1) is true for $n = n_1 + 1$. But (1) is true for $n = 1$, by definition; hence, according to the usual argument by mathematical induction, it is true for all values of n.

Suppose that (2) is true for $m = m_1$,

$$a_{m_1} = a^{2^{m_1}}.$$

Then $a_{m_1+1} = a_{m_1} \circ a_{m_1}$, by definition (B),

$= a^{2^{m_1}} \circ a^{2^{m_1}}$, by hypothesis,

$= a^{2^{m_1}+2^{m_1}}$, by (1)

$= a^{2^{m_1+1}}$, by the properties of exponents.

Thus (2) is true for $m = m_1 + 1$. But (2) is true for $m = 1$, since by definitions (B), (A),

$$a_1 = a \circ a = a^2;$$

hence (2) is true for all values of m.

* Here 2^m is of course merely an ordinary algebraic power.

Proof of H.'(III.1) from H.'(I.,II.,VI.)*

Since the set is finite, the sequence of elements

$$a, a_1, a_2, \ldots$$

must contain repetitions; it must be true for some m and p, that

$$a_{m+p} = a_m.$$

Then define a function of a by the recursion formula,

$$(C)\quad x_{k+1} = x_k \circ a_{m+k},\ x_1 = a_m.$$

in which x_k is <u>not</u> a function related to x, as is a_k to a, but a function of a defined solely by the law just stated. I wish to prove that the element

$$i = x_p$$

is idempotent.

First, let x_k beexpressed in terms of a with upper subscripts. We have at once, by (2),

$$(3).\qquad x_1 = a_m = a^{2^m}.$$

More generally, it is true that $x_k = a^{2^m(2^k-1)}$

This is seen to be true for $k=1$. If it is true for $k=k_1$, $x_{k_1} = a^{2^m(2^{k_1}-1)}$,

then
$$\begin{aligned} x_{k_1+1} &= x_{k_1} \circ a_{m+k_1}, && \text{by definition (C)} \\ &= a^{2^m(2^{k_1}-1)} \circ a^{2^{m+k_1}}, && \text{by (3),(2),} \\ &= a^{2^m(2^{k_1}-1)+2^{m+k_1}}, && \text{by (1),} \\ &= a^{2^m(2^{k_1}-1+2^{k_1})}, && \text{by the properties of exponents.} \\ &= a^{2^m(2^{k_1+1}-1)}, && \text{by the properties of exponents.} \end{aligned}$$

so that it is true for $k=k_1+1$; hence it is true for any value of k. Therefore we can restate the problem in these terms,-- we know that

$$(4).\qquad a^{2^{m+p}} = a^{2^m}$$

See note, next page.

and wish to prove that

$$(5).\quad i^2 = \left[a^{2^m(2^p-1)}\right]^2 = a^{2^m(2^p-1)} = i.$$

But $$\left[a^{2^m(2^p-1)}\right]^2 = a^{2^{m+1}(2^p-1)}$$
$$= a^{2^{m+p+1}-2^{m+1}}.$$

Now if $p >$, then $2^{m+p} > 2^{m+1}$, and we can write the above expression

$$i^2 = a^{2^{m+p}} \circ a^{2^{m+p}-2^m-2^m}$$
$$= a^{2^m} \circ a^{2^{m+p}-2^m-2^m}$$
$$= a^{2^{m+p}-2^m} = a^{2^m(2^p-1)} = i,$$

as we wished to prove.

It has been assumed that $p > 1$. It cannot be true that $p = 0$, as in that case the assertion $a_{m+p} = a_m$ would involve no condition on a , as was intended. Suppose then $p = 1$; the known fact (4) becomes

$$a^{2^{m+1}} = a^{2^m}, \text{ or } (a^{2^m})^2 = a^{2^m}.$$

And we have $i = a^{2^m(2-1)} = a^{2^m}$, so that it is true that $i^2 = i$.

Therefore, any set satisfying H.'(I.,II.,VI.) contains some idempotent element. We can now dispose of H.'(V.) as follows:-

Proof of H.'(V.) from H.(I.,II.,III.2,IV,VI.)†.

By H.'(I.,II.,VI.), we have proved that the element $i = a^{2^m(2^p-1)}$ is idempotent.

The element

$$a' = a^u = a^{2^{m+p}-2^m-1}$$

~~Here z is of course merely an ordinary Algebraic power.~~

*This proof is given in barest outline by Moore Trans. AM. Soc. 3,p.490; and repeated in slightly greater detail by Huntington, Trans. Am. Math. Soc., 6,p.194. I have attempted the rather difficult task of preserving the spirit of the original proof without assuming any knowledge of the technical group-theory.

† See note *, next page.

satisfies both of the conditions demanded in H.'(V).

For $a \circ a'' = a' \circ a = a^{2^{m+p}-2^m-1} \circ a$

$= a^{2^{m+p}-2^m}$, by (1).

$= b$,

as was to be proved.

6. That the system H.'(I/,II.,III.2,IV.VI.) consists of independent axioms, when $n > 2$, is seen from the following sets:-

(1). All integers $\leqq n$, with

$a \circ b$ not in the set unless $a = 0$, $b = 0$, or $a + b = n$,

$a \circ 0 = 0 \circ a = a$,

$a \circ b = 0$ when $a + b = n$.

(II). All integers $\leqq n$, with

$a \circ b = 0$, unless $a = 0$ or $b = 0$,

$a \circ 0 = 0 \circ a = a$.

(III.2) All integers $\leqq n$, with

$a \circ b = 0$, unless $a = b$,

$a \circ a = a$.

(IV). All integers $\leqq n$, with

$a \circ b = 0$.

(VI). Any infinite group.

7. If $n = 1$, it is readily seen that H.'(I.,VI.) are sufficient to define the group.

If $n = 2$, H.'(I.,II.,III.2,IV.,VI.) are as before sufficient. In the preceding independence proofs (I) and (II), however, it has been assumed that there are in the

*Huntington, Trans. Am. Math. Soc., 6,p.194.

set at least three distinct elements. For $n=2$ we replace these by sets defined by the "multiplication tables":-

(I.)

	α	β
α	β	*
β	*	α

* Not in the set.

H.'(III.2,IV.) are satisfied vacuously.

(II.)

	α	β
α	β	β
β	β	α

H.'(III.2,IV.) are satisfied vacuously.

8. I shall now dispose briefly of the latest definition of Moore,* as corrected† from an earlier statement.‡ The definition is:-

M.'(I.) If a, b are elements of the set, then $a \circ b$ is an element of the set, ~~then~~

M.(II.) If $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$, and $a \circ (b \circ c)$, are elements of the set, then

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

M.(III.) There is in the set an element u such that

$$u \circ u = u.$$

M.(IV.1) If there is an idempotent element u in the set, then for every element a

$$u \circ a = a.$$

M.(V.1) If there is an idempotent element u in the set, then for every element a there is an element a' such that $a' \circ a = u$.

*Trans. Am. Math. Soc., 6, p.179.
†Trans. Am. Math. Soc., 5, p.549.
‡Trans. Am. Math. Soc., 3, p.485.

To these, as usual, we add M.'(VI. or VI), as may be desired. It will be noted that this definition is rather more neat and conclusive than Huntington's, in that the uncomfortable alternative conclusions of H.'(IV.,V.) are replaced by the more definite statements M.'(IV.,V.), and in that the uniqueness of the idempotent element is not assumed.

9. It will be sufficient proof that M.'(I.-V.1) define a group, to prove H.'(III.2), that is, the uniqueness of the idempotent element.

Theorem. M.'(VII.) If $u \circ u = u$ and $v \circ v = v$, then $u = v$.

By M.'(V.1), select v', v'' so that

$$v' \circ v = u.$$
$$v'' \circ v' = u.$$

Then
$$\begin{aligned} v \circ u &= (u \circ v) \circ u && \text{, by M.'(IV.1),} \\ &= [(v'' \circ v') \circ v] \circ u && \text{, by definition of } v'', \\ &= [v'' \circ (v' \circ v)] \circ u && \text{, by M.'(II.),} \\ &= (v'' \circ u) \circ u && \text{, by definition of } v', \\ &= v'' \circ (u \circ u) && \text{, by M.'(II.),} \\ &= v'' \circ u && \text{, by M.'(III.),} \\ &= v'' \circ (v' \circ v) && \text{, by definition of } v', \\ &= (v'' \circ v') \circ v && \text{, by M.'(II.),} \\ &= u \circ v && \text{, by definition of } v''. \end{aligned}$$

But by M.'(IV.1), $v \circ u = u$ and $u \circ v = v$, since u, v are both idempotent elements. Hence $u = v$.

