# A DEFINITION OF ABSTRACT GROUPS*

BY

ELIAKIM HASTINGS MOORE

## INTRODUCTION.

Dr. E. V. HUNTINGTON has recently given two different definitions of abstract groups by sets of respectively three† and four independent postulates; these definitions were perhaps suggested by those given by WEBER and by BURNSIDE.

Some years ago Professor J. PIERPONT and I independently hit on a type of definition very desirable from the grouptheoretic standpoint.

In § 1 I formulate a definition of this type by means of five independent postulates; the independence is proved in § 4. In § 3 the definition is related to other definitions. In this connection I am led to a slightly modified definition (p. 489) by means of six independent postulates, which, even from the standpoint of abstract logic, seems to me simpler than either of those of Dr. HUNTINGTON.

## § 1. THE DEFINITION.

We have for consideration a set‡ of elements and a multiplication-table or rule of combination whereby to every two elements $a, b$ taken in the definite order $a, b$ there corresponds a definite so-called product, in notation $a \circ b$, or, when without confusion, more simply, $ab$; this product may or may not be an element of the set. This set of elements, as related by the multiplication-table, constitutes a group in case the following postulates are fulfilled, viz.,

(1) For every two elements $a, b$ the product $ab$ is an element of the set.

(2) The associative law is fulfilled, that is, $(ab)c = a(bc)$, for every three elements $a, b, c$ such that the products $ab$, $bc$, $(ab)c$ and $a(bc)$ are elements of the set. §

---

* Presented to the Society April 26, 1902. Received for publication September 17, 1902.

† In fact, four, for the third postulate consists of two parts, each of which is used in the development of the theory. The question of the independence of the four postulates arises; for finite groups either part is redundant. – Cf. § 3.

‡ The set is supposed to contain at least one element.

§ For use in § 3, we note here the stronger statement:

(2′) For every three elements $a, b, c$ such that the products $ab$, $bc$ and either $(ab)c$ or $a(bc)$ are elements of the set the associative law is fulfilled.

This is a double statement; we denote its two parts by $(2'_1)$, $(2'_2)$.

($3_l$) There exists a left-hand identity element, that is, an element $i_l$ such that, for every element $a$, $i_l a = a$.

($3_r$) There exists a right-hand identity element, that is, an element $i_r$ such that, for every element $a$, $ai_r = a$.

($4_l$) If there exists a right-hand identity element, then for some such element $i_r$ it is true that for every element $a$ there exists a left-hand reciprocal element, that is, an element $a'_l$ such that $a'_l a = i_r$.

To these five postulates of definition of abstract groups in general the addition of a sixth postulate ($5_\alpha$) or ($5_\beta$) serves to discriminate between the groups of the various finite orders and those of infinite order: $N = n$, $N = \infty$; viz.:

($5_\alpha$) The number of elements is a certain finite integer $n$.

or

($5_\beta$) The set contains an infinitude of elements.

*Remark.* The statement ($4_r$) differing from ($4_l$) by the interchange of the terms *right* and *left* and introducing right-hand reciprocal elements $a'_r$ is a theorem; cf. theorems (6, 7) of § 2. In the definition the statement ($4_r$) might of course enter as a postulate in the place of ($4_l$).

## § 2. Auxiliary theorems.

In § 4 the independence of the postulates of the set ($1, 2, 3_l, 3_r, 4_l, 5_\alpha$) for $n \geqq 3$ and likewise the independence of those of the set ($1, 2, 3_l, 3_r, 4_l, 5_\beta$) will be proved.

In § 3 the definition of § 1 will be related to other definitions; for this purpose the following theorems are needed.

(6) Any left-hand identity element $i_l$ is equal to any right-hand identity element $i_r$. Hence, there is a single identity element $i_l$, and likewise there is a single identity element $i_r$, and these are the same element, say $i$, the identity element of the group.

(7) For every element $a$ a left-hand reciprocal element $a'_l$ is likewise a right-hand reciprocal element, that is, in view of theorem (6), $aa'_l = i$.

(8) For every element $a$ any left-hand reciprocal element $a'_l$ is equal to any right-hand reciprocal element $a'_r$. Hence, there is a single left-hand reciprocal element $a'_l$, and likewise there is a single right-hand reciprocal element $a'_r$, and these are the same element, say $a^{-1}$, the reciprocal of the element $a$ in the group.