10. Moore has not discussed the effect of M.'(VI. or VI') on the dependence or independence of the other axioms. To establish the independence of

M.!(I.-V.1) he cites the following sets:*

(I) All integers and zero, except ± 1, with $a \circ b = a + b$

(II) All integers and zero, with

$a \circ b = 0$ unless $a = 0, b = 0$, or $a = b$.

$a \circ a = 1$ unless $a = 0$ or 1.

$a \circ 0 = 0 \circ a = a$.

$0 \circ 0 = 0$

$1 \circ 1 = 1$.

(III). All positive integers, with

$a \circ b = a + b$.

(IV.1) All integers and zero, with

$a \circ b = 0$.

(V.1) All positive integers and zero, with

$a \circ b = a + b$.

*I have slightly specialized some of the sets, in order to make the examples more concrete.

#8.

1. In all definitions of a group given so far, it has been expressly postulated that the set under consideration was a field. In this section, I shall give a definition which does not demand this, but proves it as a theorem. While from the standpoint of group theory it is perhaps desirable that this should be one of the fundamental notions, the following definition is valuable, if only on account of its logical simplicity and definiteness. The definition is due to Huntington:†-

†Bull. Am. Math. Soc., 8, p.296.

‡In its original form, this axiom was:-

H."(II.) If $a, b, c, a \circ b, b \circ c$, and wither $(a \circ b) \circ c$ or $a \circ (b \circ c)$ are in the set, then $(a \circ b) \circ c = a \circ (b \circ c)$.

Moore(Trans. Am. Math. Soc., 3, p.489) noted that this is decomposable into H."(II. 1, 2), and a further discussion of this fact is

H.''(I.1) If a, b are elements of the set, there is in the set an element x such that $a \circ x = b$.

H.''(I.2) If a, b are elements of the set, there is in the set an element y such that $y \circ a = b$.

H.''(II.1) If $a, b, c, a \circ b, b \circ c$, and $(a \circ b) \circ c$ are in the set, then $(a \circ b) \circ c = a \circ (b \circ c)$ *.

We might replace H.''(II.1) by a similar statement H.''(II.2), in which it is assumed that $a \circ (b \circ c)$ (not necessarily $(a \circ b) \circ c$) is in the set. For it will be proved later that H.''(II.2) is deducible from H.''(II.1), and considerations of symmetry show that (by a symmetric re-definition of the meaning of $(a \circ b)$, the systems H.''(I.1, I.2, II.1), H.''(I.1, I. 2, II.2), are exactly equivalent.

We add the usual order-axioms, H.''(III. or III')

2. Theorem. H.''(IV.1). There is in the set a lefthand identity element u, such that for every element a,

$$u \circ a = a \quad .$$ †

For a particular element a, there is such an element u, by H.''(I.2). Let b be any other element of the set. I shall show that $u \circ b = b$.

By H.(I.1), take x so that $a \circ x = b$. Then

$$u \circ b = u \circ (a \circ x) = (u \circ a) \circ x \text{ , by H. (II.1),}$$
$$= a \circ x = b.$$

As we wished to prove.

* See note ‡, preceding page.

given by Huntington (Trans. Am. Math. Soc., 4, p.301. Both Moore and Huntington call attention to the fact, that while H.(I.1, I.2, III.) are mutually independent, after the decomposition of H.(II.), either H.(II.1 or 2) is redundant. Cf. also the succeeding remarks above.

Theorem. H.''(V.1) If $b \circ a = b' \circ a$ (both products belonging to the set), then $b = b'$.

Put $b \circ a = b' \circ a = c$

By H.''(I.2) take y such that $y \circ b = b'$ and

by H.''(I.1) take x such that $c \circ x = b$.

Then
$$\begin{aligned} b &= c \circ x && \text{, by hypothesis,} \\ &= [(y \circ b) \circ a] \circ x && \text{, by hypothesis,} \\ &= [y \circ (b \circ a)] \circ x && \text{, by H.''(I.1),} \\ &= (y \circ c) \circ x && \text{, by definition of } c, \\ &= y \circ (c \circ x) && \text{, by H.''(I.1),} \\ &= y \circ b && \text{, by definition of } x, \\ &= b' && \text{, by definition of } y. \end{aligned}$$

Thus the theorem is proved.

Theorem. H.''(II.2) If $a, b, c, a \circ b, b \circ c$, and $a \circ (b \circ c)$ are in the set, then $(a \circ b) \circ c = a \circ (b \circ c)$.

This will of course establish the proposition symmetrical to H.''(II.1). To prove it, by H.''(I.2) take y such that $y \circ c = a \circ (b \circ c)$. By H.''(I.2), take a' such that $a' \circ b = y$. Then

$$\begin{aligned} a \circ (b \circ c) &= y \circ c \\ &= (a' \circ b) \circ c \\ &= a' \circ (b \circ c) \text{ by H.''(II.1).} \end{aligned}$$

Hence, by H.''(V.1), $a = a'$, and therefore

$$(a \circ b) \circ c = (a' \circ b) \circ c = y \circ c = a \circ (b \circ c).$$

We may of course now state the theorem symmetrical to H.''(IV.1, V.1):-.

Theorem. H.''(IV.2). There is in the set a right-hand identity element v, such that for every element a,

$$a \circ v = a.$$

Theorem. H.''(V.2). If $a \circ b = a \circ b'$ (both products belonging to the set), then $b = b'$.

Theorem. H.''(VI.) If a, b are elements of the set, then $a \circ b$ is an element of the set.

By H.''(IV.2) take v so that $a \circ v = a$, and by H.''(I.2) take b' so that $b' \circ b = v$. Finally, take x so that $x \circ b' = a$, by H.''(I.2).

I shall show that

$$a \circ b = x.$$

By H.''(IV.2), $x \circ v = x$, so that $x \circ (b' \circ b)$ is in the set. Then by H.''(II.2), $(x \circ b') \circ b$ is in the set; and in fact

$$(x \circ b') \circ b = x \circ (b' \circ b),$$

or

$$a \circ b = x \circ v = x.$$

The theorems which have been proved establish W.(I.-III.), so that H.''(I.-II.) define a group.

3. The independence of H.''(I., II., III., or III.') is seen from the following sets:-

(I.1) All integers $\leqq n$, or all integers; with $a \circ b = a$.

(I.2) All integers $\leqq n$, or all integers, with $a \circ b = b$.

(II.1) All integers $\leqq n$, with

$$a \circ b = a + b \quad \text{when } a+b \leqq n,$$
$$a \circ b = a+b-n \quad \text{when } a+b > n;$$

except that

$$a \circ b = 2 \quad \text{when } a+b = 1 \text{ or } n+1,$$
$$a \circ b = 1 \quad \text{when } a+b = 2 \text{ or } n+2.$$

Or all rational numbers with $a \circ b = a/b$.

(III. or III.') Any infinite or finite group respectively,

The axioms seen to be independent for $n \geq 3$, or for an infinite group. For $n = 1, 2$ special investigations might be made simialr to those of preceding sections.*

#9.

I shal conclude the chpater with a few general observations concerning other aspects of the subject-matter into which it has not seemed profitable to enter at great length.

There is no particularly good way of estimating the relative values of the various definitions which have been given, for, as Moore says†-"The canons of relative simplicity of equivalent definitions by sets of postulates are not well established". He gives certain tentative criteria for evaluating definitions, but it has not seemed worth while for me to try to apply these in the present chapter, since their necessarily limited ~~applications~~ applicability and their incompleteness render any decision based on them rather unsatisfactory.

I have attempted to give, in this chapter, essentially all that has been done on the definition of groups by means of independent axioms based on the application of a rule of combination. This problem admits of, and has received, extension in three ways, which I shall briefly mention.

We may postulate commutativity as a property of the rule of combination. A group for which this is

*Cf. #4, #7. † Trans. Am. Math. Soc., 3, p.488.

true is called an Abelian group. The specialization and simplification of the axioms can be carried much further in the case of an Abelian group,-- it is in fact possible to define an Abelian group by two independent axioms. To this I shall return later.*

The problems arising in the definition of groups are not essentially less complex than those arising in the definition of fields, in the sense in which this term is generally used. A field in the usual sense is a field as I have used the term, for which two rules of combination are defined, both being commutative and associative, and one being distributive† with respect to the other. In all the latest literature, the two problems are discussed together.