These statements follow from the equations:

$$(6°) \qquad i_l = i_l i_r = i_r;$$

$$(7°) \qquad aa'_l = i(aa'_l) = (a''_l a'_l)(aa'_l) = \{a''_l(a'_l a)\}a'_l = (a''_l i)a'_l = a''_l a'_l = i;$$

$$(8°) \qquad a'_l = a'_l i = a'_l(aa'_r) = (a'_l a)a'_r = ia'_r = a'_r,$$

where in (7°) and (8°) the identity element $i$ of theorem (6) enters, and where further in (7°) $a''$ denotes a left-hand reciprocal element of the element $a_l'$.

(9′, 9″). For every two elements $a$, $b$ there exists one (theorem 9′) and only one (theorem 9″) element $x$ such that $ax = b$.

(10′, 10″). For every two elements $a$, $b$ there exists one and only one element $y$ such that $ya = b$.

(11′, 11″). For every two elements $a$, $b$ there exists an element $z$ and there exists an element $w$ such that $(az)b = b$, $\quad b(wa) = b$.

These are precisely the elements $x = a^{-1}b$, $y = ba^{-1}$, $z = a^{-1}$, $w = a^{-1}$.

## § 3. Comparison with other definitions.

We consider the definitions of Weber * and of Huntington †. These definitions postulate for the set of elements with a multiplication-table the following respective sets of statements:

$$(W_1)\colon\ (1, 2, 9', 9'', 10', 10''); \qquad (W_2)_{N=n}\colon\ (1, 2, 9'', 10'', 5_a);$$

$$(H_1)\colon\ (2', 9', 10'); \qquad (H_2)\colon\ (1, 2, 11', 11'').$$

We denote by $(H_1)_{N=n}$ or $(H_1)_{N=\infty}$ the set of postulates $(H_1)$ with the addition of $(5_a)$ or $(5_\beta)$, and so in general.

Weber remarks that in $(W_1)_{N=n}$ the postulates $(9', 10')$ are redundant, and thus obtains his definition $(W_2)_{N=n}$ of finite groups.

Huntington exhibits the equivalence ‡ of the various definitions $(W_1; H_1; H_2)$ of groups in general, $(W_2; H_1; H_2)_{N=n}$ of finite groups, and $(H_1; H_2)_{N=\infty}$ of infinite groups; and he proves the independence of the postulates of every one § of these definitions, with the exception of $(W_1)$ in which $(9'', 10'')$ are redundant, as one sees by use of $(H_1)$. Further he remarks that $(W_2)_{N=\infty}$ is not a definition of infinite groups, the set of positive integers with $a \circ b = a + b$ being a non-group example.

I call attention to the following definitions:

$$(W_1')\colon\ (1, 2, 9', 10'); \qquad (W_1')_{N=n}; \qquad (W_1')_{N=\infty},$$

of the three types of groups, and raise the question of the independence of the postulates of these definitions. The definition $(W_1')$ is from the grouptheoretic standpoint a more convenient modification of Weber's definition $(W_1)$ than is

* *Lehrbuch der Algebra*, vol. 2 (1899), pp. 3, 4.

† Bulletin, ser. 2, vol. 8 (April and June, 1902), pp. 296–300, 388–391.

‡ As to the theory of $(H_1)$, it should be remarked that the statements 6 and 7 of *l. c.*, pp. 297, 298 (as proved and as used) involve the (unstated) hypothesis that $a \circ b$ is of the set or assemblage. Of course the stronger statements are likewise true, for in 10, p. 299, it is proved that every product $a \circ b$ is of the set.

§ As to $(H_1)_{N=\infty}$, the proof for $(H_1)$ is readily made effective.

$(H_1)$. In my lectures of the autumn of 1900 I used this definition $(W_1')$ and the definition *

$$(M'): \quad (1, 2, 3_l, 3_r, 4_l, 4_r),$$

proving as in § 2 that the statements of $(W_1')$ follow from those of $(M')$, and further that those of $(M')$ follow from those of $(W_1')$ by the use of the theorems: †

$(\rho)$. If an element $b$ is a right-hand identity element for a certain element $a_0$ $(a_0 b = a_0)$, then it is for every element $a$ $(ab = a)$.

$(\lambda)$. Similarly: If $ba_0 = a_0$, then $ba = a$.

The redundance of $(4_r)$ in $(M')$ and the independence of the remaining postulates, those of the new definition (of § 1),

$$(M): \quad (1, 2, 3_l, 3_r, 4_l),$$

and likewise the independence of the postulates of the corresponding definitions $(M)_{N=n}$, $(M)_{N=\infty}$ were discovered in April, 1902.

The four definitions of groups in general are most closely related in the following order:

$$(M), \qquad (W_1'), \qquad (H_1), \qquad (H_2);$$

the redundance of $(9'', 10'')$ in $(W_1)$ is a consequence of the fact that the statements of $(M)$ follow from those of $(W_1')$.

From the standpoint of abstract logic the canons of relative simplicity of equivalent definitions by sets of postulates are not well established. Perhaps the only established canon is this, that a definition is simplified by the omission of a group of postulates logically deducible from the remaining postulates. One is tempted to add this, that every postulate of a desirably simple definition shall be a simple statement, that is, a single and not a multiple statement. The difficulty here would arise in the precise formulation of the terms of this second canon, especially in view of the fact that the same statement may be made in various forms. At least, a definition is simplified by the substitution, for a

* The earlier definitions of PIERPONT and of myself (already referred to) introduce an identity element $i$ and for every element $a$ a reciprocal element $a^{-1}$ by the postulates (3, 4) that they exist and satisfy respectively for every element $a$ the two double equations:

$$(3^\circ) \quad ia = ai = a, \qquad (4^\circ) \quad a^{-1}a = aa^{-1} = i.$$

PIERPONT's definition:

$$(P)_{N=n}: \quad (1, 2, 3, 3^*, 4, 5_a),$$

involved further the postulate (3*) of the uniqueness of the identity element and it is given for finite groups (Annals of Mathematics, ser. 2, vol. 2, p. 47, Oct. 1900, in the report of the lectures of the Buffalo Colloquium of September, 1896, on *Galois's theory of algebraic equations*).

The definition:

$$(1, 2, 3, 4)$$

of groups in general I used in lectures in January, 1897.

† The lemmas 4, 5 (p. 297) of HUNTINGTON's theory of $(H_1)$.

postulate consisting of an aggregate of independent statements, of those statements as distinct postulates. Further one may add as a third canon this, that of two definitions one with the smaller number of postulates is the simpler. As to this canon the case now in question seems to show that the definition with the larger number of independent postulates may reveal more immediately the fundamental properties of the object of definition. It is, of course, evident that the task of proving the independence of the postulates presumably increases with the number of postulates.

Let us compare the four definitions $(W_1')$, $(H_1)$, $(H_2)$, $(M)$ of groups in general on the basis of these three canons.

For $(W_1')$ the independence of the postulates is an open question; for the other definitions it has been proved.

The postulate $(2')$ of $(H_1)$ consists obviously of the two parts $(2_1')$, $(2_2')$, and thus the question of independence of the four postulates of the new definition *

$$(H_1'): \quad (2_1', 2_2', 9', 10')$$

arises. No other postulate of the four definitions is similarly multiple.

However, for instance, postulate (1) of $(W_1')$, $(H_2)$ and $(M)$ breaks into the aggregate of statements $(1)_{a,b}$, $a$, $b$ denoting any two elements of the set, viz.,

$(1)_{a,b}$. The product $ab$ of the two elements $a$, $b$ is an element of the set.

Similarly, all the postulates of the four definitions $(W_1')$, $(H_1')$, $(H_2)$, $(M)$, with the exception of the postulates $(3_l, 3_r, 4_l)$ of $(M)$, are at once decomposable into aggregates of constituents.

That the postulates $(3_l, 3_r, 4_l)$ are not thus decomposable may properly be considered an indication of their greater intrinsic complexity. Accordingly I replace $(M)$ by the new definition:

$$(M''): \quad (1, 2, 3'', 3_l'', 3_r'', 4_l''),$$

by means of six independent postulates. Here the new postulates are these:

$(3'')$. There exists at least one idempotent element, that is, an element $i$ identical with its square, $ii = i$.

$(3_l'')$. Every † idempotent element is a left-hand identity element; that is, for every element $a$ and every † idempotent element $i$, $ia = a$.

* One readily sees that, if for three elements $a$, $b$, $c$ the hypotheses of $(2_1')$ and $(2_1')$ itself are satisfied, $(2_2')$ is likewise satisfied for those elements, and, accordingly that the complete postulate $(2_2')$ is redundant in $(H_1')_{N=n}$, for, as HUNTINGTON has remarked, from $(9', 10', 5^a)$ follows (1) at once.

† The statements $(3_l'', 3_r'', 4_l'')$ have as hypotheses the existence of at least one idempotent element Accordingly, in any case in which $(3'')$ is not satisfied, $(3_l'', 3_r'', 4_l'')$ are satisfied in that their hypotheses are not fulfilled, or, as we may say, are satisfied vacuously. This type of validity of postulates is of considerable importance

$(3''_r)$. Every * idempotent element is a right-hand identity element.

$(4''_l)$. For every element $a$ with respect to every * idempotent element $i$ there exists a left-hand reciprocal element, that is, an element $a^{(i)}_l$ such that $a^{(i)}_l a = i$.