Bocher‡ and Huntington§ have suggested and discussed the substitution for the rule of combination $a \circ b = c$, the more symmetrical statement that a relation $R(a\,b\,c)$ is true. The results are extremely interesting, but are not useful for the purposes of this paper.

---

*Cf. Chapter IV.

†I.E.,-the rule $a \odot (b \circ c) = (a \odot b) \circ (a \odot c)$, and the symmetrical statement to this, are satisfied.

‡ Bull. Am. Math. Soc., 11, p. 126, note.

§ Trans. Am. Math. Soc., 6, p. 192.

CHAPTER II. ELEMENTS OF GROUP THEORY.

#1. Fundamental group properties.

#2. Theory of powers of elements.

#3. Relations between group and sub-group.

#4. Conjugate and self-conjugate elements and sub-groups.

#5. Isomprphism.

Chapter II. Elements of Group Theory.

#1.

1. Having discussed the definition of groups by means of independent axioms, I wish to deduce such of the fundamental properties of groups as will be useful in the future for purposes of comparison. Henceforth the sign $\circ$ for the rule of combination will be dropped, and $a \circ b$ written simply ab. Furthermore, since the associativity of a three element combination evidently involves the associativity of a k-element combination, parentheses may in general be dropped, so that any product is completely determined by the naming of its factors in order.

For convenience of reference, I collect here all group properties which have already been established in the course of the preceding chapter.

2. If only two of the three symbols a, b, c are given as elements of the group, the third is uniquely determined as an element of the group, by the condition

$$ab = c.$$

3. There is in the group an identity element 1, such that for every element a,

$$a1 = 1a = a.$$

This identity element is unique.

4. F

or ex

4. For every element a, there is in the group an inverse element a^{-1}, such that

$$aa^{-1} = a^{-1}a = 1.$$

This inverse element is unique.

5. Any continued product is unrestrictedly associative, and therefore, completely determined by naming the elements in their order.

6. The number of elements of a <u>finite</u> group is called its <u>order</u>.

A group whose elements are all elements of another group is called a <u>subgroup</u> of the latter.

#2.

1. Let us define the meaning of the symbol a^n called the n^{th} power of a, by the recurrence formula:-

(1) $a^{k+1} = a^k a.$

(2) $a^1 = a.$

This defines a^n for n a positive integer. I shall prove the following properties:-

(3) $a^m a^n = a^{m+n}$

(4) $(a^m)^n = a^{mn}$

To prove (3), suppose that for some value $n = n_1$,

(A). $a^m a^{n_1} = a^{m+n_1}$

Then

$$\begin{aligned} a^m a^{n_1+1} &= a^m a^{n_1} a && \text{, by (1),} \\ &= a^{m+n_1} a && \text{, by (A),} \\ &= a^{m+n_1+1} && \text{, by (1),} \end{aligned}$$

But for $n = 1$,

$$a^m a^1 = a^m a \quad \text{, by (2),}$$
$$= a^{m+1} \quad \text{, by (1),}$$

so that (3) is true. Therefore it is true for any value of n.

As for (4), suppose that for $n = n_1$,

(B) $$(a^m)^{n_1} = a^{mn_1}$$

Then
$$(a^m)^{n_1+1} = (a^m)^{n_1} a^m \quad \text{, by (1),}$$
$$= a^{mn_1} a^m \quad \text{, by (B),}$$
$$= a^{mn_1+m} \quad \text{, by (3),}$$
$$= a^{m(n_1+1)}.$$

But for $n = 1$,

$$(a^m)^1 = a^m \quad \text{, by (2); hence}$$

(4) is true for any value of n.

2. For zero and negative values of n, define a^n by the formula (1) of the last article, using it now as a retrogressive recurrence law. We have a ready interpretation of zero and negative powers in other terms, as will be shwon.

(5). $a^0 = 1$. That is, the zeroth power of any element is the identity element of the group.

For $a^0 a = a^1 = a$, by (1),(2),

But $1a = a$, by #1, Art. 3.

Hence $a^0 a = 1a$, so that $a^0 = 1$, by #1,Art.2.

(6). $a^{(-1)} = a^{-1}$. That is, the minus first power of an element a is its inverse element.

For $a^{(-1)} a = a^{-1+1} = a^0$, by (1),

$= 1$, , by (5),

But $a^{-1} a = 1$, , by #1,Art.4.

Hence $a^{(-1)} a = a^{-1} a$, so that $a^{(-1)} = a^{-1}$

by #1,Art.2.

(7) $a^{-n}=(a^{-1})^n=(a^n)^{-1}$ .. That is , the minus n^{th} power of an element is at once the n^{th} power of its inverse and the inverse of its n^{th} power.

Suppose that (C) $a^{-n_1}=(a^{-1})^{n_1}$.

Then $a^{-(n_1+1)}a = a^{-n_1}$, by (1),

$=(a^{-1})^{n_1}$, by (C),

Hence $a^{-(n_1+1)} = a^{-(n_1+1)}aa^{-1}$, by #1,Art.4,

$=(a^{-1})^{n_1}a^{-1}$, as just proved,

$=(a^{-1})^{n_1+1}$, by (1).

But for $n=1$, we have

$$a^{-1}=(a^{-1})^1,$$

so that for all values of $n\neq 0$,

$$a^{-n}=(a^{-1})^n$$

Again, suppose

(D) $a^{-n_1}=(a^{n_1})^{-1}$

Then $a^{-(n_1+1)}a^{n_1+1} = a^{-(n_1+1)}aa^{n_1}$, by (3),

$= a^{-n_1}a^{n_1}$, by (1),

$=(a^{n_1})^{-1}a^{n_1}$, by (D),

$= 1$, by #1,Art.4,

$=(a^{(n_1+1)})^{-1}a^{n_1+1}$, by #1, Art.4,

Hence $a^{-(n_1+1)} =(a^{n_1+1})^{-1}$, by #1,Art.2.

But for $n=1$,

$$a^{-1}=(a^1)^{-1}.$$

so that for all values of $n\neq 0$,

$$a^{-n}=(a^n)^{-1}.$$

Finally, for $n=0$,

$$a^{-0}=a^0=1=(a^{-1})^0=(a^0)^{-1}$$

so that for every value of n, (7) is true.

3. With the aid of (5), (6), and (7) we may easily verify (3) and (4) for $n \leq 0$.

Thus if $m \geq n$,

$$a^m a^{-n} = a^m (a^n)^{-1} = a^{m-n} a^n (a^n)^{-1} = a^{m-n}$$

And if $m < n$,

$$a^m a^{-n} = a^m (a^{-1})^n = a^m (a^{-1})^m (a^{-1})^{n-m}$$
$$= a^m (a^m)^{-1} a^{m-n}$$
$$= a^{m-n}$$

Again $(a^m)^{-n} = [(a^m)^n]^{-1} = (a^{mn})^{-1} = a^{-mn}$,

and $(a^{-m})^n = [(a^{-1})^m]^n = (a^{-1})^{mn} = a^{-mn}$

If $n = 0$, $(a^m)^0 = 1 = a^0$,

If $m = 0$, $(a^0)^n = 1^n = 1 = a^0$.

4. The sequence of positive powers of an element of a finite group is periodic. The identity element of a finite group is expressible as a positive power of every element of the group.

Write the sequence of powers

(E) $a, a^2, a^3, \ldots$.

Since the group is finite, this sequence must contain some repetitions. Suppose that two members of the sequence are equal:-

(F) $a^m = a^{m+\rho}$

Then if n be any integer,

$a^n = a^m a^{n-m}$, by (3),

$a^n = a^{m+\rho} a^{n-m}$, by (F),

(G) $a^n = a^{n+\rho}$, by (3).

Therefore the sequence is periodic. In particular, put $n = 0$.

(H) $a^\rho = a^0 = 1$, by (G), (5).

If ρ be the smallest positive integer for which $a^\rho = 1$,

p is called the order* or period† of a.

5. If $a^n = 1$, n is a multiple of the order of a

Let $n = pq + r$, where $0 \leqq r < p$.