It is easy to see that the sets of statements $(3_l, 3_r)$, $(3'', 3''_l, 3''_r)$ are equivalent, and that, if either set is valid, there is but one idempotent element, the identity element of (6), and hence that with respect to these equivalent sets of statements the statements $(4_l)$ and $(4''_l)$ are equivalent.—Accordingly, the proof to be given in § 4 of the independence of the postulates of $(M)$, $(M)_{N=n}$, $(M)_{N=\infty}$ respectively applies at once to prove the independence † of the postulates, except $(3'', 3''_l, 3''_r)$, of $(M'')$, $(M'')_{N=n}$, $(M'')_{N=\infty}$ respectively. One proves the independence of $(3''_l)$ and that of $(3''_r)$ for $N = n \geqq 2$ or $N = \infty$ by the examples given in § 4 for $(3_l)$ and $(3_r)$ respectively.

The postulate $(3'')$ is independent in $(M'')$ and in $(M'')_{N=\infty}$, as one sees by the set of elements $a_h$ with positive integral indices $h$ with the multiplication-table $a_{h_1} a_{h_2} = a_{h_1+h_2}$. In the definition $(M'')_{N=n}$ of finite groups, however, the postulate $(3'')$ is redundant. For in any finite set of elements with multiplication-table satisfying (1, 2) there exists a closed cycle of (one or more) elements, each of which is the square of the preceding element in the cycle; these elements are in multiplication commutative, being all of them powers of any one; their product is an idempotent element, for the square of that product is the product of the squares of the elements, that is, it is that product itself.

To recur to the comparison of the definitions $(W'_1)$, $(H'_1)$, $(H_2)$, $(M'')$.—The new postulates $(3'_l, 3''_r, 4''_l)$ are decomposable in the manner desired. For the new definitions arising by this decomposition of the postulates the question of independence arises. In none of these new definitions are all the postulates independent. For, in the first place, upon the statements (1), (2) and respectively

$$(9')_{a,b}, \qquad (10')_{a,b}, \qquad (11')_{a,b}, \qquad (11'')_{a,b}$$

depend respectively the statements

$$(9')_{ca,cb}, \qquad (10')_{ac,bc}, \qquad (11')_{a,bc}, \qquad (11'')_{a,cb}$$

for every element $c$. And, as already noted, for every postulate $(2'_1)_{a,b,c}$ non-vacuously verified, the corresponding postulate $(2'_2)_{a,b,c}$ is redundant. And, further, the postulate $(4''_l)^{(i)}_{ab}$ depends upon the postulates $(1, 2, 3'', 3''_l, 3''_r)$ and $(4''_l)^{(i)}_a, (4''_l)^{(i)}_b$; for, in the notations of $(4''_l)$, since $(b^{(i)}_l a^{(i)}_l)(ab) = i$, the element $b^{(i)}_l a^{(i)}_l$ is an element $(ab)^{(i)}_l$ satisfying the condition of postulate $(4''_l)^{(i)}_{ab}$.

* Cf. footnote † on the preceding page.

† For $N = n > 2$ or $N = \infty$. — As to the cases $N = n = 1, 2$ one readily finds that for $n = 1$ all the postulates depend upon (1) and $(5_a)_{n=1}$ which are independent, and that for $n = 2$ the postulates $(3'')$, $(3''_l)$, $(3''_r)$, $(4''_l)$ and $(5_a)_{n=2}$ are independent, while (1), (2) depend upon them.

Finally, it seems worth while in a fairly definite way to apply the third canon of comparison to the four definitions. As a unit-operation of the determination that a given set of $N$ elements with a given multiplication-table constitutes a group we consider the reading from the table of a single entry $ab$, with necessary checking.

The verification of postulate (1) requires $N^2$ of these unit-operations, while (2), $(2'_l)$ require each $4N^3$ operations.* Similarly (9'), (10'), (11'), (11'') require each at least $N^2$ and at most $N^3$ operations, while (3'') requires at least 1 and at most $N$ operations, and then † $(3''_l)$, $(3''_r)$ require each $N-1$ operations, and $(4''_l)$ at least $N-1$ and at most $N^2-N$ operations. Thus the verification of the group-property of the given set of $N$ elements according to the various definitions requires

| | at least | at most |
|---|---|---|
| $(W'_1)=(1, 2, 9', 10')$: | $4N^3+2N^2$, | $6N^3$; |
| $(H'_1)=(2'_1, 2'_2, 9', 10')$: | $4N^3+2N^2$, | $6N^3$; |
| $(H_2)=(1, 2, 11', 11'')$: | $4N^3+2N^2$, | $6N^3$; |
| $(M'')=(1, 2, 3'', 3''_l, 3''_r, 4''_l)$: | $4N^3+3N-2$, | $4N^3+N^2+2N-2$ |

operations. Here it is understood that $N$, $N^2$, $N^3$, and the symbols of addition and multiplication have a rather definite meaning, even if $N=\infty$, in connection with the notion of reading from the multiplication-table.