Then
$$\begin{aligned} a^n = a^{pq+r} &= a^{pq} a^r && \text{, by (3),} \\ &= (a^p)^q a^r && \text{, by (4),} \\ &= 1\, a^r && \text{, by (H),} \\ &= a^r. && \text{, by \#1, Art.3.} \end{aligned}$$

But then $a^r = 1$, and since p is the smallest positive integer such that $a^p = 1$, must have $r = 0$; therefore

$$n = pq,$$

as we wished to prove.

Corollary. The order of a power of a is a factor of the order of a.

Let $b = a^m$,

and let p, q be the orders of a, b respectively.

Then $b^p = a^{mp} = (a^p)^m = 1$; so that, as just proved, p must be a multiple of q.

#3.

1. If by A we denote any group, by bA, Ab we denote the set of left or right-hand products of the elements of A by b.

Let

$$A = \{1, a_1, a_2, \ldots\ldots a_{n-1}\}$$

be any finite group, of which a sub-group is

*Burnside, Theory of Groups of Finite Order.
†Dickson, Theory of Algebraic Equations.

$$B = \{1, a_1, a_2, \ldots\ldots a_{\nu-1}\}.$$

If $\nu < n$, let b_1 be any element of A not in B; construct the set $Bb_1 = \{b_1, a_1b_1, a_2b_1, \ldots\ldots a_{\nu-1}b_1\}$. If the group is not yet ~~existed~~ exhausted, let b_2 be an element of A not in B or Bb_1,; construct

$$Bb_2 = \{b_2, a_1b_2, a_2b_2, \ldots\ldots a_{\nu-1}b_2\},$$

Continue this process until the group is exhausted, obtaining finally, $Bb_{\mu-1} = \{b_{\mu-1}, a_1b_{\mu-1}, a_2b_{\mu-1}, \ldots a_{\nu-1}b_{\mu-1}\}$. We can then write symbolically,

$$(1) \quad A = B + Bb_1 + Bb_2 + \ldots\ldots + Bb_{\mu-1}.$$

2. The order of a subgroup is a factor of the order of the group. We have the above representation (1) of A, where

$$(2) \quad \begin{aligned} B &= \{1, a_1, a_2, \ldots\ldots a_{\nu-1}\} \\ Bb_1 &= \{b_1, a_1b_1, a_2b_1, \ldots\ldots a_{\nu-1}b_1\}. \\ Bb_2 &= \{b_2, a_1b_2, a_2b_2, \ldots\ldots a_{\nu-1}b_2\}. \\ &\quad\ldots\quad\ldots\quad\ldots\quad\ldots\quad\ldots \\ Bb_{\mu-1} &= \{b_{\mu-1}, a_1b_{\mu-1}, a_2b_{\mu-1}, \ldots\ldots a_{\nu-1}b_{\mu-1}\}. \end{aligned}$$

I shall show that the $\mu\nu$ elements of the group A tabulated in (2) are all distinct. By hypothesis every b is distinct from every element previously written. Suppose, if possible, that two members of the same set were equal,

$$a_{i_1}b_j = a_{i_2}b_j.$$

Then by #1, Art.2, $a_{i_1} = a_{i_2}$, which is untrue.

Now suppose any two elements of different sets equal,

$$a_{i_1}b_{j_1} = a_{i_2}b_{j_2}.$$

We may suppose $j_1 > j_2$

Since a_{i_1} is in B, so will be $a_{i_1}^{-1}$ and also $a_{i_1}^{-1}a_{i_2}$, which

denote by a_k . Then

$$a_{i_1}^{-1} a_{j_1} b_{j_1} = a_{j_1}^{-1} a_{i_2} b_{j_2},$$

or

$$b_{j_1} = 1 b_{j_1} = a_k b_{j_2},$$

so that b_{j_1} would have been equal to a previously written element, contrary to hypothesis.

Hence all the elements in (2) are distinct, and $\mu\nu = n$, as we were to prove.

The integer $\mu = n/\nu$ is called the <u>index</u> of B under A.

3. Corollary. The order of a group is divisible by the order of any element of the group.

Let a be any element of order ν The set

$$B = \{1, a, a^2, \ldots a^{\nu-1}\}$$

is a group, since $a^\alpha a^\beta = a^{\alpha+\beta}$ is a member of B. Hence n/ν is an integer.

A group or subgroup composed exclusively of powers of one element is called a <u>cyclic</u> group or subgroup.

4. The set of elements C common to two groups A and B form a group. The order of C is a common divisor, of the orders of A and B. For if a, a' are common to A and B, then aa' is common to A and B and hence is in C.

#4.

1. If a, b are any two elements of a group, the element $b^{-1}ab$ is called <u>a conjugate of a</u>, or more

specifically, the transform of a by b.

If B is a sub-group of A, it will be shown in Art.5, that the set of elements obtained by transforming every element of B by an element b of A not in B, is a group; this is called a conjugate sub-group of B, or more specfically, the transformed subgroup of B by b.

An element or a subgroup, all of whose conjugates are identical with itself, is called a self-conjugate element or subgroup.

For a reason which will be evident from Art. 2, if a subgroup B is identical with its transformed subgroup by an element b, then B and b are said to be commutative. This definition does not assume, nor is it necessary true, that b is commutative with the elements of B.

2. An element a is identical with its transform by an element b when and only when a and b are commutative.

If $b^{-1}ab=a$,

then $bb^{-1}ab=ba$,

or $ab=ba$.

Conversely, if $ab=ba$,

then $b^{-1}ab=b^{-1}ba$,

or $b^{-1}ab=a$.

3. Any power of a conjugate to a certain element is the conjugate of that power of the element.

The order of a conjugate to an element is the same as the order of the element.

To prove the former statement, suppose that

$(b^{-1}ab)^{n_1}=b^{-1}a^{n_1}b$.

Then $$(b^{-1}ab)^{n_1+1} = (b^{-1}ab)^{n_1}(b^{-1}ab)$$
$$= b^{-1}a^{n_1}bb^{-1}ab$$
$$= b^{-1}a^{n_1}ab$$
$$= b^{-1}a^{n_1+1}b.$$

But $$(b^{-1}ab)^1 = b^{-1}ab = b^{-1}a^1b.$$

Hence for any positive (and therefore,-- by diminishing the exponent by necessary multiples of ρ , the order of ,-- for zero or negative) value of n ,

$$(b^{-1}ab)^n = b^{-1}a^nb.$$

In particular, put $n = \rho$, the order of a.

$$(b^{-1}ab)^\rho = b^{-1}a^\rho b = b^{-1}1b = 1.$$

If for any integer $\pi < \rho$,

$$(b^{-1}ab)^\pi = 1,$$

we have $$b^{-1}a^\pi b = 1,$$

so that $$b^{-1}a^\pi = b^{-1}a^\pi bb^{-1} = b^{-1},$$

and $$a^\pi = 1,$$

contrary to the supposition that ρ is the order of a.
Thus the second statement is proved.

4. The elements ab and ba are conjugate, whatever elements a, b may be.

For transforming ab by a,

$$a^{-1}\cdot ab\cdot a = a^{-1}a\cdot ba = ba,$$

and transforming ba by b,

$$b^{-1}\cdot ba\cdot b = b^{-1}b\cdot ab = ab.$$

5. The transforms of the elements of a subgroup by any element of the group, form a group.

Let the group be

$$A = \{1, a_1, a_2, \ldots\ldots a_{\nu-1}\};$$

and the transforming element, b. We wish to show that

$$b^{-1}Ab = \{1, b^{-1}a_1 b, b^{-1}a_2 b, \ldots\ldots b^{-1}a_{\nu-1} b\}$$

is a group. It is only necessary to show that the combination of two elements of the set produces a third element. But $(b^{-1}a_i b)(b^{-1}a_j b) = b^{-1}a_i a_j b$ which is in $b^{-1}Ab$, since $a_i a_j$ is in A.

6. The elements commutative with a certain element form a subgroup whose index under the group is the number of elements conjugate to the fixed element.

If $A = \{1, a_1, a_2, \ldots\ldots a_{\nu-1}\}$ represents the set of elements commutative with b, then

$$a_i b = b a_i, \quad a_j b = b a_j.$$

Hence

$$\begin{aligned}(a_i a_j) b &= a_i (a_j b)\\ &= a_i (b a_j)\\ &= (a_i b) a_j\\ &= (b a_i) a_j\\ &= b(a_i a_j),\end{aligned}$$

so that $a_i a_j$ is in A. Hence A is a group. Let the order of the whole group be n, and that of A, ν : let there be μ elements conjugate to b (including b itself). Let X be any element not in A, and denote by b' the transform of b by X. Then the transform of b by any element of AX is b'. For

$$(a_i X)^{-1}(a_i X) = 1 = X a_i^{-1} a_i X,$$

so that

$$(a_i X)^{-1} = X^{-1} a_i^{-1};$$

and

$$\begin{aligned}(a_i X)^{-1} b (a_i X) &= (X^{-1} a_i^{-1})(b a_i) X\\ &= X^{-1}(a_i^{-1} a_i)(bX)\end{aligned}$$

$$= x^{-1} bx$$
$$= b'.$$

No other elements transform b into b'; for

if $$y^{-1} by = b' = x^{-1} bx,$$

then $$yy^{-1} byx^{-1} = yb'x^{-1} = yx^{-1} bxx^{-1},$$

or $$b(yx^{-1}) = (yx^{-1}) b$$

so that yx^{-1} must belong to **A**, say

$$yx^{-1} = a_i ;$$

then $$y = a_i x .$$

Thus the number of elements which transform b into b' is the same as the number which transforms b into itself--all of the latter being contained in A.

There are μ choices of b' ; for each choice we can construct a set ~~of~~ Ab' of ν elements, and all such sets exhaust the group; hence

$$\mu\nu = n,$$

as was to be proved.

7. The elements commutative with a certain subgroup form a sub-group whose index under the group is the number of sub-groups conjugate to the fixed sub-group.

If $A = \{1, a_1, a_2, \cdots a_{\nu-1}\}$

represents the set of elements commutative with B, then

$$a_i^{-1} B a_i = B, \quad a_j^{-1} B a_j = B.$$

Hence $$(a_i a_j)^{-1} B (a_i a_j) = a_j^{-1} (a_i^{-1} B a_i) a_j$$
$$= a_j^{-1} B a_j = B,$$

so that $a_i a_j$, is in A. Hence A is a group.

Let χ he any element not in A, and denote by B' the transformed sub-group of B by χ . Then the transformed

subgroup of B by any element of A x is B . For

$$(a_i x)^{-1} B (a_i x) = x^{-1} (a_i^{-1} B a_i) x = x^{-1} B x = B'.$$

No other elements transform B into B' : for

if $$y^{-1} B y = B' = x^{-1} B x,$$

then $$xy^{-1} B y x^{-1} = x B' x^{-1} = x x^{-1} B x x^{-1}$$

or $$(yx^{-1})^{-1} B (yx^{-1}) = B;$$

so that yx^{-1} must belong to A ; say

$$yx^{-1} = a_i;$$

then $$y = a_i x.$$

Thus the number of elements which transform B into B' is the same as the number which transform B into itself,-- all of the latter being contained in A.

As in the preceding theorem, if μ denote the number of sub-groups conjugate to B (including B itself), then

$$\mu \nu = n.$$

8. The elements common to all sub-groups conjugate to a given sub-group (including itself) form a self-conjugate sub-group.

The elements commutative with each of the sub-groups conjugate to a given sub-group(including itself) form a self-conjugate sub-group.

The two statements are evidently true.

#5.

1. If two groups A and A' can be put into a correspondence such that to every element a of A corresponds one and only one element a' of A, and that to the product ab of A corresponds the product $a'b'$ of A', then A and A' are

said to be simply isormorphic.

If two groups A and A' can be put into a correspondence such that to every element a of A corresponds one and only one element a' of A, and that to the product ab of A, corresponds the product $a'b'$ of A, then A is said to be multiply isomorphic with A'.

2. If a group A is multiply isomorphic with a group A', then those elements of A which correspond to the identity of A', form a self-conjugate sub-group of A.

Let $A = \{1, a_1, a_2, \ldots a_{n-1}\}$
and $A' = \{1, a_1', a_2', \ldots a_{n-1}'\}$;
and let $B = \{1, a_1, a_2, \ldots a_{\nu-1}\}$
be the set of elements of A which correspond to the element 1 of A'. B is a group: for if a_i, a_j correspond to 1, then $a_i a_j$ corresponds to $1 \cdot 1 = 1$, and is hence in B.

To show that B is self-conjugate, let b be any element of A, and b' the corresponding element of A'. Then if a_i belongs to B, to the element $b^{-1} a_i b$ of A corresponds $b'^{-1} \cdot 1 \cdot b'$, that is 1, of A', so that $b^{-1} a_i b$ belongs to B. Therefore $b^{-1} B b = B$, and B is selfeconjugate.

3. If a group A is multiply isomorphic with a group A', then to each element of A' correspond the same number of elements of A; the order of A is a multiple of the order of A'.

Let X of A correspond to X' of A'; then every element of xB in A corresponds to X' in A', since every element of B corresponds to 1. Conversely, if y in A corresponds to x' in A', then $x^{-1}y$ corresponds to $x'^{-1}x = 1$, and hence belongs to B, so that

$$x^{-1} y = a_i, \quad i < \nu,$$

and $$y = x a_i , \quad i < \nu;$$

which shows that y belongs to xB. Thus to each element x' of A' corresponds ν elements of A.

It follows directly that $n = \nu n'$.

4. Let A be any group ~~that~~ having a self-conjugate sub-group

$$B = \{1, a_1, a_2, \ldots a_{\nu-1}\}.$$

As before, write the scheme:-

B: $1, a_1, a_2, \ldots a_{\nu-1}$

$b_1 B$: $b_1, b_1 a_1, b_1 a_2, \ldots b_1 a_{\nu-1}$

$b_2 B$: $b_2, b_2 a_1, b_2 a_2, \ldots b_2 a_{\nu-1}$

" " " " "

$b_{\mu-1} B$: $b_{\mu-1}, b_{\mu-1} a_1, b_{\mu-1} a_2, \ldots b_{\mu-1} a_{\nu-1}$.

Consider the product of an element of $b_i B$ by an element of $b_{i'} B$.

$$(b_i a_j)(b_{i'} a_{j'}) = b_i (a_j b_{i'}) a_{j'}.$$

Since B is self-conjugate, $b_{i'}^{-1} a_j b_{i'}$ is some element of B, say a_k ; put $a_k a_j = a$; then

$$a_j b_{i'} = b_{i'} a_k,$$

and $$(b_i a_j)(b_{i'} a_{j'}) = b_i (b_{i'} a_k) a_j = (b_i b_{i'}) a.$$

Thus the product of any two elements belonging to $b_i B, b_{i'} B$ will always be an element belonging to bB , where

$$b = b_i b_{i'}.$$

Now define a set, whose elements are the rows of the scheme above, with the notation

B_0 for B , B_1 for $b_1 B$, $\ldots\ldots$ $B_{\mu-1}$ for $b_{\mu-1} B$;

and with the rule of combination

$$B_i B_j = B_k,$$

where $$b_i b_j = b_k ;$$

as just proved this determines the product uniquely. This set is evidently a group, with which A is multiply isomorphic. Its identity element is B_0 . The inverse of an element B_i is $B_{i'}$, where $B_{i'}$ is the row in which b_i^{-1} occurs.

The group thus defined is called the quotient group or quotient of A by B . Its order is evidently μ , the index of B under A . The theory of the quotient group is of considerable importance in the applications of group theory.

CHAPTER III. THEORY OF CENTROIDAL FIELDS.

Chapter III. Theory of Centroidal* Fields.

1. I shall now undertake the discussion of fields governed by laws other than that which characterizes groups,-- that is, the associative law. I shall in this chapter give one such, numerous examples of which are be found both of arithmetical and geometrical character. It is suggested however, not so much by the number of examples as by the familiarity†, in another form,- of the law which gives it its individuality.

The distributive law, as ordinarily understood,† involves two rules of combination. Make these two rules of operation the same, and we have a law which very naturally suggests itself as a substitute for the associative law. This I propose to use.*

The interest will be centered in this chapter, not on the axioms defining the system, but on the results,- the facts which are true in the system. With a few exceptions‡ no attention will be paid to the interdependency of the several axioms.

2. A set will be called a centroidal field, if the following laws hold among the elements:-

(I.) If a, b are elements of the set, then ab is an element of the set. (That is, the set is a field.)

*The term "distributive field" might also well also be used. The use of "centroidal field" is suggested by the examples in #2, Art. 5.

†Cf. footnote † , page 49. ‡Cf. Atrs. 3,4,5 of this section.