Thus, as stated in the introduction, the definition $(M'')$ seems to me to be an advantageous one both from the grouptheoretic and the logical standpoints.

It remains to prove the independence of the postulates of $(M)$.

## § 4. The independence of the postulates. ‡

The postulates of the set $(1, 2, 3_l, 3_r, 4_l, 5_\alpha)$ or $(1, 2, 3_l, 3_r, 4_l, 5_\beta)$ are proved independent by the exhibition of six sets of elements with multiplication-tables satisfying all the postulates but one.

As to $(5_\alpha)$ or $(5_\beta)$. We consider any group containing an infinitude or a finite number of elements.

As to (1).—We consider the elements $a_{g\,h}$ with the multiplication-table

$$a_{g_1 h_1} a_{g_2 h_2} = a_{g_1+g_2\; h_1+h_2}.$$

* On finding (2) or $(2'_1)$ verified for every triad $a, b, c$ of elements, one sees that (1) or $(2'_2)$ is verified.

† Since there is only one idempotent element, if for one idempotent element the conditions $(3''_l, 3''_r)$ are satisfied.

‡ For $N=n>2$ or $N=\infty$. As to the cases $N=n=1$, 2 one readily finds that for $n=1$ all the postulates depend upon (1) and $(5_\alpha)_{n=1}$ which are independent, and that for $n=2$ the postulates (1), (2) depend upon $(3_l)$, $(3_r)$, $(4_l)$ and $(5_\alpha)_{n=2}$ which are (as proved in the text) independent.

Here the first index is an integer taken modulo 2 and the second index is an integer taken either modulo $2m$ or without modular condition.

The set of all such elements with this multiplication-table constitutes a group of order $N = 2.2m$ or $N = \infty$.

The non-group sets of order $N = n$ or $N = \infty$ satisfying all the postulates except (1) are obtained from this set of elements with properly chosen $m$ by the omission of certain elements.

In case $N = n \geqq 3$, we take $m \geqq 2$ so that $n = 2m - 1$ or $2m$, and omit from the $2.2m$ elements $a_{gh}$ these elements: $a_{0m}$ and the $2m$ or $2m - 1$ elements $a_{1h}(h = 0, 1, 2, \cdots, 2m - 1$ or $h = 1, 2, \cdots, 2m - 1)$. The product $a_{01}a_{0m-1} = a_{0m}$ is not in this set.

In case $N = \infty$, we omit the elements $a_{1h}(h = \pm 1, \pm 2, \pm 3, \cdots)$. The product $a_{01}a_{10} = a_{11}$ is not in this set.

As to (2).—The non-group example is the set of $N = n \geqq 3$ or $N = \infty$ elements $i$ and $a_h$ where $h = 1, 2, \cdots, n - 1$ or $h = 1, 2, 3, \cdots$ with the multiplication-table

$$ii = i, \qquad ia_h = a_h i = a_h, \qquad a_h a_h = i, \qquad a_{h_1}a_{h_2} = a_{h_1} \quad (h_1 \neq h_2).$$

Here

$$a_1(a_1a_2) = a_1a_1 = i, \quad \text{while} \quad (a_1a_1)a_2 = ia_2 = a_2.$$

As to $(3_l)$.—The non-group example is the set of $N = n \geqq 2$ or $N = \infty$ elements $a_h$ where $h = 1, 2, 3, \cdots, n$ or $h = 1, 2, 3, \cdots$, with the multiplication-table

$$a_{h_1}a_{h_2} = a_{h_1}.$$

Here there is no left-hand identity element.

As to $(3_r)$.—The example for $N = n \geqq 2$ or $N = \infty$ is the example for $(3_l)$ with the modified multiplication-table

$$a_{h_1}a_{h_2} = a_{h_2}.$$

As to $(4_l)$.—The non-group example for $N = n \geqq 2$ or $N = \infty$ is the set for (2) with the multiplication-table

$$ii = i, \qquad ia_h = a_h i = a_h, \qquad a_{h_1}a_{h_2} = a_1.$$

Here the only right-hand identity element is $i$, and there is no element $x$ such that $xa_1 = i$.

OCEAN VIEW, VA.,
*September* 17, 1902.