(II.1). If a, b, c are elements of the set, then

$$(ab)c = (ac)(bc).$$

(II.2). If a, b, c are elements of the set, then

$$a(bc) = (ab)(ac).$$

(That is, the distributive law for one operation holds.)

(III.1). If a, b, b' be elements of the set such that $ab = ab'$, then $b = b'$.

(III.2). If a, b, b' be elements of the set such that $ba = b'a$, then $b = b'$.

(IV.1). If a, b be elements of the set, there is in the set an element x such that $ax = b$.

(IV.2). If a, b be elements of the set, there is is in the set an element y such that $ya = b$.

3. For finite sets, it is easily shown that (IV.1,2) are redundant. I shall prove (IV.1):- If a, b be elements of the set, there is in the set an element X such that $ax = b$. *Suppose all the elements written out in order: $x_1, x_2, \ldots\ldots x_n$. (1)

Form the set of elements

$$ax_1, ax_2, \ldots ax_n. \quad (2).$$

Since every ax_i is an element of the original set (1), by (I.), the set (2) satisfies (I.-IV.) and is therefore a centroidal field, contained in the centroidal field (1). But it contains the same number of elements as (1); hence, unless some of the elements of (2) are equal, (1) and (2) must contain precisely the same elements.

Now no two elements of (2) are equal; for if $ax_i = ax_j$, we should have $x_i = x_j$, by (III.1). Hence

*This proof is identical with that used in Chapter.I#1,Art.3.

the elements of (2) must be simply those of (1). But b is an element of (1), therefore an element of (2). Therefore there is some x_j, such that $ax_i = b$; and the theorem is proved.

The proof of (IV.2) is conducted in a similar manner.

4. Another proof will be given, which has the peculiarity of exhibiting the quantity x desired, not as an element correlated to a known element in a scheme of one-to-one correspondence, but as one element of a determinate recurrence-period.

Define a function of a and b by the recurrence formula,-

$$x_{k+1} = ax_k \quad , \quad x_0 = b.$$

Since the number of elements is finite, this sequence must contain repetitions; suppose

$$x_{m+p} = x_m .$$

Since we may write this $ax_{m+p-1} = ax_{m-1}$, we have by (III.1),

$$x_{m+p-1} = x_{m-1} .$$

Likewise, we derive for progessively decreasing values of i,

$$x_{i+p} = x_i .$$

For $i = 0$, $\quad x_p = x_0 .$

That is $\quad ax_{p-1} = b.$

So that $x = x_{p-1}$ will satisfy $ax = b$.

Similarly, to prove (IV.2), we should use the recurrence formula

$$y_{k+1} = y_k a \quad , \quad y_0 = b,$$

in just the same manner.

5. It is possible to prove that for a set of two elements, the axioms laid down are inconsistent.; for a set of three elements, (I.,III.1,2) are sufficient to define a centroidal field, and for a set of four elements, (I.,III.1,2), with the assumption $a \neq a$, are sufficient.

#2.

1. We need not seek far to find an example of a set which fulfils the requirements for a centroidal field. The set of all real numbers, with the operation of combination defined to mean the taking of the arithmetic mean, is such a set.

It is apparent from the definition that (I.) is true; since, too, the set is commutative, the truth of (II.1,III.1,IV.1) involves that of (III.2, III.2, IV.2), so that we need only consider the former.

(II.1) We are to prove that

$$(a \circ b) \circ c = (a \circ c) \circ (b \circ c),$$

where

$$a \circ b = \frac{a+b}{2}.$$

Then $$(a \circ b) \circ c = \frac{\frac{a+b}{2} + c}{2} = \frac{a}{4} + \frac{b}{4} + \frac{c}{2}.$$

Also $$a \circ c = \frac{a+c}{2}, \quad b \circ c = \frac{b+c}{2},$$

and $$(a \circ c) \circ (b \circ c) = \frac{\frac{a+c}{2} + \frac{b+c}{2}}{2} = \frac{a}{4} + \frac{b}{4} + \frac{c}{2}.$$

Thus (II.1) is proved.

(III.1) If $a \circ b = a \circ b'$, it must be proved that $b = b'$

Evidently $\frac{a+b}{2} = \frac{a+b'}{2}$, so that $b = b'$.

(IV.1). It is to be shown that x can be found such that $a \circ x = b$. Take $x = 2b - a$.

Then $$a \circ x = \frac{a+x}{2} = \frac{a+(2b-a)}{2} = b.$$

Thus the requirements for a centroidal field are satisfied.

It is of course possible to make the set less extensive,- as by considering, not all real numbers, but all rational numbers; or, making still further restrictions,- the set of all numbers expressible as the sum of an integer and a finite number of fractions whose denominators are powers of 2.

2. It is not at all difficult to generalize the preceding rule of combination. Instead of defining $a \circ b = \frac{a+b}{2}$, we may define

$$a \circ b = \frac{pa+qb}{p+q}, \text{ where } p+q \neq 0; p \neq 0, q \neq 0;$$

p, q being definite constants. This set is not, in general, (i.e., $p \neq q$) commutative, but the symmetry of p, a with q, b makes it necessary only to prove (II.1, III.1, IV.1)

(II.1) Here $a \circ b = \frac{pa+qb}{p+q}$,

so that

$$(a \circ b) \circ c = \frac{p\frac{pa+qb}{p+q} + qc}{p+q} = \frac{p^2a+pqb+(pq+q^2)c}{(p+q)^2}.$$

Also $a \circ c = \frac{pa+qc}{p+q}$, $b \circ c = \frac{pb+qc}{p+q}$,

and

$$(a \circ c) \circ (b \circ c) = \frac{p\frac{pa+qc}{p+q} + q\frac{pb+qc}{p+q}}{p+q} = \frac{p^2a+pqc+pqb+q^2c}{(p+q)^2};$$

which verifies this property.

(III.1). If $\frac{pa+qb}{p+q} = a \circ b = a \circ b' = \frac{pa+qb'}{p+q}$,

then $qb = qb'$, and $b = b'$, since $q \neq 0$.

(IV.1). Take $x = \frac{p}{q}(b-a)+b$.

Then $a \circ x = \frac{pa+qx}{p+q} = \frac{pa+p(b-a)+qb}{p+q} = \frac{pb+qb}{p+q} = b$.

We may state the rule of combination just investigated in a form more convenient for some purposes, by replacing the coefficients $\frac{p}{p+q}$, $\frac{q}{p+q}$ by simple letters P, Q.

we then have,

$$a \circ b = Pa + Qb, \text{ where } P+Q=1,\ P\neq 0,\ Q\neq 0.$$

3. The sets thus far exemplified have been infinite. The question is presented,- can we obtain similar finite centroidal fields? The traditional method of making a finite number of quantities out of an infinite number is the substitution of the relation of congruence* for that of equality. It is essential, however, if we are to carry over such a set directly, that the rule of combination should give only integers.

Consider the m distinct integers modulo m. In order that the expression $Pa+Qb$ should always denote an integer when a, b are any integers, it is necessary and sufficient that P , Q be integers. We have

$$P+Q=1,$$

or putting

$$Q=-k,$$

we have

$$P=k+1.$$

Thus the rule of combination becomes

$$a \circ b = (k+1)a - kb \pmod{m}.$$

which satisfies (I.)

$$(II.1)\quad (a\circ b)\circ c \equiv (k+1)[(k+1)a-kb] - kc \pmod{m}$$
$$\equiv (k+1)^2 a - (k^2+k)b - kc \pmod{m}.$$

And
$$(a\circ c)\circ(b\circ c) \equiv (k+1)[(k+1)a-kc] - k[(k+1)b-kc] \pmod{m}.$$
$$\equiv (k+1)^2 a - (k^2+k)c - (k^2+k)b + k^2 c$$
$$\equiv (k+1)^2 a - (k^2+k)b - kc \pmod{m}.$$

$$(II.2)\quad a\circ(b\circ c) \equiv (k+1)a - k[(k+1)b - kc] \pmod{m}$$

*The elementary theory of congruences will be assumed. Cf. any standard work on number theory, as Dirichlet-Dedekinds's Vorlesungen über Zahlentheorie.

$$\equiv (k+1)a-(k^2+k)b+k^2c \pmod{m}.$$

And $(a\circ b)\circ(a\circ c)\equiv(k+1)[(k+1)a-kb]-k[(k+1)a-kc]$

$$\equiv(k+1)^2a-(k^2+k)b-(k^2+k)a+k^2c$$

$$\equiv(k+1)a-(k^2+k)b+k^2c \pmod{m}.$$

In order that (III.,IV.) be true, further restrictions must be made.

(III.1,IV.1) We want to be able to conclude from the fact that $(k+1)a-kb\equiv(k+1)a-kb' \pmod{m}$, that $b\equiv b' \pmod{m}$; and we want always to be able to find x so that

$$(k+1)a-kx\equiv b \pmod{m}.$$

when a and b are given.

For the latter purpose, we need only be able to solve the congruence

$$kx\equiv(k+1)a-b \pmod{m}$$

for x. This is certainly possible if k is prime to m. With this assumption, also, if

$$(k+1)a-kb\equiv(k+1)a-kb' \pmod{m},$$

then $k(b-b')\equiv 0 \pmod{m}$,

whence $b\equiv b' \pmod{m}$.

(III.2,IV.2) Similarly, to satisfy these axioms, assume that $k+1$ is prime to m. The result is as follows:-

Let m be any integer, and let $k, k+1$ be two consecutive integers both prime to m. Then the set of distinct integers modulo m with the rule of combination

$$r.\ a\circ b\equiv(k+1)a-kb \pmod{m}$$

form a centroidal field.

4. At the end of this section are given tables of some centroidal fields formed in this way. For convenience, numbers are replaced by letters. Under each table is given the rule of combination upon which it is formed.

It will be noted that this scheme can give only sets of odd order. This fact alone is sufficient to show that it does not account for all centroidal fields of finite order, since two such of order 4 are given at the end of this section. The questions of the existence of centroidal fields of even order, greater then 4, of their representation by some special scheme, of the sufficiency or insufficiency of the scheme of congruence-fields presented, to account for all centroidal fileds of odd order, I have been unable to investigate satisfactorily, so that they remain open.

Some extensions of the above scheme are possible, such as the extension to complex (ordinary abstract) numbers of the rule of combination, but it does not seem worth while to enter into them, since they throw no further light on the subject.

5. We may easily derive geometrical fields from those considered previously. Let a, b be any points on a line, in a plane, or in space. Any algebraic expression or equation in a and b will be taken as denoting symbolically that expression or equation formed separately for each set of coordinates of a and b.

Then if P, Q be any numbers such that $P + Q = 1$,

$P \neq 0, Q \neq 0$, it is evident that all points (in space, in a plane, or on a line), with the rule of combination that $a \circ b$ denotes the point dividing the line ab in the ratio P, Q ,- so that is

$$a \circ b = Pa + Qb,$$

form a centroidal field.

Stating the same fact otherwise, we may say that if we assign as the "product" of two points, the center of gravity of the system formed by placing assigned masses at the two points, in definite order, then for any fixed assignment of the two masses, all points (on a line, in a plane, or in space) form a centroidal field. It is this example, which has suggested the name given to these sets.

I shall denote a centroidal field of this sort by the notation $\mathcal{G}_{p,q}$; for instance that in which arithmetic mean furnishes the rule of combination, is denoted by $\mathcal{G}_{11}$.

Table of Centroidal Fields.

I.

	A	B	C
A	A	C	B
B	C	B	A
C	B	A	C

2a-b.
Commutative.

II.

	A	B	C	D	E
A	A	E	D	C	B
B	C	B	A	E	D
C	E	D	C	B	A
D	B	A	E	D	C
E	D	C	B	A	E

2a-b.

III.

	A	B	C	D	E
A	A	D	B	E	C
B	D	B	E	C	A
C	B	E	C	A	D
D	E	C	A	D	B
E	C	A	D	B	E

3a-2b.
Commutative.

IV.

	A	B	C	D	E	F	G
A	A	G	F	E	D	C	B
B	C	B	A	G	F	E	D
C	E	D	C	B	A	G	F
D	G	F	E	D	C	B	A
E	B	A	G	F	E	D	C
F	D	C	B	A	G	F	E
G	F	E	D	C	B	A	G

2a-b.

V.

	A	B	C	D	E	F	G
A	A	F	D	B	G	E	C
B	D	B	G	E	C	A	F
C	G	E	C	A	F	D	B
D	C	A	F	D	B	G	E
E	F	D	B	G	E	C	A
F	B	G	E	C	A	F	D
G	E	C	A	F	D	B	G

3a — 2b

VI.

	A	B	C	D	E	F	G
A	A	E	B	F	C	G	D
B	E	B	F	C	G	D	A
C	B	F	C	G	D	A	E
D	F	C	G	D	A	E	B
E	C	G	D	A	E	B	F
F	G	D	A	E	B	F	C
G	D	A	E	B	F	C	G

4a — 3b.

Commutative.

VII.

	A	B	C	D	E	F	G	H	J
A	A	J	H	G	F	E	D	C	B
B	C	B	A	J	H	G	F	E	D
C	E	D	C	B	A	J	H	G	F
D	G	F	E	D	C	B	A	J	H
E	J	H	G	F	E	D	C	B	A
F	B	A	J	H	G	F	E	F	E
G	D	C	B	A	J	H	G	F	E
H	F	E	D	C	B	A	J	H	G
J	H	G	F	E	D	C	B	A	J

2a-b.

Three commutative subfields of order 3.

VIII.

	A	B	C	D	E	F	G	H	J
A	A	F	B	G	C	H	D	J	E
B	F	B	G	C	H	D	J	E	A
C	B	G	C	H	D	J	E	A	F
D	G	C	H	D	J	E	A	F	B
E	C	H	D	J	E	A	F	B	G
F	H	D	J	E	A	F	B	G	C
G	D	J	E	A	F	B	G	C	H
H	J	E	A	F	B	G	C	H	D
J	E	E	F	B	G	C	H	D	J

5a — 4b.

Commutative; with three sub-fields of order 3.

IX.

	A	B	C	D
A	A	C	D	B
B	D	B	A	C
C	B	D	C	A
D	C	A	B	D

X.

	A	B	C	D
A	A	D	B	C
B	C	B	D	A
C	D	A	C	B
D	B	C	A	D

#3.

1. In the discussion of ordinary groups, we studied a kind of continued product, depending on one element, and called a power of that element. We might expect a similar subject of study here. Turning to the examples just given, however, we see that for every a, in every field, $aa=a$.

This will evidently be true in every congruence-filed; for by aa we mean $(k+1)a-ka=a$, as anticipated.

It is also true for every g_{pq}; since the "product" of two coincident points must obviously be coincident with them. The proof of the theorem, for abstract fields is easily given, as follows:-

2. Theorem of the Equivalence of Powers. If a be any element of a centroidal field, then $aa=a$.

Referring to the fundamental laws defining a field, we have

$(aa)a=(aa)'(aa)$, , by (II.1)

Hence $a=aa$, by (III.1)

And the theorem is proved.

3. By (IV.1,2), there are elements in the set such that $ax=a$, $ya=a$.

From the analogy of group-theory, we should be tempted to call these, identities of a, or if they happen to be the same, the identity of a. There is of course, no reason for supposing that here as in ordinary group-theory, every element has the same identity.

Supposing that we have a single identity $\bar{a}$ for a, there are elements such that $ax = \bar{a}$, $ya = \bar{a}$, and these we should be inclined to call inverses of a, or in case they are the same, the inverse of a.

In any case, by (II.1,2) the identity or identities will be unique, as will the inverse or inverses. But we have just proved that $aa = a$. Hence, stating this fact, otherwise,-

Theorem. Every element is its own unique identity, and every element is its own unique inverse.

4. In group-theory, we called the expression $b^{-1}ab$ the transform of a by . The corresponding expression in the present theory would therefore be $b(ab)$ or $(ba)b$, between which, from an à priori standpoint, we seemingly ought to distinguish. Let us consider some special examples. Take for instances, Set. IV., and form the expression $(bA)b$, letting b run through all the elements. The result is as follows:-

b	A	B	C	D	E	F	G
bA	A	C	E	G	B	D	F
$(bA)b$	A	D	G	C	F	B	E

Form similarly $b(Ab)$:-

b	A	B	C	D	E	F	G
Ab	A	G	F	E	D	C	B
$b(Ab)$	A	D	G	C	F	B	E

Again try Set X., forming (say), $b(Cb)$ and $(bC)b$:-

b	A	B	C	D
bC	B	D	C	A
$(bC)b$	C	C	C	C

b	A	B	C	D
Cb	D	A	C	B
$b(Cb)$	C	C	C	C

In all these cases, the two expressions give the same result.

Consider any congruence-field. The combination

$(ba)b$ gives

$$(k+1)[(k+1)b-ka]-kb;$$

while $b(ab)$ gives

$$(k+1)b-k[(k+1)a-kb];$$

now $(k+1)[(k+1)b-ka]-kb=(k^2+k+1)b-(k^2+k)a,$

and $(k+1)b-k[(k+1)a-kb]=(k^2+k+1)b-(k^2+k)a;$

so that the two results are equal.

The same considerations serve to establish the fact for a geometrical field. Stated generally we have:-

5. Theorem. The expression bab depends only on a and b, not on the order of grouping; that is, bab is associative,- $(ba)b=b(ab)$.

By (II.1), we have $(ba)b=(bb)(ab)$.

But by 2, $bb=b$, so that $(ba)b=b(ab)$.

I shall write $(ba)b=b(ab)$ in the form bab, and call it the transform of a by b.

6. Consider Set II.; select all products of the form Aa, and transform them by B; the result is:-

	a	A	B	C	D	E
	Aa	A	E	D	C	B
$B(Aa)B$		D	A	C	E	B

Now find χ so that $D\chi$ shall be the transform of Aa by B, as found above; we have

a	A	B	C	D	E
χ	D	B	E	D	C

It will be seen that in every case χ is the transform of a by B,-- $\chi=BaB$.

This gives the formula $B(Aa)B=D(BaB)$;

where it may be noted that is itself the transform of A by B .

Similar facts may be verified in other cases.

7. Theorem. The transform of the product of two elements is the product of their transforms.

Let b be the transforming element; and a_1, a_2 any two elements. Then

$$\begin{aligned} b(a_1 a_2)b &= b[(a_1 a_2)b] \\ &= b[(a_1 b)(a_2 b)] \quad \text{, by II.1,} \\ &= [b(a_1 b)][b(a_2 b)] \text{, by II.2,} \\ &= (ba_1 b)(ba_2 b); \end{aligned}$$

as we wished to prove.

8. Let two elements of a set be commutative, as for instance B, H in set VII.; take their products and transforms by every element in the set,--

a	A	B	C	D	E	F	G	H	J
aB	J	B	D	F	H	A	C	E	G
aH	C	E	G	J	B	D	F	H	A
aBa	H	C	G	B	F	A	E	J	D
aHa	E	J	D	H	C	G	B	F	A

It will be noted that in every case aA , aH belong to one of the sets ADG, BEH, CFJ, which are commutative; the same is true of aBa, aHa .

9. Theorem. If two elements are commutative their products by an element are commutative, and their transforms by any element are commutative.

Suppose $a_1 a_2 = a_2 a_1$.

Then $b(a_1 a_2) = (ba_1)(ba_2)$,

And $b(a_2 a_1) = (ba_2)(ba_1)$,

so that $(ba_1)(ba_2) = (ba_2)(ba_1)$

Similarly $(a_1 b)(a_2 b) = (a_1 a_2) b = (a_2 a_1) b = (a_2 b)(a_1 b)$.

And $(ba_1 b)(ba_2 b) = b(a_1 a_2) b = b(a_2 a_1) b = (ba_2 b)(ba_1 b)$.

#4.

1. A centroidal field, all of whose elements are elements of another centroidal field, will be called a centroidal subfield, or more briefly, a sub-field of the latter.

Obviously, each separate element of a centroidal field constitutes a subfield. Also the field is a sub-field of itself. It is easily seen that a field may have subfields other than itself and single elements, since Sets VII., VIII., each contain three subfields ADG, BEH, CFJ, of order 3.

We may easily make a sort of generalization of this last operation:-

2. Theorem. A congruence-field of composite order will be decomposable into subfields in ways corresponding to every divisor of the order.

Let the field be of order $m = dn$, and let the rule of combination be given by $(k+1)a - kb$. If α be any integer $< d$, the set

$$\alpha, \alpha+d, \alpha+2d, \ldots\ldots, \alpha+(n-1)d,$$

is a subfield of order n. For

$$(k+1)(\alpha+id) - k(\alpha+jd) = \alpha + [(i-j)k+i]d.$$

Now there are d possible choices of α, thus giving d different subfields.

Hence corresponding to the divisor n of m, the field is decomposable into m/n subfields of order n.

I have not proved that no other subfields of a

congruence field exist, nor have I succeeded in establishing any general relation between the order of an abstract centroidal field, and the order of a subfield.

3. Take the subfield ADG of Set VII, and multiply its elements successively by every element : we have:-

	A	D	G
A	A	G	D
B	C	J	F
C	E	B	H
D	G	D	A
E	J	F	C
F	B	H	E
G	D	A	G
H	F	C	J
J	H	E	B

Left-handedly.

	A	B	C	D	E	F	G	H	J
A	A	J	H	G	F	E	D	C	B
D	G	F	E	D	C	B	A	J	H
G	D	C	B	A	J	H	G	F	E

Right-handedly.

In every case we get one of the sets ADG, BEH, CFJ, which are subfields. We may state generally:-

4. Theorem. If every element of a subfield be multiplied right- or left-handedly by any element, the resulting set is a subfield.

For if a_1, a_2 be any two elements of the original subfield, such that $a_1 a_2 = a_3$, then $(ba_1)(ba_2) = b(a_1 a_2) = ba_3$, and $(a_1 b)(a_2 b) = (a_1 a_2) b = a_3 b$.

If we apply both right- and left-handed multiplication, we have the

Corollary. The transforms of all the elements of a subfield, by any element, form a subfield.

5. Theorem. The set of all elements of a centroidal field commutative with a given element, is a subfield.

This is easily verified for any of the examples previously given.

The general proof is simple.

Let a_1, a_2 be elements commutative with b, and let $a_1 a_2 = a_3$.

Then
$$\begin{aligned} a_3 b &= (a_1 a_2) b \\ &= (a_1 b)(a_2 b) \\ &= (b a_1)(b a_2) \\ &= b(a_1 a_2) = b a_3 . \end{aligned}$$

6. Theorem. The set of all elements which a given fixed element transforms into another given fixed element is a subfield.

Let b transform each of the elements
$$a_1 , a_2 , \ldots\ldots , a_n$$
into c. Then we have
$$\begin{aligned} b(a_1 a_2) b &= (b a_1 b)(b a_2 b) && \text{, by \#3, Art.7,} \\ &= c \quad c \\ &= c . && \text{, by \#3, Art.2.} \end{aligned}$$
So that the set a_i is a subfield.

7. Theorem.on the Order of Commutative Sets. A finite commutative centroidal field contains an odd number of elements.

Let c be any elements of the field. If there are no others, the theorem is proved.

If there are other elements, choose $a_1 \neq c$.

There exists an element b_1, such that $a_1 b_1 = c$, by (IV.1). Write down a_1 and b_1. If the field is not yet exhausted, choose a_2 different from the preceding elements, and find b_2 so that $a_2 b_2 = c$. Proceed thus, always choosing a_i different from any preceding element, and finding b_i so that $a_i b_i = c$.

c

$a_1 \quad b_1$

$a_2 \quad b_2$

" "

" "

" "

$a_k \quad b_k$

The field must finally be exhausted; let a_k, b_k be the last pair of elements. We have written down $2k+1$ elements, an odd number; and unless some of the elements written down are equal, the theorem is proved. We know that any $a \neq$ any preceding element; we must therefore prove that the two elements of any pair are unequal, and that any b is unequal to any previous a or b or to c.

1). Suppose $a_i = b_i$.

Then $a_i = a_i a_i = a_i b_i = c$, while a_i was chosen $\neq c$.

2). Suppose $b_i = b_j$. Then $a_i b_j = a_i b_i = c = a_j b_j$, whence $a_i = a_j$; but a_i, a_j were taken unequal.

3). Suppose $b_i = a_j$, where $i > j$.

Then $a_i b_i = c = a_j b_j = b_i b_j = b_j b_i$,

whence $a_i = b_j$, where $i > j$; contradicting the hypothesis that $a_i \neq$ any preceding element.

4). Suppose $b_i = c$ Then $a_i c = a_i b_i = c = cc$,

so that $a_i = c$, which is again impossible.

Thus the field contains an odd number of elements.

[redacted] to leave this room.

[redacted] is it to be checked out overnight.